Procurer

REPUBLIC OF ESTONIA
MINISTRY OF DEFENCE

Development and application of cryptography in the Estonian public and private sectors

REPORT

2019

CYBERNETICA

Euroopa Liit
Euroopa
Regionaalarengu Fond

Eesti
tuleviku heaks

Development and application of cryptography in the Estonian public and private sectors

Technical document

Version 2.0

May 14, 2019

77 pages

Doc. A-116-1

Project leaders:	Ivar Janson (Estonian Ministry of Defence)
	Mari Seeba (Cybernetica)
Contributing authors:	Ahto Buldas, PhD (Cybernetica)
	Tarmo Kalvet, PhD (Institute of Baltic Studies and TalTech)
	Peeter Laud, PhD (Cybernetica)
	Alisa Pankova, PhD (Cybernetica)
	Marek Tiits, PhD (Institute of Baltic Studies)
	Jan Willemson, PhD (Cybernetica)
Steering committee:	Ministry of Defence
	Ministry of Economic Affairs and Communications
	Ministry of the Interior
	Police and Border Guard Board
	State Information Agency
	Estonian Foreign Intelligence Service

Ministry of Defence, Sakala 1, 15094 Tallinn, Estonia.
E-mail: info@kaitseministeerium.ee, Web: http://www.kmin.ee, Phone: +372 717 0022.

Cybernetica AS, Mäealuse 2/1, 12618 Tallinn, Estonia.
E-mail: info@cyber.ee, Web: https://www.cyber.ee, Phone: +372 639 7991.

This research was commissioned by the Estonian Ministry of Defence as part of the "Valdkondliku teadus- ja arendustegevuse tugevdamine" (RITA) program. The project is funded 50% by the European Regional Development Fund and 50% by the Estonian Ministry of Defence.

Contents

Executive summary

The objective of the current research is to give an overview of the state of art in development of cryptography in Estonia, and to analyse the technological and economic potential of the field.

First, disruptive and emerging technologies in the field of cryptography are identified. This serves as a background for analysing the specialisation of the Estonian universities and private sector companies and their technological capabilities. Thereafter, the domestic needs, potential market niches and public procurement of innovation are discussed. Finally, a number of actions are proposed for further development of cryptography in Estonia.

As the result of the analysis of the priorities for research and technology development in leading nations, post-quantum cryptography, quantum key distribution, electronic identity, secure computation and privacy-preserving (big) data analysis, radio frequency protocols, Internet of Things (cryptography in limited environments), cryptographic protocol analysis, long-term protection of systems, anonymous networks, and block-chains were identified as particularly promising disruptive and emerging technologies.

There are three companies that conduct world class R&D in the above areas, and form the core of the indigenous cryptography rich industry in Estonia. These companies are, given the nature of their business, strongly integrated with the Estonian and European education and R&D systems. The above companies cater both for domestic and foreign markets, and their labour productivity is significantly higher than the Estonian ICT sector average.

There are, on top of the above, around 10 local companies with own ICT products and services that implement advanced cryptographic solutions. Additionally, a limited number of cryptography intensive early stage start-up companies can be identified in Estonia. Furthermore, Estonia hosts also a number of subsidiaries of foreign owned cryptography-related companies; these companies are weakly connected to the Estonian education and R&D systems.

Estonian universities have offered basic cryptographic education for almost two decades. What is more, cryptography is one of the strongest research fields in the Estonian computer science scene. Hence, one would expect to be able to find well qualified developers of crypto-rich applications on the local labour market. Yet, the supply of cryptography experts falls short of the booming demand, while the cyber security domain continues to gain more and more importance from security and defence points of view. The limited availability of cryptography experts in Estonia holds the companies but also the government itself back from defining and developing cutting edge crypto-rich products and services.

Estonia falls significantly behind its Nordic neighbours in R&D investments. The gross domestic expenditure on R&D was around 3% of GDP in Finland and Sweden, whereas

business sector R&D investment was around 2% of GDP in 2017. Gross domestic expenditure on R&D was only 1.3% of GDP in Estonia in 2017. Business sector contributed half of it. In Finland, ICT sector invested into R&D 1.3 billion euros in purchasing power standards (PPS), while the Estonian ICT companies invested only 0.1 billion euros in PPS in 2015.

In conclusion, limited availability of highly specialised workforce, and suboptimal investment into R&D hold back the development of a competitive high-tech industry in Estonia. What is more, lowering of the level of mathematics and science education in high schools has become a major obstacle that undermines preparation of students for a future career in cryptography, or in fact, any mathematically sophisticated field.

Estonia has had a notable success in cryptography and cyber security domain. However, it now needs to do more to be prepared for future opportunities and challenges. Accordingly, the following recommendations are given for increasing the competitiveness of the cryptography-related companies, and adoption of advanced cryptographic technologies and services in the Estonian public sector.

- Estonian cryptography and information security companies are tiny on the global scale. Advancement of cluster co-operation is, therefore, inevitable for promoting and supporting the interests of the Estonian enterprises and universities in the field of cryptography and cyber security. The potential joint actions could include development of a mid- to long-term roadmap for Estonian cryptography and cyber security industry, advancement of collaboration between enterprises and universities in curricula development, fostering the participation in European collaborative research and development programmes, promotion of Estonian products and services internationally, etc.
- Establishment of a national cryptographic competence centre. The functions of the centre would include advising on the development of cyber security architectures, participating in the analysis phase of all major IT system procurements in Estonia and establishing requirements, carrying out threat intelligence tasks, and establishing requirements for maintenance of cryptographic systems.
- Attestation of cryptographic solutions. There is a need for development of capability for independent assessment of information security hard- and software products, even if it may not be feasible to immediately establish a fully fledged certification body.
- Capacity building in key emerging technologies. Out of the disruptive and emerging technologies listed above, there are some that require more attention than others, namely post-quantum cryptography, electronic identity, long-term protection of systems, secure computation and privacy preserving (big) data analysis, and cryptographic protocol analysis. Increasing such capacities in important – we know from the recent past that major Estonian innovations in the field of eGovernance (such as X-Road or Public Key Infrastructure) have largely originated from the competent and visionary engineers.
- Industrial R&D and product development. Governmental institutions need to take a more active role in public procurement of innovation. This presumes capacity building within these organisations as well. Products that deserve consideration as candidates for innovation procurement include several communication security solutions, quantum-safe eID, federated identity management, cross-jurisdictional data aggregation, and long-term security framework.

- Boosting math and science education on the primary and secondary school level. High-tech R&D can not exist in isolation from the rest of the society. Most notably, many potential employees with strong math and science background are needed. Estonian government needs to considerably rise the priority of math and science education as the core facilitator of R&D (not only in cryptography, but also many other areas of engineering).

1 Introduction

Cryptography (from ancient Greek κρυπτός "hidden, secret" and γράφειν "to write") is the practice and study of techniques for secure communication in the presence of malicious third parties (adversaries). In this definition, the term "secure" may refer to several different properties of information, like confidentiality, integrity or authenticity.

The problem of secure communication has been tackled for several millennia, being mostly motivated by military needs. Still, contemporary treatment of the subject based on rigorous mathematical foundations is only a few decades old. Fast development of information technology applications has allowed deployment of strong cryptographic methods in a vast majority of the communication channels we use today.

However, the lifetime of such methods has proven to be limited by the history. Advances in computing and mathematical methods lead to weakening of cryptographic algorithms, whereas development errors may introduce a large spectrum of unintended vulnerabilities. This makes cryptography an "arms race" between attackers and defenders pretty much the same way it happens with other kinds of military equipment.

In any kind of a race, staying ahead is crucial for the overall success. This is why cryptographic research and development plays an important role in both supporting the Estonian e-society and national cybersecurity.

Roughly speaking, we can distinguish three levels of deployment of cryptographic applications.

1. Using off-the-shelf cryptographic products as they are.
2. Auditing off-the-shelf products for compliance, absence of hidden functionality, etc.
3. Having full control over the development of cryptographic applications.

Of course, level 3 would give the strongest level of assurance, but considering the limited resources Estonia has, this is mostly not realistic. However, we should still be targeting this level whenever possible, improving our auditing capability for level 2 at the same time.

1.1 Research questions

The report seeks answers to the following questions.

- What are the key needs of Estonian state institutions in terms of cryptographic developments?
- What is the current capability of developing cryptographic applications from the viewpoint of

  - private enterprises developing and certifying new cryptographic solutions,
  - public institutions procuring and deploying them,
  - educational system preparing specialists competent in cryptography?
- What would be suitable development models for cryptographic applications in Estonia?
- What are the required policy changes in Estonian public administration?

1.2 Methodology

The current research builds upon Michael Porter's well-established clusters framework for analysing the competitiveness of industries.

According to Porter, a cluster is "a geographically proximate group of interconnected companies and associated institutions in a particular field, linked by commonalities and complementarities" [70, 71].

The key benefit of the clusters concept is that it brings together various elements of the business ecosystem that exists in a particular location, and links them with the economic performance of the whole national economy. Porter argues that it is the interplay between and co-ordination of the following four factors that determines the competitiveness of the industries and of the whole national economies:

- factor conditions characterise the availability, cost and quality main production inputs, including qualified labour, raw materials and infrastructure;
- demand conditions determine market dynamics, sophistication of end users, and economies of scale;
- related and supporting industries are about the availability and quality of the related component providers, manufacturing and support service providers, etc.;
- strategy, structure and rivalry relate to the way in which companies interact, and whether the market competition is about outperforming each other with superior products or lower costs.

Porter's clusters approach favours strongly creative free market competition. Often, nonetheless, governments act as important catalyst of the development of industrial clusters. They can stimulate early demand for advanced products, and foster the development and introduction of specialised factors, such as knowledge and new technologies. Also, the governments stimulate local rivalry of the competitors in introduction of new and even better products. Finally, chance events denote the idea that sometimes new exploitable market opportunities emerge as a result of completely unforeseen events (see Figure 1).

Clusters are about industrial agglomeration and development of a location based strategy. Yet, no cluster or national economy operates in isolation in the modern globalised world. Quite the contrary, clusters are often part of larger cross-border or even global value chains that span across continents.

Therefore, the discussion of industrial competitiveness should also consider carefully the broader international context. Accordingly, when analysing the potential future economic opportunities, we rely on our own intelligent piggy-backing approach to the technology-led catching up in small countries [81]. This approach acknowledges that the main trends in

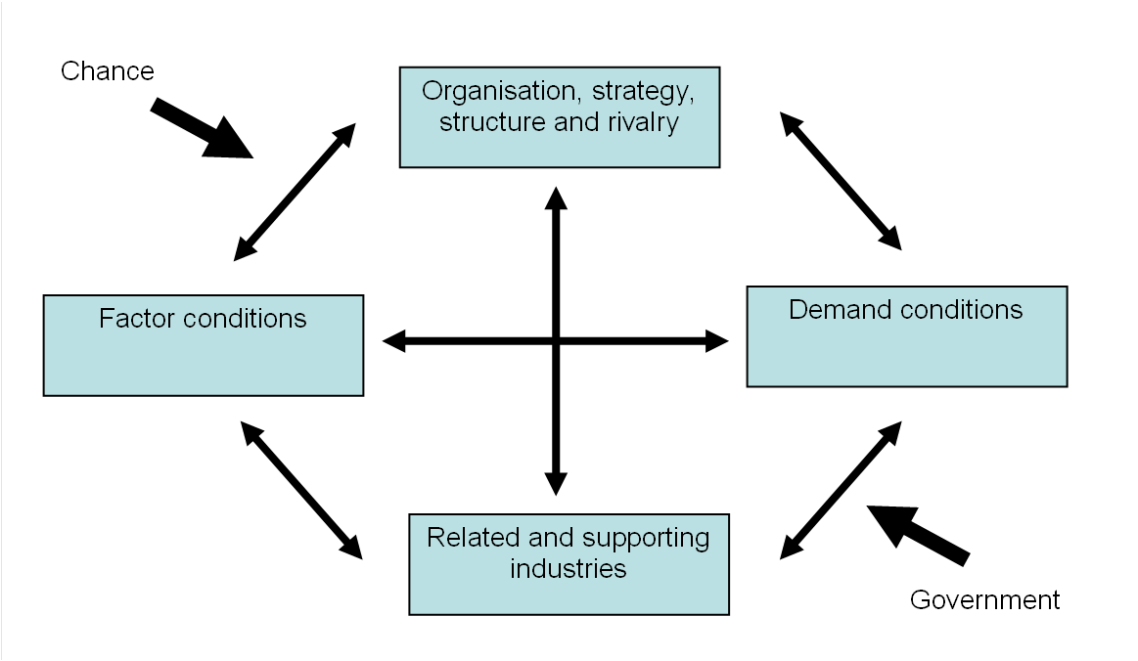

Figure 1. Porter's diamond

the basic research and key technologies are, for the most part, established in the major advanced economies rather than in small catching-up countries.

In the intelligent piggybacking approach, priority setting for a catching-up strategy should carefully consider the following.

- Global technology trends are, for the most part, set in the larger advanced economies and characterise major future technological possibilities. In this respect, the techno-economic paradigm [68] offers an excellent framework for analysing the evolution of longer-term priorities in science and technology, and in global industrial dynamics brought about by the development and dissemination of new knowledge and technologies.
- Existing technological capabilities and industrial specialisation define the starting point(s) of any future development scenarios or roadmaps. Here a combination of Porter clusters approach [70], the global-value-chains [38], foreign direct investment and trade theory [28] provide good starting points for analysing the existing industrial specialisation of a particular economy.
- Major domestic and international socio-economic challenges serve as an indication of likely changes in future market demand as well as decision points for the willingness of domestic actors to rethink their future production and innovation activities. Here, trend analysis and participatory foresight techniques such as scenario-writing, road-mapping, etc., can prove useful (see Figure 2).

Timely take-up of disruptive new technologies allows relatively smaller players to outperform bigger established actors, who tend to become increasingly reliant on their ageing technology. The key questions in this context are: what new products or even industries are the emerging disruptive technologies likely to bring about, and how would it be possible to enter the related new markets in a relatively early phase?

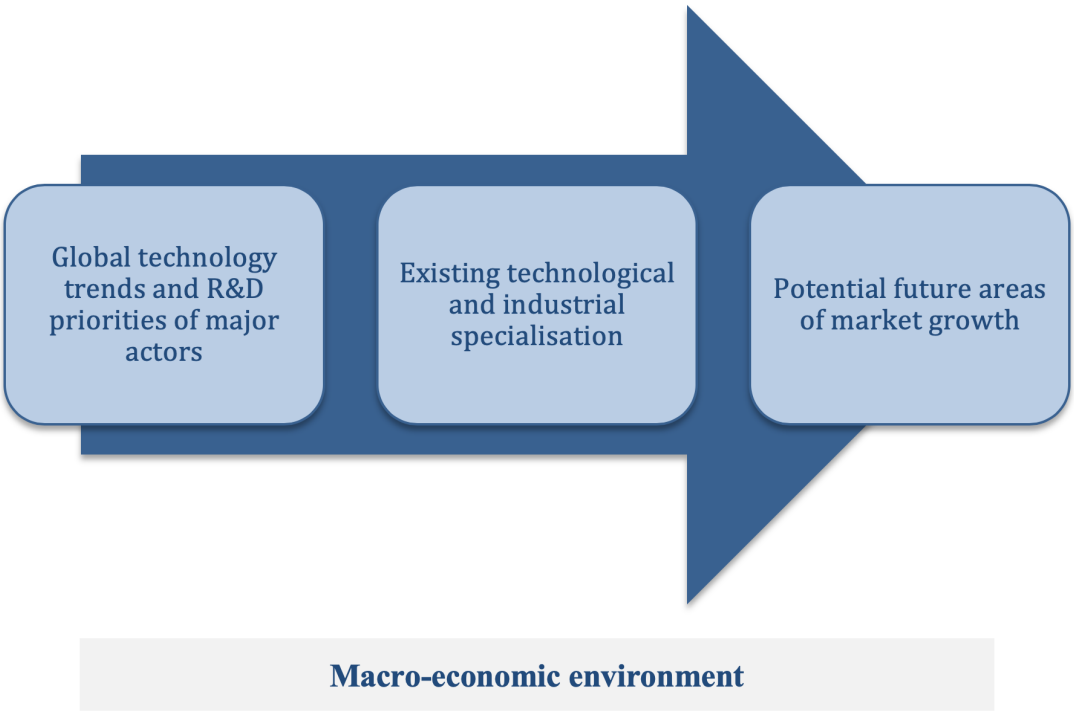

Figure 2. Intelligent Piggybacking: A priority-setting analytical framework in the small catching-up economies

1.3 Data collection

During the research phase of the project, we conducted interviews with the following Estonian governmental institutions, universities and private companies:

- Ministry of Defence,
- Ministry of Economic Affairs and Communications,
- State Information Agency (RIA),
- Ministry of the Interior,
- Police and Border Guard Board,
- Information Technology Department of the Ministry of Interior,
- Estonian Foreign Intelligence Service,
- Technical Regulatory Authority,
- Tallinn University of Technology (TalTech),
- Tartu University,
- Cybernetica,
- Aktors,
- Guardtime,
- Rangeforce.

Additionally, a scenario workshop, which brought together researchers, entrepreneurs and civil servants, was held for the discussion of future outlooks of the Estonian cryptographic developments on November 7th, 2018. As a part of this workshop, main external drivers that establish the context for the medium to long-term developments in Estonia were mapped. Participants of the workshop included:

- Mati Sepp,
- Jaan Priisalu,
- Rain Ottis,
- Uko Valtenberg,
- Priit Kleemann,
- Kirsti Melesk,
- Mait Heidelberg,
- Kati Korm,
- Jaak Vilo,
- Marek Metsalu,
- Kaur Virunurm.

For the financial analysis of the Estonian cryptography-related companies, respective data was obtained from the Estonian Business Registry.

There were also several other persons and organisations who contributed to this research with their comments and inputs. We would like to take the opportunity to thank everyone who made this report possible. Our special thanks goes to the members of the steering committee who helped to review and validate this research. The steering committee consisted of the following organisations:

- Ministry of Defence,
- Ministry of Economic Affairs and Communications,
- Ministry of the Interior,
- Police and Border Guard Board,
- State Information Agency,
- Estonian Foreign Intelligence Service.

In the following chapters, we outline and analyse disruptive and emerging technologies in the domain of cryptography. Thereafter, we map the state of the art of cryptographic development in Estonia, and outline domestic development needs and potential market growth areas. Finally, we propose a limited number of specific actions for increasing the competitiveness in the field of cryptography in Estonia.

2 Disruptive and emerging technologies

In this section, we list some technologies that were receiving special attention of research community at the time of writing this report. The list has been composed based on various Horizon 2020 calls [1, 2, 3, 4, 5], US Department of Homeland Security Cyber Security Division projects[1], Intelligence Advanced Research Projects Activity (IARPA) programmes[2] and personal experiences of the report authors.

For each technology, we describe what it does, what is its current state, and which strengths or weaknesses it has.

2.1 Post-quantum cryptography

Description

Quantum computing is by far the most disruptive technology expected to cause a change in most of the cryptographic algorithms we use today. A quantum computer can potentially break most of the existing cryptography, so we need new algorithms that are able to survive this event. The development field of such algorithms is called post-quantum cryptography.

History and Current State

Proposed as a theoretical possibility already in early 1980s [15, 58, 34], building a scalable universal quantum computer still remains a challenge. Estimates concerning when this would succeed vary greatly, with the most optimistic ones predicting already the period of 2025–2035 [12].

Whether such an optimism is justified remains to be seen, but the research community seems to agree that implementing a quantum computer capable of breaking most of the contemporary asymmetric algorithms is only a matter of time. More details about quantum computing and its implications to cryptography can be found in reports [10, 11].

In any case, global investment into quantum computing are remarkable. The U.S. is investing more than 1.2 billion USD in the period 2019–2028[3] and China is building a 10 billion USD National Laboratory for Quantum Information Sciences[4]. The European Union has launched its own 1 billion euro Quantum Flagship initiative for the next decade[5].

[1] https://www.dhs.gov/science-and-technology/csd-projects
[2] https://www.iarpa.gov/index.php/research-programs
[3] https://fcw.com/articles/2018/12/14/quantum-senate-bill-gunter.aspx
[4] https://www.popsci.com/chinas-launches-new-quantum-research-supercenter
[5] https://qt.eu

At the time when quantum computers come, vast majority of today's computer applications will become insecure. Old cryptographic primitives require replacement, and someone needs to do it.

Strengths and Weaknesses

A major road block in the activity of replacing old cryptographic algorithms is the lack of standardised post-quantum primitives. The National Institute of Standards and Technology (NIST) of US issued a call of proposals in 2017. As a result, international research community submitted 69 candidates for various asymmetric post-quantum primitives[6]. The First Post-Quantum Cryptography Standardization Conference only took place in April 2018, and NIST currently estimates that the first draft standards will be available some time between 2022 and 2024[7].

Despite this, several of the existing cryptographic libraries have forks or branches containing experimental implementations of quantum-safe algorithms [83]. As the NIST standardisation process continues, they can be expected to change and evolve significantly.

At the moment, none of the main Estonian cryptographic infrastructure components (eID solutions, web technologies used in e-services) is ready for the transition to quantum-safe algorithms. For example, the next generation of ID-cards will only have classical asymmetric cryptographic capabilities.

2.2 Quantum key distribution

Description

Quantum key distribution (QKD) is a technology that allows two parties (e.g. a client and a server) to exchange a key in such a way that security does not depend on the assumption that some mathematical problems are difficult to solve [56]. Instead, it relies on the assumption that the currently used mathematical model of quantum states indeed corresponds to physical reality. In the research community, the current understanding is that QKD is information-theoretically secure thanks to the the laws of physics.

History and Current State

Quantum key distribution is not directly related to general purpose quantum computers, and for this technology we already have something that is actually working. The first reported quantum key distribution protocol was run in the beginning of 1990-s in a laboratory setting, where the distance between two parties was 32 cm [16]. The technology has evolved since that time, and nowadays it is possible to run the protocol through an optical fibre several hundred kilometres long [48, 17]. Moreover, the feasibility of satellite-based QKD has been demonstrated [53], so there is a potential for making QKD possible globally.

Strengths and Weaknesses

In principle, QKD protocols could provide information-theoretically secure key exchange without using public key cryptography. This is good, as most of public key cryptography

[6] https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions
[7] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline

would be broken by quantum computers, and for the rest there is no certainty that it will not be broken as well.

Currently, there are still problems with practicality of QKD. While the expected error can be quite small in theory, it is hard to achieve it in practice, as it is impossible to establish a fully isolated system, and there are always some unexpected measurements coming from the environment. The errors are smaller on shorter distances, for which it would be cheaper and easier to perform the key exchange e.g. using physical interaction. However, in small countries like Estonia, the currently achieved distance of 400 km [17] could be meaningful.

While QKD protocols are relatively simple and nice, exchanging a pair of keys between two parties is not enough by itself. For example, in reality, the parties require authentication before the key exchange. Since the goal of QKD is to remove public key cryptography, the authentication should also not rely on it (or at least be used in a justified way like remaining unbroken for a sufficiently long period [56]). This needs additional tricks and requires more thorough planning of being arranged in practice, e.g. on a e-government level.

2.3 Electronic identity

Description

Strong electronic identity has been one of the core success factors in the development of Estonian e-society. Essence of the notion of identity is deeply philosophical and we won't go in there in this report, but some of the key points relevant for the Estonian context are the following.

- There exists an up-to-date Population Registry. Every citizen or resident having a record in the Population Registry also has a unique Personal Code.
- The Personal Code is universal across all the other registries, too, and can be used to link queries.
- Estonian citizens and residents have been provided with strong cryptographic tokens (ID-cards, mobile-ID, Smart-ID), allowing to authenticate oneself to e-service providers and give digital equivalents of hand-written signatures.

Strengths and Weaknesses

Turning a strong digital identity (like the one used in Estonia) into an international technology has proven to be quite challenging. One of the reasons is that Personal Codes are in many societies perceived as an enabler of mass surveillance or other kind of governmental violation of citizen rights and privacy. Another reason may be that there are several competing digital identity providers, none of whom is able to cover the whole population and as a result usefulness is all of the identity solutions is limited.

One way or another, state of the art in many countries seems to be that there are several partial identity solutions which sometimes need federation, but this can happen only to the extent privacy regulations or business interests allow it to.

An interesting application domain of electronic identity is federated data analysis. This applies to settings where one needs identities to combine personal data from several sources in order to make policy decisions based on aggregated analysis results. In this case, secure computation methods may be used, respecting the data subjects' privacy (see Section 2.4).

Another aspect of digital identity is the one of advanced digital tokens. Until recently, there were only two officially recognised tokens in Estonia (ID-card and mobile-ID) both relying on foreign platform vendors. As the control over foreign platform providers is limited, information about potential vulnerabilities may be delayed, and the choice of solution strategies may be very narrow (as was clearly seen in the ROCA case in 2017). In case of mobile-ID, an additional problem is that the keys are generated outside of the chip [8].

During the time of writing this report (fall 2018), a third, locally implemented cryptographic identity token Smart-ID received Common Criteria certification, giving it a Qualified Signature Creation Device status and making signatures given by it legally equivalent to those of ID-card and mobile-ID.

2.4 Secure computation and privacy-preserving (big) data analysis

Description

Secure computation and privacy-preserving data analysis allow to compute some aggregated statistics on data without letting anyone learn anything else about the data from which these statistics were computed.

History and Current State

The World's economy is moving fast towards being more and more data-centric. With e-services growing both in numbers and in volumes, the information about the users and their behaviour piles up almost automatically and it makes a lot of sense to make use of it. When done right, citizens can benefit a lot from better informed governmental policy decisions and personalised commercial services.

However, there is a darker side to this development. While analysing large sets of personal data, it is very easy to breach privacy of individuals and perhaps even start manipulating with them in ways not universally accepted in the society (just recall the recent Cambridge Analytica and Facebook scandal[8]).

Striking a balance between individual privacy and societal good is not always easy. In EU, there is the General Data Protection Regulation (EU) 2016/679 (GDPR) in force, but it only specifies the legal framework of do-s and don't-s (mainly don't-s). GDPR itself does not recommend and specific compliant software products, but they need to be created by someone. Even in many (maybe even majority) of non-EU-countries, the conflict between personal privacy and the need to use data for informed decision making is acknowledged and solutions are being searched for.

A possible way to resolve the conflict of individual privacy and societal good is to use secure computation. The first works related to privacy-preserving computation started emerging in the late 1970-s and early 1980-s (e.g. papers by Shamir [76] and Yao [86]). At those times, applying secure computation to big data would have been infeasible due to excessive performance penalty on the originally proposed methods. By today, both the methods and the machinery to run them on has been improved a lot, making privacy-preserving big data analysis a possible.

[8] https://en.wikipedia.org/wiki/Facebook-Cambridge_Analytica_data_scandal

Categories, their Strengths and Weaknesses

There are several methods for privacy-preserving data analysis currently actively developed around the world, all with their own specific strengths and weaknesses.

- **Fully homomorphic encryption** is a technique that, in principle, allows computation outsourcing to a completely untrusted environment. However, it comes with a significant performance drop which currently makes it unsuitable for even moderately-sized datasets.
- **Secure multi-party computation (SMC)** enables data processing by a group of semi-trusted agents. Privacy is preserved as long as not too many of the agents behave too maliciously. Performance of SMC techniques has improved a lot in recent years, and pilot studies with relatively large datasets have been performed. However, SMC typically requires non-standard setup and security assumptions (e.g. threshold trust) that are not always straightforward to implement.
- **Trusted execution environments (TEE)** are hardware products that offer certain data protection mechanisms while operating as parts of generally untrusted setups. The prime example in this category is Software Guard eXtensions (SGX) by Intel, providing also a capability of remote attestation of the applications running in it. On the other hand, one has to trust Intel and there are still side-channel attacks known against SGX. Also, setting SGX up and producing applications for it is non-trivial.

2.5 Radio frequency protocols

Description

Contactless cards and applications have become integral parts of our everyday lives. We use them to open the doors and cars, take public transportation, prove our customer loyalty and even make payments. Speed and convenience at what this all happens is the key success factor behind wide-spread acceptance of contactless technology.

Strengths and Weaknesses

There are several aspects of Near Field Communication (NFC) protocols that make them more vulnerable compared to, say, chip-and-PIN solutions. First, NFC cards and tags typically come without an on-board power source (who would like to change the batteries on their door cards?). This severely limits the selection of cryptographic primitives available on NFC platforms. As a result, rather resource-consuming asymmetric cryptography is not available on commodity tags, making use of strong authentication protocols impossible. Vendors of these platforms have invented a number of *ad hoc* solutions, all of them having issues of some kind [10].

Quite probably the vendors themselves are well aware of the potential problems, so as one precaution they are trying to hide the protocols. This has been proven to be a poor strategy on numerous occasions [10]. However, security by obscurity is still a popular approach that should raise an alarm among the users. The prime example are contactless payments, the cryptographic protocols of which have never been publicly released.[9]

[9] This claim reflects the state of knowledge of one of the authors of this report. He has made numerous attempts of obtaining a cryptographic description of contactless payment protocol from various sources, but

It is unlikely that Estonia will have its own NFC chip manufacturer. However, product developers are there (e.g. for public transport ticketing system). They need consultancy in cryptographic protocol analysis (even though they sometimes ignore this need); see Section 2.7.

2.6 Internet of Things / cryptography in limited environments

Description

The term Internet of Things (IoT) is a paradigm of communication, in which everyday devices (*things*) have sensors to collect data, network connectivity to communicate, and sometimes actuators to take action. IoT application domains include household devices, transportation, manufacturing, supply chains, healthcare, agriculture, city management, etc.

History and Current State

The concept of ubiquitous computing was given in the early 1990s by Mark Weiser [84], proposing the idea of integrating computers seamlessly into the world at large. In recent years, IoT is becoming deeply interwoven into our daily lives by automating our homes, routine work, and personal tasks. IoT is envisioned to extend network connectivity to almost every useful physical object. There is an opinion that IoT will play a leading role in shaping the destiny of humanity in the near future [75].

Functionality

An IoT device often has poor computational resources and limited energy supply. Data collection, computation, and communication need to consume as little energy as possible. In some cases, heavy computations can be delegated to a cloud, so that the device does not have to consume its own energy. However, since a device often collects and processes sensitive data, privacy is an issue. A device should be able to establish secure and reliable communication with the other devices, which in turn requires energy, even if the device itself does not need to perform any other heavy computations. In general, an IoT device should support the following functionalities:

- unique identifiability,
- sensing the environment,
- communication,
- data storage and analytics.

Some advanced properties like dynamic self-adaptation or intelligent decision-making capability may be required from a device.

has systematically failed. He will be happy if a reader of this report will be able to refer him to the correct source. If this is the case, please use the contact information provided in the front matter of this report to contact the authors.

Strengths and Weaknesses

Wide distribution and openness of IoT objects makes them an ideal target for attackers. The fast growth of IoT services led to deployment of many vulnerable and insecure nodes, which may pose a threat to the other, non-compromised nodes in the system. Therefore, detection of malicious activity and forensics are of extreme importance for IoT networks. Data mining tasks such as evidence identification, collection, and analysis, are among important research fields.

From the general infrastructure point of view, an interesting task is developing compact software blocks that would be useful for different types of IoT. The main issue of IoT devices is their computational weakness, and more efficient protocols are always welcome. The survey [75] lists some issues of the current solutions in IoT field.

- Authentication schemes designed for specific IoT scenarios are not able to protect against all possible threats associated with them.
- There is need for lightweight key management and revocation schemes that would be appropriate for different IoT application domains.
- Existing schemes often lack proofs of their viability (whether energy consumption is acceptable in practice) and have limited security guarantees.
- There is need to investigate the fate of existing lightweight cryptographic schemes for securing IoT devices in the era of quantum computing.
- There is need to develop more reliable and resource efficient nanoelectronic security primitives.

2.7 Cryptographic protocol analysis

Description

The goal of cryptographic protocol analysis is to verify whether a certain protocol (e.g. TLS) indeed satisfies the security properties that it is assumed satisfy. Hence, it has potential use in protocol certification (see Sec. 4.4 for more details).

History and Current State

Attempt to ground security analysis of protocols on rigorous mathematical foundations started in early 1980's [27]. Technically, it is difficult to work directly with the program source code, so the protocol is modelled on a more abstract level, and some mechanism is applied to verify whether the model satisfies certain properties. This can be done using different formal verification techniques, and numerous tools for automated protocol analysis have emerged (e.g. ProVerif[10], EasyCrypt[11] and Tamarin[12] just to name a few). Nowadays, all existing protocol analysers still have their limitations, and are more academic prototypes rather than ready-to-use tools. Nevertheless, they can be used to prove security or find vulnerabilities in some real protocols. For example, the Needham-Schroeder public-key protocol was believed secure for 17 years before a flaw was discovered in it. This flaw can be found by applying formal methods of protocol analysis [13].

[10] http://prosecco.gforge.inria.fr/personal/bblanche/proverif/

[11] https://github.com/EasyCrypt/easycrypt

[12] https://tamarin-prover.github.io/

Categories, their Strengths and Weaknesses

There exist two main approaches to protocol modelling (see e.g. [27]).

- **Symbolic approach** assumes that the transmitted messages are of certain form. It treats cryptographic primitives as perfect and does not take into account e.g. probabilities of guessing. Nevertheless, it fully models interactions of parties and supports algebraic properties of the primitives. It is relatively easy to model protocols in this way, and the verification can be fully automatised (although support of algebraic properties has certain limitations [49]).
- **Computational approach** allows messages to be arbitrary bit strings, which is more realistic. It also takes into account probabilities. It is generally acknowledged that security proofs in this model offer powerful security guarantees, but the proofs may become too long even for smaller protocols. Automating such proofs is a very complex problem. There do exist some proof assistants, but they are quite hard to use, and it is even hard for an independent auditor to verify whether the protocol has been modelled correctly in the first place.

In both approaches, we need to know the answer to the question *which properties does the protocol have to satisfy?* It does not make sense simply to state that "a protocol has to be secure" without specifying what it means to be secure. Formally specifying an intuitive notion of security is sometimes highly non-trivial. For example, when modelling a key establishment protocol, it is not sufficient to verify that the attacker cannot learn the key that the parties exchange. We also need to check whether two honest parties indeed agree on the same key, and whether the attacker may tamper with the key in any way, e.g. force parties to use a key from some earlier protocol session.

2.8 Challenges to Long-Term Protection of Systems

Description

Measures that made systems sufficiently protected yesterday are not necessarily safe today or in future. Understanding new threats, introducing new protection measures, revisiting the principles of system engineering, as well as designing a suitable legal framework are all important challenges today. This introduces the need for long-term cryptography.

History and Current State

Cryptography has a central role in the protection against many types of potential attacks against today's systems, but on the other hand, cryptographic attributes need protection against ageing effects related to the growing computational resources available to attackers, including possible creation of quantum computers in the future. Some examples of eventually broken cryptography can be found e.g. in the overview by Buchmann *et al.* [19].

For example, in 1978 when the RSA cryptosystem was proposed, the authors originally suggested having 200 decimal digit modulus for long-term security [72]. However, the first official factoring of a 200-digit number happened in 2005, even without using a quantum computer. Numerous cryptographic hash functions have already been broken, and new vulnerabilities are continuously being announced.

Long-living systems must be flexible enough to enable the change of cryptographic schemes in use. For example, one possible challenge is to change the hash functions used in today's block-chains in case they become too weak.

Categories, their Strengths and Weaknesses

Reconfigurable Cryptography

The idea of reconfigurable cryptography was first proposed by Hesse, Hofheinz and Rupp in 2016 [45]. Reconfigurable cryptographic schemes have long-term and short-term public and secret keys. Long-term keys are generated once for each user, and the long-term public key is published.

Short-term keys are derived from long-term keys and a publicly available information, which in the cryptographic model is represented as a common reference string (CRS). Short term keys are used in actual operations. If short-term keys become insecure, only the CRS needs to be updated. As long-term keys are used only for deriving short-term keys (based on the CRS) and are not used in actual operations, they can be kept off-line at a secure storage.

Reconfigurable cryptography is a very promising research line, the results of which will certainly be used in the cryptographic schemes of the near future. However, this approach still assumes that the overall scheme does not break and the long-term keys stay secret. In practice, even the reconfigurable cryptographic schemes may broken and the long-term keys may become insecure. Therefore, reconfigurable cryptography alone does not solve all long-term security issues.

Long-Term Security Models

The currently used cryptographic schemes are not designed to fulfil the requirements posed to archival documents. As the cryptographic attributes of long-lived documents will almost certainly break during the documents' lifetime, there have to be procedures for renewing the cryptographic attributes in a way that preserves the evidentiary value of the documents. Such a renewal procedure for digitally signed documents and time stamps was proposed by Bayer, Haber and Stornetta in 1993 [14]. However, they did not even try to formally prove the security of the renewal scheme.

Comprehensive security analysis and general theory for long-term security and the renewal procedures is still missing. In [36], the existing security models for long lived systems are discussed and a new model that allows to formally analyse timestamp-based long-term integrity schemes is proposed.

One of the most important issues in modelling long-term security is the need to model human ignorance, i.e. the fact that, from time to time, new and more efficient attacking methods are discovered. In the classical model, the strength of a cryptographic primitive does not change over time, which is clearly not the case in practice. In view of this, Buldas, Geihs and Buchmann [20, 21] proposed a new computational model, where adversaries can "learn" new attacking algorithms over time. In the new model, it was possible to present a formal security proof of the renewal scheme. The security proofs were provided in the model that contains ideal components. Proofs in the plain model are still missing.

Correct modelling of the ageing effects of cryptography is a very important practical research topic, as the theory of long-term security provides a basis of constructing long-term secure IT-applications.

Long-Term Secure Storage

The design of proper archival storage mechanisms of long-lived data is crucial for practical long-term security. Not much research has been done in this area, though it is of great importance, especially in the context of e-government systems of the leading IT-countries like Estonia.

In [18], Braun et. al. proposed the LINCOS long-term secure storage system, the first system that protects long-term integrity, authenticity and confidentiality at the same time. Later, Geihs, Karvelas, Katzenbeisser and Buchmann [37] proposed a variation of LINCOS called PROPYLA: a system that also ensures that no information is leaked to the storage servers due to the data access patterns.

Design for Long-Term Security

The central question of this line of research is how to design critical IT-systems, such as e-government system and databases, as well as their components (like PKI, ID-cards, signature devices, block-chains) in a flexible and fault tolerant fashion. The ultimate goal is developing systems in such a way that even if the cryptographic components break, they can be replaced without stopping the whole system. We learned from the Estonian ID-card crisis of 2017 that there is much room for improvement in the fault-tolerant design of e-government systems.

Nowadays we witness the development of numerous block-chain systems some of which are intended to use for a long period of time. However, almost no research has been conducted on the long-term security of block-chains. For example, how to proceed if the hash functions that the block-chains rely on will be broken? Suitable replacement schemes must be invented and designed before block-chains can be used as components of critical IT-systems.

Interdisciplinary Aspects

Long-term security includes many interdisciplinary aspects that have not received necessary attention. For example, the key security question in case of block-chains is how to guarantee and check the uniqueness of a particular block-chain, i.e. that no alternative versions exists about the particular block-chain. Some of the security arguments of block-chains used in white papers and also in properly published scientific works [26] are social. For example, the security of the so-called *proof of stake* type block-chains uses a claim that those having cryptocurrency in a particular block-chain are not interested in attacking the same block-chain. Another argument is that the cryptocurrency-based incentives are sufficient for keeping the so-called permissionless block-chains alive. Such questions would require intensive social-scientific research before permissionless block-chains could seriously be considered as components in critical IT-systems, like e-governments.

2.9 Anonymous networks

Description

Confidentiality and integrity of data communicated in the network can be achieved through encryption and signature mechanisms. However, no matter how strong encryption is used, there is still some information that the attacker may extract from communication metadata. As the attacker is able to observe the network flow, it will see who is communicating with whom, when, from where, in which quantities and for how long. The goal of anonymous networks is to conceal such metadata.

History and Current State

The milestone paper published in 1981 by Chaum [24] introduces the concept of anonymous communication, and some proposals for implementing an anonymous email service. Nowadays, this concept has been extended to more scenarios like censorship-resistance and anonymous web browsing. Real applications like Tor or I2P are available for use.

Functionality

The aim of anonymous communication is to enforce three main properties [32].

- **Anonymity**: the state of being not identifiable within a set of subjects, called the anonymity set.
- **Unlinkability:** any particular message sent through the network is not linkable to a particular sender in the sender set (and/or a particular receiver in the receiver set).
- **Unobservability:** it is not noticeable whether any sender within the sender set sends the message (and/or any receiver in the receiver set receives the message).

Categories

There are many types of anonymity networks. They can be divided into two main categories. High-latency anonymity systems are slow, but often provide stronger anonymity. They are mostly used for non-interactive applications that can tolerate higher delays, such as file downloads. Low-latency systems minimise the delay overhead and are suitable for real-time applications such as instant messaging and web browsing. The general idea is that communicating peers transmit data through a special cascade of proxy nodes. If there is an independent set of nodes that provides anonymity for the actual users, we have a client-server (centralised) communication system. If there is no distinction between a user and a proxy node, we have a peer-to-peer based (decentralised) communication system. The proxy nodes may act in one of the following ways [77].

- **Mix networks:** A mix node does not output the messages immediately upon arrival, but instead collects a certain number of messages into a batch. It re-encrypts and shuffles all batch messages before outputting, so that an adversary is not able to establish a correlation between input and output messages. Such networks can be used in anonymous e-mailing, such as *Mixmaster*.
- **Onion routing:** The initial message is encapsulated into several layers of public-key encryption, which resembles adding layers of onion around the message. Each

public key corresponds to a secret key of some onion router. As the next onion router receives the message, it peels the outermost onion layer from it. Each node knows only its predecessor and successor, and encryption prevents it from discovering the other links. When the message finally arrives at its destination, all encryption has been peeled off, and the receiver can read the message. This approach is used in the famous anonymity network *Tor*. To cause even more confusion for the attacker, several messages of different senders may be encrypted together like garlic cloves in a garlic bulb. This is called Garlic Routing, employed by *I2P*.

- **Random walk protocols:** The sequence of proxy nodes is not fixed, and it is chosen each time in a certain random way. This approach is used by *Crowds* and *Freenet*.
- **Dining cryptographer (DC) networks:** The dining cryptographers problem got its name from an example that illustrates possibility of sending a message without disclosing the sender. The example itself is very simple: a group of cryptographers wants to learn whether one of them has paid for the meal, but they should not know who exactly has done it. Instead of sending a single bit of information that "someone has paid for the meal", any message can be sent anonymously using this method. This approach offers non-interactive anonymous communication using secure multiparty computation with information-theoretically secure anonymity. However, it is difficult to keep such system efficient on large scale, especially if malicious nodes are assumed (the original protocol assumed honest dining cryptographers). This approach is used by the systems *Herbivore* and *Dissent*.

Strengths and Weaknesses

As discussed in [32], it is easier to attack anonymity on application level, so that the protection mechanisms of the anonymity network would be simply bypassed. For example, identifying information can be leaked through the anonymity network, being treated as an ordinary message, which at some point gets rid of all the onion layers, exposing the identity in plain. In general, the user is the one responsible for protection against such attacks.

Network level attacks are often out of the user control. Some kinds of attacks can be reduced by insertion of random traffic payload and random delaying of message transmissions, which unfortunately is an overhead for the entire anonymous network. The good news is that such attacks are easier to perform in a small network, and as the number of users grows, the attacks become computationally too expensive.

While breaking anonymity is just one particular goal of the attacker, there is some other knowledge that the attacker may want to extract. Such additional information may in turn help in breaking anonymity, assuming that the attacker already has some prior knowledge. An open research field is the Traffic Classification (TC). TC mechanisms label traffic flows with specific types, possibly using power of machine learning [69]. For example, it is possible to train a classifier that is able to guess the searched keyword (from a set of predefined keywords) using a particular search engine [65]. Unfortunately, it is not easy to prevent the attacker from traffic analysis (and hence traffic classification) [40].

It seems that the main source of new attacks is the problem that the protocols are provably secure only against certain types of attackers. The largest hazard comes from traffic analysis, which may discover quite interesting things when combined with machine learning. There exist nice solutions such as Dining Cryptographer networks, which are based

on secure multiparty computation and eliminate traffic analysis problem. However, such protocols are slower, and still rely on some assumptions like non-collusion of the parties that share the keys.

2.10 Block-chains

In this section, we will be relying on a recent overview paper by Heiberg *et al.* [42]. An interested reader can also find further information concerning block-chains in the report [11].

Description

The concept of a block-chain does not have a single, universally agreed upon mathematical definition. However, different implementations seem to have a few common points.

- Data storage occurs in *blocks*, where the exact content of a block or its semantics may vary (e.g. it may contain transactions for cryptocurrency applications).
- The blocks are linked into a sequence (also called a *ledger*) using a cryptographic hash function.

History and Current State

The idea of hash linking data items is not at all new, going back to at least early 1990s to the works of Haber, Stornetta *et al.* on digital time stamping [39, 14]. However, it seems to be exactly this idea of hash linking that gives block-chains the attractive property of integrity assurance, since cryptographic hash functions are supposedly hard to invert, making it difficult to revert the linking once it has been performed.

The real renaissance of block-chains happened in late 2008, when a researcher (or a group of researchers) hiding behind the pseudonym Satoshi Nakamoto published what is nowadays known as Bitcoin white paper [60]. Essentially, Nakamoto showed how to use available cryptographic and networking tools to achieve a new type of decentralised consensus protocol.[13]

The core innovation of Nakamoto's proposal is introducing computationally difficult puzzle solving (proof of work) together with financial incentives to consensus building. Whoever solves the puzzle first can create the next ledger block and is rewarded with a certain amount of bitcoins. Due to some similarity with gold mining, the participants in this joint effort are called *miners* or *mining nodes*.

Functionality

Nakamoto's original motivation was to build a monetary system and there the need for consensus is clear – value exchange can only function correctly when there is a universally accepted way of deciding who has how much money.

However, the problem of obtaining a coherent view on the system in a distributed manner is more general, and this is why the original Bitcoin protocol and infrastructure have been used for a myriad of alternative applications.

[13] The origin of the term "block-chain" is somewhat unclear. It seems to haver been used in some cryptography-related mailing lists in mid 1990-s, but the first occurrence is hard to track. It is interesting to note that Nakamoto's white paper only uses the term "chain of blocks" and not "block-chain".

It is worth noting that the original Bitcoin white paper does not present any formal definitions of targeted properties, and contains only a simplified security analysis. Follow-up work by Garay *et al.* [35] and Pass *et al.* [66] have formalised several aspects of block-chains and clarified the necessary assumptions to prove the security of Bitcoin protocol.

Another functionality making block-chains appealing for various applications is the ability to run smart contracts. Originally proposed already in mid-1990-s by Nick Szabo [79, 80], smart contracts can be thought of as a scripting layer on top of a block-chain, allowing to check fulfilment of certain conditions, and enforcing predefined actions in the respective cases. There are several block-chain frameworks that offer this functionality in a form of a programmable execution environment, including Ethereum Solidity[14], Hyperledger Fabric[15] and Cardano Plutus[16].

Categories

Block-chains come in several flavours. Bitcoin block-chain is an extreme example of a distributed ledger where there is no single trusted entity to coordinate the work, nor to decide which blocks to accept from whom, etc. In this case we speak of a *permissionless ledger*.

However, this is not the only option. It is also possible to set up a block-chain where data commitments are only accepted from a predetermined set of nodes, and there may even be an authority deciding that some of the blocks will not be admitted. Such a ledger is called *permissioned*. Block-chains built within the Hyperledger framework are examples of such a paradigm.

Similarly, it is not necessarily the case that anyone is given access to the block-chain for reading. Depending on whether or not general access is allowed, we speak of *public* or *private* block-chains, respectively.

Strengths and Weaknesses

As a core technology, block-chain offers mainly (if not only) integrity properties. This on its own may be useful in some applications (like time-stamping system logs to detect later tampering), but in many real systems also other security properties like authenticity and confidentiality are required. These properties must be provided by other components of the system. It seems that on many occasions the problems caused by integration of these components result in an overall decrease of the security level [42, 67, 54, 87]. This makes assessing the exact value obtained when implementing a block-chain based solution a challenging task. Cryptocurrencies like Bitcoin and Ethereum still remain the main application of block-chains having a direct economic impact. On the other hand, such applications are highly speculative as can be clearly seen from a very volatile exchange rate between cryptocurrencies and classical monetary assets.

[14] https://ethereum.org/
[15] https://www.hyperledger.org/projects/fabric/
[16] https://cardanodocs.com/technical/plutus/introduction/

3 Current state of cryptography in Estonia

3.1 Private enterprises

In this Section, an overview of the Estonian private sector actors that are influenced by the developments in the field of cryptography is provided. The list of companies given below is non-exhaustive, but the authors of the report believe it to be representative nevertheless.

We have grouped the companies into five categories as the business models and the nature of (local) clustering, developmental challenges and expectations regarding policy measures are rather different.

Locally owned R&D based companies whose core products are strongly based on cryptography

Locally owned well established medium-sized companies whose core products are strongly based on cryptography are, for example, Cybernetica AS and Guardtime AS. We also include Smartmatic-Cybernetica Center of Excellence for Internet Voting (SCCEIV) into this group.

Cybernetica AS is an R&D intensive ICT company that develops and sells mission-critical software systems and products, maritime surveillance and radio communications solutions.[17]

Guardtime AS is a data integrity service provider that offers a service architecture that enables users to check whether data has been tampered with.[18]

SCCEIV is a company providing Internet voting solutions based on the Estonian experience and local competence.[19]

Key data of these companies can be found in Table 1.

The companies in this group

- understand key technology trends;
- are strongly integrated with the local R&D and education systems, and are key providers of governmental R&D solutions;
- depend on local and international R&D grants (Guardtime a bit less so);
- depend also on local public procurements (as testing grounds).

[17] https://cyber.ee/
[18] https://guardtime.com/
[19] https://www.ivotingcentre.ee/

Table 1. Key locally owned and cryptography based R&D companies

Name	Established	Employees (FTE, 2017)	Turnover (2017)	Exports (2017)
Cybernetica AS	1997	115	8.1M EUR	2.7M EUR
Guardtime AS	2006	47	4.6M EUR	4.5M EUR
SCCEIV	2014	9	0.3M EUR	0 EUR

Local companies with own ICT products and services that implement advanced cryptographic solutions

These are generally locally owned, often small or medium sized companies, whose core products or services are strongly based on cryptography. Examples of such companies include, for example, the following.

SK ID Solutions AS (38 employees, established in 2001)[20] specialises in international e-identity solutions.

Ridango AS (46 employees, established in 2009)[21] is a transportation solutions provider with core focus on account based ticketing and real-time passenger information.

Clarified Security OÜ (11 employees, established in 2011)[22], delivers practical security services, with the focus on manual web application penetration testing.

Pipedrive OÜ (231 employees, established in 2010)[23] develops web-based customer relationship management and sales pipeline management software, implementing advanced cryptographic solutions.

Furthermore, Estonia has a lively financial sector sector and companies in that sector depend largely on locally developed advanced ICT, including advanced cryptographic solutions. Examples of such companies include a relatively older AS LHV Pank (326 employees, from 1999)[24], but also newcomers, such as AS Pocopay (15 employees, from 2014)[25]. Or, now globally operating Transferwise's local operational unit – Transferwise Ltd Estonian department (680 employees, from 2013)[26]. Monese Ltd Estonian department (85 employees, from 2015)[27] is another innovative financial services firm. Funderbeam (31 employees, from 2013)[28] is developing a block-chain based global fundraising and trading platform for companies that are in the early phases of their development.

These companies

- understand key technology trends in their specific niches;
- have internal ICT development teams and occasionally co-operate with R&D partners

[20] http://www.sk.ee/
[21] http://www.ridango.com/
[22] http://www.clarifiedsecurity.com/
[23] http://www.pipedrive.com/
[24] https://www.lhv.ee
[25] https://www.pocopay.com/
[26] https://transferwise.com/
[27] https://monese.com
[28] https://www.funderbeam.com/

to solve their specific challenges; in some cases the co-operation is extensive, for example, in the case of SK ID Solutions;

- those that are offering services in Estonia, such as Rigango's ticketing and SK ID Solutions Estonian identity, do depend on local public procurements;
- the companies offering global financial services are not influenced by R&D grants nor by public procurements.

IT systems integrators

IT systems integrators are ICT service providers, mostly small or medium-sized companies, whose core products or services sometimes have cryptographic relevance. This includes general development and integration of tailor-made ICT systems.

An example of a locally owned small or medium-sized company whose core products have cryptographic relevance, is Aktors OÜ (52 employees, from 2011)[29]. It is a software development company mostly for government and financial services sectors.

These companies

- do not have specific cryptographic R&D teams;
- rely on cryptographic solutions on the market that they are then integrating into their solutions;
- have activities that are largely influenced by the local and international public procurements.

Early stage start-up companies in the field of cryptography

These are start-ups and other emerging ventures that are in the development of viable business models around cryptographic products or services, and/or are validating the market fit of their products and services. Cryptography-intensive start-ups include companies that develop own products or services that depend on strong cryptography.

Some of the examples of such companies are Cuber Technology OÜ (established in 2015)[30] that has partnered up with LHV bank to experiment with cryptographically protected securities.

Rangeforce (established in 2015)[31], registered in the US, offers game-based online cyber security training for developers and security experts.

CybExer Technologies OÜ (17 employees, from 2016)[32] offers an easily deployable solution for complex technical cyber security exercises based on experience in military grade ranges.

These companies

- depending on their technology intensity, are sometimes integrated with the local R&D system;

[29] http://www.aktors.ee/
[30] http://www.cuber.ee
[31] https://rangeforce.com/home
[32] https://cybexer.com

- are generally less aware of the disruptive technologies, other than in their specific field;
- have a shorter time perspective, around 2-3 years, due to the need to demonstrate the viability of the business model to the funders.

Branches or subsidiaries of foreign owned companies

These foreign owned companies can be branches of parent companies, or mostly, subsidiaries, businesses opened by a foreign company in Estonia with a majority of share capital owned by it, and are fully integrated into the value networks of the parent companies.

Foreign owned companies are, for example, Arvato Services Estonia OÜ, part of international service provider Arvato that has more than 70,000 employees developing and implementing innovative solutions for business customers from all over the world, including CRM, SCM, finance and IT solutions. Arvato is wholly owned by Bertelsmann[33].

Symantec Estonia OÜ is part of Symantec, global leader in cyber security, with more than 11,000 employees in more than 35 countries[34].

Malwarebytes Estonia OÜ is part of Malwarebytes that develops malware prevention and remediation solutions.

Ericsson Estonia is particularly interesting. 4G network infrastructure has a strong cryptographic element. Furthermore, Ericsson is responsible for roughly 10% of Estonian manufactured exports. Yet, there are basically no local hardware or software components (incl. cryptographic solutions) involved. There is a lot of unused potential in this area for Estonia from joint R&D to inclusion of locally developed components or products into Ericsson's portfolio, even if this would not materialise immediately.

These companies

- are rather disconnected from local R&D and innovation system;
- do not see local support measures, such as R&D grants and Estonian public procurements, as influencing them in a major way.

Summary: Competencies and Integration with the Estonian R&D system

Depending on the integration with the local R&D system and on the competencies regarding cryptography, the positioning of those previously identified groups of companies, is rather different.

We have locally owned R&D based medium-sized companies whose core products are strongly based on cryptography. Those companies, as identified during the analysis carried out within the project, have excellent understanding of the key technology trends and are strongly integrated with the local R&D, innovation and education systems.

Local companies with own ICT products and services that implement advanced cryptographic solutions are less aware of the general trends, but are nevertheless strongly in-

[33] https://www.bertelsmann.com/company/company-profile/
[34] https://www.symantec.com/about/corporate-profile

tegrated with and depend largely on the local educational system, are co-operating occasionally with the local R&D organisations, and are largely influenced by local public procurements.

IT systems integrators, mostly small or medium-sized companies whose core products or services have cryptography relevance, are also integrated with the local system (although more on the educational system, and less on R&D) and have strong (public procurement based) partnership with Estonian public sector.

Early stage start-up companies in the field of cryptography are less integrated with the local innovation ecosystem, they are mostly focused on the global market from the start.

Branches or subsidiaries of foreign owned companies are even less integrated with the local R&D and education system.

Although the number of companies active in the field of cryptocurrencies is relatively high in Estonia (515 licensed companies as of November 2018), their overall contribution to the long-term knowledge- and science-based development of the Estonian ICT sector is estimated to be quite limited. They are disconnected from the local R&D and educational system and their knowledge-intensity is relatively low.

Labour productivity per person employed in the two largest locally owned R&D based companies whose core products are strongly based on cryptography is ca 60 thousand euros (2016). This is significantly higher compared to other similar companies as well as for the Estonian ICT sector in general. For example, the same figure for the companies active in the field of computer programming, consultancy and related activities is 37.1 thousand euros (2016) and for the companies active in scientific research and development it is 39.1 thousand euros (2016) (Statistics Estonia, data table FS008[35]). Both companies are also very export-focused in their cryptography related activities, exporting to highly developed and competitive markets, such as the US.

There is sharp contrast with the companies providing services of exchanging a virtual currency against a fiat currency and/or providing a virtual currency wallet service. The number of those companies has been increasing rapidly (mostly established in 2018). But even those established earlier remain very small: according to 2017 annual reports to the Estonian Business Registry, only one of them has 10 employees (with labour productivity per person employed only 17 thousand EUR). One has 4 employees and the remaining companies less than that.

Various business models are depicted in Figure 3.

3.2 Public administration

From the results of the interviews and workshop discussions with the representatives of the governmental institutions, the following observations were made by the authors of the report.

[35] http://pub.stat.ee/px-web.2001/I_Databas/Economy/databasetree.asp

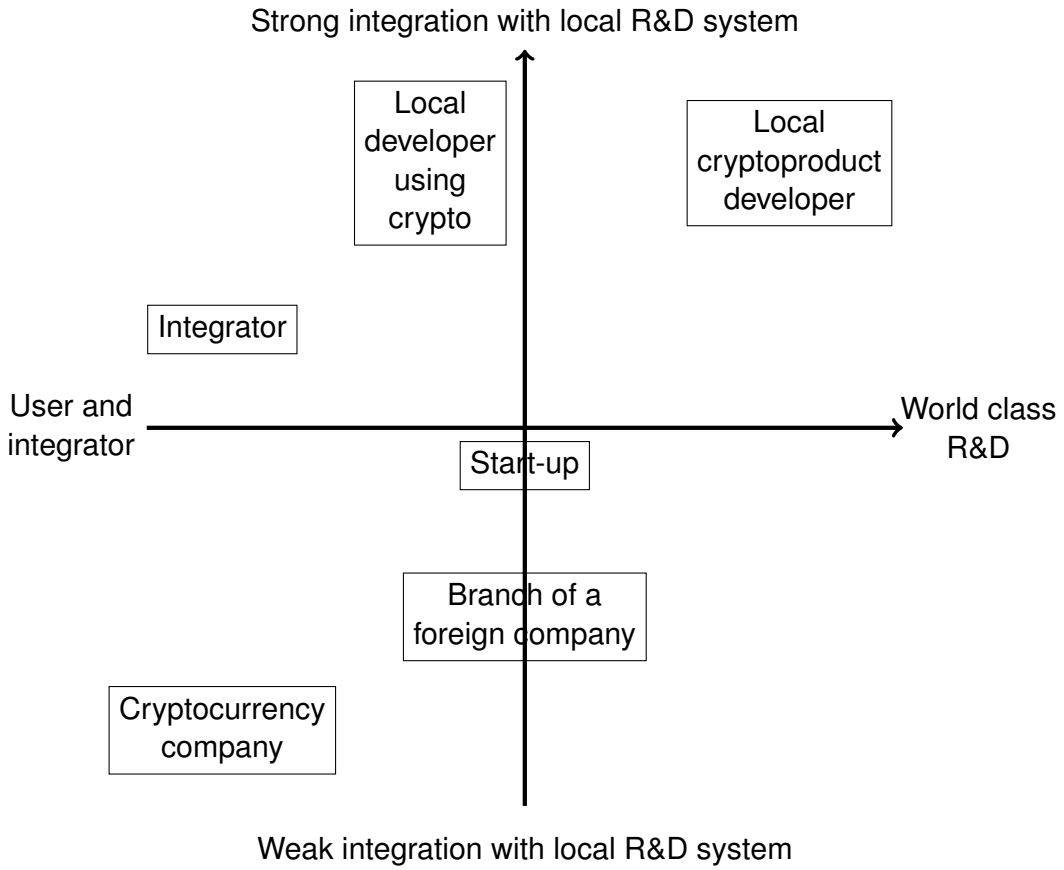

Figure 3. Business models of crypto-rich enterprises

Low average level of cryptographic competence

Some of the interviewees openly identified their communication usage scenarios and security understanding as that one of Average Joe ("tädi Maali"). None of the interviewees were able to explain which cryptographic protocols or primitives are in use in their everyday communication security applications. Even more, it was also unclear whether anyone in the institution had this overview. The only exceptions were eID solutions that use widely publicised cryptographic primitives.

Lack of cryptographic competence for development and procurement

In a typical development/procurement scenario, a governmental institution does not have competence to set cryptographic requirements. In this case, the institution hopes to get this competence from another one, which, in turn, may delegate acquiring this competence further, etc.

These delegation sequences ends mostly State Information Agency (RIA). However, the State Information Agency has lost a number of people with information security and cryptography competences in recent years. This is nicely illustrated by the fact that the interviewee from RIA's side was a person, who has not actually worked in the institution for more than a year.

Lack of long-term vision

One of the questions we asked during our interviews concerned the ideas and needs for future development. The answers were disappointing. In the best case, the respondents were able to envision message exchange applications with a bit enhanced security properties, but nothing more advanced than that. There are no ideas comparable to X-Road or Internet voting that once put Estonia into the forefront of digital development.

Lack of strong vision in the public administration manifests itself in a historically relatively low success rate of public procurement of innovation. This type of procurement can only be successful if the procurer knows well what it needs. When research institutions (which in Estonia means mostly universities) are given a leading role, they will develop whatever is academically interesting to them, but this is not the idea behind public procurement of innovation.

Insufficient economies of scale

Relatively limited volume of public procurement of innovation has not led to the emergence of highly demanding lead markets that would be sizeable enough, so that the behaviour of enterprises would actually change. The relatively small domestic market will remain an important constraint in making full use of public procurement of innovation even if the amount of such calls for tenders will increase. Joint calls for tenders with the neighbouring Nordic countries or EU members more broadly would be one of the possibilities, e.g. in the context of European Defence Fund, for overcoming the limits of small domestic market in Estonia. Joint actions are also likely to simplify further interoperability and standardisation efforts.

3.3 Research and education

The history of cryptographic research and education in Estonia can be tracked back to at least 1935, when lieutenant colonel Artur Normak published a textbook on what where then considered to be state of the art ciphers [62]. Another Estonian officer, colonel Olav Õun, was reportedly involved in deciphering Russian military communication during the World War II [55]. However, Soviet government ended both the independent Estonian army and all the cryptologic research within.

Contemporary period of cryptography in Estonia started in 1990s when Institute of Cybernetics initiated development of communication security devices (firewalls, virtual private network appliances, etc.) for the newly established Estonian government. The first major paper by Estonian cryptographers was published in 1998 at Cybernetica (then already an independent descendant of Institute of Cybernetics) [22].

From early 2000s, also the two major Estonian universities, namely University of Tartu and Tallinn Technical University (now also known as TalTech), started education and research in the field of cryptography. By 2018, three out of ten top cited computer scientists (ordered by Google Scholar based Hirsch index) working in Estonia are cryptographers.[36]

[36] See http://kodu.ut.ee/~lipmaa/cites/cites.php?data=estonia&sorted=h . This list also includes computer scientists who originate from Estonia, but do not work here; we have excluded them from this study. On the other hand, we include researchers who come from abroad, but work in Estonia. Thus, the list (with cryptographers displayed in bold) together with their Hirsch index as of fall 2018 becomes: 1. Marlon

In 2006–2015, an Erasmus Mundus master's programme dedicated to mobile computing and information security (called NordSecMob) was run jointly by 5 major Nordic universities (including University of Tartu).[37]

Since 2009, University of Tartu and TalTech run a joint MSc programme in Cyber Security. The number of admissions and graduates over the years (based on the information obtained from TalTech) is presented in Table 2.

Table 2. Intake and graduates of Cyber Security MSc programme in 2009–2019

	09/10	10/11	11/12	12/13	13/14	14/15	15/16	16/17	17/18	18/19
Intake	27	37	42	51	52	77	77	68	63	60
Grads	N/A	3	21	17	23	15	36	33	42	N/A

Most of the cryptography courses (except for one) in this curriculum are actually electives given at the University of Tartu. Thus we may say that University of Tartu is the primary source of crypto education with its six courses on the subject:

- MTAT.07.002 Cryptology I
- MTAT.07.003 Cryptology II
- MTAT.07.014 Cryptographic Protocols
- MTAT.07.017 Applied Cryptography
- MTAT.07.022 Research Seminar in Cryptography
- MTAT.07.024 Quantum Cryptography

Trying to define and assess the levels of general cryptographic competence among the graduates, we asked University of Tartu to find out how many students have completed one, two, ..., six of these courses over the years. The results, separately for foreign and local students, are given in Table 3 (non-cumulative). Note that the Cyber Security programme students who have taken crypto electives are included in this table.

Table 3. Students of crypto courses at the University of Tartu

	1 course	2 courses	3 courses	4 courses	5 courses	6 courses
Foreigners	60	15	11	12	8	
Locals	136	24	6	8	5	5
Total	196	39	17	20	13	5

Looking at Tables 2 and 3, we may say that in principle there could be hundreds of people on the Estonian job market with at least some competence in information security and/or cryptography. Of course, a number of the graduates have probably not stayed in Estonia, but statistics about the exact quantity is not available.

Dumas (66), 2. Jaak Vilo (39), **3. Helger Lipmaa (29)**, 4. Raul Vicente (28), 5. Dietmar Pfahl (27), 6. Sherif Sakr (27), 7. Luciano García-Bañuelos (26), **8. Dominique Unruh (24)**, 9. Tarmo Uustalu (24), **10. Jan Willemson (23)**.

[37] http://nordsecmob.aalto.fi/en/

Cryptography is a deeply mathematical subject and reaching proficiency in it presumes a strong mathematical background. A serious problem pointed out by the universities is the decreasing level of math and science knowledge of secondary school graduates in Estonia. We have conducted no studies to find out the reasons, but we argue that a combination of different factors plays a role here.

Right after Estonia regained its independence from Soviet Union, the number of hours allocated for mathematics in schools started dropping considerably [52].

Even though the Estonian primary school students constantly score high in international comparison studies like PISA [82], they can choose between wide and narrow math curriculum when entering gymnasium. For a young person, the choice may be over-simplified – narrow curriculum means less work on a complicated subject without realising that it will cut off a number of choices at the later stages of education. In recent years, roughly half of the gymnasium graduates have taken the final math exam following the narrow curriculum.[38]

Also, many of the public schools are struggling increasingly trying to find competent teachers who would be willing to work for a rather moderate pay. According to some estimates, about 80 additional mathematics teachers would have been needed in fall 2018 across Estonia. Unfortunately, the Ministry of Education and Research refuses to acknowledge seriousness of the problem.[39]

The immediate result of the weakness of the education system is that the whole R&D system continues to underperform. Inspired by the EU Lisbon strategy, Estonia continues to seek to increase its gross R&D investment to 3% of GDP, whereas business R&D investment is expected to reach 2% of GDP [25, 64]. Yet, the high-tech sector continues to be unable increase its R&D workforce that is the prerequisite for increase of business R&D investment. Gross investment into R&D reached 1.3% of GDP, whereas business R&D investment contributed 0.6% of GDP in Estonia in 2017 [33]. Estonia is not alone with these challenges. Other EU cohesion regions face similar problems, and this has become a serious problem for the whole EU that fails to modernise and upgrade its industry fast enough (Figure 4).

What is more, business sector R&D investment are increasingly concentrated in the world, as large multinational companies compete for establishment of dominant technology platforms and ecosystems. Amazon, Alphabet, Intel, Microsoft and Apple invested 69 billion euros into R&D in 2017 [59]. This is roughly double of that of the whole European Union investment into ICT sector R&D in 2015. Table 4 displays R&D investments in selected countries based on the purchasing power standard (PPS).

For Estonia, the obvious response to the above constraints of smallness would be to punch above its weight, and to invest significantly more into education, R&D, and acquisition of foreign made technologies than one would expect. This is largely what we see in successful small countries, such as Sweden, Finland or Israel that have succeeded in building up a sizeable high-tech industry.

What is more, it follows from the above that small countries have limited chances for suc-

[38] https://eis.ekk.edu.ee/eis/eksamistatistika

[39] https://www.err.ee/858176/suur-hulk-koole-alustab-uut-oppeaastat-opetajate-puudusega

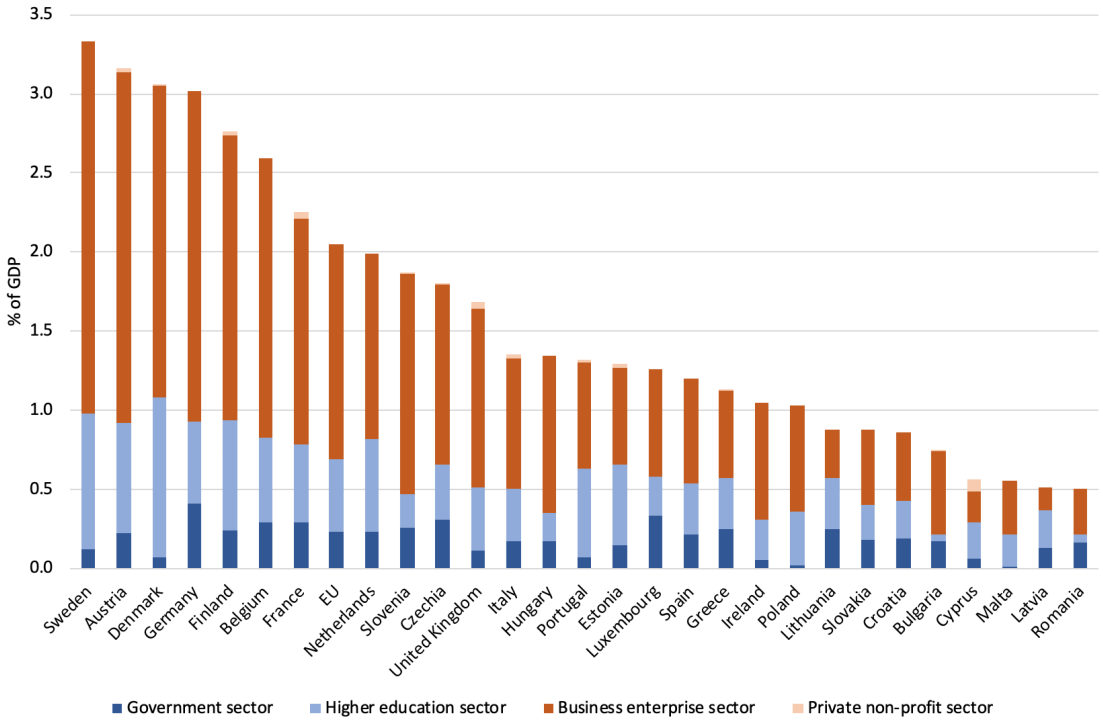

Figure 4. Gross domestic expenditure on R&D in 2017

Table 4. ICT sector R&D investments in selected countries in 2015

Country	Billions of euros PPS	Euros PPS per capita
United States	84	261.7
China	39	28.4
European Union	30	59.0
Germany	6.5	80.0
France	6.2	93.4
United Kingdom	3.3	50.9
Sweden	1.8	185.6
Finland	1.3	236.4
Estonia	0.1	76.9

ceeding in basic R&D that would lead to establishment of basic platform technologies. Instead, they should aim at capability building for early adoption of new disruptive technologies. This is for example what Singapore has been doing in order to establish radically new high-tech industries.

4 The needs and opportunities of Estonia for development and attestation of cryptographic solutions

4.1 General background of development needs

Why does Estonia (or any other country) need cryptographic development and competence building in the first place? There are a few interconnected reasons for that.

First and foremost, cryptography is the key component in modern information and communication security solutions. Of course, many of these solutions have been already developed and integrated into everyday products like operating systems, web browsers, etc.

On the other hand, our digital environment is changing rapidly, with new vulnerabilities and attack vectors being discovered on a daily basis. More often than, out-of-the box products fail to meet these new challenges and additional measures are needed. A good example is here given by the need for post-quantum cryptography. From the time of this writing (late 2018), at least 5 years will be needed to develop post-quantum cryptography standards, After that, it will take a few more years when major application developers will implement them in products, and another unknown amount of time until the legacy systems will get a post-quantum upgrade.

At the same time, already today we need to think about protecting information with confidentiality requirements spanning across decades, i.e. with high probability after the point when quantum computer will become a reality. In this situation, the main solution is to start working on upgrading our systems with our local efforts as much as we can. Given the extent and important role cryptography plays in deep layers of digital communication, developers with advanced skill-sets are required for that.

Another major reason to invest into local cryptographic capacity is the one of national security. Cryptographic solutions utilised in public and defence domains are (to the best of the authors' knowledge) quite similar in principle. However, the corresponding risk assessments differ substantially. Leakage of or tampering with a company's data may in the worst case lead to economic losses for this company. In case of the whole country/nation, the risks have potentially much deeper impact. Thus, the decision which data protection measures to use must also be considered much more carefully.

Ultimately, this decision will be reduced to the question of whom to trust. In the foreseeable future, Estonia will not be developing general-purpose CPU-s or operating systems. However, everything above that level can in principle be controlled locally. This control can mean either directly developing or at least auditing software applications implementing the

cryptographic information protection layer. The more we are able to perform these tasks in Estonia, the more control we can have over our own mission critical communication. This, in turn, presumes locally available know-how and development capacity.

Last but not the least, timely investment into emerging disruptive technologies and related capabilities will allow Estonian companies to develop superior new products and services that have a potential to secure a substantial market share.

4.2 Specific prospective development areas

At the first stage of preparing this report, the authors identified 10 trending areas of information technology and security, having potential to give rise to interesting crypto-rich applications within the next 5-10 years (see Chapter 2). During the interviews conducted at the next stage, we asked our interviewees to reflect on two aspects of these trends (see Appendix A):

- What is your organisation's current competence level in this field?
- What is the level of competence required within the next few years in this field?

Figure 5 displays the averaged replies gathered on 1-2-3 point scale.

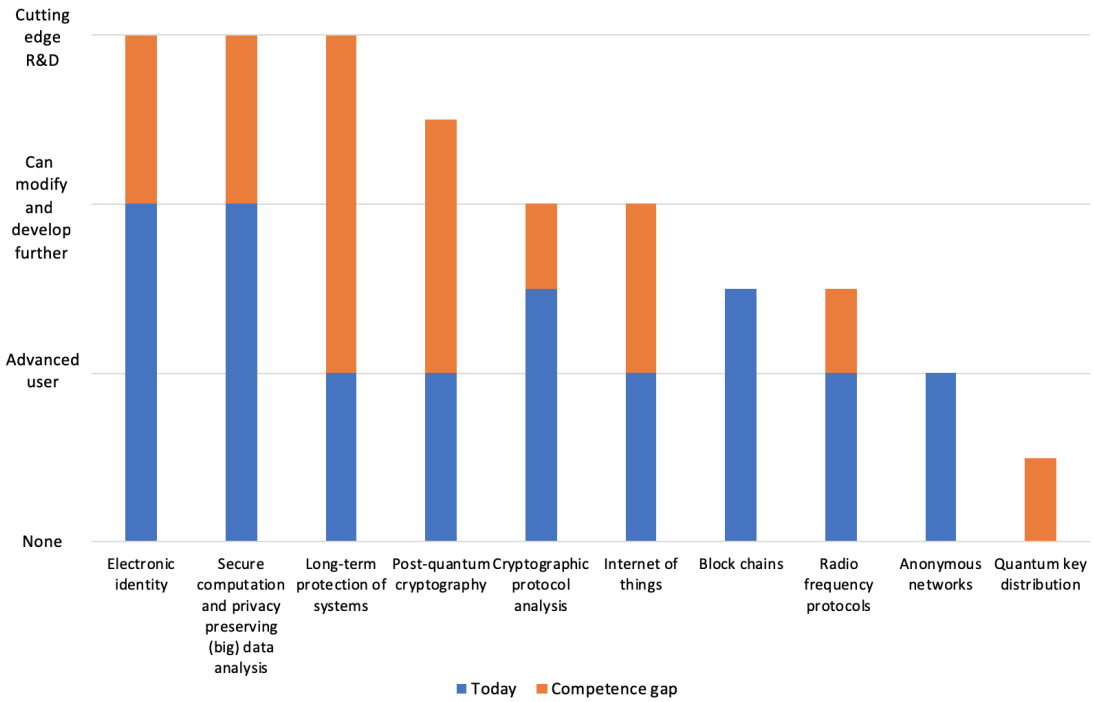

Figure 5. Estonian current technological competences and competence gaps

We can see that three areas of future development clearly stand out as having the most need for, which we can on turn interpret as having the largest (economic) potential:

- Electronic identity,
- Secure computation and privacy preserving (big) data analysis, and

- Long-term protection of systems.

All of the three have a strong bias towards applications, with two first already having Estonian own products (Smart-ID/SplitKey and Sharemind, respectively) on the market.

There is still need for other products in these fields as well. For example, due to historic-societal reasons, many countries can not introduce a strong single digital identity. They have to rely on federating partial identities coming from various sources (like citizen/customer databases of local municipalities, banks, utility service providers, etc.). Such federations often lack automation and clear understanding of security properties.

On the other hand, the need to compose identities of a number of smaller partial identities also introduces the problem of data processing in a way that would still respect the privacy concerns these societies have in respect to moving towards a single strong identity as a result of federation. Such problems have been proven to be solvable using secure computation techniques. Thus, a framework having both identity federation and secure data processing components has its marked potential.

Another challenge not well solved by currently available products is cross-organisational and cross-border aggregated data analysis. Not all of the problems here are technical, but presume also a compatible legal framework. Looking at the recent developments within EU (acceptance of GDPR, moving towards digital single market, etc.) we can envision that such legislative obstacles will decrease in time, increasing the market potential of cross-jurisdiction data analysis solutions as well.

The third area of long-term protection is still very much in the stage of theoretical development. However, the first products can be expected to hit the market in upcoming years as the need for them is clear. Thus, this field looks the most promising one in terms of potential for the first-to-market advantage.

The three top fields are followed by

- Post-quantum cryptography, and
- Cryptographic protocol analysis.

These two are clearly competence-building items. Post-quantum cryptography is not very interesting on its own, but in the upcoming years it will play a crucial role in many communication security products. Similarly, it will not be possible to sell cryptographic protocols as standalone products, but the ability to rigorously assess their properties will be a key component in developing new information security applications.

4.3 Communication security

During the interviews, several representatives of defence structures expressed interest towards various communication security applications.

On one hand, communication security applications are so well established on the market that it is hard to find an innovative niche with a lot of international growth potential here. On the other hand, the interest of defence structures in locally built products is understandable from the viewpoint of increased control. Thus we list the ideas picked up from the interviews here.

- eID-authenticated message exchange platform in the spirit of Signal.
- Air-gapped file/message encryption and transmission solution, preferably with long-term confidentiality, e.g. against quantum computers.
- Transparent/free key establishment for an existing voice communication system.

4.4 Attestation

Attestation is a generic term referring to some sort of an approval process. Many different processes are used in practice, and they differ widely both in the effort required and in the level of assurance obtained as the result. In this chapter, we are going to discuss the main processes that are used to review and approve cryptographic mechanisms.

Deployment of cryptography can be viewed on (at least) three levels.

1. **Cryptographic primitives and schemes** such as block ciphers (e.g. AES), key exchange (e.g. Diffie-Hellman), digital signatures (e.g. RSA, ECDSA), encryption schemes (e.g. RSA, ECIES), hash functions (e.g. SHA-3), etc.
2. **Cryptographic protocols** such as Kerberos and TLS. We must also distinguish the specifications and implementations of the protocols as many practical vulnerabilities emerge from implementation flaws.
3. **Cryptographic applications** both in software (e.g. web browsers) and hardware (e.g. cryptographic tokens and hardware security modules (HSM)).

As these levels are very different in their nature, the respective approaches to attestation and the strength of the resulting claims differ significantly as well.

Cryptographic primitives and schemes

The simplest and perhaps best-understood level is the one of cryptographic primitives. For many of them, security properties can be mathematically defined and proved. There is a large research community specialising at such cryptanalytic activities which form an important part of what we could call a community-based attestation effort.

For example the main reason why RSA and Diffie-Hellman key exchange are considered generally secure as of today is that a lot of researchers have tried to attack them and only succeeded in special cases.

The power and importance of community efforts has also been acknowledged by standardisation bodies. A public proposal call and subsequent analysis period has been applied e.g. by NIST when selecting the Advanced Encryption Standard (AES) and hash function standard SHA-3. Also, the current selection process of post-quantum cryptography standards is following the same pattern.

On the other hand, when selecting the current standards for elliptic curve cryptography (ECC), NIST adopted a much more closed approach. As a result, the NIST ECC standards have been criticised for unclear design choices that could in principle lead to back doors. We refer to the report [9] for a further discussion on this issue.

It should also be noted that in order to successfully coordinate the development of new cryptographic primitives, the coordinating organisation has to be really well established

and resourceful. There exist examples of primitives that have been proposed and successfully standardised by countries and bodies around the world, but have not enjoyed the same level of utilisation as the NIST ones (e.g. German Brainpool family of ECC algorithms and Japanese block cipher Camellia). Of course, several countries like China, Russia, Ukraine and South Korea have developed and standardised their own primitives, but these standards are only enforced and usable within the country, providing very limited interoperability across the borders.

We can see that Estonia is a country way too small to develop and maintain an independent cryptographic standard. Consequently our best option is to rely on primitives assessed, accepted and standardised by the international community and foreign organisations. We do have a little bit of choice when deciding which standard to follow. For example, instead of NIST ECC standard's somewhat questionable design choices, German Brainpool is a conceivable alternative.

Cryptographic protocols

Compared to low-level cryptographic primitives and schemes, the term "protocols" refers to higher level and more complicated constructions. They typically aim at implementing a complete security-related use case (e.g. authenticate a user for an e-service and establish a secure communication channel with him/her). To achieve such a goal, protocols make use of several primitives and basic schemes, combining them and adding non-cryptographic extensions to improve usability, performance, etc.

This is where things are becoming fragile. All the protocol components make some operational assumptions and provide some properties, but it is not necessarily the case that the properties of one component match the needs of another one exactly. Also, the whole protocol implementation must operate in some real environment and hence make assumptions about it. If these assumptions do not hold, a vulnerability may emerge.

Cryptographic protocols are typically developed by interest groups (e.g. large companies) needing them in their own products or services. It is a good practice to release protocol specifications to improve interoperability and collect public feedback. Similar to the way community efforts are used to assess the security of cryptographic primitives, protocol validation also largely relies on international researchers.

However, contrary to the lower-level primitives, protocols often have no mathematically rigorous security definitions. Hence, assessing their security is much more a heuristic process, involving a lot of trial and error. It is quite typical for cryptographic protocols to evolve through many versions which were considered as secure once, but turned out to have vulnerabilities later.

The prime example is the Transport Layer Security (TLS) protocol suite. Its predecessor Secure Sockets Layer (SSL) was originally developed by Netscape, and its version 1.0 was so flawed that it was never even published. Versions 2.0 and 3.0 were released in 1995 and 1996, respectively. Over the years a number of vulnerabilities were found in both of them, which lead to their explicit prohibiting in 2011 and 2015, respectively. TLS 1.0 was defined in January 1999, but as of 2018, it is recommended to be dropped in favour of TLS 1.1 or higher. The latest stable version of the standard is TLS 1.2, with TLS 1.3 being in

the status of a proposed standard (although considered to be rather stable already).[40]

The body responsible for standardising TLS (and many other network security protocols) is Internet Engineering Task Force (IETF) within their Request For Comments (RFC) publication series.

On top of the vulnerabilities in the protocol itself, the implementation may add extra weaknesses as demonstrated e.g. by the history of OpenSSL, one of the main SSL/TLS implementations. Thus, we may to assess the security of the implementation separately.

However, this may be too huge of a task. For example, OpenSSL source consists of 496,818 lines of code.[41] As a result, full OpenSSL certification has never been attempted, but its carefully selected subset has been certified according to FIPS 140-2.[42]

While it was easy in Section 4.4 to recommend against developing one's own cryptographic primitives, the situation is not so clear-cut for protocols. The spectrum of everyday business cases is very wide and standardised security solutions exist only for a limited number of them. Sometimes one has to invent own protocols.

A nice example is given by Estonian Internet voting. Since early 2000s, Estonia has been unique in its eID infrastructure, and when political will materialised into a development project, there was no readily available cryptographic protocol to make use of. It had to be developed from scratch, starting as a simple web component implementing a digital equivalent of a double envelope postal voting [57], and evolving into both individually and centrally verifiable protocol suite featuring mix-net for voter privacy protection [43, 41]. To ensure correct operations of the protocol, provable decryption and vote commitments are used. As an attempt to make use of community-based assessment, all of the server side source code has been publicly released[43].

We must say that the number of public code reviews has not been as large as originally hoped for. There are several reasons for that. First, code unavailability was used by Internet voting opponents as an argument to prove its unreliability, but after the code was released in 2013, they had no real motivation to contribute to the review. Secondly, the implementation is rather involved and it would require a huge effort to go through the whole code base.

We can see a recurring pattern here. On one hand, sometimes developing a new cryptographic protocol is unavoidable, but making formal claims about it is not always so easy. Cryptographic community has acknowledged the problem and is developing tools to assist protocol analysis (see Sec. 2.7 for more details). However, all of them have their limitations, and are still more like academic prototypes rather than off-the-shelf tools ready for general use.

One recommendation we can give is to avoid creating new home-brewed cryptographic protocols whenever possible as risks of unintended vulnerabilities is high. For standard tasks there probably exist solutions that at least someone has tried to assess from the security viewpoint. It is a general belief in the cryptographic community that the larger the number of reviewers, the higher are the chances that significant vulnerabilities have been spotted. Formal verification methods may be of help as well.

[40] https://en.wikipedia.org/wiki/Transport_Layer_Security

[41] https://www.openhub.net/p/openssl, checked on August 29th, 2018.

[42] https://www.openssl.org/docs/fips.html

[43] https://github.com/vvk-ehk/ivxv

One of the problems we have encountered in practice is that software developers sometimes do not even realise that they are implementing a cryptographic protocol, nor does it occur to them that a cryptographer should look at it before it is deployed. Using freely available libraries and calling primitives like encryption or signing is so easy that the surrounding context (e.g. where do the keys come from and how are they managed?) remains outside of the developer's attention frame. This in turn may lead to making assumptions that later prove wrong, resulting in vulnerabilities. The only way around this problem is educating software developers in cryptography and security issues in general.

Cryptographic applications

By an application we mean here complete hardware or software solution to a specific (information security) problem, performing a certain high-level task. Examples of such applications include cryptographic chip cards, firewalls, authentication servers, etc.

Such high-level applications must operate in a real environment, provide interfaces both for developers and end users, and achieve several (perhaps even contradictory) security goals. Consequently, their architecture is typically rather complex, consisting of various hard- and/or software components. Thus, ensuring correct operation of these applications is a very important, but on the other hand also a very challenging task. This is where certification procedures come into play.

To the best of our knowledge, there exists no cryptographic end user product about which some recognised certification body would have issued a statement that it is secure under any circumstances. Most of all, such a statement would have no meaning, since the term "security" needs to be properly defined first. After giving a security definition, it will become possible to assess the system from the standpoint of this definition.

A caveat with this approach is that giving a formal definition that would adequately reflect the real-world desired security target is far from being trivial. A typical problem is that the definition should be relatively compact in order to allow reasonable analysis, but the threats coming from the real environment may vary a lot, remaining partly (maybe even mostly) outside of the scope of the analysis. If this is the case (and we argue that it mostly is), one has to read very carefully what the security certificate actually covers and what is left outside.

Common Criteria

As a specific example of a certification scheme, let us look at Common Criteria (CC).[44] Some of the central notions of the CC framework are the following.

- **Target of Evaluation (ToE)** is the product or system to be evaluated.
- **Protection Profile (PP)** is a document identifying security requirements for a class of devices or solutions (say, smart cards). The manufacturer seeking CC certification may use some of existing PPs or write a new one. In any case, this is the document that defines what is exactly meant by security of the particular evaluation subject.
- **Security Target (ST)** is the document that identifies the security properties of ToE. ST may refer to **Security Functional Requirements (SFRs)**, a list of individual functions that the product may provide.

[44] https://www.commoncriteriaportal.org/

It is important to note that the ToE is evaluated against SFRs stated in ST, no more, no less. On one hand, this forces the manufacturers to explicitly list all the product's security features, but it says very little about the correspondence of these features to the end user needs. Ultimately, it will be the responsibility of the end user to make sure that the PP and ST (which are usually public) match his/her real life security goals.

In case of Common Criteria, seven different levels of evaluation assurance (EAL) are distinguished:

- EAL1: Functionally Tested
- EAL2: Structurally Tested
- EAL3: Methodologically Tested and Checked
- EAL4: Methodologically Designed, Tested and Reviewed
- EAL5: Semiformally Designed and Tested
- EAL6: Semiformally Verified Design and Tested
- EAL7: Formally Verified Design and Tested

Certification procedures and costs depend on the EAL level. In 2012 Young estimated[45] that

- EAL2 costs $100.000 to $170.000 and takes four to six months to certify;
- EAL4 costs $300.000 to $750.000 and takes one to two years to certify.

These estimates have likely been increased by 2019.

Case study: Smart-ID Common Criteria certification

Smart-ID electronic identity solution was awarded eIDAS Qualified Signature Creation Device status in November 2018. Prior to that, it had to be certified to Common Criteria. A client component was certified to EAL2 and a server component to EAL4.

According to the rough estimate given by the representative of SK ID Solutions, costs of certification could be approximated to be in the range of 0.5...2 million euros. There are some caveats, though.

- The development of Smart-ID was not originally planned having certification in mind. This incurred some extra cost due to the need to change some of the design principles, rewrite documentation from scratch, etc.
- Retaining the certification will also introduce some future costs.

What would be required to set up a Common Criteria certification centre in Estonia?

The organisation of CC certification is described in the *Arrangement on the Recognition of Common Criteria Certificates* [46] (CCRA). The hierarchy of CC includes parties like Certificate Authorising Participant (representing the country), Certification Body (CB, a special

[45] http://www.cs.utexas.edu/~byoung/cs361/lecture80.pdf
[46] https://www.commoncriteriaportal.org/ccra/

organisation responsible for overseeing the day-to-day operation of an evaluation and certification/validation scheme), and IT Security Evaluation Facility (ITSEF, the laboratory that actually makes the evaluation). Here the CB and the Participant may be one and the same organisation, but the CB is independent of the ITSEFs. The systematic organisation of the functions of evaluation and certification/validation under the authority of CB is referred to as the Scheme.

Here is a summary of requirements for CB.

- The services of CB are to be available without undue financial or other conditions.
- The procedures under which the CB operates are to be administered in a non-discriminatory manner.
- The CB is to be impartial. It should have permanent staff responsible to a senior executive enabling day-to-day operations to be carried out free from undue influence or control by anyone having a commercial or financial interest in certification/validation.
- The personnel of the CB are to be "competent for the functions they undertake".
- CB should ensure confidentiality of the information obtained in the course of its certification/validation activities.
- There is a long list of paperwork that CB needs to do, documenting everything.

Once per five years, a special delegation makes a site visit and evaluates how the Scheme works. The evaluation team should be provided a private room with the ability to have copies and printouts made for use during the site visit. They monitor the evaluation and certification/validation of a particular IT product at least on EAL4 level, so it seems that applying for doing only small certification levels is not an option. The CCRA does not specify any differences between requirements for performing certification on different levels.

It seems that RIA could potentially become a CB, as they need to do more organisational or supervision work, and the actual technical competence is required from ITSEFs. An ITSEF has to demonstrate to the satisfaction of the CB that it is "technically competent in the specific field of IT security evaluation" and that it is in a position to comply in full with the rules of the Scheme concerned. CB should ensure that ITSEF is in turn competent, impartial, and keeps data confidential.

The technical competence requirements are not specified, and there are no precise numbers of required degrees or the number of workers. A small hint is a reference to ISO/IEC 17025 standard, related to calibration and testing laboratories. Risk-based thinking is mentioned as an important thing.

The *Common Criteria for Information Technology Security Evaluation* [47] describes the main concepts of the evaluation. It seems that most of the work on security proofs should be done by the developer who composes the *security target* whose correctness the evaluators need to verify, and the list of tests that need to be performed is more or less already specified there, so the evaluators mostly do mechanical work. It is likely that in the case when a protocol is verified using formal methods like ProVerif tool, the protocol model is constructed by the developer, and the evaluator verifies its correctness. It is not clear, however, what is easier, and e.g. the proofs of EasyCrypt are an overkill for the one who

[47] https://www.commoncriteriaportal.org/cc/

reads them. It is also not clear whether a freeware tool is enough for CC, since one should have trust in correctness of such tools, unless generated proofs can be reviewed manually.

SOG-IS

The SOG-IS[48] ("Senior Officials Group Information Systems Security") agreement was produced in response to the EU Council Decision of March 31st 1992 (92/242/EEC) in the field of security of information systems, and the subsequent Council recommendation of April 7th (1995/144/EC) on common information technology security evaluation criteria. Participants in this agreement are government organisations or government agencies from countries of the European Union or EFTA (European Free Trade Association), representing their respective countries. Originally developed independently, the agreement was updated in 1999 to incorporate the use of Common Criteria in the certification process.

The agreement provides for member nations to participate in two fundamental ways:

- as certificate consuming participants, and
- as certificate producers.

Currently, France, Germany, Italy, Netherlands, Norway, Spain, Sweden and United Kingdom possess certificate production capacity. Out of them, only the bodies in France, Germany, Netherlands, Spain and United Kingdom can issue certificates on all the levels EAL1-7, the others can only go up to the level EAL4.

Austria, Croatia, Denmark, Estonia, Finland, Luxembourg and Poland participate in SOG-IS only as consumers.

The authors of this report were asked by the procurer whether it would be possible to establish a certificate producing body in Estonia, and how much it would cost. The latter question is very hard to answer, as the budgets of the respective agencies in other European countries were not available for the authors. However, looking at the list of other certificate consuming countries (most of which are larger than Estonia) we conclude that aiming at certificate production capability would probably not be economically feasible in the foreseeable future.

European Commission has issued a statement that ENISA is expected obtain a stronger mandate in certification in EU, but the exact details and extent of the mandate still remain unclear.[49]

[48] https://www.sogis.org/

[49] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-eu-cybersecurity-agency-and-eu-framework-cybersecurity-certification

5 Public procurement of innovation in the field of cryptographic solutions

5.1 Sophistication of domestic demand and public procurement of innovation

This section builds and extends on Lember *et al.* [51].

Sophistication of local demand is very important in the Porter's model of clustering that we rely on; it argues that international industrial success tends to follow in the fields where local demand is more advanced than the market demand elsewhere. Typically, such early demand emerges as the result of knowledgeable clients and dense market competition, which drive companies towards development of more advanced products. Often public sector plays an important role in defining the nature of market competition, especially in government dominated industries, such as security and defence [70].

In fact, the recent decade has witnessed a growing interest in using public procurement to spur innovation and development. An increasing number of governments are claiming that public procurement – often worth of 10-30 % of a country's GDP as exemplified by the EU member countries – should be used more extensively and explicitly to promote innovation, technology, and economic development.

Thus, public procurement of innovation refers to "purchasing activities carried out by public agencies that lead to innovation" [73] (see also [31, 85, 63]). Public procurement of innovation is about giving the market the possibility to come up with innovative solutions. Usually, this is about calling in tender documents for products and services that are functionally more advanced than any of the existing solutions [30].

Today, in most cases, innovation-oriented public procurement is carried out without any wider economic policy goals linked to it. It is the specific public sector needs or social challenges that usually drive government purchasing. Yet, if public procurement would lead to to new products or services that would be also taken up by other public agencies or private markets, this would contribute to economy-wide innovation and/or market upgrading. Therefore, economy-wide innovation and market upgrading can also be a deliberate aim of government purchasing and respective policies. Hence, public procurement is often considered as an instrument of demand-side innovation policy, which aims at overcoming "structural hindrances hampering the market introduction and the market diffusion on the demand side, as well as the transformation of needs into market signals" [29].

The demand-side innovation-policy goals are often addressed through public procurement aiming at new products and systems (or even emerging industries) that go beyond the state of the art – the public sector can either act as a testing-ground for innovative products or encourage innovation by providing a "lead market" for new technologies [74].

To sum it up, innovation-oriented public procurement has the potential to enhance providers' skills and innovativeness, to support innovation diffusion and support economic development.

However, in contrast to regular procurement in which governments place orders for ready-made or off-the-shelf products, procurement for innovation involves procuring products that might require additional R&D efforts and, consequently, carry additional risks. The European Commission Expert Group (2010) has identified five major types of risk in public procurement for innovation [7]:

1. Technological risks include all risks that result in non-completion, underperformance or faulty performance of the procured service or product for reasons attributable to technical operation. Technological risks may arise because suppliers were not able to achieve the solution agreed on, chose a wrong or sub-optimal technology (i.e. the product does not work as expected, does not suit the purpose intended, does not match the required standards, etc.), chose a technology prematurely, failed to take account of technological compatibilities, failed to develop the solution in-house or to buy components and knowledge as claimed in the tender process.
2. Market risks occur when private demand does not respond adequately or as expected, when public markets remain fragmented or when there is a lack of companies that deliver innovations. One of the reasons for this may be that the specification requirements are too stringent.
3. Organisational risks refer to risks that relate to the procurement's failure or underdelivery for reasons based within the procuring organisation. Indeed, there are usually too many goals a public administrator must achieve in modern public procurement cost savings, transparency, sectoral policies (e.g. environmental, energy, industrial, etc.) which often contradict each other. This may lead to a misallocation of resources, where agency goals conflict with wider policy aims. A dilemma exists between the micro cost effectiveness of a contract and the higher costs of R&D-based product/services which boost innovation [23]. Procurement for innovation demands a strong coordination between stakeholders, and continuous evaluation and learning. Also, societal risks refer to a lack of acceptance and uptake by the users of the new or modified service delivered within society.
4. The financial risks in public procurement are twofold: one is associated with the uncertainty of meeting target costs, and the other with the ability to secure the funds needed to begin with.
5. Finally, turbulence risks are primarily linked to large-scale projects. Risks emerge from a range of unforeseen events which may cause various actors involved in the process to reassess their priorities and change their expectations, which, in turn, may lead to further dysfunctional responses by other actors involved in the process, and so on and so forth. Such risks may occur within organisations, but are often a result of the interplay between various actions and actors involved in the entire process.

5.2 Public procurement of innovation in the field of cryptographic solutions in Estonia

In the light of the above and on the basis of the interviews and workshops carried out, the following key conclusions can be made regarding the Estonian context and the possibilities

for public procurement of innovation in the field of cryptographic solutions.

So far, Estonia has made very limited use of public procurement of innovation as a policy instrument. The overall approach to public procurement in Estonia is that procurement activities should be geared towards efficiency in public money spending as a first priority, the understanding also reflected in the World Trade Organisation's (WTO) agreement on public procurement [50].

Still, public procurement for innovation has been used for the development of information systems in the public sector and for various public e-services. Not only direct procurement was carried out, but some of the purchased products or services are used widely by other end users for the introduction of other related innovative products and services, helping drive the clustering among innovation-system actors even further (in the case of Public Key Infrastructure, for example) [47].

Based on the interviews carried out the following act as barriers for more extensive use of the public procurement of innovation in the field of cryptographic solutions in Estonia.

1. Price-dominated procurement practices, where no incentives are left for innovative or complex solutions;
2. Wide use of open procedures that squeezes out innovation and limited use of innovation-friendly procedures (e.g., competitive dialogue);
3. Using the logic of annual state budgets (as opposed to multiyear-based budgeting for procurements), which leads to unrealistic deadlines, a mismatch between available funds and the quality of solicited solutions, and a short-term view instead of long-term partnerships;
4. Weak technology competencies and market knowledge within the public sector, coupled with limited willingness to invest in preparatory stages (e.g., creating technical specifications in ICT or allowing substantial market consultations before formal bidding in almost every field).

While the first three points refer to common deficiencies in the Estonian public procurement of innovation, the technological risks are particularly acute considering the rapidly developing nature of cryptography related technologies. And, respectively, increasing considerably the technological competencies of the procurers is the key, to manage those associated technological risks and act as "smart procurers".

Actually, defence is one of the few sectors where the government of Estonia has launched a dedicated public procurement of innovation program with a strong emphasis on innovative and R&D-intensive solutions. The first time the Estonian Ministry of Defence contracted for R&D was in 2001. The projects supported have targeted basic and applied research, R&D up to the prototype stage, as well as ready-to-use equipment. This included technologies like unmanned aerial and ground vehicles, portable analyser of chemical warfare agents, and an improvised explosive device neutraliser [46].

It has been argued that these R&D projects have "made little or no impact on the capabilities or the performance of the defence organisation" [46]. However, other research suggests that several positive spill-overs had emerged, in terms of new technology capabilities and commercially viable prototypes for the universities and private companies involved. Still, reliance on supply-push rather than carefully specified user needs (i.e., military), weak

user-provider linkages (defence forces involved only formally), low level of coordination and technology capacity in government, involvement of a limited number of suppliers (mostly universities with no commercialisation initiatives), and nonexistent attention to market creation or business opportunities are all reasons why the effects have remained limited [50].

So, there is some experience in using public procurement for innovation in the field of defence and this could be potentially extended to the procurement of cryptographic solutions. According to the Estonian Public Procurement Act the contracting authorities in the areas of civil defence, civil protection and danger prevention services could be even excluded from public procurement process (§11; §170). Still, whatever the procedure, the approach assumes strong capacities from the side of the procuring organisation to formulate and consolidate public sector demand and match that with what the market can realistically provide, and that solutions procured and/or competencies obtained will be afterwards developed further and result with the increase in high-value-added exports.

Another issue brought up in several interviews with company representatives is related to commercial licensing of solutions created in Estonia. Perhaps one of the best examples is X-Road that was (and to a certain extent, still is) a leading solution in federated database management. Estonian government has issued several commercially non-sustainable statements concerning intellectual property of X-Road. Open-sourcing and giving it for free to other countries (such as Finland) are of course fine, but the state has proven to be not very good at providing support to it. A sustainable operation model for customers, on the other hand, assumes continuous support and development. We argue that fostering commercial exploitation of state-owned IP is in the long run a better solution compared to offering “free” products which will soon be lagging behind.

6 Analysis of market niches

6.1 Future outlooks of the cryptographic development in Estonia

A scenario workshop which brought together researchers, entrepreneurs and civil servants, was held for the discussion of future outlooks of the Estonian cryptographic development on November 7th, 2018. As the part of this workshop, main external drivers that establish the context for the medium to long-term developments in Estonia were mapped.

Further development of the Digital Single Market, and the increasing use of electronic authentication and electronic signatures came up as key enablers along with establishment of even closer security and defence co-operation between the Nordic countries and within the European Union more broadly. The emergence of a multipolar world, where Europe, the United States and China all play an important role was also brought up as a major megatrend.

Finally, it was emphasised that a major new technological breakthrough, such as quantum computer or discovery of a significant weakness in a critical cryptographic component is always a possibility that should not be ruled out. Estonia has to embrace the opportunities the European and global environment offers, while being also able to mitigate the high-impact risks, even if the likelihood of these is not necessarily very high.

In the following, we synthesise main elements of different scenarios, and outline a vision that addresses key market niches with a view to maximising the benefits from existing competences. Inspired from the ideas of the Boston Consulting Group classic growth-market share approach [44], we start from the existing technological and market strength. Thereafter, we consider new rapidly growing market segments, where Estonia has a technological potential, but low or no market presence. Finally, we outline a number of success factors which may become significant in medium to long term.

6.2 Existing areas of technological and market strength

The Estonian citizens have been eager to embrace the benefits of electronic identity. Widespread use of on-line authentication and electronic signatures has allowed Estonia to develop a myriad of public and private sector e-services that are not available elsewhere in the world. The adoption of EU eIDAS regulation has also enabled secure cross-border electronic transactions. Yet, securing interoperability of various national systems remains an open challenge in Europe and beyond. Therefore, exporting Estonian eID and electronic signature solutions is not a straightforward affair. Maintenance of electronic identities and related back-office systems is one of the Estonia's strongholds, and the related competences and experience should be put into full use internationally.

X-Road federated database management solution is another crypto-rich core area of Estonian e-government architecture, and a good candidate for further internationalisation and exports.

Block-chain backed data assurance, validation of services and data bridge management in public and private sectors have been hyped a lot in recent years. Estonian image as a block-chain nation has even reached government-backed rhetoric[50].

The reality is, however, a bit more modest. According to the Gartner 2019 CIO survey, "only 5% of CIOs rated blockchain as a game changer for their organisations, far below artificial intelligence, cloud, and data and analytics"[51]. Gartner also notes that block-chain is "often offered as a solution in search of a problem" and that companies should give a more thorough thought to whether this technology is what they really need[52]. We conclude that even though the block-chain technology itself has promising aspects, it does not make sense to rush onto the first hype train.

There are a number of further new avenues for R&D in the domain of cryptography, such as integration of biometric identity checks into on-line transactions in a secure and privacy preserving manner, securing the above core solutions for the post-quantum era, and reduction of the technological dependence from external components and service providers.

6.3 Rapidly growing new market segments, where Estonia has technological potential

Critical services and infrastructure protection (especially with a view to telecommunications networks, e-government services, finance and industrial control systems) is one of the areas, where there is a need for rapid progress. The international community has witnessed strengthening and emergence of new threat actors and highly targeted attacks in this domain. Therefore, development of new products that would allow to cater for the rapidly increasing market of threat intelligence is an important necessity and opportunity. This is an area, where Estonia can exploit its existing research strength in privacy preserving (big) data analysis and data assurance, while developing such capabilities further.

Security and dependability of microelectronics and systems is another growing market, as the number of connected devices continues to grow exponentially. Yet, the consequences of security flaws in mainstream computer hardware (when deployed in e.g. vehicles) can be fatal. Estonia has a significant research strength and broad international co-operation that includes industry giants like Intel. However, the related industries are typically capital-intensive and entry barriers tend to be high. It is therefore crucial to find a suitable market entry strategy.

The increasing use of electronically signed and encrypted documents will increase the need for long-term security solutions that allow to ensure integrity and/or confidentiality of data over decades. Long-term security is an area of on-going research, where Estonia itself has an obvious need for a solution that would bring the data protection to a new level, while there is a much larger global market that lacks an established off-the-shelf solution.

[50] https://medium.com/e-residency-blog/welcome-to-the-blockchain-nation-5d9b46c06fd4
[51] https://www.gartner.com/smarterwithgartner/the-reality-of-blockchain/
[52] https://blogs.gartner.com/smarterwithgartner/the-cios-guide-to-blockchain/

Another field where Estonia has pioneered a lot of development is the one of electronic identity. In addition to the hardware-based tokens of ID-card and mobile-ID there is also Smart-ID implemented fully in software on the client side. This allows for much greater flexibility in deployment giving a potential market edge.

However, not all the societies are so fond of the idea of a single digital identity. Entering such markets would require developing new identity management products, but our current experience could, on the other hand, prove quite useful while doing so.

Last, but not the least, Estonia has taken some first steps in the field of post-quantum cryptography that will prove in medium to long term absolutely crucial in securing the various communication systems and applications that rely on asymmetric encryption.

The case of hardware-token based eID solutions like ID-card and mobile-ID is somewhat specific, since adding new cryptographic algorithms to already manufactured chips is nearly impossible with the current state of technology. Consequently, if we want a quantum-safe ID-card, the respective algorithms should be implemented by the vendor on the hardware level. On the other hand, given the time and monetary investment needed for development and certification of the hardware tokens, the vendors have very limited motivation to start working on quantum-safe chips before the NIST standardisation effort has come to an end. There is very little that Estonia could do to speed up this process.

The software-only solutions are in a much better situation in this respect. They can be built in a much more modular fashion so that for example cryptographic primitives could be pulled and plugged on demand rather easily. Of course, just changing the cryptographic primitives in one infrastructure component is not sufficient as there are many other components (e.g. e-services) that need to interact with it; they also need to be upgraded and tested to maintain service continuity. To guarantee painless transition, intermediate hybrid schemes probably need to be developed supporting both the old and new algorithms at the same time.

It is fair to say that no country in the world has even tried that on a large scale, and if Estonia could manage it successfully, it would be something that would put us on the forefront of digital societies once again.

The primary choices for the technologies to try this out are X-Road/UXP and Smart-ID as both their full source code and the associated know-how are maintained in Estonia. On the other hand, X-Road as the data exchange hub and Smart-ID as one of the main eID solutions are basic technologies for many e-services that are offered in Estonia.

Benefits of post-quantum transition try-out are twofold. First, the applications upgraded to support post-quantum algorithms will have a definite edge on the international market. And second, the know-how obtained in the process will be truly unique, establishing a good foundation to develop new products and offer consulting.

6.4 Potential future areas of growth

There are also a number of emerging new markets that rely heavily on strong encryption. Some of these have been followed more closely, but some have been also largely overlooked by the Estonian researchers, businesses and government.

Financial technology (fintech) tech is one of the obvious rapidly growing and cryptography

rich business areas, where many start-ups seek to win a market share from large, heavily regulated and often slow-moving banks. Estonia has already a number of start-ups in this area, and more are likely to occur, even if the use of advanced cryptographic techniques may have been limited so far. Anonymous cryptocurrencies, including coin mining and cryptocurrency wallets, is one of the unregulated and highly risky domains, where speculative business activities have clearly outperformed R&D and competence building efforts in Estonia. Still, irrespective of the speculative boom, the question remains open, if, when and how Estonian crypto-rich businesses could enter fintech area more actively.

Manufacturing of equipment for radio and data communications infrastructure, including 4G and 5G networks, is an increasingly important area where Estonia has a manufacturing potential thanks to the proximity of Nordic countries. This industry is increasingly dominated by large multinational companies, but advancement of strategic partnership with major global actors, such as Ericsson and Nokia, could potentially open new avenues for the development and sales of secure data and radio communications systems.

Internet voting is a high-profile crypto-rich solution that has been developed and put successfully into use in Estonia. There are, however, on top of the slow adoption of eID, a number of legislative and political aspects that hinder the exports of the Estonian Internet voting solution. For one, many countries are still not convinced in security and privacy preservation aspects of Internet voting as a such. The reports on attempted manipulation with voter registries and the cyber security flaws that have been discovered in proprietary voting machines add to such fears. Therefore, we consider this as a highly risky market that should be held on the radar nonetheless.

6.5 Critical success factors

On the basis of semi-structured expert interviews (see Appendix A), scenario workshop and subsequent synthesis of the various inputs, the following key success factors for the development of cryptography in Estonian have been identified.

Cryptographic advice and requirement setting

Cryptographic competence is not much different from any other deep technical competence – you do not need it every day, but when you do, it has to be timely and accurate. The needs of an average public body or a company are typically not sufficient to employ a full-time highly specialised cryptography expert. Usually, this leads to delegation of competences or subcontracting. However, potentially critical competences can be only delegated to a body that can be trusted, and will be there when a need arises.

Currently, one of the endpoints of such delegation is the Information System Authority (RIA). Semi-officially, some of the cryptography related queries end up in Cybernetica or in universities. One can hardly call this a reliable system.

There is a definite need for a well-resourced crypto competence centre, which would have the official mandate to advise public entities on their use of cryptographic routines, and to establish formal requirements to development and maintenance of cryptographic systems.

Threat intelligence

The above advisory and oversight activities go closely hand in hand with threat intelligence and situational awareness.

Information security events are usually foreseeable, and do not occur overnight. For example the very same team that discovered the ROCA flaw [61], studied hardware generated RSA moduli already at least a year earlier [78]. If there would have been an adequate threat intelligence service, this activity would have been noticed, and ROCA would not have had such an impact.

ROCA was a somewhat unique event, but many more cyber security threats emerge on daily basis. The core question is not really whether a next critical flaw would be discovered in future, but rather that of the speed of threat discovery and of the mitigation of risks. Estonia has already on-going efforts in threat intelligence domain. CERT-EE receives many alerts every day. Distinguishing critical threats from less important ones is a huge task, not to speak of even more time consuming incident resolution efforts. Therefore, more resources are needed in this field in Estonia.

Export of crypto-rich products

Estonia has a relative strength in some of the crypto-rich products, such as electronic identity systems or X-Road solution for federated database management, that are in widespread use in Estonia. Estonia has been a highly useful lead market for such products. Yet, there are a number of road blocks that have not allowed to turn this into success at major export markets.

The quality of Estonian products is good, but Estonian companies have usually a weaker hand in marketing their products internationally. Estonian interests should be represented more convincingly, when it comes to international standardisation or definition of the requirements of the relevant European regulations, etc.

Also, Estonia should make more conscious use of public procurement in supporting the development of innovative commercial products, and the related intellectual property regime needs to be improved.

Research and development

Estonia needs to invest significantly into R&D that will allow to sustain the existing strengths in cryptography and crypto-rich products, and will lead to the development of new technological strength. Also, greater participation in international collaborative R&D would allow to learn from the leading scholars elsewhere, and lay the grounds for the development of specialised components for larger technological systems that Estonia would not be able to develop with its own resources alone.

Education and attraction of foreign talent

The relaxed mathematics curricula that has been introduced to the school system over the last decades has become an obstacle for advancement of science, technology and engineering studies in universities. Therefore, it has become critical for Estonia to increase the quality and volume of science and mathematics education. This, in turn, will allow to

increase quality standards and graduation numbers of STEM disciplines (Science, Technology, Engineering, and Mathematics), including cryptography, in higher education system.

Attraction of foreign talent at all qualification levels from graduate students to professors is another area, where Estonia needs to do better. This includes both the provision of higher education and subsequent employment of the promising foreign talents in academia and industry.

7 Conclusions and recommendations

7.1 Strengthening of the emerging cryptography and cyber security cluster

The analysis of the cluster development in the field of cryptography in Estonia has led to the identification of several strengths as well as significant weaknesses that hinder the competitiveness of Estonian crypto-rich companies. Some of these constraints can be overcome by joint private sector initiative, some require public sector support.

Cryptography is clearly one of the strongholds of the ICT R&D in Estonia. Yet, limited availability of highly qualified labour is the main constraint on the development of the field. This is mostly caused by insufficient public sector funding in higher education and academic research in computer sciences and electronics. Weakening mathematics and science education on the primary and secondary school levels is further limiting the quality of higher education.

Demand conditions pose challenges as well. Estonian market alone is too small for the development of unique crypto-rich information security products. Hence, the Estonian companies should consider the whole European market as their home market. Still, one should bear in mind that the Estonian companies are more likely to succeed at the export markets in the areas where the domestic demand is more advanced than the demand elsewhere in the world. This is why advancing the public procurement of innovation is so important in government dominated markets, such as security, defence, electronic ID, etc.

What is more, Estonian cryptography and information security companies are tiny on the global scale. Advancement of cluster co-operation is, therefore, inevitable for promoting and supporting the interests of the Estonian enterprises and universities in the field of cryptography and cyber security. The action plan of such a cluster initiative should include:

- development of mid- to long-term roadmap for Estonian cryptography and cyber security industry;
- advancement of collaboration between enterprises and universities in curricula and course development;
- fostering participation in European collaborative research and development programmes, such as Horizon 2020 (Horizon Europe), European Defence Fund, etc.;
- market research, and international promotion of Estonian products and services;
- standardisation of new cryptographic solutions to support international acceptance.

These activities should also be supported on the governmental level.

Lead: Ministry of Defence, Ministry of Economic Affairs and Communications

Resources: Around 0.5 million euros of public co-funding would be required for launching and operating a cluster organisation during the first 3-4 years. The members of the cluster organisation would be asked to double the public subsidy by collecting membership fees, and other contributions that would allow to meet the costs of specific activities, such as joint international marketing or brokerage events.

7.2 Establishment of a national cryptographic competence centre

The current study has revealed that the majority of end users in public sector lack in-depth cryptographic competences, and this may potentially lead to cyber security weaknesses in systems various agencies procure, build and maintain. Some of such weaknesses may be built in due to inadequate use of cryptography, and some arise in the course of the time as the information systems age and previously secure cryptographic protocols cannot be considered secure any more.

Currently, various branches of government consider RIA, which hosts also CERT-EE, as the point of reference for advice on cyber security. The Estonian cyber security strategy [6] foresees strengthening of RIA as a competence centre, and establishment of a national cyber security centre (NCSC) in it. This is a very welcome development.

There are, however, on top of the role that is already foreseen to NCSC, also a number of functions which have to do with development and maintenance of cryptographic systems across the public entities in Estonia that need to be covered centrally. These functions include:

- advising on the development of cyber security architectures, including the use of cryptographic primitives, in Estonia by participating in the analysis phase of all major IT system procurements in Estonia;
- establishing requirements (and minimum standards) for the use of cryptographic primitives that will be used in the development of all critical ICT projects;
- carrying out threat intelligence tasks following the latest international research and vulnerability reports, providing recommendations to the various public and private actors in Estonia;
- establishing requirements for maintenance of cryptographic systems, especially with a view to risk assessment an phasing out of outdated cryptographic primitives;
- overseeing and auditing, in co-operation with the Data Protection Inspectorate, public entities with a view to implementation and maintenance of cryptographic systems and data protection;
- advising the government on the development of European regulations and standards, promoting the Estonian best practices where relevant;
- liaising with the European Union Agency for Cybersecurity (ENISA) with a view to the security and dependability of cryptographic protocols and products, including establishment of joint EU-level certification procedures.

To implement these functions, we recommend establishment of a national cryptographic competence centre. Whether this centre should be founded as a new organisation, as a part of NCSC, or based on some existing entity, is a question requiring separate analysis

and political decision. In any case, it should foster close collaboration between public sector, academia and private companies.

Lead: Ministry of Economic Affairs and Communications, RIA

Resources: This would be a permanent task, which would require about 4-5 highly experienced cryptography and cyber security engineers, with an annual budget in the range of 1 million euros.

7.3 Attestation of cryptographic solutions

The Common Criteria (CC) webpage[53] lists the recognised evaluation laboratories around the world. Some of them are parts of multinational companies, such as Thales or CGI, offering also other products and services besides CC certification. Some are smaller governmental institutions.

As a general pattern, CC certification centres are maintained in industrialised and rapidly industrialising nations that host sizeable software and/or electronics industry. This reflects largely the role of CC certification centres in assuring the quality of the products that have been developed by the respective domestic industries.

The organisational arrangements of certification centres vary internationally, but impartiality is an obvious requirement to any certification centre. An independent, privately maintained CC certification centre would need to be sizeable enough to be able to maintain its professional standards. Also, the revenue stream would need to be diversified enough to allow for financial and organisational independence. Establishment of a CC certification centre would presume, therefore, dozen(s) of products to be certified by a team of at least 25-30 experts. An annual budget starting from 10 million euros as an absolute minimum for operation of an independent certification centre.[54]

It is, in our view, too early to consider the establishment of a fully fledged CC certification centre in Estonia from the business case point of view. Estonian crypto-rich industry is still in early phases of its development, and as such it would benefit more from certification at main export markets rather than domestic assurance.

There is, still, from the public security and defence points of view, an obvious need for domestic evaluation and certification of some of the devices and systems from their security, trustworthiness and maintenance procedures points of view. This would call for a relatively small, dedicated task force that would liaise closely with all relevant agencies, including national cryptographic competence centre. Establishment of such a task force would also facilitate capability building for establishing a CC certification centre at a later stage.

Lead: Ministry of Defence

Resources: Certification and related activities would be a permanent task, which would require about 4-5 highly experienced cryptography and cyber security engineers, with an annual budget in the range of 1 million euros.

[53] https://www.commoncriteriaportal.org/labs/

[54] **Disclaimer:** The authors of this report do not have a reliable methodology to calculate the required resources, thus the numbers given above should be taken as only very rough estimate. We made several attempts to gather the data for CC certification centre budget, but this is a closely guarded information that is not available for independent researchers.

7.4 Capacity building in key emerging technologies

Estonia, or any other small actor would not be able to achieve a competitive edge simply by imitating the established off-the-shelf products that are readily available at the market. Instead, one should seek integrating the emerging disruptive technologies, which are typically developed elsewhere, into own radically new products that outperform the competition.

New disruptive technologies, which have a major impact on the whole cryptography and cyber security landscape, emerge as a rule outside Estonia and often even outside Europe. Smaller catching up economies are, therefore, in need of a driver for detection and dissemination of knowledge on emerging disruptive technologies. It is of paramount importance that the universities and research institutes would fulfil this role, supporting, thereby, also businesses and the various government agencies in early adoption of the latest knowledge and technologies. This is a crucial role for an academic research and higher education that builds on it.

Estonia currently has around two dozen highly trained cryptography experts, and a very limited number of cryptographic R&D intensive businesses. This is, to an extent, sufficient for covering the major established cryptographic techniques, but clearly insufficient for an international technological breakthrough. This is why Estonia has to increase the pool of highly trained cryptography experts, prioritising the investments into capacity building in emerging new technologies.

More specifically, the cryptographic capacity building effort should focus on the following five technology areas:

- post-quantum cryptography,
- electronic identity,
- long-term protection of systems,
- secure computation and privacy preserving (big) data analysis, and
- cryptographic protocol analysis.

Such capacity building would prove the most effective if arranged in the form of doctoral studies that involve individual research based training in close interaction between local universities and research institutes, and leading research labs in Europe and in the United States. The minimum capacity building target would be to train 2-3 additional PhDs in each of the 5 emerging technology areas within the next 5 years. It would be advisable to combine the above targeted doctoral studies programme with an initiative for attraction of promising post-docs, who have already graduated in leading research labs, and seek to establish their own independent research career. This would allow both to build up much needed international research networks, and to speed up capacity building efforts overall.

Eventually, such a capacity building effort should lead to new tenured professorships and research groups in Estonian universities. These research groups would be encouraged to engage actively in domestic industrial R&D co-operation and strategic R&D partnerships in Horizon Europe, so that a continued basis would be established for research and dissemination of knowledge both to students, but also to a broader community of cyber security experts in Estonia.

Lead: Ministry of Education and Research, Ministry of Defence (co-funding)

Resources: This capacity building action that would lead to the emergence of 12-15 new cryptographic PhD scholars. In financial terms, this effort would require a sustained annual investment of 2.5 million euros for the period of 5 years, i.e. altogether 12.5 million euros.

7.5 Industrial R&D and product development

Limited availability of human resources is one of the major weaknesses of the Estonian ICT and cryptographic business ecosystem. The obvious way for overcoming this is to significantly increase investments into industrial R&D and product development, and to devise scalable business models, where the increase in sales would not be tightly connected to increase of the required manpower.

This is an area where the industrial R&D and product development grants are in place for promoting industrial development throughout Europe. Likewise, Enterprise Estonia offers similar supports to Estonian businesses, and there is a myriad of seed and early stage investment funds that seek for new companies in need.

Still, one can identify a number of areas, where the government itself could take a more proactive approach, both to meet its own security and data protection needs, and to foster the development of new products. Innovation procurement is the obvious modality for addressing the markets, where the public sector itself has identified a need, but where there are no suitable ready-made products on the market. However, the procurer would need to have very clear vision on the product and an in-depth knowledge of the area in order to be able to define a completely new product.

Estonia has started to promote the use of innovation procurement relatively recently. We recommend to step up these efforts, and establish, learning from business sector, a chief product officer (CPO) role for cryptographic and cyber security products in the relevant branches of administration. CPO would be responsible for conception and management of a product, including the progress beyond established products, organisation and follow-up of procurement, establishment of an intellectual property regime that would allow the supplier to develop and market the product independently further, support and maintenance requirements, modalities for agreement on additional functionalities in the context of next releases, etc.

Some of the potential product ideas that could be developed further include:

- experimental transition to post-quantum cryptography in selected applications (eID, communication security, X-Road/UXP, etc.);
- federated identity and data management framework;
- cross-jurisdictional data aggregation solution;
- long-term security framework (with applications in e.g. archival of electronic documents with long-term security requirements);
- specific communication security products.

Strengthening of strategic partnerships between Estonian and foreign business entities is another potential goal that should be considered when planning for innovation procurement. For example, championing of joint project ideas for participation in Horizon 2020 or in European Defence Fund projects could prove useful both in terms of the access to

complementary technological and industrial capabilities, and subsequent joint sales and marketing actions.

Lead: Ministry of Defence

Resources: For specific product ideas, the communication security applications are less innovative, but can at the same time be built from readily available components, keeping the approximate price range between 0.5-1M EUR depending on the exact requirements. Other ideas (quantum-safe eID, federated identity management, cross-jurisdictional data aggregation, long-term security framework) do not have direct analogues on the international market. On one hand, this gives them potential for a market advantage, but at the same time the very same aspect makes it very difficult to assess the associated costs. Our best guess is that for an investment of about 3M EUR it should be possible to build a marketable prototype, but more accurate estimates assume initiating a more detailed analysis phase. All in all, the rough annual budget need for innovation procurement is around 5M EUR annually.

Also, establishment of the new CPO role(s) requires investments in the same order of magnitude as for any other high-profile public official position.

7.6 Boosting math and science education on the primary and secondary school level

Estonian students may perform well in PISA tests, but the situation observed at the universities is sad: the math and science level of secondary school graduates is not sufficient to get them to a productive level for crypto development during 3+2 years of higher education. There are several steps that can and should be taken to improve the situation.

- Math and science education should be acknowledged on the governmental level as a critical priority from the national digital security point of view.
- Additional resources are required for preparation and hiring high-level teachers.
- As a supporting activity, extracurricular math and science education must be systematically supported (right now it relies too much on personal initiatives in the Youth Academy of University of Tartu).

Lead: Ministry of Education and Research

Resources: Assuming that each year, about 40 new teachers are required, annual extra investment needed is 0.5M EUR for teacher training in the universities. Another 1M EUR is required annually for raising math and science teachers' salaries. Besides that, a political decision is required to restore the amount of math classes per week in the official curriculum to a sustainable level, and discontinuing the narrow math curriculum in the gymnasium level in favour of wide curriculum only.

A Questionnaires

In order to gather input from the field experts, three questionnaires were put together. The questionnaires had a large intersection, but also some notable differences due to the rough division by the field of activity. More precisely, the three types of questionnaires were targeted towards

1. producers, i.e. companies that deliver crypto-rich information security products;
2. procurers, being interested in running information systems, digital services, etc., requiring cryptography as a measure to achieve security guarantees;
3. universities that prepare new workforce by giving crypto courses, and every once in a while generate some spin-off companies.

The interviews were mostly conducted in Estonian, hence the questionnaires were too. We will present them here in their original form, not translating them into English.

A.1 Producer questionnaire

Küsimused ettevõtte profiili kohta

1. Palun kirjeldage lühidalt ettevõtte äritegevust ja fookust.
2. Palun kirjeldage ettevõtte teadusmahukamaid tooteid ja teenuseid ning T&A tegevust üldisemalt.
3. Kas te toodate krüptograafiarikkaid lahendusi? Palun kirjeldage mõnda iseloomulikumat.

Küsimused toodete ja turunõudluse kohta

1. Kas te tunnetate, et mõne krüptograafiarikka toote järele oleks turul nõudlust, aga mitte piisavalt pakkumist? Millise valdkonna tooted need oleksid?
2. Kas te näete tulevasi Euroopas ja kaugemal potentsiaalikaid tooteid või teenuseid, mille järele ei ole Eestis praegu (veel) nõudlust?

Küsimused ettevõtte krüptograafiga seonduva klasterdumise osas

1. Kes on ettevõtte põhilised kliendid ja koostööpartnerid Eestis, Euroopa Liidus ja mujal?
2. Kellele konkreetsemalt tarnite Eesti (avaliku sektori) organisatsioonidest? Kirjeldage suhteid klientidega, nende kompetentsi, hankeprotsesside jms osas ning probleeme.

3. Kes on teie krüptograafiarikaste toodetega seotud peamised tarnijad?

Küsimused tehnoloogiatrendide kohta

1. Kui, siis millistes krüptograafia ja infoturbega seotud teemades vajaks teie asutuse kompetentsibaas tugevdamist?
2. Kui tugevaks te hindate oma asutuse kompetentsi järgmistes tehnoloogia valdkondades? (1. . . 5) Kui suur mõju on neil tehnoloogiatel olla Eesti tulevastele arengutele? (1. . . 5)
   - Postkvant-krüptograafia
   - Kvantvõtmevahetus
   - Identiteedihaldus
   - Turvaline arvutus ja privaatsust säilitav (suur)-andmete analüüs
   - Raadiosageduslikud protokollid
   - Vähese ressursinõudlusega krüptograafilised primitiivid (IoT)
   - Krüptograafiliste protokollide analüüs (Krüptograafiliste protokollide omaduste automaattõestamise meetodid)
   - Pikaajaline turve
   - Anonüümsed võrgud
   - Krüptorahad/plokiahelad

Küsimused takistuste kohta

1. Millised on olulisemad takistused krüptograafiarikaste toodete ja teenuste väljatöötamise ning ekspordi kasvatamise osas? (1. . . 5)
   1.1 teadurid ja inseneeride puudus
   1.2 turundus- ja müügitöötajate puudus
   1.3 keskastme- ja tippjuhtide puudus
   1.4 välismaise tööjõu kaasamise keerukus
   1.5 toodete või teenuste sertifitseerimise keerukus/kallidus
   1.6 finantseerimine
   1.7 muu
2. Kas te tegelete ka oma toodete sertifitseerimisega? Kui jah, siis milliste organisatsioonide poolt ja milliste sertifitseerimisskeemide alusel?

Küsimused poliitikameetmete kohta

1. Kas te olete saanud avalikult sektorilt toetust oma krütograafia alasele tegevusele, nt Euroopa Liidu programmidest, EAS-ilt, start-up kiirenditelt või muudest allikatest?
2. Kui jah, siis kas olete olnud rahul skeemi ning selle mõjuga?
3. Kui ei ole kasutanud, siis miks?
4. Mida saaks riik Eesti krüptograafiatoodete arendamise ja nendega rahvusvahelisele turule mineku toetamiseks täiendavalt teha?

Küsimused teiste ettevõtete kohta

1. Kas saaksite palun nimetada mõned vähemtuntud, kuid perspektiivikad krüptograafia valdkonnas tegutsevaid ettevõtted, kellega peaksime kindlasti tutvuma?

A.2 Procurer questionnaire

Küsimused organisatsiooni ja krüptograafiliste lahenduste hankimise kohta

1. Kas teil on ülevaade, milliseid krüptograafilisi rakendusi teie asutuses kasutatakse? Kui jah, siis milliseid? Kui ei, siis millised on plaanid selle ülevaate saamiseks?
2. Kas te tellite ise turvakriitilisi rakendusi, milles krüptograafia olulist rolli mängib? Kui jah, siis millistel põhimõtetel vastavad nõuded koostatakse?
3. Kas olete püüdnud (nt. krüptograafiliste algoritmide elutsükli uuringu põhjal) hinnata, millised teie infosüsteemid on enam ohustatud ning kui suured oleksid rünnaku korral võimalikud kahjud?

Küsimused krüptograafiga seonduva klasterdumise osas

1. Kes on Teie põhilised tarnijad ja koostööpartnerid Eestis, Euroopa Liidus ja mujal?
2. Kes konkreetsemalt Eesti ettevõtetest tarnib teile? Palun kirjeldage suhteid tarnijatega, nende kompetentsi, hankeprotsesside jms osas, samuti võimalikke probleeme.
3. Kas teie praktikas on olnud olukordi, kus te vajaksite mingit krüptograafilist lahendust, kuid sobivaid tooteid pole turul võtta? Kui jah, siis milliste toodete järele olete puudust tundnud?

Küsimused tehnoloogiatrendide kohta

1. Kui, siis millistes krüptograafia ja infoturbega seotud teemades vajaks teie asutuse kompetentsibaas tugevdamist?
2. Kui tugevaks te hindate oma asutuse kompetentsi järgmistes tehnoloogia valdkondades? (1. . . 5) Kui suur mõju on neil tehnoloogiatel olla Eesti tulevastele arengutele? (1. . . 5)
    - Postkvant-krüptograafia
    - Kvantvõtmevahetus
    - Identiteedihaldus
    - Turvaline arvutus ja privaatsust säilitav (suur)-andmete analüüs
    - Raadiosageduslikud protokollid
    - Vähese ressursinõudlusega krüptograafilised primitiivid (IoT)
    - Krüptograafiliste protokollide analüüs (Krüptograafiliste protokollide omaduste automaattõestamise meetodid)
    - Pikaajaline turve
    - Anonüümsed võrgud
    - Krüptorahad/plokiahelad

Küsimused takistuste kohta

1. Millised on olulisemad takistused krüptograafiarikaste toodete ja teenuste väljatöötamise ning ekspordi kasvatamise osas? (1. . . 5)
   1.1 teadurid ja inseneeride puudus
   1.2 turundus- ja müügitöötajate puudus
   1.3 keskastme- ja tippjuhtide puudus
   1.4 välismaise tööjõu kaasamise keerukus
   1.5 toodete või teenuste sertifitseerimise keerukus/kallidus
   1.6 finantseerimine
   1.7 muu

Küsimused poliitikameetmete kohta

1. Kuidas saaks riik aidata kaasa krüptograafiarikaste toodete paremale kättesaadavusele ja kohandamisele, mida saaks teha nende toodete kasutuselevõtu lihtsustamiseks?
2. Kuidas võiks teie hinnangul toetada ettevõtete krüptograafia-alast tegevust krüptograafiatoodetega rahvusvahelisele turule jõudmist?

Küsimused teiste ettevõtete kohta

1. Kas saaksite palun nimetada mõned vähemtuntud, kuid perspektiivikad krüptograafia valdkonnas tegutsevaid ettevõtted, kellega peaksime kindlasti tutvuma?

A.3 University questionnaire

Küsimused krüptograafia-alase haridus osas

1. Millised on teie koolis pakutavad krüptograafiakursused? Kui palju neid on, kui sügavale nad krüptograafias lähevad? Kui palju räägitakse krüptograafiat ümbritsevast, nt üldisemalt infoturbest, infoturbe majanduslikest aspektidest jne?
2. Milliseid teadmisi ja oskusi kursuste läbijad omavad? Kui palju on hands-on koolitusi, ise krüptorakenduste programmeerimist jms?
3. Kui palju üliõpilasi neid kursuseid iga-aastaselt võtab? Kui palju (hinnanguliselt) viimase 5 aasta jooksul neilt kursustelt inimesi kokku läbi käinud on?
4. Kui palju (hinnanguliselt) krüptograafia kursuste läbijaid te prognoosite eelolevaks 5 aastaks?

Küsimused krüptograafiga seonduva klasterdumise osas

1. Milliseid krüptograafia valdkonna teadus- ja haridusprojekte teil praegu käimas on? Kas osalete Horisont 2020, ETAG, EAS või mõne muu programmi projektides?
2. Kes on Teie põhilised koostööpartnerid Eestis, Euroopa Liidus ja mujal?

3. Milline on teie asutuse krüptograafia-alane koostöö ettevõtete ja teiste asutustega?
4. Kas teie ülikoolist on võrsunud või ülikooli lõpetanud asutanud krüptograafia valdkonnas tegutsevaid *start-up*'e? Palun loetlege neid! (Oleme väga tänulikud ka vastavate kontaktide eest. Millistele probleemidele need ettevõtted lahendusi pakuvad?)

Küsimused tehnoloogiatrendide kohta

1. Kui, siis millistes krüptograafia ja infoturbega seotud teemades vajaks teie asutuse kompetentsibaas tugevdamist?
2. Kui tugevaks te hindate oma asutuse kompetentsi järgmistes tehnoloogia valdkondades? (1. . . 5) Kui suur mõju on neil tehnoloogiatel olla Eesti tulevastele arengutele? (1. . . 5)
    - Postkvant-krüptograafia
    - Kvantvõtmevahetus
    - Identiteedihaldus
    - Turvaline arvutus ja privaatsust säilitav (suur)-andmete analüüs
    - Raadiosageduslikud protokollid
    - Vähese ressursinõudlusega krüptograafilised primitiivid (IoT)
    - Krüptograafiliste protokollide analüüs (Krüptograafiliste protokollide omaduste automaattõestamise meetodid)
    - Pikaajaline turve
    - Anonüümsed võrgud
    - Krüptorahad/plokiahelad

Küsimused tööturu nõudluse kohta

1. Kas te tunnetate tööturul nõudlust mõne krüptograafia alase kompententsi järele, mida ei ole täna Eestis piisavalt? Palun täpsustage!
2. Kas te näete tulevasi Euroopas või kaugemal potentsiaalikaid krüptograafia kompetentsivaldkondi, mille järele ei ole Eesti tööturul praegu (veel) nõudlust?
3. Kui tugevaks te peate Eestis olemasolevat toodete ja teenuste sertifitseerimise alast kompetentsi? Kas olete sellele teemale õppekavade arendamisel mõelnud?

Küsimused takistuste kohta

1. Millised on olulisemad takistused valdkonna hariduse pakkumisel? (1. . . 5)
    1.1 üldhariduskoolide lõpetajate matemaatika teadmiste ja oskuste tase
    1.2 kõrghariduse finantseerimine
    1.3 teaduse finantseerimine
    1.4 välisõppejõudude ja teadurite kaasamise keerukus
    1.5 muu

Küsimused poliitikameetmete kohta

1. Kuidas saaks riik aidata kaasa hariduse edendamisele krüptograafia valdkonnas?
2. Mida saaks riik Eesti krüptograafiatoodete arendamise ja nendega rahvusvahelisele turule mineku toetamiseks täiendavalt teha?

Küsimused teiste ettevõtete kohta

1. Kas saaksite palun nimetada mõned vähemtuntud, kuid perspektiivikad krüptograafia valdkonnas tegutsevaid ettevõtted, kellega peaksime kindlasti tutvuma?

Bibliography

[1] HORIZON 2020. Work Programme 2014–2015. 14. Secure societies – Protecting freedom and security of Europe and its citizens. European Commission Decision C (2013)8631 of 10 December 2013.

[2] HORIZON 2020. Work Programme 2014–2015. 5. Leadership in enabling and industrial technologies. i. Information and Communication Technologies. European Commission Decision C (2013)8631 of 10 December 2013.

[3] HORIZON 2020. Work Programme 2016–2017. 14. Secure societies – Protecting freedom and security of Europe and its citizens. European Commission Decision C(2016)4614 of 25 July 2016.

[4] HORIZON 2020. Work Programme 2016–2017. 14. Secure societies – Protecting freedom and security of Europe and its citizens. European Commission Decision C(2018)4708 of 24 July 2018.

[5] HORIZON 2020. Work Programme 2018–2020. 5.i. Information and Communication Technologies. European Commission Decision C(2018)518 of 31 January 2018.

[6] Küberturvalisuse strateegia 2019–2022. Majandus- ja kommunikatsiooniministeerium, 2018, https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019_vv-s_kinnitatud.docx.

[7] Risk management in the procurement of innovation. Concepts and empirical evidence in the European Union, Expert Group Report. European Commission, Brussels, 2010. http://ec.europa.eu/invest-in-research/pdf/download_en/risk_management.pdf.

[8] Krüptograafiliste algoritmide kasutusvaldkondade ja elutsükli uuring (Report on the life cycle of cryptographic algorithms). https://www.ria.ee/public/PKI/kruptograafiliste_algoritmide_elutsukli_uuring_II.pdf, 2013. Cybernetica report no. A-77-5 (in Estonian).

[9] Krüptograafiliste algoritmide kasutusvaldkondade ja elutsükli uuring (Report on the life cycle of cryptographic algorithms). https://www.ria.ee/public/RIA/Kruptograafiliste_algoritmide_uuring_2015.pdf, 2015. Cybernetica report no. A-101-1 (in Estonian).

[10] Cryptographic algorithms lifecycle report 2016. https://www.ria.ee/public/RIA/Cryptographic_Algorithms_Lifecycle_Report_2016.pdf, 2016. Cybernetica report no. A-101-3.

[11] Cryptographic algorithms lifecycle report 2017. https://www.ria.ee/public/RIA/kruptograafiliste_algoritmide_elutsukli_uuring_2017.pdf, 2017. Cybernetica report no. A-101-9.

[12] Divesh Aggarwal, Gavin K Brennen, Troy Lee, Miklos Santha, and Marco Tomamichel. Quantum attacks on Bitcoin, and how to protect against them, 2017. arXiv preprint arXiv:1710.10377, https://arxiv.org/pdf/1710.10377.pdf.

[13] Matteo Avalle, Alfredo Pironti, and Riccardo Sisto. Formal verification of security protocol implementations: a survey. *Formal Aspects of Computing*, 26(1):99–123, January 2014.

[14] Dave Bayer, Stuart Haber, and W Scott Stornetta. Improving the efficiency and reliability of digital time-stamping. In *Sequences II*, pages 329–334. Springer, 1993.

[15] Paul Benioff. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of statistical physics*, 22(5):563–591, 1980.

[16] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *J. Cryptol.*, 5(1):3–28, January 1992.

[17] Alberto Boaron, Gianluca Boso, Davide Rusca, Cédric Vulliez, Claire Autebert, Misael Caloz, Matthieu Perrenoud, Gaëtan Gras, Félix Bussières, Ming-Jun Li, Daniel Nolan, Anthony Martin, and Hugo Zbinden. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.*, 121:190502, Nov 2018.

[18] Johannes Braun, Johannes A. Buchmann, Denise Demirel, Matthias Geihs, Mikio Fujiwara, Shiho Moriai, Masahide Sasaki, and Atsushi Waseda. LINCOS: A storage system providing long-term integrity, authenticity, and confidentiality. In Ramesh Karri, Ozgur Sinanoglu, Ahmad-Reza Sadeghi, and Xun Yi, editors, *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, AsiaCCS 2017, Abu Dhabi, United Arab Emirates, April 2-6, 2017*, pages 461–468. ACM, 2017.

[19] Johannes Buchmann, Alexander May, and Ulrich Vollmer. Perspectives for cryptographic long-term security. *Commun. ACM*, 49(9):50–55, September 2006.

[20] Ahto Buldas, Matthias Geihs, and Johannes A. Buchmann. Long-term secure commitments via extractable-binding commitments. In Josef Pieprzyk and Suriadi Suriadi, editors, *Information Security and Privacy - 22nd Australasian Conference, ACISP 2017, Auckland, New Zealand, July 3-5, 2017, Proceedings, Part I*, volume 10342 of *Lecture Notes in Computer Science*, pages 65–81. Springer, 2017.

[21] Ahto Buldas, Matthias Geihs, and Johannes A. Buchmann. Long-term secure time-stamping using preimage-aware hash functions - (short version). In Tatsuaki Okamoto, Yong Yu, Man Ho Au, and Yannan Li, editors, *Provable Security - 11th International Conference, ProvSec 2017, Xi'an, China, October 23-25, 2017, Proceedings*, volume 10592 of *Lecture Notes in Computer Science*, pages 251–260. Springer, 2017.

[22] Ahto Buldas, Peeter Laud, Helger Lipmaa, and Jan Willemson. Time-Stamping with Binary Linking Schemes. In Hugo Krawczyk, editor, *Advances in Cryptology – CRYPTO '98, 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23-27, 1998, Proceedings*, volume 1462 of *Lecture Notes in Computer Science*, pages 486–501. Springer, 1998.

[23] Luis Cabral, Guido Cozzi, Vincenzo Denicolò, Giancarlo Spagnolo, and Matteo Zanza. Procuring innovation. In *Handbook of Procurement*. Cambridge University Press, 2006.

[24] David L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM*, 24(2):84–90, February 1981.

[25] European Council. Presidency Conclusions: Lisbon European Council 23-24 March 2000, 2000. http://www.europarl.europa.eu/summits/lis1_en.htm.

[26] Bernardo David, Peter Gazi, Aggelos Kiayias, and Alexander Russell. Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*, volume 10821 of *Lecture Notes in Computer Science*, pages 66–98. Springer, 2018.

[27] Stéphanie Delaune and Lucca Hirschi. A survey of symbolic methods for establishing equivalence-based properties in cryptographic protocols. *Journal of Logical and Algebraic Methods in Programming*, 87:127 – 144, 2017.

[28] John H Dunning. Toward an eclectic theory of international production: Some empirical tests. *Journal of international business studies*, 11(1):9–31, 1980.

[29] Jakob Edler. Demand oriented innovation policy. *The Theory and Practice of Innovation Policy An International Research Handbook, Edward Elgar: Cheltenham*, pages 177–208, 2010.

[30] Jakob Edler and Luke Georghiou. Public procurement and innovation—resurrecting the demand side. *Research Policy*, 36(7):949–963, 2007.

[31] Charles Edquist and Jon Mikel Zabala-Iturriagagoitia. Public Procurement for Innovation as mission-oriented innovation policy. *Research policy*, 41(10):1757–1769, 2012.

[32] E. Erdin, C. Zachor, and M. H. Gunes. How to find hidden users: A survey of attacks on anonymity networks. *IEEE Communications Surveys Tutorials*, 17(4):2296–2316, Fourthquarter 2015.

[33] Eurostat. Eurostat database, 2018. https://ec.europa.eu/eurostat/data/database.

[34] Richard P Feynman. Simulating physics with computers. *International journal of theoretical physics*, 21(6-7):467–488, 1982.

[35] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. In *EUROCRYPT 2015: Advances in Cryptology – EUROCRYPT 2015*, volume 9057 of *LNCS*, pages 281–310. Springer, 2015.

[36] Matthias Geihs, Denise Demirel, and Johannes A. Buchmann. A security analysis of techniques for long-term integrity protection. In *14th Annual Conference on Privacy, Security and Trust, PST 2016, Auckland, New Zealand, December 12-14, 2016*, pages 449–456. IEEE, 2016.

[37] Matthias Geihs, Nikolaos P. Karvelas, Stefan Katzenbeisser, and Johannes Buchmann. PROPYLA: privacy preserving long-term secure storage. In Aziz Mohaisen and Qian Wang, editors, *Proceedings of the 6th International Workshop on Security in Cloud Computing, SCC@AsiaCCS 2018, Incheon, Republic of Korea, June 04-08, 2018*, pages 39–48. ACM, 2018.

[38] Gary Gereffi, John Humphrey, and Timothy Sturgeon. The governance of global value chains. *Review of international political economy*, 12(1):78–104, 2005.

[39] Stuart Haber and W. Scott Stornetta. How to Time-Stamp a Digital Document. In Alfred J. Menezes and Scott A. Vanstone, editors, *Advances in Cryptology-CRYPT0' 90*, volume 537 of *LNCS*, pages 437–455. Springer Berlin Heidelberg, 1991.

[40] Ramzi A. Haraty, Maram Assi, and Imad Rahal. A systematic review of anonymous communication systems. In Slimane Hammoudi, Michal Smialek, Olivier Camp, and Joaquim Filipe, editors, *ICEIS 2017 - Proceedings of the 19th International Conference on Enterprise Information Systems, Volume 2, Porto, Portugal, April 26-29, 2017*, pages 211–220. SciTePress, 2017.

[41] Sven Heiberg, Tarvi Martens, Priit Vinkel, and Jan Willemson. Improving the verifiability of the Estonian Internet Voting scheme. In Robert Krimmer, Melanie Volkamer, Jordi Barrat, Josh Benaloh, Nicole Goodman, Peter Y. A. Ryan, and Vanessa Teague, editors, *International Joint Conference on Electronic Voting*, number 10141 in LNCS, pages 92–107. Springer, 2016.

[42] Sven Heiberg, Ivo Kubjasand Janno Siim, and Jan Willemson. On Trade-offs of Applying Block Chains for Electronic Voting Bulletin Boards. In *Proceedings of the Third International Joint Conference on Electronic Voting E-Vote-ID 2018*, pages 259–276. TUT press, 2018.

[43] Sven Heiberg and Jan Willemson. Verifiable internet voting in Estonia. In *2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE)*, pages 1–8. IEEE, Oct 2014.

[44] Bruce Henderson. The product portfolio, 1970. `https://www.bcg.com/publications/1970/strategy-the-product-portfolio.aspx`.

[45] Julia Hesse, Dennis Hofheinz, and Andy Rupp. Reconfigurable cryptography: A flexible approach to long-term security. In Eyal Kushilevitz and Tal Malkin, editors, *Theory of Cryptography - 13th International Conference, TCC 2016-A, Tel Aviv, Israel, January 10-13, 2016, Proceedings, Part I*, volume 9562 of *Lecture Notes in Computer Science*, pages 416–445. Springer, 2016.

[46] Tomas Jermalavičius. Estonia's Defence Research and Development: Lessons from the past, outlook for the future, 2011. International Centre for Defence Studies, Tallinn.

[47] Tarmo Kalvet. Innovation: a factor explaining e-government success in estonia. *Electronic Government, an International Journal*, 9(2):142–157, 2012.

[48] Boris Korzh, Charles Ci Wen Lim, Raphael Houlmann, Nicolas Gisin, Ming Jun Li, Daniel Nolan, Bruno Sanguinetti, Rob Thew, and Hugo Zbinden. Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nature Photonics*, 9:163–168, 2015.

[49] Pascal Lafourcade, Denis Lugiez, and Ralf Treinen. Intruder deduction for ac-like equational theories with homomorphisms. In Jürgen Giesl, editor, *Term Rewriting and Applications*, pages 308–322, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

[50] Veiko Lember and Tarmo Kalvet. *Public Procurement, Innovation and "No Policy" Policy*, pages 127–149. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014.

[51] Veiko Lember, Rainer Kattel, and Tarmo Kalvet. Public procurement and innovation: Theory and practice. In *Public Procurement, Innovation and Policy*, pages 13–34. Springer, 2014.

[52] Lea Lepmann, Tiit Lepmann, and Jüri Afanasjev. The development of national mathematics curriculum in Estonia at the beginning of the 21st century. In *Teaching Mathematics: Retrospective and Perspectives. Proceedings of the 10th International Conference*, pages 102–112, 2009. http://www.tlu.ee/bcmath2009/Tallinn%202009_proceedings.pdf#page=102.

[53] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, Feng-Zhi Li, Xia-Wei Chen, Li-Hua Sun, Jian-Jun Jia, Jin-Cai Wu, Xiao-Jun Jiang, Jian-Feng Wang, Yong-Mei Huang, Qiang Wang, Yi-Lin Zhou, Lei Deng, Tao Xi, Lu Ma, Tai Hu, Qiang Zhang, Yu-Ao Chen, Nai-Le Liu, Xiang-Bin Wang, Zhen-Cai Zhu, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Satellite-to-ground quantum key distribution. *Nature*, 549:43–47, 2017.

[54] Iuon-Chang Lin and Tzu-Chun Liao. A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*, 19(5):653–659, 2017.

[55] Nicolai Liventhal. Krüptoloogia osast ajaloos. *Teataja*, May 5th 1995. https://dea.digar.ee/cgi-bin/dea?a=d&d=teatajapoliit19950506.1.5.

[56] Hoi-Kwong Lo, Marcos Curty, and Kiyoshi Tamaki. Secure quantum key distribution. *Nature Photonics*, 8:595–604, 2014.

[57] Ülle Madise and Tarvi Martens. E-voting in Estonia 2005. The first Practice of Country-wide binding Internet Voting in the World. In Robert Krimmer, editor, *Electronic Voting 2006: 2nd International Workshop, Co-organized by Council of Europe, ESF TED, IFIP WG 8.6 and E-Voting.CC, August, 2nd - 4th, 2006 in Castle Hofen, Bregenz, Austria.*, volume 86 of *LNI*, pages 15–26. GI, 2006.

[58] Juri Manin. *Vychislimoe i nevychislimoe*. Sovetskoje radio, 1980.

[59] Rani Molla. Amazon spent nearly $23 billion on R&D last year - more than any other U.S. company, 2018. https://www.recode.net/2018/4/9/17204004/amazon-research-development-rd.

[60] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008. https://bitcoin.org/bitcoin.pdf.

[61] Matús Nemec, Marek Sýs, Petr Svenda, Dusan Klinec, and Vashek Matyas. The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli. In Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*, pages 1631–1648. ACM, 2017.

[62] Artur Normak. *Šifri käsiraamat*. Tallinn, 1935.

[63] Nikolaus Obwegeser and Sune Dueholm Müller. Innovation and public procurement: Terminology, concepts, and applications. *Technovation*, 74-75:1–17, 2018.

[64] Ministry of Education and Research. Estonian Research and Development and Innovation Strategy 2014-2020, 2014. https://www.hm.ee/sites/default/files/estonian_rdi_strategy_2014-2020.pdf.

[65] Se Eun Oh, Shuai Li, and Nicholas Hopper. Fingerprinting keywords in search queries over tor. *Proceedings on Privacy Enhancing Technologies*, 2017(4):251–270, 2017.

[66] Rafael Pass, Lior Seeman, and abhi shelat. Analysis of the Blockchain Protocol in Asynchronous Networks. In *Advances in Cryptology – EUROCRYPT 2017*, volume 10211 of *LNCS*, pages 643–673. Springer, 2017.

[67] Morgen E. Peck. Blockchain world – Do you need a blockchain? This chart will tell you if the technology can solve your problem. *IEEE Spectrum*, 54(10):38–60, October 2017.

[68] Carlota Perez. *Technological Revolutions and Financial Capital: The Dynamics of Bubbles and Golden Ages*. Cheltenham: Edward Elgar, 2002.

[69] A. Pescape, A. Montieri, G. Aceto, and D. Ciuonzo. Anonymity services tor, i2p, jondonym: Classifying in the dark (web). *IEEE Transactions on Dependable and Secure Computing*, pages 1–1, 2018.

[70] Michael E Porter. *The Competitive Advantage of Nations*. New York: Free Press, 1990.

[71] Michael E Porter. Location, competition, and economic development: Local clusters in a global economy. *Economic development quarterly*, 14(1):15–34, 2000.

[72] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[73] Max Rolfstam. Understanding public procurement of innovation: definitions, innovation types and interaction modes, 2012. https://ssrn.com/abstract=2011488.

[74] Roy Rothwell. Issues in user–producer relations in the innovation process: the role of government. *International Journal of Technology Management*, 9(5-7):629–649, 1994.

[75] Musa G. Samaila, Miguel Neto, Diogo A. B. Fernandes, Mário M. Freire, and Pedro R. M. Inácio. Challenges of securing internet of things devices: A survey. *Security and Privacy*, 1(2):e20, 2018.

[76] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.

[77] Fatemeh Shirazi, Milivoj Simeonovski, Muhammad Rizwan Asghar, Michael Backes, and Claudia Diaz. A survey on routing in anonymous communication protocols. *ACM Comput. Surv.*, 51(3):51:1–51:39, 2018.

[78] Petr Svenda, Matús Nemec, Peter Sekan, Rudolf Kvasnovský, David Formánek, David Komárek, and Vashek Matyás. The Million-Key Question – Investigating the Origins of RSA Public Keys. In Thorsten Holz and Stefan Savage, editors, *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016.*, pages 893–910. USENIX Association, 2016.

[79] Nick Szabo. Smart contracts: building blocks for digital markets. *EXTROPY: The Journal of Transhumanist Thought, (16)*, 1996.

[80] Nick Szabo. Formalizing and Securing Relationships on Public Networks. *First Monday*, 2(9), 1997.

[81] Marek Tiits and Tarmo Kalvet. Intelligent piggybacking: A foresight policy tool for small catching-up economies. *International Journal of Foresight and Innovation Policy*, 9:253 – 268, 2013.

[82] Gunda Tire, Imbi Henno, Regina Soobard, Helin Puksand, Tiit Lepmann, Hannes Jukk, Kristina Lindemann, Maie Kitsing, and Karin Täht. PISA 2015 Eesti tulemused. Eesti 15-aastaste õpilaste teadmised ja oskused loodusteadustes, funktsionaalses lugemises ja matemaatikas, 2016. https://www.innove.ee/wp-content/uploads/2017/11/PISA-2015_EESTI_ARUANNE_FINAL.pdf.

[83] Jesús Antonio Soto Velázquez. Practical Implementations of Quantum-Resistant Cryptography, 2017. Seminar report, Tartu University, https://courses.cs.ut.ee/MTAT.07.022/2017_fall/uploads/Main/antonio-report-f17.pdf.

[84] Mark Weiser. The computer for the 21st century. In Ronald M. Baecker, Jonathan Grudin, William A. S. Buxton, and Saul Greenberg, editors, *Human-computer Interaction*, pages 933–940. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 1995.

[85] Joeri H Wesseling and Charles Edquist. Public procurement for innovation to help meet societal challenges: a review and case study. *Science and Public Policy*, 45(4):493–502, 2018.

[86] Andrew Chi-Chih Yao. Protocols for secure computations (extended abstract). In *23rd Annual Symposium on Foundations of Computer Science, Chicago, Illinois, USA, 3-5 November 1982*, pages 160–164. IEEE Computer Society, 1982.

[87] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. Where is current research on blockchain technology? A systematic review. *PloS one*, 11(10), 2016.