Oude Waalsdorperweg 63
2597 AK Den Haag
P.O. Box 96864
2509 JG The Hague
The Netherlands

www.tno.nl

T +31 88 866 10 00

TNO report

TNO 2022 R10712

EZK Valorisation Chains: Crypto Communication Value Network

Date	September 2022
Author(s)	Dr. D. Tiggelman Ir. Y.J. Meijaard Drs. ir. J.T. Rabbie Drs. L.I. Soldaat Drs. V. Szijjarto Dr. ir. T.M.M. Laarhoven Drs. M.S.C. van Leuken Drs. M. Breure
Number of pages	56 (incl. appendices)
Number of appendices	2
Sponsor	Ministry of Economic Affairs and Climate Policy
Project name	EZK: Valorisation Chains Crypto Communication
Project number	060.50500

Summary

The Netherlands is one of the leaders within Europe when it comes to digitalisation, and must continue to develop itself rapidly within this digital domain in order to maintain its position. However, digitalisation must take place in a secure way. Crypto communication is at the foundation of secure, digital communication and data exchange. It refers to cryptography in the broadest sense of the word, with a particular emphasis on cryptography in a larger context of information technology and its use for operational processes. To conclude, crypto communication is the usage of cryptography for the secure transmission, processing, storage and exchange of information.

In this report, we will outline the valorisation chain of crypto communication, which serves as the foundation for the crypto communication roadmap. The roadmap has three objectives: the development of innovative products and services related to crypto communication, the promotion of economic activity and the stimulation of the strategic autonomy of the Netherlands. Insight into the valorisation chain is of importance here – an economically healthy and properly functioning value network helps with the attainment of the objectives in the crypto communication roadmap.

This report first outlines the exploration of the crypto communication ecosystem, based on European market research. It then outlines the crypto communication value network analyses, conducted within the energy (specifically offshore wind) and the automotive industry. To conclude it identifies barriers, or ‘valleys of death’, and offers recommended tracks that can be used in shaping and refining the crypto communication roadmap.

Market research
The market research at European Union (EU) level has been carried out on the basis of literature research and interviews with selected parties, chosen for their knowledge position within the ecosystem. The research revealed that the previously identified innovation initiatives, as formulated in ‘Nederland Cryptoland’, are highly consistent with current innovation initiatives within the European market. Germany and France in particular have a proper knowledge position when it comes to crypto communication. The Netherlands has a good reputation within Europe, characterised by strong cooperation, taking place at both EU and global level.

The research highlighted various barriers experienced by parties that stand in the way of the development of innovations in the cryptographic landscape. The most important of these are:

- A shortage of technical personnel, particularly with regard to innovations
- (Too much) academic pressure on the publication of scientific publications within cryptography
- Underinvestment in cryptanalysis
- A conflict of interests in the development of standardisation
- Insufficient cooperation between individual EU Member States
- Difficulty of achieving crypto-agility in hardware.

Value network analyses
A value network analysis is a structured method in which a combination of interviews and literature review is used to map an innovative ecosystem. Such an analysis reveal a number of roles, each of them mutually connected by means of value exchanges. The value network thus visualises the different relationships that exist within the ecosystem and focuses not only on money, but on other values, such as knowledge, personnel and innovative strength. In addition, it helps to provide insight into and visualisation of partnerships and barriers. In this study, the value networks for crypto communication into two sectors have been mapped: offshore wind as part of the energy industry and (direct) vehicle-to-all (V2X) communication as part of the automotive industry.

For offshore wind, there is a clear valorisation chain from knowledge building as far as product integration. The transmission grid operator occupies a relatively central position within the value network. The operators of the wind farms and suppliers of infrastructure components have an important role as well, as they cooperate with universities and other institutions to foster their knowledge building. In this context, the grid operator and the operators are customers, who can set requirements for suppliers, which may also include requirements in relation to cryptography. This is an important driver for innovation on the part of the suppliers. In terms of policy and supervision, all relevant parties are covered by the Security of Network and Information Systems Act (Wbni), thereby preventing visible gaps in legislation. One of the principal barriers to innovation is the shortage of specialist personnel with adequate knowledge of both cyber security and the energy industry.

In contrast to the offshore wind industry, no value network is visible yet for the V2X part of the automotive industry due to a lack of valorisation of crypto communication. The majority of developments relating to (direct) V2X communication are still in the pilot phase, with no large-scale roll-out of self-driving vehicles, which means that there is not a commercial market yet either. Numerous technological and non-technological challenges exist that need to be resolved in order to overcome this particular phase. The greatest impediment to innovation is integrating IT into the current operational technology: vehicles have a long life cycle (30 years), which requires the integration of relevant technology for the same duration. This puts a limit on the speed of innovation. In addition, there is currently no party that can take a leadership role in the innovation ecosystem. (Transport) security has high priority in this industry, which means that new technologies that could affect it are subject to critical examination, and there is little economic incentive for companies to implement crypto communication in their products. Consequently, most parties are taking a wait-and-see approach for now.

Foundation roadmap
The conducted research has been used to identify ‘valleys of death’ (i.e. barriers existing between the development phases of innovation) within both sectors:

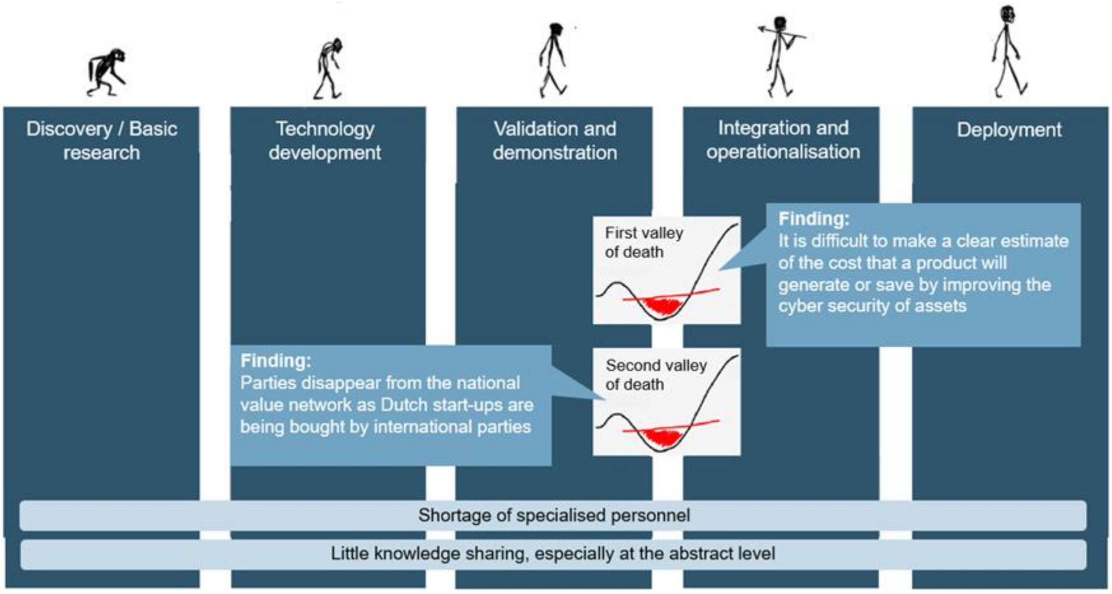

Figure 1 The identified valleys of death and more generic barriers in the development phases within the energy industry.

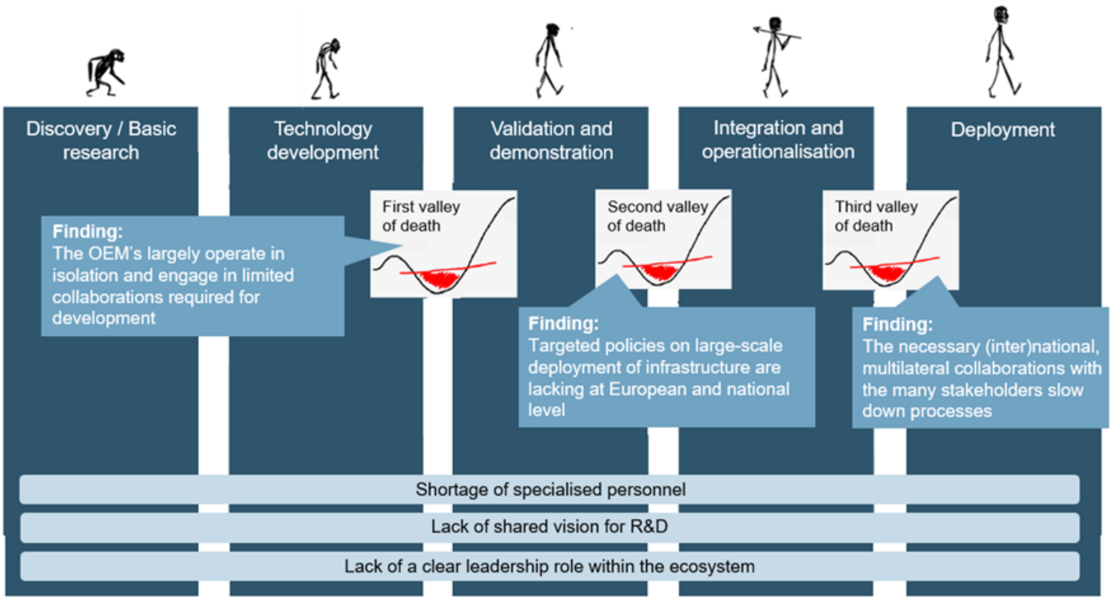

Figure 2 The identified valleys of death and more generic barriers in the development phases within the automotive industry.

Potential solutions to the identified valleys of death have been translated into four cross-industry tracks, which can be used to shape and refine the crypto communication roadmap:

1 **Education, people and retention of knowledge:** a shortage of qualified personnel is a generally observed barrier for the value chains. Concrete steps need to be taken to strengthen knowledge of crypto communication within the industries; safeguarding (academic) research; and ensuring the retention of national start-ups by ensuring a good business climate, healthy growth

opportunities and specific regulation.

2 **Pre-competitive collaboration:** a lack of a clear leadership role in the ecosystem and a lack of shared vision between parties in the industry when it comes to setting R&D priorities exist. Targeted collaboration with clear leadership and policy, can help break down these barriers and in turn expand the overall market.

3 **Collaboration support/community management:** it is important to create a safe environment for collaboration and coordination between parties within the value network. Standardisation at national level (e.g. via NEN) can lead to trust and guidelines for collaboration. As a collaboration platform, dcypher can play a valuable role in this.

4 **Fieldlabs:** fieldlabs can offer a safe environment for open innovation by multiple parties from the industry, in which ideas and new technological solutions can be tested freely. The fieldlabs will have to be a supported activity, for which working on concrete and shared risks is leading. A starting point are the industry-specific barriers identified in this report.

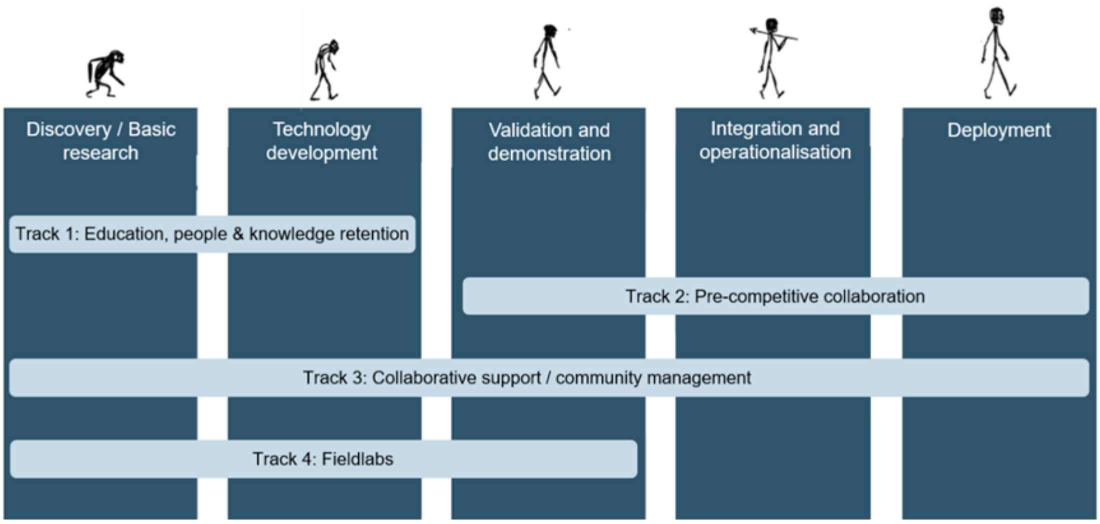

Figure 3 The four tracks for the crypto communication roadmap.

Table of contents

1 Introduction and context

The Netherlands is one of the leaders within Europe when it comes to digitalisation[1] [2], for example with its fixed and mobile communication infrastructure. If the Netherlands want to retain this position, it must continue to develop itself rapidly within this digital domain. Of importance here is that everyone within society is able to participate in digitalisation, on the condition that more effort is put into security, privacy protection, self-determination and digital skills. As the Netherlands Cyber Security Agenda states[3], the Netherlands must be able to 'securely capitalise on the economic and social opportunities presented by digitalisation and protect national security within the digital domain.'

Keeping systems secure in our digitalised society is, therefore, extremely important. For secure digital communication and exchange of data, cryptography is the foundation. In the Netherlands, coordination of innovation in crypto communication is entrusted to dcypher, where it is a key topic that is being tackled as part of public/private partnerships (PPP) and where it is a priority in the Knowledge and Innovation Agenda (KIA) Security, mission cyber security.[4] Crypto communication refers to the use of cryptography for the secure and protected transmission, processing, storage and exchange of information.[5]

In this report, we will outline the valorisation chain of crypto communication, which serves as the foundation for the crypto communication roadmap. The roadmap focuses on the period 2022 to 2032 and has three objectives:

1 The development of innovative products and services relating to crypto communication;
2 The promotion of economic activity in the Netherlands;
3 The stimulation of the strategic autonomy of the Netherlands.

Insight into the valorisation chain is of importance here – an economically healthy and properly functioning value network helps with the attainment of the objectives in the crypto communication roadmap.

Two methods have been used in this study of the valorisation chain of crypto communication:

- *Market research:* This involved an examination of the crypto communication ecosystem, by examining the Dutch and European markets through literature research and conducting interviews
- *Value network analyses*: A value network analysis is a method designed for taking a wide-ranging look at an innovation ecosystem. This provides a richer picture than a value chain analysis, in which there is a single central actor, as it

---

[1] ITU (2017), Measuring the Information Society Report, 2017 (Vol. 1).
[2] European Commission (2018), FinTech action plan: For a more competitive and innovative European financial sector.
[3] NCTV (2018), Nederlandse Cybersecurity Agenda: Nederland digitaal veilig.
[4] Topsector High Tech Systemen en Materialen (HTSM), Team Dutch Digital Delta, Topsector Creatieve Industrie, Topsector Logistiek en Topsector Water & Maritiem (2019), *Kennis en innovatieagenda (KIA) Veiligheid*, p. 26-34.
[5] Ministerie van Economische Zaken en Klimaat, TNO, CWI & dcypher (2021), Nederland Cryptoland. Startpunt routekaart cryptocommunicatie: de vier belangrijkste uitdagingen in de cryptografie.

maps a complex network. Within a value network analysis a number of roles is visible, each of which is mutually connected by means of value exchanges (money, knowledge, personnel, etc.). The value network analyses in this report have been carried out for two industries:

- *The energy industry*: specifically for ‘offshore wind’ actors
- *The automotive industry*: specifically for ‘direct communication’ actors

In addition to providing a foundation for the crypto communication roadmap, this report also provides input for the field labs. Consequently, the study was carried out and completed within a relatively short period of time. Therefore emphasis within the study was focused on extracting as many relevant findings in relation to crypto communication in the broadest sense possible, and more specifically within the energy (offshore wind) and automotive (V2X communication) industries during the value network analyses. Follow-up studies are required to be able to further generalise these findings (to the industries as a whole), to nuance and validate them and to expand them in order to give further substance to the roadmap.

This report consists of four substantive sections. Section 2 outlines the exploration of the crypto communication ecosystem, based on an examination of the European market. This study has been carried out through literature research and conducting interviews with various parties within the ecosystem, resulting in an overview of ongoing innovation initiatives, active actors within each of the innovation developments in crypto communication and the barriers that these actors experience during development. Section 3 outlines the value network analyses for crypto communication within the energy and automotive industries in respect of the use of crypto communication. The value network, as outlined above, has been mapped through a combination of desk research and interviews with actors in the respective industries. The analyses indicate the roles of these parties within the network, the interests at play and where the bottlenecks for innovation in terms of cyber security within the two industries are situated. In addition, the analyses also highlight the most important similarities and differences between the energy industry and the automotive industry. Section 4 outlines the way in which the results from the value network analyses can be used in the shaping and refining of the crypto communication roadmap. Which players have a role within the five development phases (*Discovery/basic research, Technology development, Validation and demonstration, Integration and Operationalisation, Deployment*)? And what are the ‘valleys of death’ that impede product development and what measures are needed to overcome these impediments to attain the roadmap’s objectives?

2 Market research: The Crypto Communication Ecosystem

2.1 Introduction

Crypto communication refers to cryptography in the broadest sense of the word, with a particular emphasis on cryptography in a larger context of information technology and being embedded into various processes. In short, crypto communication is the use of cryptography for the secure transmission, processing, storage and the protected exchange of information.

Within the cryptography landscape, four developments have been identified within the cryptography roadmap ‘Nederland Cryptoland’ (2021)[6], developed by the Ministry of Economic Affairs, TNO, CWI and dcypher. These four developments constitute the greatest challenges and the greatest opportunities for the upcoming years (see Figure 4). The market research was carried out along the axis of these developments. The four developments are as follows:

1. **Securing new technical environments**: An ever increasing number of technical environments is connected to the outside world, including OT as well as IoT devices. This gives rise to technical environments and products that often have insufficient protection due to limitations on the use of the security-by-design principle. This necessitates development of new security products that are suitable for use in situations in which security has utmost importance.

2. **Migration to post-quantum cryptography**: The development of the quantum computer puts commonly used cryptographic applications at risk. This means that there is a need to migrate to ‘post-quantum cryptography’, which is resistant to attacks by future large-scale quantum computers.

3. **Use of cryptography for new, decentralised applications**: The development of state-of-the-art, multilateral cryptography makes new, decentralised applications technically feasible. This means that it is possible to develop new products and services that make use of this modern cryptography.

4. **Formal verification of cryptography and cryptographic source code**: Formal verification is a method by which a computer carries out automated checks on cryptographic protocols, primitives and their software implementations. The use of formal verification techniques on cryptographic protocols and source code offers greater certainty regarding the security of cryptographic products.

[6] EZK, TNO, CWI & dcypher (2021), *Nederland Cryptoland*.

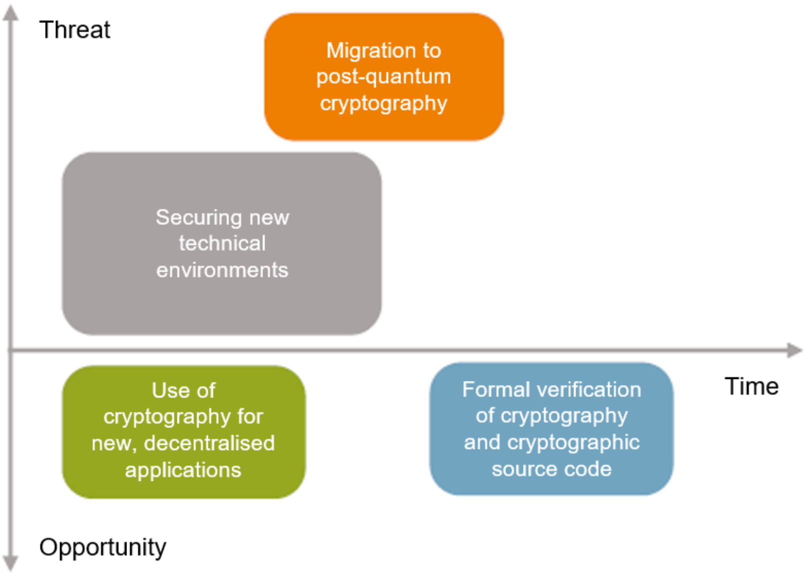

Figure 4 Presentation of the four developments in cryptography, split into opportunities and threats over time.[7]

This market research of the innovation landscape relating to cryptography consists of the following five components:

- An explanation of the used methodology of how the market research has been carried out;
- A number of overarching findings relating to cryptography in the Dutch and European ecosystem;
- An overview of ongoing innovation initiatives within the four developments relating to cryptography and the corresponding actors;
- A description of the experienced barriers within the ecosystem which impede innovation initiatives – both generic barriers and innovation-dependent barriers
- A number of focus areas for European governments (including the Netherlands) to reduce or even eliminate the barriers that were highlighted in this study.

2.2 Methodology

Firstly, literature research has been carried out to identify the actors in the European market and the corresponding market developments. To determine the scope of the research, a number of criteria were used to select the actors investigated, namely:

- Their knowledge position within the ecosystem, with lesser focus on geographical distribution of actors;
- Distribution amongst types of actors, namely standardisation and evaluation parties, knowledge institutions, crypto providers and product developers;
- Distribution of actors amongst developments in crypto communication and the techniques covered by it.

For insights into the crypto communication ecosystem within the Dutch market, research conducted for the ‘Nederland Cryptoland’ roadmap was used. For further research into the Dutch cryptography landscape, we refer to this study.

[7] EZK, TNO, CWI and dcypher (2021), *Nederland Cryptoland*, p. 16.

In addition to literature research, six interviews were carried out with select parties (see Annex A), with the aim of verifying findings and uncovering the barriers experienced within the European ecosystem. A broader request for input has been put out, in addition to the interviews, by means of a questionnaire, to which three parties responded (see Annex A and B).

The market survey aimed to provide the most accurate *representation* of the European market possible. Additional research is needed to obtain a full picture of the European cryptography landscape.

2.3 Overarching findings

The conducted market research showed that the previously identified Dutch innovation initiatives (as formulated in the 'Nederland Cryptoland' roadmap) are highly consistent with current innovation initiatives within the European market. The focus here varies by EU country. In Denmark, for example, there is considerable expertise in relation to multiparty computation (decentralised applications) and in France substantial academic research is being carried out into code-based cryptography (post-quantum cryptography). Within the EU, Germany and France in particular have a proper knowledge position when it comes to cryptography.

The conclusions of the 'Nederland Cryptoland' roadmap have shown that the Netherlands have a good knowledge position. In terms of post-quantum cryptography and multilateral cryptography, the Netherlands is considered to be an international leader with an outstanding knowledge position. Moreover, the Netherlands also participates in a 'strong academic ecosystem of internationally renowned universities and knowledge institutions in which the full breadth of cryptography is the subject of research.'[8] This has been confirmed in the conducted literature research and interviews during this market research. The Netherlands has a good reputation within Europe, characterised by strong cooperation. This takes place at both EU and global level. The most pioneering projects in cryptography in Europe are summarised in paragraph 2.4.5 'Pioneering European projects'.

Out of scope for this market research, but nevertheless worthy of mention, are Switzerland, the UK and Israel, with the former two having a strong presence in the cryptography landscape. In addition, Israel has traditionally been strong in cryptography and cyber security on account of historical tensions with its neighbouring countries.

2.4 Ongoing innovation initiatives within the European market

Ongoing innovation initiatives within the EU's crypto communication ecosystem are mapped below under the four developments that have been identified within the cryptography landscape – securing new technical environments, migration to post-quantum cryptography, use of cryptography for new, decentralised applications and formal verification of cryptography and cryptographic source code. Finally, in the last paragraph we take a look at some leading European projects, both completed and ongoing.

[8] EZK, TNO, CWI and dcypher (2021), *Nederland Cryptoland*, p. 14.

2.4.1 *Securing new technical environments*

Our society is digitalising at an ever increasing rate, with more and more products interconnected via the internet and other wireless networks. Examples include the ability to control lights, to lock vehicles using a smartphone app and numerous other IoT (Internet of Things) applications. The demand for securing new technical environments, which in the past had no need for cryptographic solutions, is increasing. In many cases, these solutions involve lightweight cryptography – unilateral cryptography that must be able to run on resource-constrained devices with limited processor capacities, memory storage, etc. This often necessitates new trade-offs in the design and choice of applicable cryptographic methods, as different applications may introduce specific constraints and requirements on the cryptographic solutions. In addition, cost is often the principal consideration in many of these low-end applications, with a need to ensure that the cryptography comes with almost no overhead. To this end, there is also continuous development and optimisation of cryptographic hardware.

2.4.2 *Migration to post-quantum cryptography*

It has been known since the 1990s that the quantum computer poses a serious threat to many of today's cryptographic technologies – the existence of a large-scale quantum computer would mean that many cryptographic methods in use today could be cracked with relative ease. Building such a large-scale quantum computer still remains a challenge. Nevertheless, progress is being made, and existing applications of cryptography must begin migrating to new cryptographic methods that are resistant to quantum attacks.

The field of quantum-resistant cryptography can currently be divided into five streams of solutions, each with different properties:

1. *Lattice-based cryptography* is based on mathematical grids and is one of the foremost candidates for the development of practical post-quantum cryptography on account of its general efficiency and versatility: where other methods are often strong in just one area, such as the speed of encryption/decryption, and less strong in others, such as key sizes, lattice-based cryptography is a good 'all-round' candidate. Examples include Kyber[9] (encryption), Dilithium[10] and Falcon[11] (signatures).
2. *Code-based cryptography* is based on the difficulty of decoding problems, which also appear in the theory of 'error-correcting codes'. This stream is the oldest within post-quantum cryptography, with the McEliece scheme[12] dating from the end of the 1970s. In view of its lengthy existence, but its somewhat reduced efficiency when compared to lattice-based cryptography, this stream is seen primarily as suitable for applications involving highly-classified information.
3. *Hash-based cryptography* is based on the difficulty of inverting cryptographic hash functions. These hash functions are widely used in various cryptographic applications, such as storing passwords and detecting the compromised integrity of data. There is considerable trust in the security of cryptography based on hash functions, as fundamental weaknesses have never been

[9] https://pq-crystals.org/kyber/
[10] https://pq-crystals.org/dilithium/
[11] https://falcon-sign.info/
[12] https://classic.mceliece.org/

detected. The SPHINCS scheme[13] is one of the candidates for the post-quantum standardisation of NIST.

4 *Multivariate cryptography* is based on the difficulty of finding solutions for systems of multivariate comparisons. As with hash-based and code-based cryptography, this stream leads to somewhat reduced efficiency, in this case in relation to key sizes; various attempts have been made to make the cryptography more efficient (e.g. Rainbow[14]), but the additional structure has always caused weaknesses in the security[15]. A reliable, but not quite as efficient system is unbalanced oil and vinegar (UOV).[16]

5 *Isogeny-based cryptography* is based on elliptical curves and their isogenies. This approach is relatively new and still gives rise to slow encryption/decryption algorithms. Like (non-post-quantum) cryptography based on elliptical curves, however, it provides sound efficiency in terms of both key lengths and cypher texts. Examples include SIKE[17] and CSIDH.[18]

Sometimes suggested as an alternative to post-quantum cryptography is quantum cryptography, the security of which is based on the impossibility of certain operations in quantum physics (non-cloning theorem). Systems such as quantum key distribution (QKD) are being researched by numerous parties, but at present offer no viable alternative to post-quantum cryptography. This is because of, inter alia, the need for specialised quantum hardware, challenges relating to long-distance communication, authentication and problems with practical implementations. The use of QKD is discouraged by, inter alia, the national security services in both the Netherlands[19] and Germany[20].

2.4.3 Use of cryptography for new, decentralised applications

New cryptographic methods allow the owner of sensitive data to be separated from the party that will work with those data (performing calculations or verifications), without whoever is working with the data learning more about the data than the owner of the data permits. This offers a range of new possibilities, allowing parties to jointly carry out calculations on sensitive data, for example, without endangering the security of the underlying privacy-sensitive data.

The following streams have been identified within decentralised applications:

1 At technical level, *secure multiparty computation (MPC)* is about carrying out joint calculations on sensitive input data with different parties, without those data having to be shared with all parties. In many cases, numerous parties wish to carry out calculations on personal data to allow them to optimise predictive models, but due to the General Data Protection Regulation (GDPR) and other

---

[13] https://sphincs.org/
[14] https://www.pqcrainbow.org/
[15] Beullens, W. (2022), 'Breaking Rainbow takes a weekend on a laptop', *Cryptology ePrint Archive*, Paper 022/214.
[16] Goubin, L., Kipnis A. & J. Patarin (1999), 'Unbalanced Oil and Vinegar signature schemes', *Advances in Cryptology – EUROCRYPT '99*, p. 206-222.
[17] https://sike.org/
[18] Castryck, W. & T. Lange, et al. (2018). 'CSIDH. An efficient post-quantum commutative group action', *ASIACRYPT 2018*, p. 395-427.
[19] Algemene Inlichtingen- en Veiligheidsdienst (AIVD) (2021), *Bereid je voor op de dreiging van de quantumcomputers*.
[20] Federal Office for Information Security (BSI) (2021), Quantum-safe cryptography: Fundamentals, current developments and recommendations.

privacy legislation, this is not a possibility. MPC offers a potential solution here and within MPC, there are a number of models that are used in practice. Homomorphic encryption uses encryption methods, whereby calculations can be carried out on encrypted data, without the data first being decrypted. Fully homomorphic encryption can be identified as a promising sub-field within this, where arbitrary calculations can be carried out on encrypted data. In practice, however, this comes at the expense of efficiency and practicality. Secret sharing is an alternative stream, whereby sensitive data are 'divided up', with each part giving away nothing about the data contained therein. These divided data are then distributed amongst different parties, which means that none of the parties can see the data but can still jointly process the data. This is possible through the use of joint calculations carried out on their part of the data.

2 At a higher level, *self-sovereign identities (SSI)* are about the secure and privacy-friendly sharing of personal information, helping to enhance the privacy of individuals in digital society. In this model, users have greater control over the sharing of their own data. These data are stored in a mobile application – the SSI wallet – together with their associated guarantees, such as their origin and integrity. Consequently, the data can be used for both sensitive information (BSN, medical data) and non-sensitive information (Netflix login).

Affording the user greater control over his/her data and minimising the quantity of information that is shared helps to meet the requirements of the 'Regie op Gegevens' programme and the GDPR. Cryptography is used to ensure control, privacy and the security of information. Different forms of cryptography are used within SSI, including encryption, digital signatures, zero-knowledge proofs and distributed ledger technologies

3 *Distributed ledger technologies (DLT)* include blockchains and ring signatures and refer to decentralised registers where the same information (often publicly verifiable) is stored in multiple locations. The data are protected by using encryption and digital signatures. In addition, the information is not stored in a single location but is distributed amongst various nodes in the network, which means that there is no single point of failure. Zero-knowledge proofs can be used to publicly verify the integrity of the block chain. DLTs are used in cryptocurrencies as well as in multiparty computation and self-sovereign identities.

4 The use of *zero-knowledge proofs (ZKPs)* is on the increase in the technical field. These are mathematical proofs that a party is able to produce to prove the fact that privacy-sensitive data satisfy certain requirements, without actually having to display the data themselves. An example of the use of ZKPs within SSI is customers in a supermarket proving that they are 18 years of age or above without having to disclose their age or year of birth. In addition to within SSI, this topic frequently occurs within the context of MPC to prove that calculations on encrypted data have been carried out correctly. This also plays a major role in DLTs to prove the fact that an update of the ledger satisfies all rules of the underlying protocol, without having to release too many details about the update in question.

2.4.4 *Formal verification of cryptography and cryptographic source code*

This development is also referred to as computer-aided cryptography (CAC), given that computers help to check the design, analysis and implementation of cryptography. This involves using the power of automation to enable a computer to carry out methodological steps instead of leaving these to a human being. This topic can be subdivided into the following three techniques:

1 *Formal verification of cryptographic primitives.* Proving the formal accuracy and security of a primitive (such as an encryption method) requires considerable effort and practice to both prove the accuracy and for another person to verify that proof. In addition, these proofs are often very technical in nature, which means that minor errors (such as not considering a peripheral case) are easily made. By automating this process, the primitive can be verified more efficiently and without errors.[21]

2 *Formal verification of cryptographic protocols.* At a higher level, high-level protocols should work correctly, whereby these often use different low-level cryptographic techniques. Tooling such as ProVerif[22] allows the user to prove the security features of a cryptographic protocol in an automated fashion with the aid of a computer. An example of this is the VPN WireGuard verified by INRIA with CryptoVerif.[23]

3 *Formal verification of cryptographic implementations*. Finally, it is important to draw a distinction between the cryptographic algorithms (often provided in pseudocode) and actual implementations of these algorithms in a specific programming language. The correct implementation of cryptography is essential owing to the errors that may be made during implementation that could compromise the security of the system as a whole.

   In addition to the need for the implementation to be correct, it is of even greater importance that 'side-channel attacks' are taken into account. For example, by looking at the time that it takes to carry out a decryption, an attacker may be able to deduce from a naive implementation that the private key has certain bits set to 0. The formal verification of cryptographic implementations is, therefore, often about confirming that the implementation is not vulnerable to side-channel attacks. To illustrate, the libjade library[24] is used to ensure that an implementation of a cryptographic primitive is constant-time and memory-safe.

2.4.5 *Leading European projects*

Figure 5 shows a number of projects at EU level relating to cryptography, based on desk research and interviews (see Annex A). We will now highlight a number of leading projects that have been elected because, together, they cover all developments. KYBER-VESI, PRESERVE are EVITA are concerned with the application areas of the value network analysis (offshore wind and automotive). These projects are covered by the *securing new technical environments*

[21] Barbosa, M. & G. Barthe, et al. (2019), 'SoK: Computer-Aided Cryptography', *Cryptology ePrint Archive,* 1393.
[22] https://opam.ocaml.org/packages/proverif/
[23] Bhargavan, K. & B. Blanchet, et al. (2019), 'A mechanised cryptographic proof of the WireGuard Virtual Private Network protocol', *Inria Paris*, p. 50.
[24] https://github.com/formosa-crypto/libjade

development. The other projects referenced here are concerned with the other three developments within the crypto communication ecosystem.

- Horizon Europe (2013-2020) and (2021-2027)[25]
  An EU project that aims to facilitate collaboration and to reinforce the impact of research and innovation relating to the development, support and implementation of EU policy relating to global challenges. A number of projects in relation to innovations in cryptography are being and have been financially supported on this basis. These projects include migration to post-quantum cryptography[26], securing new technical environments (with post-quantum cryptography)[27] and homomorphic encryption[28]. This also includes PROMETHEUS and PRIViLEDGE.
- PROMETHEUS (ongoing)[29]
  'Privacy preserving post-quantum systems from advanced cryptographic mechanisms using lattices'. A research project currently being carried out by CWI with external funding and a number of (international) partners.
- PRIViLEDGE (2018-2021)[30]
  Accomplishment of cryptographic protocols to support privacy, anonymity and efficient decentralised consensus for DLTs. Financially supported by the EU, a number of different EU parties in both the fintech and blockchain domains have contributed to the cryptographic research.
- KYBER-VESI (2016-2018)[31]
  Coordinated by the Finnish research Institute VVT, aimed at developing assessment tooling and the guidelines designed to improve the cyber security of water supplies. This tooling is currently available for use within the Finnish water industry and serves as a tool for ensuring the continuity of the water supply in Finland.
- PRESERVE (2011-2015)[32]
  Also known as 'Preparing SEcuRe Vehicle-to-X Communication Systems', the aim of this project was to contribute to the security and privacy of future vehicle-to-vehicle and vehicle-to-infrastructure communication systems.
- EVITA (2008-2011)[33]
  Led by Fraunhofer Institute for Secure Information Technology and co-financed by the EU, to design, verify and prototype an architecture for automotive onboard networks.

---

[25] https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en
[26] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2022-cs-01-03;callCode=HORIZON-CL3-2022-CS-01;freeTextSearchKeyword=;matchWholeText=true;typeCodes=1;statusCodes=31094501,31094502,31094503;programmePeriod=null;programCcm2Id=null;programDivisionCode=null;focusAreaCode=null;destination=null;mission=null;geographicalZonesCode=null;programmeDivisionProspect=null;startDateLte=null;startDateGte=null;crossCuttingPriorityCode=null;cpvCode=null;performanceOfDelivery=null;sortQuery=sortStatus;orderBy=asc;onlyTenders=false;topicListKey=callTopicSearchTableState
[27] https://cordis.europa.eu/project/id/946280
[28] https://cordis.europa.eu/project/id/644209
[29] https://www.h2020prometheus.eu/
[30] https://cordis.europa.eu/project/id/780477
[31] https://www.vttresearch.com/en/news-and-ideas/new-tools-water-utility-cyber-security-kyber-vesi-project
[32] https://www.preserve-project.eu/
[33] https://www.evita-project.org

2.4.6 Overview

The following page (Figure 5) provides an overview of the players currently in the European market, with an estimation of the share of the market in which they are active. This overview is by no means exhaustive, but is intended to serve as the best possible *representation* of the European cryptographic landscaping. The parties shown have been selected based on their knowledge position within the ecosystem, with lesser focus on geographical distribution within the EU. It would appear that Dutch crypto providers focus primarily on the development of cryptographic hardware. One explanation for this is that the other developments have a lower TRL (Technology Readiness Level), which means that it is still difficult to offer concrete products within those developments.

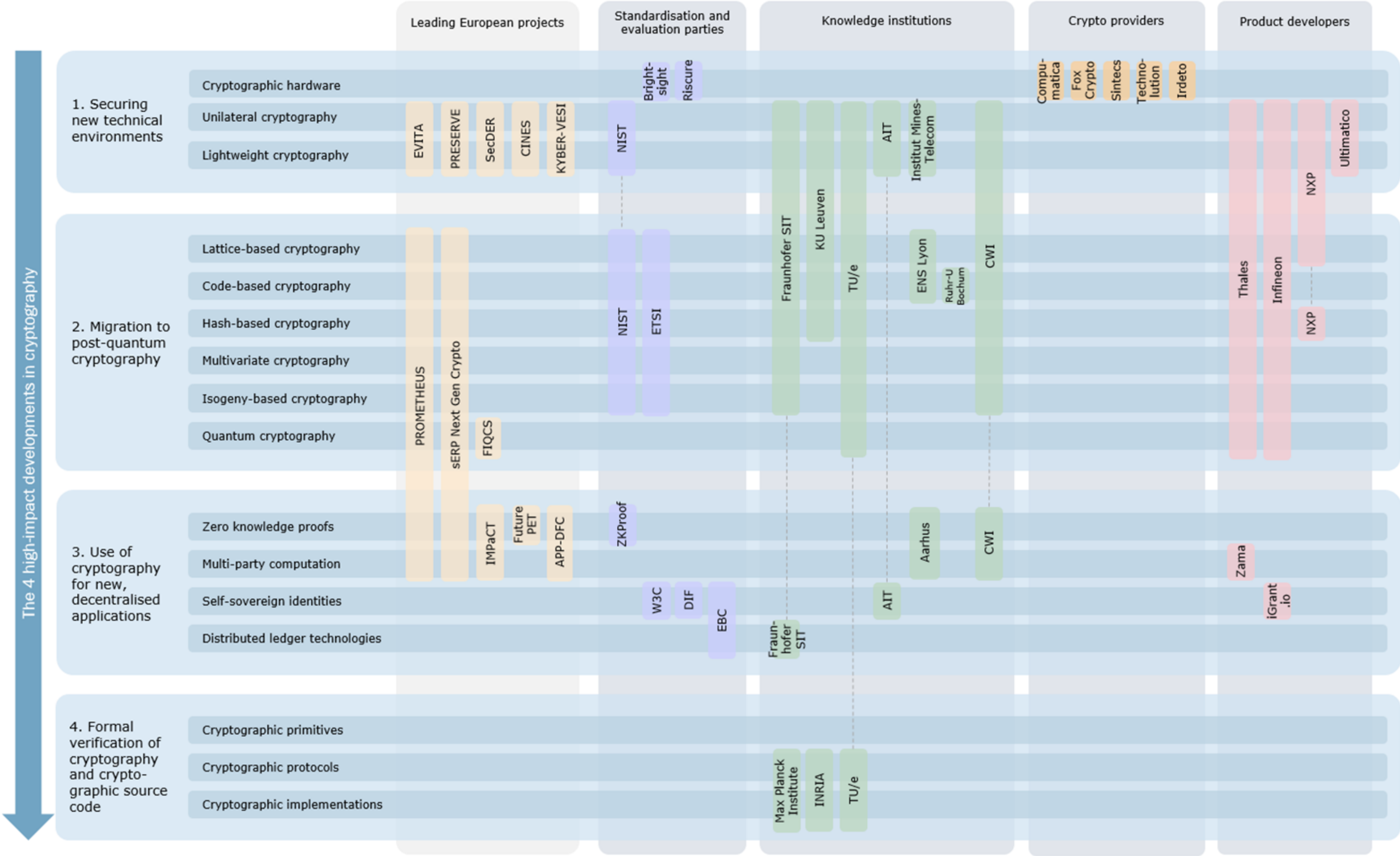

Figure 5 Overview of important players in the European market, with an estimation of the share of the market in which they are active. This overview is not exhaustive and serves as an initial point of departure.

2.5 Barriers for innovations in the cryptographic ecosystem

This survey highlighted various barriers experienced by parties that stand in the way of the development of innovations in the cryptographic landscape. These barriers were identified in particular in the interviews conducted (see Annex A). A distinction is drawn between general barriers, i.e. barriers applicable throughout the cryptographic ecosystem, and barriers that are dependent on development.

The general barriers identified are as follows:

- *Shortage of technical personnel.* A recurring problem that was expressed in all interviews is the difficulty that parties face in finding personnel with knowledge of current developments and innovations in cryptography. Furthermore, these innovations are often absent from the curriculum of bachelor and master programmes, as it is considered a niche area and institutions prefer to devote more time to the transfer of knowledge and to traditional cryptography.
- *'Publish or perish' in the academic world.* In view of the pressure to publish that prevails within the academic world, time and money are mainly devoted to researching a subject that is worthy of publication. This is at the expense of documenting the software that has been developed and researching important, but less spectacular, topics or reporting 'negative' results. As a consequence, researchers often encounter the same problems, such as having to work out for themselves how the software works. As an example, in cryptanalysis, a cryptographic technique not being broken after a certain amount of time is still considered to be a valuable result, even though this cannot be published.
- *Under-investment in cryptanalysis.* As the industry often invests only in cryptography with the potential to earn money (new, more efficient methods that the company itself can use), there is very little investment in cryptanalysis – researching vulnerabilities in algorithms or systems. After all, there is no practical advantage from demonstrating that a system is vulnerable. As sound cryptanalysis plays a crucial role in establishing secure cryptography and in building trust in the underlying methods, it is thus important that cryptanalysis continues to receive investment through other routes.
- *Conflicts of interest in standardisation.* When it comes to agreeing standardisations, there is often a large number of organisations around the table. These organisations all have their own interests and preferences for certain standards, which can give rise to friction and delays.
- *Insufficient collaboration within the EU.* Research into new cryptographic development is carried out primarily by own organisations, with very little collaboration between different EU Member States.
- *Difficulty of achieving crypto-agility in hardware.* In order to be flexible with cryptography and to be able to switch easily to other cryptography, additional space and components are often needed to provide support to different cryptographic methods. As a consequence, a single method is often chosen for cost and performance reasons and innovations experience delays as hardware needs to be fully replaced in order to support new cryptography.
- *Priorities.* Companies generally run a greater (financial) risk in the event of problems with current cryptographic methods and with the surrounding security architecture than in participating/not participating in new cryptographic innovations. Many companies do not, therefore, consider innovation to be

critical to their success and prefer to devote their attention to resolving other security problems.

2.5.1 *Barriers to securing new technical environments.*

During the interviews with different parties, the following problems within the innovative new technical environments were identified:

- *Hardware updates and certifications.* As hardware is often specially made and optimised for certain applications, it can be difficult to carry out modifications/updates for the cryptography that is used/supported on certain hardware. In addition, hardware is often certified and new hardware requires new certification, which means that there is often a preference for continuing to use older hardware.
- *Launching customer.* Some developments lack a ‘launching customer’ who can ensure that the product has been made (properly) and that a new product actually reaches the market.

2.5.2 *Barriers to migration to post-quantum cryptography.*

The following barriers were identified in discussions with parties currently active in migration to post-quantum cryptography:

- *Waiting for standardisation.* Due to difficulties with patent threats, the American standardisation organisation NIST has delayed the announcement of standards for future post-quantum cryptography by more than six months. As companies wish to respond to the new standards, they are having to wait for the standardisation, causing them to delay their migration plans.
- *Minimal regulation.* Many companies view cryptography more as a cost that they have to meet; provided that a product is compliant with the standards, companies are satisfied. As there is currently little/no regulation for post-quantum security, many companies do not yet have this migration on their agenda.
- *Little awareness about urgency.* Quantum attacks and the associated long-term risks require rather technical, specialist knowledge. Many parties lack this knowledge and so do not understand the urgency of this migration. End users need to be given awareness about the risks and associated costs of not migrating to post-quantum cryptography in good time.

2.5.3 *Barriers to decentralised developments.*

The following barriers were identified within decentralised developments:

- *Lack of knowledge amongst cryptographers about legislation.* Although cryptographers often possess the technical expertise about what is possible from a technical point of view, they are not usually familiar with the legal restrictions regarding (encrypted) exchange of data for applications with, for instance, MPC.
- *Lack of knowledge amongst legislators about cryptography.* There is often a lack of knowledge amongst legislators – they may know, for example, what the implications of the GDPR are when it comes to exchanging personal data, but do not know how cryptography can/cannot contribute to help enable certain processes within the legislation.
- *Lack of clarity about standardisation.* There remains a considerable lack of clarity about what needs to be standardised for MPC and there is, as yet, no critical mass in favour of the standardisation of SSI. Standardisation is needed for selecting secure parameters and for the correct use of these methods.

2.5.4 Barriers to formal verification in cryptography.

Finally, we also observed the following barriers relating to formal verification:

- *Tools are created ad hoc, without documentation.* This often requires considerable time investment to ensure that these tools are understood and used and to reuse previously attained results. This is linked to the current low Technology Readiness Level (TRL) of this particular area of innovation, and the fact that the academic world generally under-prioritises the creation of well-documented tools.
- *Little interest in concrete verification for academics.* Linked with the low TRL, the majority of the work is carried out in the academic world, but at the same time that world has little interest in analysing concrete protocols from, for example, commercial parties as it is not considered a result that can be published at an academic conference. Making this applicable is not something the academics can do and steps still need to be taken before the techniques can be widely used in the industry. In addition, concrete protocols often contain a large number of potential states, all of which need to be verified one by one. This means that there is uncertainty as to whether intensive research will lead to a result at any given point in time.
- *Too little awareness about these tools.* There is a considerable lack of familiarity with the existence of formal verification tools and how these tools can be used to gain greater certainty as to the accuracy of the implementations.
- *Clarity about the functionality that needs to be verified.* Formal verification of cryptographic functionalities on hardware requires advance knowledge and clarification of which functionalities are actually there. In many cases, there is little transparency on the hardware side, which means that there are more functionalities than have been documented. In practice, this sometimes leads to incidents, such as Spectre and the Meltdown[34].

2.6 Focus areas for eliminating perceived barriers

Based on the perceived barriers experienced within the European cryptography ecosystem, TNO has formulated a number of areas for EU countries, including the Netherlands, to focus on in the long-term, in order to reduce or even eliminate the barriers highlighted in this study.

- **Train, attract and retain more qualified personnel**
  One barrier that was mentioned repeatedly in the interviews was the shortage of qualified personnel and the difficulty in attracting new people to help shape innovations. Specific points for attention in this regard are:
  - Training more students in crypto communication
  - Promoting greater focus on relevant innovations in the curriculum of university programmes
  - Attracting more cryptographic experts to the Netherlands and/or Europe
  - Providing an attractive working environment so that cryptographic experts stay in the Netherlands and/or Europe

- **The government as a launching customer**
  Some developments lack a 'launching customer' who can ensure that the product has been made (properly) and can ensure that a new product actually

[34] https://meltdownattack.com/

reaches the market. The government could/should assume this role in order to encourage innovations.

- **Less academic pressure on scientific publications within cryptography**
  To prevent the repeated rediscovery of problems with certain approaches/methods and to prevent the loss of knowledge about these setbacks, it is important that research that does not ultimately give rise to a ‘positive’ result is still documented. There is considerable pressure on academics within Europe to publish. Research that leads to results that cannot be published is often not published or not documented at all. In addition, some academics are also involved in standardisation pathways that in many cases do not count as ‘publications’ and are thus less attractive when it comes to encouraging an academic career. Specific points for attention in this regard are:
  - Encouraging the documentation of ‘negative results’ wherever possible
  - Encouraging and valuing other types of contributions to developments within cryptography, such as standardisation initiatives
  - Removing the burden of publication pressure on academics working on crypto communication that contributes to the exclusive focus on publishable results

- **Greater investment in cryptanalysis**
  Where ‘constructive’ cryptography (the establishment of new protocols) is, for commercial reasons, often tackled and steered from within the industry, there is little interest from a commercial perspective in working on cryptanalysis, i.e. cracking systems and testing security – notwithstanding the fact that analysing the security of cryptography is an essential component of the development process. Specific points for attention in this regard are:
  - Investing in more cryptanalytical research, from an academic perspective, in order to safeguard the quality of the cryptanalysis
  - Entering into more collaborations with relevant industrial partners in relation to research into ‘constructive’ cryptography.

- **Regulation relating to post-quantum migration**
  Where it is clear to experts that migration to quantum-secure solutions is essential (and for certain applications even urgent), the industry is primarily concerned about *compliance* – provided that all legal conditions are satisfied, there is no need for further investment in cryptography. In this regard, it is desirable for European governments to put clear regulations in place on (compulsory) timely migration to quantum-secure systems, so that the industry can satisfy legislation and regulations.

- **Encouraging crypto-agile solutions**
  Today’s cryptographic methods are often hard-coded into software and into hardware solutions in particular, which makes subsequent modifications to the cryptography harder to accomplish. This is partly due to a lack of knowledge about the benefits of flexible solutions, and partly due to deliberate choices to save time and money by opting for one solution and implementing it to the optimum. By better emphasising the benefits of crypto-agile solutions, and by filling in any gaps in knowledge, the industry will be in a better position to respond to crypto-agility.

- **Exchange of knowledge between cryptography experts and legislators in relation to decentralised applications and privacy legislation**
  Making it possible for these parties to exchange more knowledge will allow both parties to gain a more comprehensive insight into where the opportunities for cryptographic innovation lie in different domains, where legislation, such as the GDPR, is fundamentally impeding this innovation and where both parties could collaborate to actually accomplish the innovation using the correct methods.

3 Crypto communication value network analyses

In this section, we outline the value network analyses relating to crypto communication within the Dutch automotive and energy industries. More specifically, we focus on direct communication within the automotive industry and offshore wind within the energy industry. Our findings are based on a combination of interviews and literature review and may be used to supplement the crypto communication roadmap[5], which is discussed in Section 4.

Value network analysis is a method of taking a broad look at an innovation ecosystem. This provides a richer picture than a value chain analysis, in which there is a single central actor, as it maps a complex network. A number of roles are visible within this, each of which is mutually connected by means of value exchanges. Each role is fulfilled by at least one actor, which could be a business or an executive body of the government. The value network thus visualises the different relationships within the ecosystem and focuses not only on money, but on other values, such as knowledge, personnel and innovative strength. In addition, it could also help to provide insight into partnerships and barriers.

A value network analysis is also a suitable method of mapping a complex innovation ecosystem in a structured fashion.[35] Innovation in crypto communication within the offshore wind and automotive industries takes place through a variety of different parties, interests, relationships and knowledge areas. A value network analysis can depict the dynamics of these relationships in more detail than, for example, the traditional value chain analysis, which takes a more process-oriented look at a single-actor ecosystem.

For this study, we opted to carry out a value network analysis for two industries – the Dutch energy industry and the Dutch automotive industry. These are part of the category A and category B critical infrastructure respectively.[36] Both industries contain physical infrastructure that will last for many decades, which means that it is essential that both cyber security and cryptography are in place and can be updated as needed. This is because there is no way of predicting what level of computing power, including quantum computing, might be available in the year 2040 that could be used for hacking. At the same time, this also acts as a motivation to look more closely not only at the security of new technical environments, but at the applicability of post-quantum cryptography (PQC), as referred to in paragraph **Fout! Verwijzingsbron niet gevonden.**.

It is important to note that the value network is a snapshot in time of an ecosystem that is in a constant state of flux. To ensure the findings remain up to date, a value network needs to be periodically evaluated and assessed.

[35] Allee, V. (2008), 'Value network analysis and value conversion of tangible and intangible assets', *Journal of intellectual capital*, Vol. 9, Issue 1, pp. 5-24.
[36] https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen

3.1 Methodology

The following is a brief description of the method used for the value network analysis. The method comprises four steps which are specified in figure 6. Below, we explain the goal of each step.

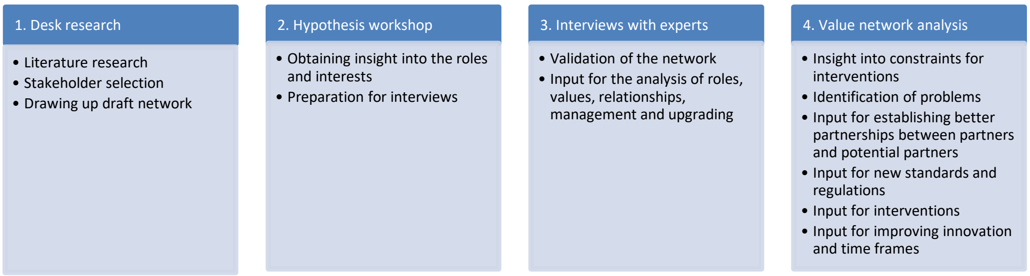

Figure 6 Methodical approach for a value network analysis.

Step 1: Desk research
The aim of the desk research is to identify stakeholders and to establish basic knowledge about the value network and the corresponding roles and value exchanges by means of a literature review. This helps to form a picture of the way in which the ecosystem functions and of the existing problems from an independent perspective. The results can then be used to prepare a draft of the value network. This will be further detailed and validated in the steps that follow.

Step 2: Hypothesis workshop
The next step is a hypothesis workshop. The aim of the hypothesis workshop is to establish and discuss hypotheses about the interests and dynamics of the stakeholders in the value network, within the project team. The hypotheses are constructed with regard to the way in which the value network works – the most important roles, values and interests. This serves as preparation for the interviews with experts in the next step. It also serves as a basis for assessing the impact for the various stakeholders. In addition, it also ensures that all team members have a common basic level of knowledge.

Step 3: Interviews with experts
The next step is interviews with experts who are a part of the organisations that play a particular role in the network. In this case, these could include chief information security officers (CISOs) and/or products owners of (cryptographic) software products. The aim of the interviews with experts is to collate the information required for the validation and further expansion of the value network. Each expert brings his/her own piece of the puzzle from his/her own perspective and together they form a nuanced picture of the functioning and dynamics of the overall ecosystem. Finally, the results of the interviews are also validated wherever possible and further expanded with findings from the literature review.

Step 4: Value network analysis
The final step is to put together and analyse all of the information that has been collated. The results of the interviews are used to adapt the value network and to draw conclusions about the way in which the ecosystem functions. The distribution

of power, imbalance and value transactions between stakeholders, barriers and problems within the system are then made transparent.

To the fullest extent possible, interviews are focused on the use of crypto communication in both industries. If, however, this scope was too narrow for an organisation's representative, the questions will be adapted to focus on cyber security and secure communication as a whole. This is because the same dynamics and barriers play a role. An overview of the parties to whom we spoke for the value network analysis can be found in Annex A.

3.2 Industry: Offshore wind

3.2.1 Introduction

As part of the energy transition, the Netherlands has set ambitious goals in terms of the generation of renewable energy. Offshore wind is category A critical infrastructure. Dutch legislation applies to an area extending from the land to twelve miles out to sea, which makes protection against bad actors a national responsibility.[37] Beyond this, however, there is a grey area in which the responsibility for protecting the infrastructure is unclear.

The installation of wind farms is an incremental process, with limited space available due to the need to take fishing, military, shipping, sand extraction and nature conservation activities into account.[37] As soon as it is known where a wind farm can be installed, a call for tenders is put out to private parties to lease the site and actually install the wind farm. This means that wind farms belong to different, competing parties, each with its own partners and operators. In addition, many of the parts of wind energy converters themselves are produced in Asia.[38] This means that each wind farm may have its own physical parts and, most importantly in this context, its own cryptographic solutions.

Irrespective of which private party actually installs the wind farm, TenneT, as the transmission grid operator, is responsible for installation of the infrastructure (including the high-voltage cables at sea and the transformer stations) that allows the wind farm to be connected to the onshore electricity grid. This introduces a familiar 'tension field' for the cyber security of operational technology, which includes all physical infrastructure.[39] In this case, there is a need for a trade-off between remote management and the possibility of bad actors gaining access and negatively affecting the stability of the network.

In turn, the electricity market is extremely competitive, which means that private parties have an incentive to share as little information that could affect this market as possible, such as the amount of electricity that is (expected to be) produced and the times at which maintenance is carried out. The closed market dynamics give rise to a lack of transparency, which goes against the idea of uniformity within cryptography. In addition, parties are sometimes forced to switch certain wind energy converters on and off if significantly more or less electricity is being

[37] The Hague Centre for Strategic Studies (2021), *The High Value of The North Sea*.
[38] Straver, F. (2017, 29 November), Windlobby waarschuwt: Aziatische massamolen hijgt Europa in de nek. *Trouw* (https://www.trouw.nl/duurzaamheid-natuur/windlobby-waarschuwt-aziatische-massamolen-hijgt-europa-in-de-nek~b30cf380/)
[39] TNO (2019), *Succesfactoren voor digitaal veilige Operationele Technologie* (TNO 2019 R11304)

produced than expected, as this can disrupt the balance in the electricity grid. This remote access can then be used as an attack vector.

3.2.2 *Results*

Figure 7 shows the value network relating to crypto communication within the Dutch offshore wind industry. This shows the valorisation chain of offshore wind farms, from left to right, including the parts that play a role in crypto communication. In addition, it also broadly outlines the supply chain of offshore wind energy converters and electricity, surrounded by the ecosystem for crypto communication innovations. The roles that are fulfilled in the ecosystem and the value transactions between them are visualised here using nodes and connections respectively. The network is specifically focused on roles and transactions that are directly involved in offshore wind energy and excludes parties who are responsible for maintaining the (other) onshore network. The value network of the entire electricity industry, including distribution operators and consumers, has been outlined in an earlier study.[40]

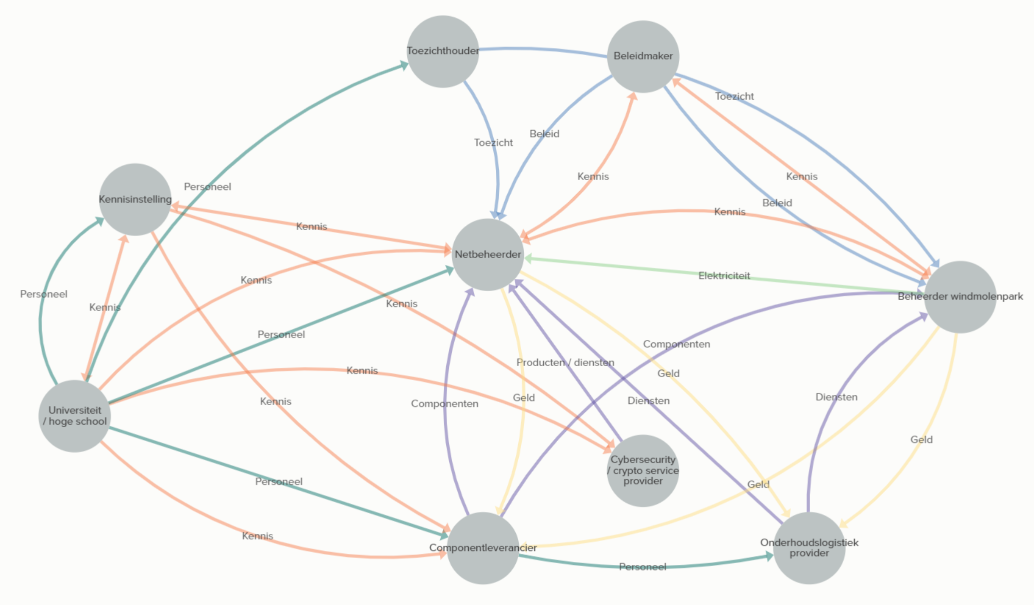

Figure 7 Value network for the offshore wind industry.

Some of the characteristic dynamics that are visible in this value network are:

- In terms of value exchange, the (transmission) grid operator is central to the value network. Consequently, it has a defining, guiding role in the ecosystem and the ability to influence innovation within communication. This stems from the requirements that they impose in tenders in respect of market parties, in which they can provide some guidance relating to priorities and room for innovation.
- Financial support for products for which cryptography is relevant comes primarily from the operators of wind farms and from the grid operator (the customers in this context).
- There are no visible gaps in policy and/or supervision for this ecosystem, as there are lines of communication to the most important actors.

[40] TNO (2020), *EZK Verdieping Valorisatieketens: Verkenning van het ecosysteem en waardenetwerk Automated Security* (TNO 20220 R12224).

- Expertise and personnel enter the ecosystem primarily from universities and knowledge institutions.
- Component suppliers are central to the supply of parts for wind energy converters. Subsequently, these play a role in maintenance by deploying their own experts.

The key findings from our value network analysis have been categorised into three groups – general findings, drivers of innovation and barriers. These are individually outlined below. The findings are partly descriptive of the current ecosystem, but also contain proposals for changes that the interviewees consider desirable.

3.2.2.1 General findings

- **'Traditional' convergence of operational technology (OT) and information technology (IT) is also characteristic of offshore wind.**
  OT has traditionally been crucial to the energy industry, but IT has become increasingly important over time as a result of digitalisation and automation; new OT includes IT elements *by design* and IT components are being added to old OT. The addition of IT brings with it many benefits (such as improved efficiencies and remote management), but there are a number of areas where it creates challenges:
  - In principle, OT hardware must be as simple as possible so that it can be used for decades without the need for major changes or additions, and must be able to run without disruption (security of supply). Things are different for IT, which needs to be updated at regular intervals. It is difficult to find time to install patches on wind energy converters as doing so requires the converter to be shut down, but it remains essential from a cyber security perspective.
  - Innovation in the field of OT is generally (much) slower than in the field of IT. OT components typically have a lifecycle that extends over many decades, while IT components, including software, may become obsolete after just a few years.[41]
  - Working with OT or IT in the energy industry requires varied and specific knowledge. The integration of cryptography lies at the interface of these two fields and having specialist knowledge of both areas is essential to understanding it properly. Personnel with this kind of knowledge are difficult to come by and at the same time, highly sought after by multiple parties in the ecosystem.

- **Crypto communication is relatively new in this industry, but will play an increasingly important role in the (near) future.**
  - Research and experiments being carried out by parties in the ecosystem *are* focusing on cryptography for offshore wind, but there is nevertheless a general need to raise awareness about its importance. As digital communication is an ever-present reality in this industry, the use of good cryptography and innovation into it will become inevitable.[42] The topic is discussed in industry-wide meetings, for example, but does not yet have high priority.
  - There is currently little need for innovation in crypto communication. Transport Layer Security (TLS) is currently used by many parties as a de-

[41] https://www.digitaltrustcenter.nl/informatie-advies/operational-technology
[42] A. Aazami, (2021), Digitalisering en energie: Méér dan de som der delen.

  facto solution. Consequently, most communication in practice can be properly secured using TLS, with the exception of firmware management. There is very little demand for innovative network security from the majority of parties.
  - Communication for offshore wind takes place over both WiFi and fixed-line connections, but the data that are communicated are seldom of a highly sensitive nature, thus reducing the likelihood of an attack. For the time being, the most crucial communication in this industry is not over the internet but over closed, private networks, which sometimes makes the physical security of infrastructure more relevant in practice than cyber security, including cryptography.

- **All wind farms are supervised by the Radiocommunications Agency Netherlands (AT) via the Network and Information Systems Act (Wbni).**
  - The limit for parties covered by this particular supervision is the point at which production exceeds 100 MW. In view of the fact that modern wind energy converters produce around 10 MW of energy, this limit will always be exceeded by operators of offshore wind farms. In contrast to onshore wind, therefore, the problem of small, decentralised producers falling outside of this supervision does not exist in the offshore wind industry.
  - Operators of wind farms indicate that in certain areas, more supervision and more frequent testing may be preferable. Energy networks are becoming increasingly dynamic and fluctuate more, which means benefit may be gained from more frequent testing of a network to check that it continues to satisfy security standards and requirements. At a sub-station or medium voltage, there is a big difference between a consumer constructing a wind energy converter and an entire offshore wind farm.

- **Standardisation for this particular field is complex and ambitious, which may deter many manufacturers.**[43]
  Some frameworks or minimum requirements that must be satisfied could be enough to prevent limitations to innovation.

3.2.2.2 Drivers of innovation

- **Security of supply and regulatory compliance are the most important drivers of innovation in cryptography.**
  - The principal reason for improving crypto communication is to enhance the security of supply by minimising the risks of cyber-attacks. There are (hefty) financial penalties for non-compliance with market agreements on electricity supplies, and large-scale failure of infrastructure additionally leads to substantial societal damage on top. Prevention is thus extremely important and one of the main drivers of innovation.
  - For the time being, one of the principal aspects on which wind energy converter (component) and station producers compete is price. As such, there is a trade-off between the level of cyber security in place and costs involved. As price is a deciding factor in a free market, cyber security does not always have top priority, so long as it meets the minimum requirements.

---

[43] CE Delft, TNO en Quintel (2021), *Afspraken maken: van data tot informatie, Informatiebehoeften, datastandaarden en protocollen voor provinciale systeemstudies – Deel II technische rapportage.*

- Operators of wind farms and the transmission grid operator are, to one extent or another, researching the impact of quantum computing and post-quantum cryptography, but are also waiting on the NIST to publish the standards (at the time of writing, only the prospective algorithms have been announced). They do not engage in innovation of cryptography themselves, and generally prefer secure and proven solutions. This means that they do not take a leading role in cryptographic innovation, but they do remain up to date on important trends and future patterns in the field.
- Innovation is primarily carried out by cyber security service providers and the manufacturers of hardware components. Station and wind energy converter construction is often outsourced to contractors and sub-contractors, with the cyber security requirements lacking detail in their definition. This provides space for new solutions and innovation, but within the frameworks created by price competition.
- The government has begun preparations for a nationwide programme to implement post-quantum cryptography now that the NIST candidates for standardisation have been announced. This is anticipated to be a multi-year process, starting with implementation of PQC within the government itself, but which could later be translated to critical infrastructure.

- **For offshore wind as a whole, relatively little policy currently exists, aside from a few European directives.**
  As the North Sea is extremely busy and is likely to become busier still, with the need for the exchange of large amounts of information, there is huge economic potential. A lack of policy could ultimately become a barrier if it is not addressed in time.

- **Innovation and knowledge sharing are driven and stimulated by partnerships** such as dcypher, in which cryptography suppliers, universities and knowledge institutions are involved.
  - There is some degree of knowledge sharing with competitors by operators of wind farms, primarily at a highly abstract level in order to identify solution directions or to carry out peer reviews, but not for the procurement of specific components (in order to prevent the formation of cartels).
  - Component suppliers undertake considerable in-house development, but also collaborate with universities and other suppliers on cyber security innovations.
  - The grid operator has considerable knowledge within the organisation. Nevertheless, there are, to some extent, collaborations with universities on cyber security innovation.
  - At international level, relevant knowledge is also shared within the framework of existing partnerships and programmes.

3.2.2.3 Barriers

- One thing that emerged during discussions was the **shortage of personnel with combined knowledge of cyber security (IT) and the energy field (OT) throughout virtually the entire chain.** The number of people who possess this combined knowledge is relatively small, and all parties within the ecosystem are competing for that knowledge.

- **The Netherlands has a fairly small cryptography market**, and Dutch cyber security start-ups are frequently acquired by foreign companies, further weakening this position. [44, 45]

- **Security of supply and maintenance can cause friction, which can also impede innovation.**
  - A goal is to keep OT as simple as possible for performance, while adding IT can improve it – although the link to IT in turn creates new security risks.
  - In addition, the converter needs to be shut down for (major) maintenance, which is something that is avoided to the fullest extent possible. The more patching, the more secure the system can remain, but also the greater the impact on the supply (and thus the market), which means that patching is often delayed.

- **Market parties often fail to see the importance of crypto communication as they focus more on the relatively short term.** Similarly, application is not enforced by policy. In the longer term, this topic is expected to become more relevant, such as with the emergence of quantum computers, although the investment time frames are currently too short. There is, to a certain extent, a lack of a sense of urgency and, additionally, budgets do not constitute a bottleneck when it comes to cyber security innovation.

- **At some levels, there is limited communication between certain parties in the ecosystem, such as in relation to maintenance.** Communication is relatively fragmented and takes place on a one-on-one basis in agreements with component suppliers and providers of logistics services. Improving this could benefit all stakeholders, thus making the maintenance of digital solutions more cost effective overall.

3.2.3 Conclusions

In the offshore wind industry, digital communication takes place on a vast scale, something that is expected to accelerate in the decades to come. The merging of OT and IT brings with it new safety risks and requires hard-to-come-by personnel with specialist knowledge of both areas. Cryptography is a topic that comes up regularly during discussions between parties in the ecosystem, but does not have top priority. The requirements for cryptographic solutions are mainly imposed by the transmission grid operator and operators of wind farms, both of whom are then covered by policy and government supervision. Consequently, innovation in cryptography is driven primarily by the suppliers of hardware components. Ultimately, price also plays an important role when it comes to procuring infrastructure. Finally, this research has identified a number of distinctive barriers that could give rise to concrete recommendations to help shape the roadmap.

3.3 Industry: Automotive

3.3.1 Introduction

The transformative effect of digitalisation also has a sizeable impact on the automotive industry. As vehicles transition from being fully mechanical devices to

[44] https://www.agconnect.nl/artikel/techleap-dit-heeft-nederland-nodig-om-techstartups-meer-te-stimuleren
[45] https://executivefinance.nl/2022/05/buitenland-tuk-op-onze-startups/

'driving computers', the infrastructure of the road network is also transitioning – from a static state to a fully dynamic state. This is all necessary to allow vehicles to communicate with one another and with their environment, something that is known as V2X communication. V2X (vehicle-to-all) communication mainly comprises V2V (vehicle-to-vehicle) and V2I (vehicle-to-infrastructure) communication. The former facilitates the operation of autonomous vehicles and helps to prevent collisions, while the latter can be used to realise time-critical and safety-critical applications, such as congestion-state detection, and to optimise the movement of vehicles in traffic, which in turn helps to minimise emissions and congestion. These new forms of communication do, however, introduce an immediate need for the right form of cryptography. There is the possibility of unnecessarily distracting a driver with notifications about relatively innocent systems. The more advanced driver assistance systems (ADAS) are integrated into vehicles, including blind spot monitoring and parking sensors, the more the risks of distraction increase. It is also important to realise that these ADAS systems are the first step towards autonomous vehicles.

The greatest safety risks are in the electric control units (ECUs) responsible for acceleration, braking and steering[46]. Securing communication via which motion-related decisions are made at high speed is important, because human life could be at risk if mistakes are made. Malicious actors also have the potential to cause enormous damage if they are able to manipulate information. In addition, the integration of communication technology, such as chips and SIM cards, into vehicles also offers greater opportunity for vehicle theft, such as by hacking the digital access key through a combination of sniffing and spoofing. Finally, espionage and privacy also play a key role as vehicles will increasingly monitor and store more sensitive data.

There are various entry points for someone wishing to hack a vehicle; the manufacturer could create an entry point by overlooking incorrect software or by leaving back doors into the integrated communication technology, and dealers and garages are also potential weak links. These both have access to the hardware and software via advanced tools. Hackers could capitalise on the less secure locations of dealers and garages to try to gain access.
Chips in vehicles can be hacked by gaining physical access, but due to increasing connectivity of vehicles via methods such as Bluetooth, WiFi and SIM cards, there are ever more ways to gain access to vehicles remotely.

If every device (both vehicles and infrastructure) were to use a cryptographic solution, single point of failure would not put a large proportion of users at risk. The same also applies to V2I server platforms, for example, which can provide access to large numbers of sensors.[47]

Another risk to the cyber security of vehicles is their long lifecycle. Where some 'regular' IT consumer goods need to be replaced after three to five years, vehicles typically last for ten or even 30 years. Over this lengthy period of time, cryptographic algorithms or decryption techniques may be developed that did not previously exist, such as post-quantum cryptography. Society's developments and

---

[46] https://www.saksen.com/insights/white-papers/automotive-security
[47] https://cybersecurity.ieee.org/blog/2017/06/28/christof-paar-on-why-cryptography-is-key-for-automotive-security/

safety threats also apply to older vehicles, which have to both deal with them and satisfy new standards at the same time. Providing hardware and software that can be upgraded is, therefore, important, at the risk of the patch mechanism itself being hacked. After all, vehicles spend a lot of their time in public, unmonitored areas, thus making them easily accessible to bad actors.

In addition to cryptography, intrusion detection prevention schemes (IDPS) also have an important role to play in security. These are systems that monitor for anomalies in communication, something that may point to unauthorised access or device manipulation. These can be integrated into vehicles with relative ease and, most importantly, involve considerably reduced cost. Ultimately, a blend of multiple, independent security mechanisms will be able to offer the most effective overall package.

From a cryptographic perspective, the automotive industry has a number of unique challenges, such as the high variability of the network, the fact that all communication takes place wirelessly and the need to exchange information and make decisions at high speed.[48] From a security perspective, it is important that the authentication of messages and driver privacy are safeguarded, that information and communication are always available and that the right level of confidentiality is maintained. Only certain parties should be permitted access to sensitive information, such as the police when investigating an accident.
Finally, the automotive industry is highly competitive and uses both safety and ADAS as a unique selling proposition. The cyber security of the technology used is, however, of secondary importance to its function, and the risks of inadequate cyber security are not (yet) visible. OEMs are not expected to be forthcoming in this regard, as this could harm their developments in autonomous driving. This means that the risks may only become visible afterwards, when they have already given rise to damage. As a result, it may be difficult to pass on the additional costs incurred during innovation of cyber security to customers.

3.3.2 Results

Based on the value network analysis for the automotive industry, it can be concluded that the value network for crypto communication within the context of (direct) V2X communication cannot currently be outlined. Most projects are currently in pilot phases (low TRL) and there is currently no valorisation chain, partly because legislation and standards in this area do not yet exist. Due to the early stage of (technological) development, it is still unclear how the innovation ecosystem will look in the future and what players, market dynamics, partnerships, opportunities and barriers are likely to play a role. A value network is not, therefore, a suitable means of mapping the ecosystem, considering that the valorisation chain is still to be formed. In addition, we did not succeed in speaking to the two most important Dutch vehicle manufacturers, DAF and VDL, during this study, which means that we have been unable to verify whether or not they endorse these findings. Nevertheless, we will explain the findings that the survey did bring to light in this section. These offer a number of interesting insights into the current dynamics relating to cyber security innovation in the industry. The findings have been categorised as general findings, barriers, drivers of innovation and findings relating to the ecosystem. The findings are partly descriptive of the current

[48] https://www.hindawi.com/journals/wcmc/2018/1640167/

ecosystem, but also contain proposals for changes that the interviewees consider desirable.

3.3.2.1 General findings

Cryptography in the automotive industry could be a (future) market to exploit the Netherlands' leading edge in cryptography, but there is currently a large number of technical and non-technical barriers. Consequently, innovation for cryptography in the automotive industry is still in its early stages of development (low TRL), with collaboration between parties taking place primarily in (European) consortia. Topics like post-quantum cryptography are not on the radars of any of the parties spoken to for the coming years.

In the future, self-driving cars will not be responsible for gathering all sensor information themselves, but will communicate the information available both amongst themselves and with the environment to help them make the right decisions. This makes securing connections and authenticating the sender of messages the principal aim for now, with cryptography being only one possible means of achieving this level of security. Commodity products are currently the most used: TLS and solutions that use certificates. These technologies are tried and tested, already longstanding and undergo scarcely any innovation. They are also more cost effective than state-of-the-art, innovative cryptography solutions that are still to be developed. If there is little to no communication between vehicles and infrastructure in practice, there is no need for innovative cryptography. The drawback is that the tried-and-tested technologies are not resistant to quantum technology, and will introduce a lack of security in the long term, when used in vehicles. It is difficult to assess the time frame for when this innovative cryptography will become relevant. The anticipation is that if functional and technical guidelines are put together and if parties collaborate intensively, a snowball effect will occur and V2X crypto communication will occur within a time frame of around 20 years. As referred to above, quantum computing will have a facilitating effect on the development of crypto within the automotive industry on account of the higher communication security requirement.

The current picture is of a primarily incremental advance in cryptographic innovation and of a need for time to respond to the many complex issues within different domains. Within this, a combination of technological innovation, standardisation and policy have an important role to play. The incremental innovations could be accelerated by forming a shared long-term vision for smart infrastructure, in collaboration with different parties in the ecosystem and by making functional agreements on which to build. The newly launched Digital Infrastructure for Futureproof Mobility (DITM) project can contribute to this. One of our findings is the possibility of market opportunities for cryptographic products in smart infrastructure presenting themselves in the near future. In fact, cryptography is already essential to smart infrastructure as a means of ensuring secure and effective communication.

3.3.2.2 Drivers of innovation

Despite the large number of challenges that need to be resolved before the valorisation chain can be formed, there are a number of key drivers of innovation. First and foremost is the efficiency perspective. With self-driving vehicles, we could drive more efficiently and ensure better traffic flows. This would mean that we need less energy to cover the same distance[49], in turn helping to reduce emissions, inter alia. Another driver of innovation is the desire to improve road safety by being able to prevent or correct (estimation) errors. Driving could become safer overall on account of the interconnectedness of the entire smart infrastructure.[50] [51]

In addition, electrification within the automotive industry also offers opportunities for innovation in cyber security. With innovation pressure being exerted by disruptive parties, established companies are also finding themselves forced to innovate (technologically) in order to survive, which offers opportunities for the implementation of cryptographic systems. Moreover, new earnings models will also be created within the chain, such as (remote) software updates. In addition, the European Commission has also set a target of uninterrupted implementation of 5G by 2025, which will act as an incentive for the roll-out of smart infrastructure. Research has indicated that in the Netherlands, fifteen per cent of vehicles could have SAE level 3 or above by 2030.[52] [53]

3.3.2.3 Barriers

Generally speaking, there is currently a lack of shared vision about the development of V2X communication in the automotive industry, which means that parties are left to prepare for the future of self-driving vehicles and smart infrastructure independently. Parties in the ecosystem also focus primarily on the existing product range and core activities.[54] The current market-share holders have a strong brand with associated products and are currently facing up to a great many challenges, including the impact of the pandemic and a shortage of chips on production lines. To add to this, disruptive technologies have the potential to create power shifts that are not to their advantage. It is perfectly plausible that the major market-share holders will wish to ‘ride on the coattails’ of early adopters who have seen success. These run a risk, however, as the implementation of new technology can also give rise to image damage. If something goes wrong with the technology, causing consumers to perceive the vehicle as unsafe or more unsafe than other brands, the brand will subsequently lose value. Introducing new high-risk functions is of greater strategic interest if it is enforced by policy or by the market.

For many consumers, cyber security is also a passive requirement and is seen as a minimum that must be met – it only serves as a very limited incentive when it comes to purchasing decisions. This has an impact on both vehicle manufacturers and

---

[49] Sieber, L., Ruch, C., Hörl, S., Axhausen, K. W., & Frazzoli, E. (2020). Improved public transportation in rural areas with self-driving cars: A study on the operation of Swiss train lines. Transportation research part A: policy and practice, Vol. 134, pp. 35-51.
[50] Kalra, N., & Groves, D. G. (2017), The enemy of good: Estimating the cost of waiting for nearly perfect automated vehicles.
[51] Teoh, E. R., & Kidd, D. G. (2017), ‘Rage against the machine? Google's self-driving cars versus human drivers’, *Journal of Safety Research*, Vol. 63, pp. 57-60.
[52] J3016_202104: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles - SAE International
[53] Milakis, D., Snelder, M. and Arem, B. (et. al.) (2017), ‘Development and transport implications of automated vehicles in the Netherlands: Scenarios for 2030 and 2050’, *European Journal of Transport and Infrastructure Research,* Vol. 17, pp. 63-85.
[54] Hofstätter, T., Krawina, M., Mühlreiter, B., Pöhler, S., and A. Tschiesner (2020), ‘Reimagining the auto industry’s future: It’s now or never’, McKinsey & Company (https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/reimagining-the-auto-industrys-future-its-now-or-never)

component suppliers. Component suppliers suggest that manufacturers tend to be enthusiastic about the functionality if it helps to sell a vehicle, but that they do not necessarily want to have to pay extra to integrate cryptography functionality into chips. These functionalities are, in some cases, even integrated into products in principle, whereupon customers must deactivate them manually. Cryptography is seen only as one part of a whole that ultimately needs to be secure.

A related reason explaining why there is less economic pressure to innovate is the cost. Given the commercial interest in profits, minimal security procedures will be implemented in order to drive down costs. The price is often a leading factor, which means that the ‘minimum viable’ solution is often the one that is chosen. The current cost of innovation and the limited functionality that cryptography currently provides, in combination with the complexity of expressing the corresponding increase in security in monetary values, means that it is difficult to formulate a positive business case. As such, there is little economic incentive for industry parties to concern themselves with something like cryptography, which it is expected will need to be enforced primarily through legislation and standards – which take considerable time to develop.

The long lifecycle of vehicles means that the entire lifecycle needs to be taken into consideration, from the point of production onwards; technology and/or software that are/is integrated into vehicles must be capable of lasting for 30 years without difficulty. This should also allow for the integration of new components and/or functionalities at a later point in time. Within the context of crypto communication, for example, cryptographic protocols will need to be updated. In addition, retrospective parts will also need to be added to existing vehicles (in some cases) in order to enable V2X communication. Current shortages of chips are impeding their roll-out in both cases.

Finally, cyber security companies are having to deal with a shortage of personnel and there is insufficient knowledge within the rest of the market to absorb innovation in this field. Knowledge and expertise are highly concentrated and, in many cases, highly specialised, putting the brakes on innovation.

3.3.2.4 Findings relating to the ecosystem

The interviews also considered the role of players within the landscape, giving rise to the following analysis for cooperation and promotion of the ecosystem. An overview of relevant parties within the (Dutch) ecosystem is provided in figure 8.

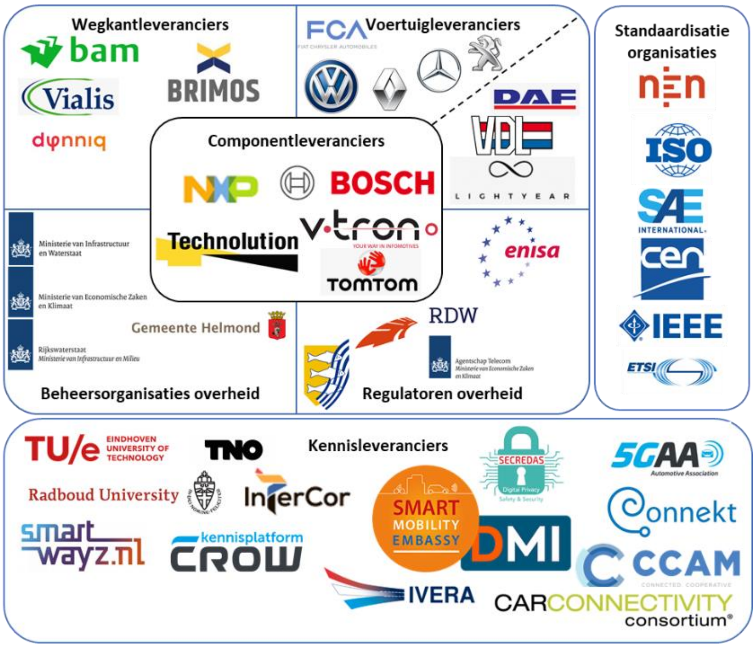

Figure 8 Overview of parties who play a role in the automotive ecosystem[55].

Knowledge providers, such as universities, are highly active in the field of cryptography, as indicated in Section 2, but there is, in some cases, a lack of connection to the market. As an example, they are not actively approached by vehicle suppliers/original equipment manufacturers (OEMs) to have their research into message encryption integrated into products or to share knowledge. Generally speaking, vehicle suppliers play a passive role in this ecosystem. In addition, they often have a lot to lose in terms of image and market share and very little to gain, as they have already achieved success and may be somewhat reluctant to share information. They are not only eager to protect their intellectual property, but wish to handle (customer) data as securely as possible. Consequently, OEMs operate in relative isolation, even though collaboration between OEMs and surrounding parties in the ecosystem is essential to developing integrated solutions. To encourage them to share information, government policy may be needed. Open innovation (e.g. open source software) may be a suitable means of encouraging collaboration and innovation, but the question is whether this will succeed with the rather conservative and ‘closed’ attitude exhibited by vehicle manufacturers.

Government regulators are primarily concerned with risk management. As cryptography is not yet an active component of the automotive industry, it is not yet subject to monitoring in this industry. Component suppliers indicate that they are followers in this ecosystem. As an example, although they design chips with cryptography functionalities, they tend to find that customers disable them or are not interested in those functionalities. Standardisation organisations such as NEN and ISO are beginning to develop standards. Suppliers of infrastructure, such as charging stations, are also active in cryptography innovation and there are a number of ongoing European initiatives as well as collaboration in cyber consortia. They suggest that security is becoming increasingly important within the charging

[55] TNO (2022), *Crypto for Automotive – WP1 Report: Toepassing cyrptografie in directe automotive communicatie* (published Q4 2022).

infrastructure, also on account of the tenders, in which a high level of security is a requirement.

Infrastructure managers within the EU are progressive within their fields, but do not wish to be ecosystem pullers. According to the findings of the interviews, it costs too much and takes too long to develop all collaborations, and doing so is too far removed from current tasks. There is, however, knowledge of functional and operational requirements amongst these parties, which means that they can play an important role in establishing the vision for the future. Rijkswaterstaat (Ministry of Infrastructure and Water Management) sets primarily functional requirements, with the precise interpretation left to market parties. Governments, network operators, infrastructure managers and service providers actively cooperate with industry organisations, such as field labs and cyber consortia.

Finally, major technology companies, such as Amazon and Google, have the network, means and opportunity to increase their market share by investing in smart infrastructure. They could play a disruptive role within the innovation ecosystem, but this would raise questions relating to data privacy and deprive the government of the opportunity to take a leading role and to set standards.

3.3.3 Conclusion

Cryptography could play an important role for the automotive industry in the future, but does not yet have that role at the moment. There are still a large number of both technological and non-technological challenges that need to be resolved before V2X communication can be applied on a wide scale. According to the interviews, cyber security is currently secondary to functionality; there is still relatively little collaboration in the ecosystem and the playing field is highly fragmented. None of the parties wishes to take responsibility if something goes wrong, which means that parties have a tendency to ‘point the finger at one another’ (government at industry and vice versa). This is quite remarkable, as physical security has a high priority within the automotive ecosystem. In conclusion, we can state that if an ecosystem that promotes cyber security innovation is to be established, it would be a good idea to offer encouragement to players within the ecosystem who already have an existing network and can capture market share.

3.4 Overarching results

Considering that both industries are part of the critical infrastructure of the Netherlands, it would be interesting to conclude by briefly looking at the key differences and similarities between the two industries. These, in conjunction with the two previous sub-sections, then give rise to a set of follow-up questions that may be answered in the future.

3.4.1 Similarities and differences

As referred to in the introduction to this section, both industries are part of the critical infrastructure of the Netherlands. This means that there is an important societal incentive for cyber security to be in place, with security of supply on the one hand and road safety on the other of importance. Another characteristic similarity is that both contain infrastructure (vehicles or wind energy converters) that need to last for decades, which means that the entire lifecycle of the product, from the initial design onwards, needs to be taken into consideration. On top of this, large-scale digitalisation has caused a transition from largely analogue hardware to a system of complex, digital infrastructure. As a result, interim patching of the cyber security, including key cryptography, is essential when it comes to remaining resilient to potential future threats. In both industries, there is a tendency on some occasions to consider cyber security only 'after the event', instead of by design, and it is seen as a problem only when something actually goes wrong (ignorance is bliss). The high costs of innovation only exacerbate this. Finally, post-quantum cryptography remains a distant point in the future for both industries. Amongst larger parties, the topic is indeed on the radar, but there are as yet no plans for concrete implementation.

However, a number of important differences exist between the two industries. To start with, the offshore wind ecosystem is already up and running and will be scaled up quite considerably over the next few decades[37]; by contrast, V2X communication in the automotive industry is largely still in the pilot phase and a large-scale roll-out of fully autonomous vehicles is only likely to occur in the (distant) future. This is also characteristic of the exceptionally high complexity involved in V2X communication, where there are major issues in terms of technology, ethics, law and geography that firstly need to be resolved. Consequently, it is still not clear what V2X communication will look like in the future and in practice, whereas in the case of offshore wind, it is already quite firmly established. The two industries also differ considerably in terms of external threats. Offshore wind farms, and the corresponding infrastructure, are not easily accessible and the threat of large-scale disruption of energy supplies is expected to be caused primarily by state actors. By contrast, the infrastructure required for V2X communication is expected to be integrated into existing infrastructure that is already publicly accessible. At the same time, there is the possibility of inflicting significant damage to human life by hacking a single vehicle when compared to hacking a single wind energy converter. There is also a difference between the two industries in terms of maintenance – in the case of offshore wind, the shutdown of wind energy converters is a barrier to (large-scale) maintenance, while this applies to a lesser extent to self-driving vehicles. Finally, there is a difference between the two industries in terms of the incentive for market parties to actually put cyber security, and thus cryptography, in place. In the case of offshore wind, this security is an important economic incentive (e.g. market agreements relating to the supply of and demand for electricity), while for V2X communication, it is less direct (e.g. image damage in the case of accidents).

3.4.2 Conclusions and follow-up questions

The value network analysis provided valuable insights into cyber security and (post-quantum) cryptography for both industries. The value network for offshore wind exhibits different roles within the existing ecosystem and the interactions between them, revealing a clearly visible valorisation chain. This sheds light on a set of important drivers and barriers, which result in concrete recommendations for stimulating innovation within the ecosystem. By contrast, the value network for the automotive industry cannot yet be outlined as innovation in V2X communication remains largely in the pilot phase and there is, as yet, no valorisation chain. Notwithstanding the above, this study has mapped the current state of the ecosystem and outlined a number of important dynamics and challenges.

The findings outlined in this section give rise to a series of follow-up questions that could give cause for future research. Examples of follow-up questions are:

- To what extent are the findings from the interviews supported by (competing) parties who have the same role in the value network? This can be looked at in additional, validating interviews.
- What are the key strengths and weaknesses of the Dutch ecosystem when compared to other countries? To answer this question, it is suggested to carry out a value network analysis at international level, including countries such as France and Germany or even the entirety of the European Union.
- The innovation ecosystem in the automotive industry is relatively fragmented and it has not been possible to speak to DAF and/or VDL about their role as OEMs. Which parties are important and should be interviewed next to form a more complete picture of the Dutch ecosystem?
- In addition to the migration to post-quantum cryptography, which technological developments, as outlined in paragraph 2, are more relevant for these two industries?
- Is there a need for new or supplementary partnerships or consortia in order to improve innovation in crypto communication in these industries?

4 Crypto communication roadmap implementation

The objective of the crypto communication roadmap is three-fold. It starts with the development of innovative products and services in the field of crypto communication, followed by a contribution to economic activity in the Netherlands and, finally, stimulation of the strategic autonomy of the Netherlands. An economically healthy and properly functioning value network helps with the attainment of the objectives in the crypto communication roadmap. The findings from the market survey and the value network analysis can serve as a foundation for the roadmap on which to build further[56]. The findings are converted into the roadmap tracks so that the identified challenges, barriers and *valleys of death* can be worked on within the valorisation chain in a way that is properly founded.

The roadmap focuses on the period 2022 to 2032. New, as yet unforeseen developments may take place during this period of time. With this in mind, it remains a dynamic and living roadmap that needs to be adjusted in the interim on the basis of new insights and developments.

The foundation for the crypto communication roadmap illustrated in this section is divided into five development phases: *Discovery/basic research, Technology development, Validation and demonstration, Integration and operationalisation* and *Deployment*. Involved parties are shown, divided amongst the five development phases, for both the energy industry and the automotive industry. This is based on the insights acquired during the value network analysis. Consequently, ‘Valleys of death’ are then illustrated for the two industries plotted on the five development phases. A ‘valley of death’ refers to a barrier between the development phases of innovation. Finally, the potential solutions are outlined and translated into four ‘tracks’. Each of these tracks outlines potential solutions designed to overcome the barriers and valleys of death, which can be tackled with the aid of the crypto communication roadmap.

4.1 Industry: Offshore wind

4.1.1 Overview 1: Parties involved

The value network of the energy industry (see Figure 7, p. 27) shows the valorisation of knowledge establishment through research to product launch and integration from left to right.[57] In terms of value exchange, the (transmission) grid operator is central to the value network, while financial support for products for which cryptography is relevant is provided primarily by operators of wind farms and the grid operator (the customers). There are, in principle, no gaps in policy and/or supervision for this ecosystem, as all relevant parties are covered by the Security of Network and Information Systems Act (Wbni). A small number of component suppliers are central to the supply of parts for wind energy converters. Subsequently, these play a role in maintenance, by deploying their own experts.

[56] As already mentioned (see p. 6), the market research and the value network analysis were carried out within a relatively short period of time, which means that follow-up research is needed to further nuance, validate and extend these findings to shape the roadmap.
[57] The value network of the entire electricity industry, including the distribution operator and consumers, has been outlined in an earlier study: TNO (2020), *EZK Verdieping Valorisatieketens: Verkenning van het ecosysteem en waardenetwerk Automated Security* (TNO 2020 R12224).

Figure 9 shows the roles in the value network (see paragraph 3.2.2, p. 28) plotted on the five development phases of the roadmap. The overlap between the individual roles can be seen between and within certain pillars, which can offer concrete opportunities for collaboration and transferring knowledge.

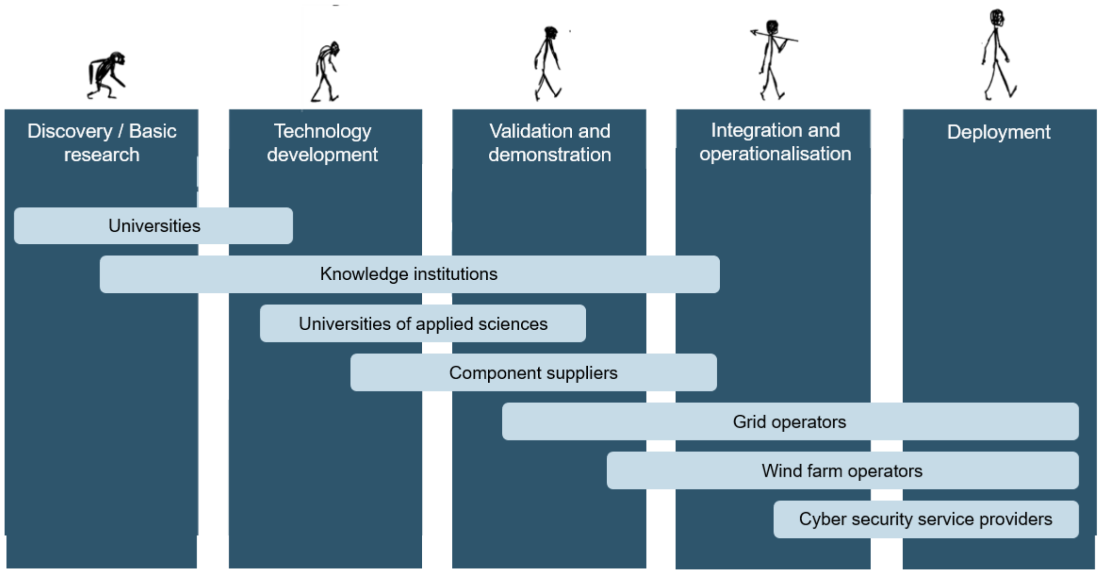

Figure 9 Outline based on the value network analysis within the valorisation chain of the offshore wind industry.

4.1.2 *Overview 2: 'Valleys of death' between development phases*

The *valleys of death* identified within the energy industry are as follows:

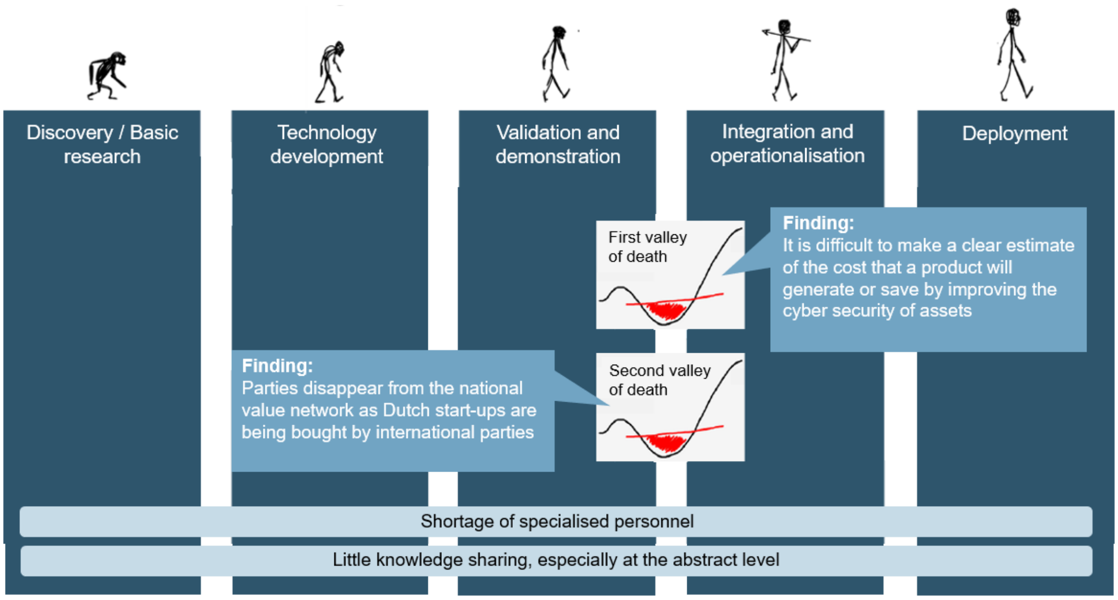

Figure 10 The 'valleys of death' and the more generic barriers in the development phases within the energy industry, that emerged through the conducted desk research and interviews.

The first valley of death in the energy industry is situated between the development phases of validation/demonstration and integration/operationalisation. This valley of death occurs primarily in the interaction between knowledge institutions, grid operators and suppliers. The importance of integrating crypto communication products is understood, but there is a cost-benefit analysis for the parties involved before actual product integration. What does a product cost, what does its implementation/deployment cost (e.g. the cost of shutting down a wind energy converter) and what does it ultimately deliver? Here, there is particular difficulty in making a clear assessment of the costs of and/or savings achieved from improving the cyber security of assets.

The second valley of death is also situated between the validation/demonstration and integration/operationalisation phases and involves primarily the cyber security service providers. The Netherlands has multiple start-ups offering cryptographic products, but given that the market is small, the step to integration/operationalisation in the Dutch market is rarely taken and start-ups tend to be acquired by international parties. Consequently, these parties then disappear from the national value network.

Lastly, there are two overarching barriers within the entire valorisation chain of this industry:

1. There is a (major) shortage of personnel with knowledge of both cyber security and cryptography as well as specialist knowledge of the industry itself.
2. In some areas, such as maintenance, there is very little communication and coordination between the parties within the valorisation chain. Improving these two factors could help to drive down the cost of, inter alia, patching cryptographic products.

4.2 Industry: Automotive

4.2.1 Overview 1: Parties involved

As referred to in the above section, it is not yet possible to map a valorisation chain for the automotive industry. figure 11 shows that the majority of parties involved in this industry (see paragraph 3.3.2.4., p. 37) are in the first three phases of development. Within the industry, none of those parties to whom we spoke have taken the step towards integration and operationalisation (phase 4) as this requires a number of major steps in relation to, inter alia, standardisation, legislation and further development of the technology. It is also unclear what the innovation ecosystem will look like in the future and which players, market dynamics, partnerships, opportunities and barriers will play a role.

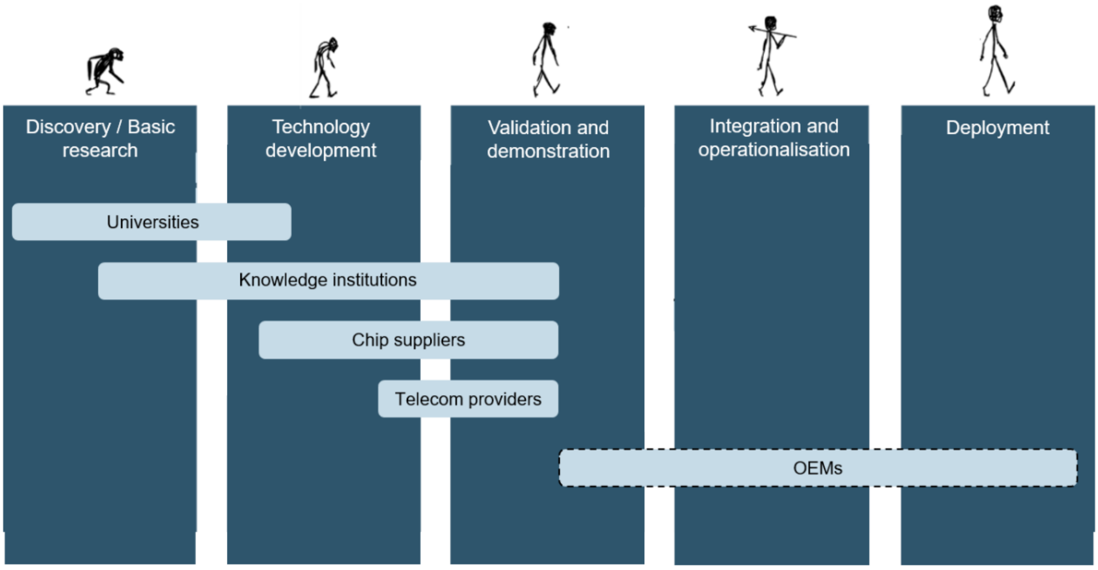

Figure 11 Outline based on the value network analysis of the parties within the automotive industry. This overview of parties involved in innovation of V2X communication is by no means exhaustive, but it is a selection of the parties to whom we spoke. It was not possible to speak to an OEM during the course of this study, so their position is outlined on the basis of the literature review. Please note that infrastructure parties also fall under the OEMs.

4.2.2 Overview 2: 'Valleys of death' between development phases

The valleys of death identified within the automotive industry are as follows:

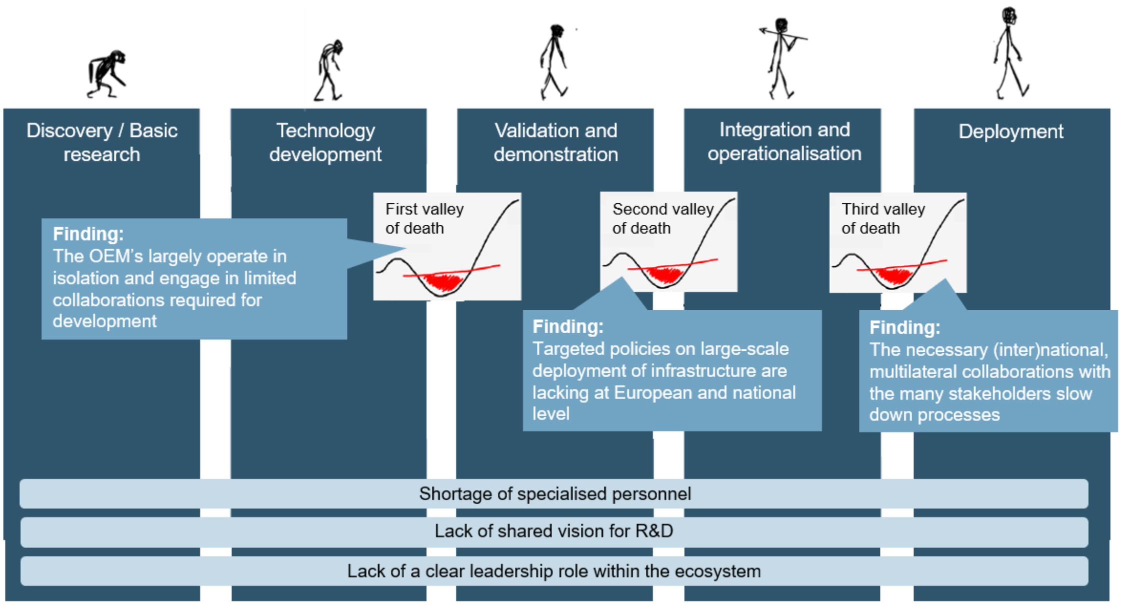

Figure 12 The 'valleys of death' and the more generic barriers in the development phases within the automotive industry, that emerged through the conducted desk research and interviews.

Firstly, a valley of death exists between the phases of technology development and validation/demonstration, as the central players in the ecosystem work in isolation and adopt more of a 'wait-and-see approach' in collaborations that lead to the implementation of new cryptography products. More specifically, as Figure 11 shows, OEMs have a very limited role in the R&D phase, which means that the transfer of technology to implementation is limited.

In addition, another valley of death is situated between the phases of validation/demonstration and integration/operationalisation due to a lack of policy and standards at both European level and national level. As crypto communication is not a core business of OEMs, there is no incentive to innovate.

The third valley of death is the slow speed at which standards for authorised deployment are developed. This development is extremely time-consuming due to the need for multilateral and international coordination.

Lastly, there are three overarching barriers within the entire valorisation chain of this industry:
1. The shortage of specialised cyber security personnel with both technical and industry-specific knowledge
2. The lack of a shared vision amongst parties in the ecosystem in order to set research and development priorities
3. A lack of a clear leadership role in the ecosystem, leading to the government and market parties looking to each other to take the first step in development.

4.3 Overview 3: Foundation for the crypto communication roadmap

The following details the foundation for the roadmap. Four tracks have been compiled on the basis of the findings from the market research and value network analyses. These tracks can strengthen the valorisation of crypto communication products, which can be worked on within the roadmap. The four tracks of the roadmap are distributed throughout the value chain, as shown in Figure 13. This section looks at the findings for each track and indicates the link to the barriers/valleys of death.

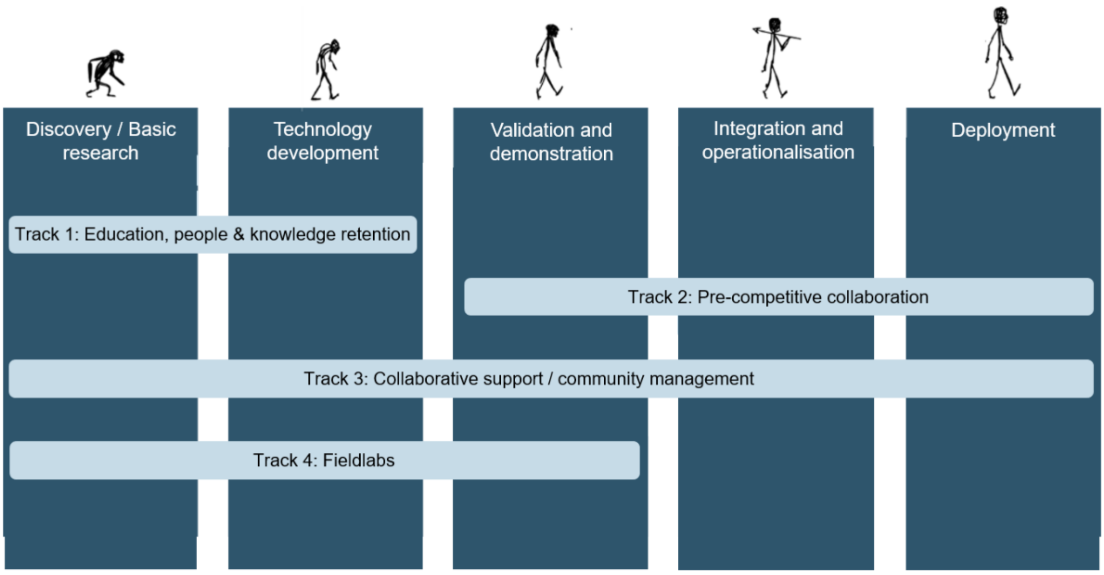

Figure 13 The four tracks for the crypto communication roadmap.

The findings from the market research and the value network analyses are categorised into four cross-industry tracks, which can be further elaborated upon in the roadmap. These tracks are as follows:

1 **Education, people and knowledge retention:** a shortage of qualified personnel is a generally observed barrier for the value chain, and was mentioned by parties in the market research as well as within the value network analyses (overarching barrier 1 in both industries). Consequently, continuing to train specialist personnel is important. This can be sharpened further by making it more attractive for domain-specific technicians to specialise in cryptography. Industry-specific knowledge can then be imparted to (market) parties through internal training programs. The basis for retention of knowledge are universities and knowledge institutions, which means that encouraging fundamental research is important. This can be achieved, inter alia, by attracting and funding doctoral studies at Dutch universities and knowledge institutions. Consideration could be given to the idea of making these ‘industry PhDs’, with candidates carrying out part of their research in industry. Farther down the value chain, it is important to work on retaining start-ups offering cryptographic products within the Dutch market, so that these start-ups remain within the national value network and to prevent the knowledge within them from disappearing (the second identified valley of death in the energy industry).

Recommendations, track 1:
Concrete steps need to be taken to strengthen knowledge of crypto communication within the industry. This could include setting up and encouraging training programmes for professionals. Safeguarding (academic) research is important when it comes to maintaining a strong knowledge position. This requires stable funding of doctoral studies. Additional benefit may be gained by using ‘industry PhDs’ in order to strengthen the knowledge position of the industry. To retain start-ups, the government can help to foster a good business climate, healthy growth opportunities and specific regulation. One concrete approach would be to offer a (shared) location in which start-ups and SMEs could operate at ABDO-certified level. This would help to establish ties to the Netherlands and eliminate a barrier to opening a start-up.

2 **Pre-competitive collaboration:** pre-competitive collaboration concerns carrying out activities that contribute to (potential) market growth. The barriers and valleys of death highlight the lack of a clear leadership role in the ecosystem, whereby government and market parties look to each other to take the first step in the development of crypto communication (the third overarching barrier in the automotive industry) and a lack of a shared vision between parties in the industry when it comes to setting R&D priorities (the second overarching barrier in the automotive industry). Targeted collaboration, with clear leadership and policy, can help to break down these barriers and, in turn, expand the overall market. Collaboration is possible between parties at all development / TRL levels, such as by developing a common partial solution, which parties can then detail individually. Market growth can also be sought by drawing a distinction between high-assurance and low-assurance products and by establishing new collaborations in the low-assurance domain. In addition, this is where the link to the first valley of death in the energy industry emerges. When an end user carries out a cost-benefit analysis for the deployment of an end product, the costs of the product itself play a role as well as the costs of implementation/operationalisation of the product. In the event that there is prior coordination between the developer and the end user, this can be taken into consideration in the development process.

Recommendations, track 2:
Led by dcypher, the Dutch ecosystem is taking a leadership role and taking steps towards collaboration by creating a shared vision for research and development with parties in the value chain by focusing on crypto communication components (modularity) rather than on a complete end product. To this end, academia, industry and end users are working together in order to jointly tackle shared problems. Early coordination on sub-products being developed helps to share and manage the costs/benefits of implementing and operationalising crypto communication products. Concrete pre-competitive collaboration can be shaped by different projects with (some of) the parties participating in the crypto communication roadmap. Logically, this collaboration starts by tackling the low-hanging fruit, with projects whose outcome is certain to add value. By starting small, discovering new and shared barriers and maintaining momentum in the approach to those barriers, collaboration can then be gradually expanded.

3 **Collaboration support / community management:** it is important to create a safe environment for collaboration and coordination (such as innovation tracks or conferences) between parties within the value network. The cyber security of the system as a whole is not, after all, the responsibility of just one or a few parties. Connecting stakeholders helps to bring about community building (i.e. national branding, Dutch international branding, briefings and conferences, establishing sub-communities, bringing the automotive and offshore wind industries together, organising working groups, etc.) and contributes to an awareness of the opportunities that crypto communication offers. As an example, improving coordination and communication between parties in the value chain can help to reduce the costs involved in patching cryptographic products (the second overarching barrier in the energy industry) and bring about an improvement in the transfer of technology to implementation (the first valley of death in the automotive industry). Standardisation at national level (e.g. via the NEN) can also lead to trust and guidelines for joint collaboration. Conversely, standardisation is more easily achieved in a well-connected community (the second and third valleys of death in the automotive industry).

Recommendations, track 3:
As a collaboration platform, dcypher can provide a secure environment (community) in which parties within the value network can exchange information and, in so doing, help to improve the valorisation of crypto communication products by means of greater awareness and understanding of the opportunities that those products offer. In addition, dcypher can also strengthen the reputation of the Dutch crypto industry at European/international level by organising conferences and trade missions.

4 **Fieldlabs:** the pre-competitive collaboration track is, to some extent, a technology push from the inside to the outside. Turned around, demand-driven technology pull can help to ensure that new products/services actually land. Field labs can offer a safe environment for open innovation by multiple parties from the industry, in which ideas and new technological solutions can be tested freely. Within this, numerous use cases can then be developed, such as testing of the integration of a new cryptographic product with the aid of a digital twin. An

important aspect that can be included in this, is to look for solutions that match concrete demands from the market. This would allow successful implementations to land more easily in an existing ecosystem.

Recommendations, track 4: Who will take the initiative, what will we do?
The fieldlabs will have to be a supported activity, for which working on concrete and shared risks is leading. A starting point for the field labs are the industry-specific barriers identified in this report. The field labs have EZK as an important catalyst, but stand and fall by the support within the industry. The fieldlabs can also serve as a source of inspiration for the development of new products/services by creating a short path from research and development.

The four tracks described provide an initial incentive for implementation, ready for further exploration in a follow-up process. It is recommended that the findings and barriers identified in this report are built upon to further shape the crypto communication roadmap.

5 Bibliography

- Aazami, (2021), Digitalisering en energie: Méér dan de som der delen.
- Algemene Inlichtingen- en Veiligheidsdienst (AIVD) (2021), *Bereid je voor op de dreiging van de quantumcomputers*.
- Allee, V. (2008), 'Value network analysis and value conversion of tangible and intangible assets', *Journal of intellectual capital*, Vol. 9, Issue 1, pp. 5-24.
- Barbosa, M. & G. Barthe, et al. (2019), 'SoK: Computer-Aided Cryptography', *Cryptology ePrint Archive,* 1393.
- Bhargavan, K. & B. Blanchet et al. (2019), 'A mechanised cryptographic proof of the WireGuard Virtual Private Network protocol', *Inria Paris*, pp. 50.
- Beullens, W. (2022), 'Breaking Rainbow takes a weekend on a laptop', *Cryptology ePrint Archive*, Paper 022/214.
- Castryck, W. & T. Lange et al. (2018). 'CSIDH. An efficient post-quantum commutative group action', *ASIACRYPT 2018*, pp. 395-427.
- CE Delft, TNO en Quintel (2021), Afspraken maken: van data tot informatie, Informatiebehoeften, datastandaarden en protocollen voor provinciale systeemstudies – Deel II technische rapportage.
- Ministerie van Economische Zaken en Klimaat, TNO, CWI & dcypher (2021), Nederland Cryptoland. Startpunt routekaart cryptocommunicatie: de vier belangrijkste uitdagingen in de cryptografie.
- Milakis, D., Snelder, M. & Arem, B. (et. al.) (2017), 'Development and transport implications of automated vehicles in the Netherlands: Scenarios for 2030 and 2050', *European Journal of Transport and Infrastructure Research,* Vol. 17, pp. 63-85.
- European Commission (2018), FinTech action plan: For a more competitive and innovative European financial sector.
- Federal Office for Information Security (BSI) (2021, oktober), Quantum-safe cryptography: Fundamentals, current developments and recommendations.
- Goubin, L., Kipnis A. & J. Patarin (1999), 'Unbalanced Oil and Vinegar signature schemes', *Advances in Cryptology – EUROCRYPT '99*, pp. 206-222.
- Hofstätter, T., Krawina, M., Mühlreiter, B., Pöhler, S. & A. Tschiesner (2020), 'Reimagining the auto industry's future: It's now or never', McKinsey & Company (https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/reimagining-the-auto-industrys-future-its-now-or-never)
- ITU (2017), Measuring the Information Society Report, 2017 (Vol. 1).
- Kalra, N., & Groves, D. G. (2017), The enemy of good: Estimating the cost of waiting for nearly perfect automated vehicles.
- NCTV (2018), Nederlandse Cybersecurity Agenda: Nederland digitaal veilig.
- Sieber, L., Ruch, C., Hörl, S., Axhausen, K. W. & Frazzoli, E. (2020), 'Improved public transportation in rural areas with self-driving cars: A study on the operation of Swiss train lines' *Transportation research part A: policy and practice*, Vol. 134, pp. 35-51.
- Straver, F. (2017, 29 November), Windlobby waarschuwt: Aziatische massamolen hijgt Europa in de nek. *Trouw* (https://www.trouw.nl/duurzaamheid-natuur/windlobby-waarschuwt-aziatische-massamolen-hijgt-europa-in-de-nek~b30cf380/)
- Teoh, E. R. & Kidd, D. G. (2017), 'Rage against the machine? Google's self-driving cars versus human drivers', *Journal of Safety Research*, Vol. 63, pp. 57-60.

- The Hague Centre for Strategic Studies (2021), *The High Value of The North Sea*.
- Topsector High Tech Systemen en Materialen (HTSM), Team Dutch Digital Delta, Topsector Creatieve Industrie, Topsector Logistiek en Topsector Water & Maritiem (2019), *Kennis en innovatieagenda (KIA) Veiligheid*.
- TNO (2020), *EZK Verdieping Valorisatieketens: Verkenning van het ecosysteem en waardenetwerk Automated Security* (TNO 20220 R12224).
- TNO (2019), *Succesfactoren voor digitaal veilige Operationele Technologie* (TNO 2019 R11304).
- TNO (2022), Crypto for Automotive – WP1 Report: Toepassing cryptografie in directe automotive communicatie (to be published in 2022).

A Overview of interviewed parties

A.1 Market survey

Table 1 Overview of parties interviewed for the market survey.

Technische Universiteit Eindhoven (2x interview) (NL)
NXP Semiconductors (interview) (NL)
Roseman Labs (interview) (NL)
Infineon (interview) (DE)
Zama (interview) (FR)
iGrant.io (questionnaire) (SE)
NTNU (questionnaire) (NO)
Airbus (questionnaire) (NL, FR, ES, DE)

For the questionnaire, see: 'Annex B: Market survey questionnaire'.

A.2 Value network analysis

Table 2 Overview of parties interviewed for the value network analysis. The first seven parties represent the offshore wind industry, the final four the automotive industry. We spoke to the other parties for both industries.

Party	Interviewee's role
Siemens	Cyber Security Specialist
Shell	Information Security Architect
Compumatica	Board Member
Ministry of Infrastructure and Water Management	Senior Information Advisor
NHL Stenden Hogeschool	Lecturer in Digital Resilience
European Network for Cyber Security	Researcher
TenneT	Cyber Security Advisor
TNO (x3)	Senior Scientist Energy Transition Studies, Program Manager Wind Energy, Senior Project Manager Automotive
Rijkswaterstaat (x2)	Quartermaster Offshore Expertise Centre, Advisor Smart Mobility
Radiocommunications Agency Netherlands	Cyber Security Inspectors
TU Eindhoven	Professor Software Engineering
NXP	Senior Systems Architect
KPN	Technical Lead Mobility Fieldlab
ElaadNL	Cyber Security Expert

B Market research questionnaire

TNO – EU Cryptography market research
On behalf of the Dutch Ministry of Economic Affairs, TNO conducts research into the current developments on cryptography within the EU. More specifically, we are looking at various parties within the EU cryptography market (i.e. knowledge institutions, product developers, end users) to identify current developments, initiatives and barriers.

1. Current research, projects and/or initiatives of your organisation
TNO currently identifies four developments that pose the greatest challenges, and simultaneously offer the greatest opportunities, in the coming years in the field of cryptography:

- <u>Securing new technical environments</u>
  Due to the constant development and adoption of new technical environments, it is necessary to secure them sufficiently, before these new technical environments are suitable for use in situations where security is of great importance. This development could be carried out with common unilateral cryptography and should be achievable on the short term.

- <u>Migration to post-quantum cryptography</u>
  The development of the quantum computer puts widely used cryptographic systems at risk. Therefore, we need post-quantum cryptography that is resistant against future quantum attacks. However, the migration to post-quantum cryptography is a challenge for the entire valorisation chain, both on the short and long term. An additional opportunity is that through the structural migration, the crypto agility of the systems can be increased.

- <u>Deployment of cryptography for new decentralised applications</u>
  The emergence of multilateral cryptography has given the opportunity to develop new decentralised techniques, such as secure multiparty computation and self-sovereign identities. Developments of new, advanced cryptographic primitives such as fully homomorphic encryption further give rise to new opportunities in the area of outsourced computing on sensitive data.

- <u>Formal verification of cryptography and cryptographic source code</u>
  Formal verification, or computer-aided cryptography, is a method that is being used to let computers validate software implementations of cryptographic primitives. This technique can also be applied to the underlying cryptographic protocols and their implementations, providing assurance on the security of cryptographic products.

1.1. Which new technical environments has your organisation identified and which of those are addressed in your organisations current efforts in research, projects and/or initiatives?

1.2. Which post quantum cryptography migration challenges has your organisation identified and which of those are addressed in your organisations current efforts in research, projects and/or initiatives?

1.3. Which deployments of cryptography for new decentralised applications has your organisation identified and which of those are addressed in your organisations current efforts in research, projects and/or initiatives?

1.4. Which formal verification of cryptography and cryptographic source code has your organisation identified and which of those are addressed in your organisations current efforts in research, projects and/or initiatives?

<u>1.5.</u> Do you identify other developments for the coming years within the field of cryptography? If so, what kind of research, projects and/or initiatives does your organisation undertake in terms of this development?

2. Barriers within the cryptography market
In our current research, we are identifying barriers that are currently at play within the cryptography market. Expectations are that certain barriers specifically exist for (new) organisations to enter the cryptography market; barriers that stand in the way of (new) innovation initiatives; and barriers to translate crypto-graphic research into (embedded) cryptographic end-products.

Examples of generic barriers that we have identified so far:

- Due to a mix of stakeholders conflicts of interest can occur during standardisation.
- Not enough collaboration within the EU, many Member States want to remain independent.
- Shortage of researchers and personnel.
- Researchers have to publish papers. For researchers working in the area of formal verification of cryptography, this leads to less available time to develop documentation / tutorials of the tooling being developed on the fly, with a lack in documentation and tutorials as a consequence.
- Lack of governmental guidelines, standardisation, and rules on how to deploy new forms of cryptography.
- Currently existing security problems obstruct organisations to look into migrating towards post-quantum cryptography, as these security issues have to be fixed first.

<u>2.1.</u> Which barriers can you identify that exist specifically for (new) organisations to enter the cryptography market? What could be done to take away these barriers?

<u>2.2.</u> Which barriers can you identify that specifically stand in the way of (new) innovation initiatives? What could be done to take away these barriers?

<u>2.3.</u> Which barriers can you identify that exist specifically in translating cryptographic research into (embedded) cryptographic end-products? What could be done to take away these barriers?

<u>2.4.</u> Are there any additional barriers that you identify in the cryptography market?

3. Standardisation and regulation
In recent years various bodies have undertaken to develop and implement standardisation and regulation relating to cryptography, on an international level (such as NIST and ISO) as well as on the national level. In our research it would be very useful to know which standardisation and/or regulation is applicable to your organisation.

3.1. Which standarisation and/or regulation is applicable to your organisation?

3.2. Which interoperability issues exist, where in your opinion standarisation and/or regulation is needed?
