RESEARCH CENTRE

Paris

IN PARTNERSHIP WITH:

CNRS, Ecole normale supérieure de Paris

2020

ACTIVITY REPORT

Project-Team

CASCADE

Construction and Analysis of Systems for Confidentiality and Authenticity of Data and Entities

IN COLLABORATION WITH: Département d'Informatique de l'Ecole Normale Supérieure

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Algorithmics, Computer Algebra and Cryptology

Contents

Project-Team CASCADE

Creation of the Project-Team: 2008 July 01

Keywords

Computer sciences and digital sciences

A4. – Security and privacy

A4.3. – Cryptography

A4.3.1. – Public key cryptography

A4.3.2. – Secret key cryptography

A4.3.3. – Cryptographic protocols

A4.3.4. – Quantum Cryptography

A4.8. – Privacy-enhancing technologies

A7. – Theory of computation

A7.1.4. – Quantum algorithms

A8.5. – Number theory

A8.9. – Performance evaluation

A8.10. – Computer arithmetic

A9.2. – Machine learning

Other research topics and application domains

B6.4. – Internet of things

B9.5.1. – Computer science

B9.10. – Privacy

1 Team members, visitors, external collaborators

Research Scientists

- David Pointcheval [Team leader, CNRS, Researcher, HDR]
- Michel Ferreira Abdalla [CNRS, Researcher, HDR]
- Georg Fuchsbauer [Inria, Researcher, until Jan 2020]
- Brice Minaud [Inria, Researcher]
- Phong-Quang Nguyen [Inria, Senior Researcher, HDR]
- Hoeteck Wee [CNRS, Researcher, until Jun 2020, HDR]

Faculty Member

- Céline Chevalier [Université Panthéon-Assas, Associate Professor, from Jul 2020, HDR]

Post-Doctoral Fellows

- Ehsan Ebrahimi [École Normale Supérieure de Paris, until Feb 2020]
- Junqing Gong [CNRS, until Feb 2020]
- Azam Soleimanian [École Normale Supérieure de Paris]

PhD Students

- Leonard Assouline [École Normale Supérieure de Paris, from Sep 2020]
- Balthazar Bauer [Inria, until Aug 2020]
- Baptiste Cottier [Wordline]
- Paola De Perthuis [Cosmian Tech SAS, from Sep 2020]
- Lenaick Gouriou [Leanear]
- Chloe Hebant [CNRS]
- Michele Orrù [CNRS, until Mar 2020]
- Antoine Plouviez [Inria]
- Michael Reichle [Inria, from Oct 2020]
- Melissa Rossi [ANSSI, until Oct 2020]
- Theo Ryffel [Inria]
- Hugo Senet [Thales, from Apr 2020]
- Quoc Huy Vu [École Normale Supérieure de Paris]

Administrative Assistants

- Nathalie Gaudechoux [Inria]
- Meriem Guemair [Inria]

2 Overall objectives

2.1 Presentation

Cryptographic algorithms are the equivalent of locks, seals, security stamps and identification documents over the Internet. They are essential to protect our online bank transactions, credit cards, medical and personal information, and to support e-commerce and e-government. They come in different flavors. Encryption algorithms are necessary to protect sensitive information such as medical data, financial information and Personal Identification Numbers (PINs) from prying eyes. Digital signature algorithms (in combination with hash functions) and MAC algorithms replace hand-written signatures in electronic transactions. Identification protocols allow to securely verify the identity of a remote party. As a whole, cryptology is a research area with a high strategic impact in industry, for individuals, and for society as a whole. The research activity of project-team CASCADE addresses the following topics, which cover most of the areas that are currently active in the international cryptographic community, with a focus on public-key algorithms:

1. Implementation of cryptographic algorithms, and applied cryptography;
2. Algorithm and protocol design, and provable security;
3. Theoretical and practical attacks.

2.2 Design of Provably Secure Primitives and Protocols

Since the beginning of public-key cryptography, with the seminal Diffie-Hellman paper, many suitable algorithmic problems for cryptography have been proposed and many cryptographic schemes have been designed, together with more or less heuristic proofs of their security relative to the intractability of the underlying problems. However, many of those schemes have thereafter been broken. The simple fact that a cryptographic algorithm withstood cryptanalytic attacks for several years has often been considered as a kind of validation procedure, but schemes may take a long time before being broken. As a consequence, the lack of attacks at some time should never be considered as a full security validation of the proposal.

A completely different paradigm is provided by the concept of "provable" security. A significant line of research has tried to provide proofs in the framework of computational complexity theory (a.k.a. "reductionist" security proofs): the proofs provide reductions from a well-studied problem (factoring, RSA or the discrete logarithm) to an attack against a cryptographic protocol. The techniques are derived from complexity theory, providing (polynomial) reductions. And the more efficient the reduction can be, the better the parameters of the schemes will be.

Unfortunately, in many cases, even just provable security is at the cost of an important loss in terms of efficiency for the cryptographic protocol. Thus, some models have been proposed, trying to deal with the security of efficient schemes: some concrete objects are identified with ideal (or black-box) ones. For example, it is by now usual to identify hash functions with ideal random functions, in the so-called "random-oracle model". Similarly, block ciphers are identified with families of truly random permutations in the "ideal cipher model". Another kind of idealization has also been introduced in cryptography, the black-box group, where the group operation, in any algebraic group, is defined by a black-box: a new element necessarily comes from the addition (or the subtraction) of two already known elements. It is by now called the "generic group model", extended to the bilinear and multi-linear setting. Some works even require several ideal models together to provide some new validations.

But still, such idealization cannot be instantiated in practice, and so one prefers provable security without such idealized assumptions, under new and possibly stronger computational assumptions. As a consequence, a cryptographer has to deal with the following four important steps, which are **all** main goals of ours:

computational assumptions, which are the foundation of the security. We thus need to have a strong evidence that the computational problems are reasonably hard to solve. Better attacks against the algorithmic problems are thus studied.

security model, which makes precise the security notions one wants to achieve, as well as the means the adversary may be given. We contribute to this point, in several ways:

- by providing security models for many primitives and protocols;
- by enhancing some classical security models;
- by considering new means for the adversary.

design of new schemes/protocols, or more efficient ones, with additional features, etc.

security proof, which consists in exhibiting a reduction.

3 Research program

3.1 Quantum-Safe Cryptography

The security of almost all public-key cryptographic protocols in use today relies on the presumed hardness of problems from number theory such as factoring and computing discrete logarithms. This is problematic because these problems have very similar underlying structure, and its unforeseen exploit can render all currently used public-key cryptography insecure. This structure was in fact exploited by Shor to construct efficient quantum algorithms that break all hardness assumptions from number theory that are currently in use. And so naturally, an important area of research is to build provably secure protocols based on mathematical problems that are unrelated to factoring and discrete log. One of the most promising directions in this line of research is using lattice problems as a source of computational hardness, which also offer features that other alternative public-key cryptosystems (such as MQ-based, code-based, isogeny-based or hash-based schemes) cannot provide. The ERC Advanced Grant PARQ aims at evaluating the security of lattice-based cryptography, with respect to the most powerful adversaries, such as quantum computers and large-scale parallel computers.

In the meantime, although a universal quantum computer may be some decades in the future, quantum communication and quantum error correcting codes are beginning to become concretely available. It is already possible to prepare, manipulate and precisely control systems involving a few quantum information bits (qubits). Such quantum technologies could help improve the efficiency and security of concrete cryptographic protocols. The ANR JCJC project CryptiQ aims at considering three possible scenarios (first, the simple existence of a quantum attacker, then the access to quantum communication for anyone, and finally a complete quantum world) and studies the consequences on the cryptographic protocols currently available. This implies elaborating adversarial models and designing or analyzing concrete protocols with formal security proofs, in order to get ready as soon as one of these scenarios becomes the new reality.

3.2 Advanced Encryption

Fully Homomorphic Encryption (FHE) has become a very active research area since 2009, when IBM announced the discovery of a FHE scheme by Craig Gentry. FHE allows to perform any computation on encrypted data, yielding the result encrypted under the same key. This enables outsourcing computation in the Cloud, on encrypted data, so the Cloud provider does not learn any information. However, FHE does not allow to share the result.

Functional Encryption (FE) is another recent tool that allows an authority to deliver functional decryption keys, for any function f of his choice, so that when applied to the encryption of a message m, the functional decryption key yields $f(m)$. Since m can be a large vector, f can be an aggregation or statistical function: on encrypted data, one can get the result $f(m)$ in clear. While this functionality has initially been defined in theory, our team has been very active in designing concrete instantiations for practical purposes.

Another approach is to focus on a type of computation over encrypted data of particular interest, namely the ability to search over encrypted data. Here, a client encrypts its data, and sends it to a distant server. The client should then be able to issue queries to the server, asking for elements within the encrypted data that fit some search criterion. The server should be able to correctly answer the query, without learning the client's data (which remains encrypted), or even the contents of the query (which is also encrypted). In this context, the server is regarded as a honest-but-curious adversary attempting to infer private information as it processes the client's queries. By restricting the range of functionalities compared to FHE and FE, and allowing a controlled amount of leakage, Searchable Symmetric Encryption (SSE) enables very efficient solutions, which can be deployed at scale.

3.3 Security amidst Concurrency on the Internet

Cryptographic protocols that are secure when executed in isolation can become completely insecure when multiple such instances are executed concurrently (as is unavoidable on the Internet) or when used as a part of a larger protocol. For instance, a man-in-the-middle attacker participating in two simultaneous executions of a cryptographic protocol might use messages from one of the executions in order to compromise the security of the second – Lowe's attack on the Needham-Schroeder authentication protocol and Bleichenbacher's attack on SSL work this way. Our research addresses security amidst concurrent executions in secure computation and key exchange protocols.

Secure computation allows several mutually distrustful parties to collaboratively compute a public function of their inputs, while providing the same security guarantees as if a trusted party had performed the computation. Potential applications for secure computation include anonymous voting, privacy-preserving auctions and data-mining. Our recent contributions on this topic include

1. new protocols for secure computation in a model where each party interacts only once, with a single centralized server; this model captures communication patterns that arise in many practical settings, such as that of Internet users on a website, and

2. efficient constructions of universally composable commitments and oblivious transfer protocols, which are the main building blocks for general secure computation.

3.4 Anonymity and Electronic Cash

Electronic cash (e-cash) was first proposed in the 1980s but has never been deployed on a large scale. But it initiated a lot of work on anonymity, with blind signatures and zero-knowledge proofs. Other means of digital payments are instead largely replacing physical cash, but they do not respect the citizens' right to privacy, which includes their right of anonymous payments of moderate sums. Recently, so-called decentralized currencies, such as Bitcoin, have become a third type of payments in addition to physical cash, and card and other (non-anonymous) electronic payments. The continuous growth of popularity and usage of this new kind of currencies, also called "cryptocurrencies", has triggered a renewed interest in cryptographic e-cash.

Our team had done some work on (decentralized) cryptocurrencies, such as Bitcoin where all transactions are publicly posted on the so-called "blockchain", or *Zcash* which respects user privacy. But apart from privacy, two pressing challenges for cryptocurrencies, and blockchains in general, are sustainability and scalability. We have thus looked at alternatives to the proof of work.

Blockchains have meanwhile found many other applications apart from electronic money. Together with Microsoft Research, our group investigates decentralized means of authentication that use cryptography to guarantee privacy.

But more generally on the privacy aspects, our group investigates "centralized" e-cash, which uses more classical approaches, and remains in line with the current economic model that has money be issued by (central) banks (while cryptocurrencies use money distribution as an incentive for participation in the system, on which its stability hinges). Of particular interest among centralized e-cash schemes is transferable e-cash, which allows users to transfer coins between each other without interacting with a third party (or the blockchain), still with privacy guarantees. This is in the same vein of anonymous credentials, as it combines both strong authentication guarantees and privacy properties.

4 Application domains

4.1 Privacy for the Cloud

Many companies have already started the migration to the Cloud and many individuals share their personal informations on social networks. While some of the data are public information, many of them are personal and even quite sensitive. Unfortunately, the current access mode is purely right-based: the provider first authenticates the client, and grants him access, or not, according to his rights in the access-control list. Therefore, the provider itself not only has total access to the data, but also knows which data are accessed, by whom, and how: privacy, which includes secrecy of data (confidentiality), identities (anonymity), and requests (obliviousness), should be enforced. Moreover, while high availability can easily be controlled, and thus any defect can immediately be detected, failures in privacy protection can remain hidden for a long time. The industry of the Cloud introduces a new implicit trust requirement: nobody has any idea at all of where and how his data are stored and manipulated, but everybody should blindly trust the providers. The providers will definitely do their best, but this is not enough. Privacy-compliant procedures cannot be left to the responsibility of the provider: however strong the trustfulness of the provider may be, any system or human vulnerability can be exploited against privacy. This presents too huge a threat to tolerate. *The distribution of the data and the secrecy of the actions must be given back to the users. It requires promoting privacy as a global security notion.*

In order to protect the data, one needs to encrypt it. Unfortunately, traditional encryption systems are inadequate for most applications involving big, complex data. Recall that in traditional public key encryption, a party encrypts data to a single known user, which lacks the expressiveness needed for more advanced data sharing. In enterprise settings, a party will want to share data with groups of users based on their credentials. Similarly, individuals want to selectively grant access to their personal data on social networks as well as documents and spreadsheets on Google Docs. Moreover, the access policy may even refer to users who do not exist in the system at the time the data is encrypted. Solving this problem requires an entirely new way of encrypting data.

A first natural approach would be **fully homomorphic encryption** (FHE, see above), but a second one is also **Functional Encryption** (FE), that is an emerging paradigm for public-key encryption: it enables more fine-grained access control to encrypted data, for instance, the ability to specify a decryption policy in the ciphertext so that only individuals who satisfy the policy can decrypt, or the ability to associate keywords to a secret key so that it can only decrypt documents containing the keyword. Our work on functional encryption centers around two goals:

1. to obtain more efficient pairings-based functional encryption;
2. and to realize new functionalities and more expressive functional encryption schemes.

Another approach is **secure multi-party computation protocols**, where interactivity might provide privacy in a more efficient way, namely for machine learning techniques. Machine learning makes an intensive use of comparisons, for the activation of neurons, and new approaches have been proposed for efficient comparisons with interactive protocols.

4.2 Searchable Encryption

Searchable Encryption (SE) is another technique that aims to protect users' privacy with regard to data uploaded to the cloud. Searchable Encryption is equally concerned with scalability, with the aim to accomodate large real-world databases. As a concrete application, an email provider may wish to store its users' emails in an encrypted form to provide privacy; but it is obviously highly desirable that users should still be able to search for emails that contain a given word, or whose date falls within a given range. Businesses may also want to outsource databases containing sensitive information, such as client data, for example to dispense with a costly dedicated IT department. To be usable at all, the outsourced encrypted database should still offer some form of search functionality. Failing that, the entire database must be downloaded to process each query to the database, defeating the purpose of cloud storage.

In many contexts, the amount of data outsourced by a client is large, and the overhead incurred by generic solutions such as FHE or FE becomes prohibitive. The goal of Searchable Encryption is to find practical trade-offs between privacy, functionality, and efficiency. Regarding functionality, the focus is mainly on privately searching over encrypted cloud data, altough many SE schemes also support simple forms of update operation. Regarding privacy, SE typically allows the server to learn *some* information on the encrypted data. This information is formally captured by a *leakage function*. Security proofs show that the cloud server does not learn any more information about the client's data than what is expressed by the leakage function.

The additional flexibility afforded by allowing a controlled amount of leakage enables SE to offer highly efficient solutions, which can be deployed in practice on large datasets. The main goal of our research in this area is to analyze the precise privacy impact of different leakage functions; propose new techniques to reduce this leakage; as well as extend the range of functionality achieved by Searchable Encryption.

4.3 Post-Quantum Standardization

In recent years, there has been very significant investment on research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of post-quantum cryptography (also called quantum-resistant cryptography or quantum-safe cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communication protocols and networks.

In 2016, NIST initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Round 3 candidates were announced on July 22, 2020. Out of the seven finalists, five are based on lattice problems: CRYSTALS-KYBER, NTRU and SABER for encryption, CRYSTALS-DILITHIUM and FALCON for signature. We intend to study the best lattice algorithms in order to assess the security of the five NIST finalists based on the hardness of lattice problems.

4.4 Provable Security for the Quantum Internet

With several initiatives such as the development of a 2,000 km quantum network in China, the access of IBM's quantum platform freely available and the efforts made in the EU for instance with the quantum internet alliance team, we can assume that in a further future, not only the adversary has potential access to a quantum computer, but everybody may have access to quantum channels, allowing honest parties to exchange quantum data up to a limited amount. Going one step further than post-quantum cryptography, it is therefore needed to carefully study the security models and properties of classical protocols or the soundness of classical theoretical results in such a setting. Some security notions have already been defined but others have to be extended, such as the formal treatment of superposition attacks initiated by Zhandry.

On the positive side, some quantum primitives which are already well-studied, unconditionally quantum secure and already deployed in practice (such as Quantum Key Distribution) allow for new security properties such as everlasting confidentiality for sensitive long-lived data (which holds even if an attacker stores encrypted data now and decrypts them later when a quantum computer becomes available). We intend to study to what extent allowing honest parties to have access to currently available (or near-term) quantum technologies allows to achieve quantum-enhanced protocols (for classical functionalities) with improved security or efficiency beyond what is possible classically.

5 Social and environmental responsibility

5.1 Footprint of research activities

Unfortunately, private computation is usually at a huge cost: it definitely costs more to compute on encrypted data than on clear inputs. However, our goal is definitely to reduce this cost, as it will improve the user experience at the same time, with shorter computation time.

5.2 Impact of research results

Strong privacy for the Cloud would have a huge societal impact since it would revolutionize the trust model: users would be able to make safe use of outsourced storage, namely for personal, financial and medical data, without having to worry about failures or attacks of the server.

Both design of new primitives and study of the best attacks are essential for this goal.

6 Highlights of the year

6.1 Awards

- Phong Nguyen has been awarded an ERC Advanced Grant on his project PARQ
- David Pointcheval has been awarded an ERC Proof of Concept on his project CryptAnalytics

7 New results

All the results of the team have been published (see the list of publications). They are all related to the research program (see Section 3) and the research projects (see Sections 8 and 9):

- Advanced primitives for privacy in the cloud
- Efficient functional encryption
- Attribute and predicate encryption schemes
- New primitives for efficient anonymous authentication
- Application of multi-party computation to machine learning
- Searchable Encryption

7.1 Dynamic Decentralized Functional Encryption

In a recent work (published at Crypto '20) [20], we introduce Dynamic Decentralized Functional Encryption (DDFE), a generalization of Functional Encryption which allows multiple users to join the system dynamically, without relying on a trusted third party or on expensive and interactive Multi-Party Computation protocols. This notion subsumes existing multi-user extensions of Functional Encryption, such as Multi-Input, Multi-Client, and Ad Hoc Multi-Input Functional Encryption. We define and construct schemes for various functionalities which serve as building-blocks for latter primitives and may be useful in their own right, such as a scheme for dynamically computing sums in any Abelian group. These constructions build upon simple primitives in a modular way, and have instantiations from well-studied assumptions, such as DDH or LWE. Our constructions culminate in an Inner-Product scheme for computing weighted sums on aggregated encrypted data, from standard assumptions in prime-order groups in the Random Oracle Model.

7.2 Functional Encryption for Attribute-Weighted Sums from k-Lin

In a recent work (published at Crypto '20) [13], we present functional encryption schemes for attribute-weighted sums, where encryption takes as input N attribute-value pairs (x_i, z_i) where x_i is public and z_i is private; secret keys are associated with arithmetic branching programs f, and decryption returns the weighted sum $\sum_{i=1}^{N} f(x_i) z_i$ while leaking no additional information about the z_i's. Our main construction achieves **(1)** compact public parameters and key sizes that are independent of N and the secret key can decrypt a ciphertext for any a-priori unbounded N; **(2)** short ciphertexts that grow with N and the size of z_i but not x_i; **(3)** simulation-based security against unbounded collusions; but still relies on the standard k-linear assumption in prime-order bilinear groups.

7.3 Approximating the Shortest Vector Problem

In a recent work (published at Crypto '20) [14], we revisited the slide reduction algorithm of Gama and Nguyen (STOC '08), by somewhat merging it with the DBKZ algorithm of Micciancio and Walters (EUROCRYPT '16). This allowed us to improve the state-of-the-art for the most famous lattice problem, namely the Shortest Vector Problem (SVP): we obtained the best SVP approximation factor known for a polynomial-time algorithm, but also the best theoretical exponential running time to achieve a sublinear SVP approximation factor beyond the square root of the lattice rank.

8 Bilateral contracts and grants with industry

8.1 Bilateral contracts with industry

CryptBloC: Cryptography for the Blockchain

Duration: October 2017 – October 2021

Partners: MSR Redmond (USA), MSR Cambridge (UK), Inria/ENS/Cascade

Inria contact: David Pointcheval

Summary: The goal of this Microsoft-Inria joint project on privacy and decentralization is to use cryptography to improve privacy on the blockchain and decentralized systems more generally. We will investigate means of privacy-preserving authentication, such as electronic currencies, and other applications of blockchain and distributed transparency mechanisms.

8.2 Bilateral grants with industry

PRESTO: PRocessing Encrypted Streams for Traffic Oversight

Program: ANR PRCE

Duration: January 2020 – June 2024

Coordinator: David Pointcheval

Partners: Inria/ENS/Cascade, IMT/Telecom SudParis, LORIA, Orange Labs, 6cure

Inria contact: David Pointcheval

Summary: While GDPR (General Data Protection Regulation) imposes some privacy constraints, growing threats against servers require traffic analysis to detect malicious behaviors. This analysis includes identification of illegitimate connections to mitigate denial of service attacks, content filtering to limit content exposition or content leakage, and log management for later forensic analysis. Security Information and Event Management (SIEM) that deals with internal and external threats should still remain effective under GDPR constraints. Data protection usually means encryption, which in turn heavily limits the traffic analysis capabilities.

The main goal of this project is to bridge the gap between these two security and privacy requirements, with advanced cryptographic tools (such as searchable encryption, functional encryption, fully homomorphic encryption, and multi-party computation) in order to provide privacy to the end-users while allowing traffic monitoring by the network security manager. While current tools already work on encrypted streams by analyzing the meta-data only, advanced encryption tools may enrich the analysis by specific researches in the encrypted payload.

ANBLIC: Analysis in Blind Clouds

Program: FUI

Duration: January 2018 – June 2021

Coordinator: Wallix

Partners: UPEC, CEA, Atos, SOGETI, CoeSSI, Inria/ENS/Cascade

Inria contact: David Pointcheval

Summary: The main goal is to industrialize for the first time several privacy enhancing technologies that are on the edge of theory and practice.

Fully Homomorphic Encryption let cloud providers compute arbitrary functions on their client's encrypted data, ensuring at the same time full privacy and functionality. Functional Encryption is a refinement of classical encryption, which allows data owners to delegate fine-grained access to their data. Thus it is possible to enable the computation of aggregated statistics over your personal data, while cryptographically ensuring its confidentiality.

However both these technologies still suffer from prohibitive inefficiencies for business applications. ANBLIC's academic partners will create new cryptographic schemes and performance models, tailored for industrial use cases, and create the first real-life scenario of encrypted queries on encrypted data and on open data.

RISQ: Regroupement de l’Industrie française pour la Sécurité Post-Quantique

Program: GDN

Duration: February 2017 – September 2020

Coordinator: Secure-IC

Partners: ANSSI, AIRBUS, C-S, CEA LIST, CryptoExperts, Inria/ENS/Cascade, GEMALTO, Inria/AriC, IRISA, Orange Labs, THALES, UVSQ, PCQC

Inria contact: Phong Nguyen

Summary: The main goal of RISQ is to help the French Industry and Academia become a significant international player in the transition to post-quantum cryptography.

9 Partnerships and cooperations

9.1 European initiatives

PARQ: Lattices in a Parallel and Quantum World

Program: H2020 ERC Advanced Grant

Duration: July 2020 – June 2025

Coordinator: Phong Nguyen

Summary: Quantum computers could one day become so powerful that they could break even the most sophisticated cryptography. This means that our internet communications and e-commerce will no longer be safe. Another future challenge is the threat posed by new environments such as Big Data, the Internet of Things and cryptocurrencies, where traditional cryptography is not enough. The goal of the PARQ project is to guarantee the security of lattice-based cryptography, which have been proposed for quantum-safe cryptography, homomorphic encryption and lightweight public-key cryptography. Specifically, the project will identify the best parallel and quantum algorithms for lattice problems, and propose practical methods to choose safe parameters according to the threat level.

CryptoCloud: Cryptography for the Cloud

Program: FP7 ERC Advanced Grant

Duration: June 2014 – May 2020

Coordinator: David Pointcheval

Summary: The goal of the CryptoCloud project is to develop new interactive tools to provide privacy in the Cloud.

aSCEND: Secure Computation on Encrypted Data

Program: H2020 ERC Starting Grant

Duration: June 2015 – June 2020

Coordinator: Hoeteck Wee

Summary: The goals of the aSCEND project are (i) to design pairing- and lattice-based functional encryption that are more efficient and ultimately viable in practice; and (ii) to obtain a richer understanding of expressive functional encryption schemes and to push the boundaries from encrypting data to encrypting software.

FENTEC: Functional Encryption Technologies

Program: H2020 ICT

Duration: January 2018 – February 2021

Coordinator: ATOS Spain SA

Partners: Inria/ENS (France), Flensburg University (Germany), KU Leuven (Belgium), University of Helsinki (Finland), Nagra (Switzerland), XLAB (Switzerland), University of Edinburgh (United Kingdom), WALLIX (France)

Inria contact: Michel Abdalla

Summary: Functional encryption (FE) has recently been introduced as a new paradigm of encryption systems to overcome all-or-nothing limitations of classical encryption. In an FE system the decryptor deciphers a function over the message plaintext: such functional decryptability makes it feasible to process encrypted data (e.g. on the Internet) and obtain a partial view of the message plaintext. This extra flexibility over classical encryption is a powerful enabler for many emerging security technologies (i.e. controlled access, searching and computing on encrypted data, program obfuscation...). FENTEC's mission is to make the functional encryption paradigm ready for wide-range applications, integrating it in ICT technologies as naturally as classical encryption. The primary objective is the efficient and application-oriented development of functional encryption systems. FENTEC's team of cryptographers, software and hardware experts and information technology industry partners will document functional encryption needs of specific applications and subsequently design, develop, implement and demonstrate applied use of functional cryptography. Ultimately, a functional encryption library for both SW and HW-oriented application will be documented and made public so that it may be used by European ICT entities. With it, the FENTEC team will build emerging security technologies that increase the trustworthiness of the European ICT services and products. Concretely, the FENTEC team will showcase the expressiveness and versatility of the functional encryption paradigm in 3 use cases: (i) Privacy-preserving digital currency, enforcing flexible auditing models; (ii) Anonymous data analytics enabling computation of statistics over encrypted data, protecting European Fundamental Rights of Data Protection and Privacy; (iii) Key and content distribution with improved performance & efficiency as foundational technology for establishing secure communication among a vast number of IOT devices.

9.2 National initiatives

SaFED: Safe and Functional Encrypted Databases

Program: ANR JCJC

Duration: October 2019 – March 2024

Coordinator: Brice Minaud

Partners: DGA, Inria/ENS/Cascade

Summary: This project addresses the security of encrypted databases, with the proposal of new searchable encryption techniques and deeper security analysis.

CryptiQ: Cryptography in a Quantum World

Program: ANR JCJC

Duration: January 2019 – June 2023

Coordinator: Céline Chevalier

Partners: Univ Panthéon-Assas

Summary: In a context where the threat of a quantum attacker which could completely break many widely-used public-key cryptosystems becomes plausible and quantum communication technologies become available in practice, the goal of the project is to anticipate these major changes in three plausible scenarios (post-quantum cryptography, quantum-enhanced classical cryptography and cryptography in a quantum world), and find in each case the most relevant security models to construct and prove concrete protocols.

ALAMBIC: AppLicAtions of MalleaBIlity in Cryptography

Program: ANR PRC

Duration: October 2016 – September 2021

Coordinator: Damien Vergnaud

Partners: ENS Lyon, Université Limoges, Inria/ENS/Cascade

Inria contact: David Pointcheval

Summary: The main objectives of the proposal are the following:

- Define theoretical models for "malleable" cryptographic primitives that capture strong practical attacks (in particular, in the settings of secure computation outsourcing, server-aided cryptography, cloud computing and cryptographic proof systems);
- Analyze the security and efficiency of primitives and constructions that rely on malleability;
- Conceive novel cryptographic primitives and constructions (for secure computation outsourcing, server-aided cryptography, multi-party computation, homomorphic encryption and their applications);
- Implement these new constructions in order to validate their efficiency and effective security.

10 Dissemination

10.1 Promoting scientific activities

10.1.1 Scientific events: organisation

- Seminars are organized: see `https://crypto.di.ens.fr/web2py/index/seminars`
- BibTeX database of papers related to Cryptography, open and widely used by the community (see `https://cryptobib.di.ens.fr`)

Steering Committees of International Conferences

- Steering committee of CANS: David Pointcheval
- Steering committee of PKC: David Pointcheval
- Steering committee of LATINCRYPT: Michel Abdalla
- Steering committee of Information-Theoretic Cryptography Conference: Hoeteck Wee

Board of International Organisations

- President of the *International Association for Cryptologic Research* (IACR): Michel Abdalla (2020 – 2022)

10.1.2 Scientific events: selection

Program Committee Member

- CT-RSA '20 (San Francisco, California, USA): Céline Chevalier, David Pointcheval
- ProvSec '20 (online due to covid): Céline Chevalier
- Asiacrypt '20 (online due to covid): Brice Minaud

10.1.3 Journal

Editor-in-Chief
- of the *International Journal of Applied Cryptography (IJACT)* – Inderscience Publishers: David Pointcheval

Associate Editor
- of *ETRI Journal*: Michel Abdalla
- of *Journal of Mathematical Cryptology*: Phong Nguyen
- of *Applicable Algebra in Engineering, Communication and Computing*: David Pointcheval
- of *Transactions on Symmetric Cryptology/FSE '20*: Brice Minaud
- of *Transactions on Symmetric Cryptology special issue on NIST competition*: Brice Minaud

10.2 Teaching - Supervision - Juries

10.2.1 Education

- Master: Michel Abdalla, Brice Minaud, Phong Nguyen, David Pointcheval, Cryptography, M2, MPRI
- Master: Phong Nguyen, Cryptography, M2, ESIEA
- Master: Céline Chevalier, Data Science, M2, Univ Panthéon-Assas
- Bachelor: Brice Minaud, David Pointcheval, Introduction to Cryptology, L3/M1, ENS
- Bachelor: Michel Abdalla, Formal Languages, Computability, and Complexity, L3/M1, ENS

10.2.2 PhD's in the Team

Defenses

- PhD: Michele Orrù, Non-interactive arguments of knowledge, ENS, April 7th, 2020 (Supervisors: Georg Fuchsbauer & Hoeteck Wee)
- PhD: Mélissa Rossi, Extended security of lattice-based cryptography, ENS, September 10th, 2020 (Supervisors: Michel Abdalla & Henri Gilbert, at ANSSI)
- PhD: Balthazar Bauer, Transferable e-cash: an analysis in the Algebraic Group Model, ENS, December 14th, 2020 (Supervisors: Georg Fuchsbauer & David Pointcheval)

Supervision

- PhD in progress: Chloé Hébant, Big Data and Privacy, from 2017, David Pointcheval (with Duong Hieu Phan, at Telecom ParisTech)
- PhD in progress: Antoine Plouviez, Privacy and Decentralization, from 2018, David Pointcheval and Georg Fuchsbauer
- PhD in progress: Quoc-Huy Vu, Cryptography in a Quantum World, from 2018, Céline Chevalier
- PhD in progress: Baptiste Cottier, Privacy-preserving anomaly detection, from 2019, David Pointcheval (with Olivier Blazy, at Limoges)
- PhD in progress: Théo Ryffel, Privacy-preserving federated learning, from 2019, Francis Bach and David Pointcheval
- PhD in progress: Lénaïck Gouriou, Advanced encryption with post-quantum security, from 2019, David Pointcheval (with Cécile Delerablée at Leanear)
- PhD in progress: Léonard Assouline, Encryption for Fine-Grained Access Control, from 2020, Michel Abdalla

- PhD in progress: Paola de Perthuis, Computations on encrypted data, from 2020, David Pointcheval (with Malika Izabachène at Cosmian)
- PhD in progress: Michael Reichle, Searchable encryption, from 2020, Brice Minaud and Michel Abdalla
- PhD in progress: Hugo Senet, Anonymous Post-Quantum Cryptographic Protocols, from 2020, Céline Chevalier (with Thomas Ricosset at Thales)

10.2.3 Committees

- PhD Guillaume Kaim. *Cryptographie post-quantique pour la protection de la vie privée* – Université de Rennes - France – December 16th, 2020: David Pointcheval
- PhD Laura Brouilhet. *Génération des protocoles en cas multi-utilisateur* – Université de Limoges - France – December 15th, 2020: Céline Chevalier
- PhD Balthazar Bauer. *Transferable e-cash: an analysis in the Algebraic Group Model* – Ecole Normale Supérieure - France – December 14th, 2020: Georg Fuchsbauer and David Pointcheval (Co-supervisors)
- PhD Martin Zuber. *Contributions to data confidentiality in machine learning by means of homomorphic encryption* – CEA, Saclay – France – December 10th, 2020: David Pointcheval (Reviewer)
- PhD Achraf Lassoued. *Composantes géantes dans les flux de données* – Université Panthéon-Assas - France – November 16th, 2020: Céline Chevalier
- PhD Angèle Bossuat. *Provable Security of Real-World Protocols* – Université de Rennes - France – October 6th, 2020: Céline Chevalier (Reviewer), David Pointcheval (Chair)
- PhD Patrick Towa. *Privacy-Preserving Cryptographic Protocols* – Ecole Normale Supérieure - France – September 30th, 2020: David Pointcheval (Chair)
- PhD Mélissa Rossi. *Extended security of lattice-based cryptography* – Ecole Normale Supérieure - France – April 7th, 2020: Michel Abdalla (Chair)
- PhD Francesco Berti. *Authentication in the presence of side-channel leakage* – Université catholique de Louvain - Belgium – September 4th, 2020: Michel Abdalla
- PhD Sandra Rasoamiaramanana. *Conception of white-box encryption schemes for mobile security* – Université de Lorraine - France – June 12th, 2020: Brice Minaud
- PhD Michele Orrù. *Non-interactive arguments of knowledge* – Ecole Normale Supérieure - France – April 7th, 2020: Georg Fuchsbauer and Hoeteck Wee (Co-supervisors), David Pointcheval (Chair)
- PhD Thomas Espitau. *Algorithmic aspects of algebraic lattices* – Sorbonne Université - France – January 14th, 2020: Phong Nguyen (Chair)

11 Scientific production

11.1 Major publications

[1] M. Abdalla, D. Catalano and D. Fiore. ‘Verifiable Random Functions: Relations to Identity-Based Key Encapsulation and New Constructions’. In: *Journal of Cryptology* 27.3 (2014), pp. 544–593.

[2] M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev and M. Ohkubo. ‘Structure-Preserving Signatures and Commitments to Group Elements’. In: *Journal of Cryptology* 29.2 (2016), pp. 363–421.

[3] F. Benhamouda, O. Blazy, C. Chevalier, D. Pointcheval and D. Vergnaud. ‘New Techniques for SPHFs and Efficient One-Round PAKE Protocols’. In: *Advances in Cryptology – Proceedings of CRYPTO ’13 (1)*. Ed. by R. Canetti and J. A. Garay. Vol. 8042. Lecture Notes in Computer Science. Springer, 2013, pp. 449–475.

[4] P. Chaidos, V. Cortier, G. Fuchsbauer and D. Galindo. 'BeleniosRF: A Non-interactive Receipt-Free Electronic Voting Scheme'. In: *Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS '16)*. Ed. by E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers and S. Halevi. ACM Press, 2016, pp. 1614–1625.

[5] Y. Dodis, D. Pointcheval, S. Ruhault, D. Vergnaud and D. Wichs. 'Security Analysis of Pseudo-Random Number Generators with Input: /dev/random is not Robust'. In: *Proceedings of the 20th ACM Conference on Computer and Communications Security (CCS '13)*. Ed. by V. D. Gligor and M. Yung. Berlin, Germany: ACM Press, 2013, pp. 647–658.

[6] R. Gay, D. Hofheinz, E. Kiltz and H. Wee. 'Tightly CCA-Secure Encryption Without Pairings'. In: *Advances in Cryptology – Proceedings of Eurocrypt '16 (2)*. Ed. by M. Fischlin and J.-S. Coron. Vol. 9665. Lecture Notes in Computer Science. Springer, 2016, pp. 1–27.

[7] S. Gorbunov, V. Vaikuntanathan and H. Wee. 'Predicate Encryption for Circuits from LWE'. In: *Advances in Cryptology – Proceedings of CRYPTO '15 (2)*. Ed. by R. Gennaro and M. Robshaw. Vol. 9216. Lecture Notes in Computer Science. Springer, 2015, pp. 503–523.

[8] V. Lyubashevsky, C. Peikert and O. Regev. 'On Ideal Lattices and Learning with Errors over Rings'. In: *Journal of the ACM* 60.6 (2013), 43:1–43:35.

[9] W. Quach, H. Wee and D. Wichs. 'Laconic Function Evaluation and Applications'. In: *59th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2018)*. Ed. by M. Thorup. IEEE, 2018.

11.2 Publications of the year

International peer-reviewed conferences

[10] M. Abdalla, M. Barbosa, T. Bradley, S. Jarecki, J. Katz and J. Xu. 'Universally Composable Relaxed Password Authenticated Key Exchange'. In: CRYPTO 2020 - 40th Annual International Cryptology Conference. Vol. 12170. Lecture Notes in Computer Science. Santa Barbara / Virtual, United States, 10th Aug. 2020, pp. 278–307. DOI: 10.1007/978-3-030-56784-2_10. URL: https://hal.inria.fr/hal-02948678.

[11] M. Abdalla, F. Bourse, H. Marival, D. Pointcheval, A. Soleimanian and H. Waldner. 'Multi-Client Inner-Product Functional Encryption in the Random-Oracle Model'. In: SCN 2020 - 12th International Conference Security and Cryptography for Networks. Vol. LNCS - Lecture Notes in Computer Science. 12238. Amalfi / Virtual, Italy, 7th Sept. 2020, pp. 525–545. DOI: 10.1007/978-3-030-57990-6_26. URL: https://hal.inria.fr/hal-02948657.

[12] M. Abdalla, D. Catalano, R. Gay and B. Ursu. 'Inner-Product Functional Encryption with Fine-Grained Access Control'. In: Asiacrypt 2020 - 26th Annual International Conference on the Theory and Application of Cryptology and Information Security - 26th International Conference on the Theory and Application of Cryptology and Information Security. Vol. 12493. Lecture Notes in Computer Science. Virtual, South Korea: https://asiacrypt.iacr.org/2020/, 5th Dec. 2020, pp. 467–497. DOI: 10.1007/978-3-030-64840-4_16. URL: https://hal.inria.fr/hal-03043537.

[13] M. Abdalla, J. Gong and H. Wee. 'Functional Encryption for Attribute-Weighted Sums from k-Lin'. In: CRYPTO 2020 - 40th Annual International Cryptology Conference. Vol. 12170. Lecture Notes in Computer Science. Santa Barbara / Virtual, United States: https://crypto.iacr.org/2020, 10th Aug. 2020, pp. 685–716. DOI: 10.1007/978-3-030-56784-2_23. URL: https://hal.inria.fr/hal-02948674.

[14] D. Aggarwal, J. Li, P. Q. Nguyen and N. Stephens-Davidowitz. 'Slide Reduction, Revisited—Filling the Gaps in SVP Approximation'. In: CRYPTO 2020 - 40th Annual International Cryptology Conference. Santa Barbara / Virtual, United States, 10th Aug. 2020, pp. 274–295. DOI: 10.1007/978-3-030-56880-1_10. URL: https://hal.inria.fr/hal-03068203.

[15] B. Bauer and G. Fuchsbauer. 'Efficient Signatures on Randomizable Ciphertexts'. In: *Security and Cryptography for Networks. SCN 2020*. SCN 2020 - 12th International Conference Security and Cryptography for Networks. Vol. LNCS - Lecture Notes in Computer Science. SCN 2020 - 12th International Conference Security and Cryptography for Networks. 12238. Amalfi / Virtual, Italy, 7th Sept. 2020, pp. 359–381. DOI: 10.1007/978-3-030-57990-6_18. URL: https://hal.archives-ouvertes.fr/hal-02968280.

[16] B. Bauer, G. Fuchsbauer and J. Loss. 'A Classification of Computational Assumptions in the Algebraic Group Model'. In: *Advances in Cryptology – CRYPTO 2020*. CRYPTO 2020 - 40th Annual International Cryptology Conference. Vol. LNCS. CRYPTO 2020 - 40th Annual International Cryptology Conference 12171. Santa Barbara / Virtual, United States, 10th Aug. 2020, pp. 121–151. DOI: 10.1007/978-3-030-56880-1_5. URL: https://hal.archives-ouvertes.fr/hal-02968271.

[17] O. Blazy, L. Brouilhet, C. Chevalier and N. Fournaise. 'Round-optimal Constant-size Blind Signatures'. In: SECRYPT 2020 - 17th International Conference on Security and Cryptography. Lieusaint - Paris / Virtual, France, 8th July 2020, pp. 213–224. DOI: 10.5220/0009888702130224. URL: https://hal.inria.fr/hal-03130894.

[18] O. Blazy, P. Towa and D. Vergnaud. 'Public-Key Generation with Verifiable Randomness'. In: *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Dadjeon South Korea, December 6-10, 2020. Proceedings, Part I*. Asiacrypt 2020 - 26th Annual International Conference on the Theory and Application of Cryptology and Information Security. Vol. 12491. Lecture Notes in Computer Science. Daejeon / Virtual, South Korea, 7th Dec. 2020, pp. 97–127. DOI: 10.1007/978-3-030-64837-4_4. URL: https://hal.archives-ouvertes.fr/hal-02929843.

[19] D. Catalano, G. Fuchsbauer and A. Soleimanian. 'Double-Authentication-Preventing Signatures in the Standard Model'. In: SCN 2020 - 12th International Conference Security and Cryptography for Networks. Vol. 12238. LNCS - Lecture Notes in Computer Science. Amalfi / Virtual, Italy, 14th Sept. 2020, pp. 338–358. URL: https://hal.inria.fr/hal-03066338.

[20] J. Chotard, E. Dufour-Sans, R. Gay, D. H. Phan and D. Pointcheval. 'Dynamic Decentralized Functional Encryption'. In: CRYPTO 2020 - 40th Annual International Cryptology Conference. Vol. LNCS. CRYPTO 2020 - 40th Annual International Cryptology Conference 12170. Santa Barbara / Virtual, United States, 10th Aug. 2020, pp. 747–775. DOI: 10.1007/978-3-030-56784-2_25. URL: https://hal.inria.fr/hal-02947359.

[21] X. T. Do, D. H. Phan and D. Pointcheval. 'Traceable Inner Product Functional Encryption'. In: *Topics in Cryptology – CT-RSA 2020*. CT-RSA 2020 - Topics in Cryptology. Vol. LNCS. 12006. San Francisco, United States, 14th Feb. 2020, pp. 564–585. DOI: 10.1007/978-3-030-40186-3_24. URL: https://hal.inria.fr/hal-02894483.

[22] D. Fiore, A. Nitulescu and D. Pointcheval. 'Boosting Verifiable Computation on Encrypted Data'. In: *Public-Key Cryptography – PKC 2020; Public-Key Cryptography – PKC 2020*. PKC 2020 - 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography. Vol. LNCS. 12111. Edinburgh / Virtual, United Kingdom, 29th Apr. 2020, pp. 124–154. DOI: 10.1007/978-3-030-45388-6_5. URL: https://hal.inria.fr/hal-02894482.

[23] J. Gong and H. Wee. 'Adaptively Secure ABE for DFA from k-Lin and More'. In: *EUROCRYPT 2020 - International Conference on Theory and Applications of Cryptographic Techniques*. EUROCRYPT 2020 - 9th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Vol. LNCS. 12107. Zagreb / Virtual, Croatia: https://eprint.iacr.org/2020/194, 1st May 2020, pp. 278–308. DOI: 10.1007/978-3-030-45727-3_10. URL: https://hal.inria.fr/hal-02894509.

[24] C. Hébant, D. H. Phan and D. Pointcheval. 'Linearly-Homomorphic Signatures and Scalable Mix-Nets'. In: PKC 2020 - IACR International Conference on Practice and Theory of Public-Key Cryptography. Vol. LNCS. 12111. Edinburgh / Virtual, United Kingdom, 29th Apr. 2020, pp. 597–627. DOI: 10.1007/978-3-030-45388-6_21. URL: https://hal.inria.fr/hal-02947353.

[25] B. Libert, A. Passelègue, H. Wee and D. J. Wu. ‘New Constructions of Statistical NIZKs: Dual-Mode DV-NIZKs and More’. In: Eurocrypt 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Zagreb / Virtual, Croatia, 10th May 2020, pp. 1–85. URL: https://hal.inria.fr/hal-02993608.

[26] L. Music, E. Kashefi and C. Chevalier. ‘Dispelling Myths on Superposition Attacks: Formal Security Model and Attack Analyses’. In: *International Conference on Provable Security, ProvSec 2020: Provable and Practical Security*. ProvSec 2020 - 14th International Conference on Provable and Practical Security. Vol. 12505. Lecture Notes in Computer Science. Singapour / Virtual, Singapore, 20th Nov. 2020, pp. 318–337. DOI: 10.1007/978-3-030-62576-4_16. URL: https://hal.archives-ouvertes.fr/hal-03097496.

[27] P. Towa and D. Vergnaud. ‘Succinct Diophantine-Satisfiability Arguments’. In: Asiacrypt 2020 - 26th Annual International Conference on the Theory and Application of Cryptology and Information Security. Vol. 12493. Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Dadjeon South Korea, December 6-10, 2020. Proceedings, Part III. Daejeon / Virtual, South Korea, 7th Dec. 2020, pp. 774–804. DOI: 10.1007/978-3-030-64840-4_26. URL: https://hal.archives-ouvertes.fr/hal-02929841.

Conferences without proceedings

[28] C. Chevalier, Q. H. Vu and E. Ebrahimi Khaleghi. ‘On Security Notions for Encryption in a Quantum World’. In: QCrypt 2020 - 10th International Conference on Quantum Cryptography. Amsterdam / Virtual, Netherlands, 10th Aug. 2020. URL: https://hal.inria.fr/hal-03130890.

[29] A. Ziller, J. Passerat-Palmbach, T. Ryffel, D. Usynin, A. Trask, I. Da Lima, J. Mancuso, M. Makowski, D. Rueckert, R. Braren and G. Kaissis. ‘Privacy-preserving medical image analysis’. In: MED-NEURIPS 2020 : Medical Imaging meets NeurIPS. Online, France, 12th Dec. 2020. URL: https://hal.inria.fr/hal-03065933.

Doctoral dissertations and habilitation theses

[30] B. Bauer. ‘Transferable e-cash: an analysis in the Algebraic Group Model’. ED 386 : École doctorale de sciences mathématiques de Paris centre, UPMC, 14th Dec. 2020. URL: https://hal.inria.fr/tel-03086982.

[31] M. Orrù. ‘Non-interactive arguments of knowledge’. ENS Paris, 7th Apr. 2020. URL: https://hal.archives-ouvertes.fr/tel-02947185.

[32] M. Rossi. ‘Extended Security of Lattice-Based Cryptography’. Équipe CASCADE, Département d’Informatique de l’ENS de Paris; Université PSL, 10th Sept. 2020. URL: https://hal.archives-ouvertes.fr/tel-02946399.

Reports & preprints

[33] M. Abdalla. *Security Analysis of Olvid’s SAS-based Trust Establishment Protocol.* IACR Cryptology ePrint Archive, 29th June 2020. URL: https://hal.inria.fr/hal-03003687.

[34] M. Brundage, S. Avin, J. Wang, H. Belfield, G. Krueger, G. Hadfield, H. Khlaaf, J. Yang, H. Toner, R. Fong et al. *Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims.* 15th Dec. 2020. URL: https://hal.inria.fr/hal-03065927.

[35] T. Ryffel, D. Pointcheval and F. Bach. *ARIANN: Low-Interaction Privacy-Preserving Deep Learning via Function Secret Sharing.* 10th July 2020. URL: https://hal.inria.fr/hal-02896127.