RESEARCH CENTRE

Saclay - Île-de-France

IN PARTNERSHIP WITH:

CNRS, Ecole Polytechnique

2021
ACTIVITY REPORT

Project-Team

GRACE

Geometry, arithmetic, algorithms, codes and encryption

IN COLLABORATION WITH: Laboratoire d'informatique de l'école polytechnique (LIX)

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Algorithmics, Computer Algebra and Cryptology

Contents

Project-Team GRACE

Creation of the Project-Team: 2013 July 01

Keywords

Computer sciences and digital sciences

A2.3.1. – Embedded systems

A4.2. – Correcting codes

A4.3. – Cryptography

A4.3.1. – Public key cryptography

A4.3.3. – Cryptographic protocols

A4.3.4. – Quantum Cryptography

A4.4. – Security of equipment and software

A4.6. – Authentication

A4.7. – Access control

A4.8. – Privacy-enhancing technologies

A4.9. – Security supervision

A7.1. – Algorithms

A8.1. – Discrete mathematics, combinatorics

A8.4. – Computer Algebra

A8.5. – Number theory

Other research topics and application domains

B5.11. – Quantum systems

B9.5.1. – Computer science

B9.5.2. – Mathematics

B9.10. – Privacy

1 Team members, visitors, external collaborators

Research Scientists

- Alain Couvreur [Team leader, Inria, Senior Researcher, HDR]
- Daniel Augot [Inria, Senior Researcher, HDR]
- Thomas Debris [Inria, Researcher]
- Benjamin Smith [Inria, Researcher]

Faculty Members

- Olivier Blazy [École polytechnique, Professor, from Sep 2021, HDR]
- Françoise Levy-Dit-Vehel [École Nationale Supérieure de Techniques Avancées, Professor, HDR]
- François Morain [École polytechnique, Professor, HDR]

Post-Doctoral Fellows

- Jade Nardi [Inria, until Sep 2021]
- Azam Soleimanian [École polytechnique]
- Gustavo Souza Banegas [Inria]
- Ilaria Zappatore [Inria]

PhD Students

- Maxime Anvari [Ministère des armées]
- Anais Barthoulot [Orange, from Sep 2021]
- Lucas Benmouffok [Institut de recherche technologique System X, Until September 2021]
- Maxime Bombar [École polytechnique]
- Sarah Bordage [École polytechnique]
- Alexis Challande [Quarkslab]
- Mathilde Chenu De La Morinerie [École polytechnique]
- Clement Ducros [Université de Paris, from Oct 2021]
- Youssef El Housni [ConsenSys - USA, CIFRE]
- Antonin Leroux [Ministère des armées]
- Simon Montoya [Idemia, CIFRE]
- Isabella Panaccione [Inria]
- Maxime Roméas [École polytechnique]
- Edouard Rousseau [Institut Telecom ex GET Groupe des Écoles des Télécommunications , until Jun 2021]
- Angelo Saadeh [Telecom ParisTech]

Interns and Apprentices

- Clemence Chevignard [Inria, from Jul 2021]
- Laetitia Debesse [Inria, from Jun 2021 until Nov 2021]
- Milena Nedeljkovic [Inria, from Jun 2021 until Jul 2021]
- Mihails Valtusovs [École polytechnique, from Feb 2021 until Mar 2021]

Administrative Assistant

- Maria Agustina Ronco [Inria]

Visiting Scientists

- Alp Bassa [Université du Bosphore Istanbul - Turquie, until Feb 2021]
- Giuseppe Cotardo [Université de la ville de Dublin - Irlande, from Sep 2021]

External Collaborators

- Philippe Lebacque [Univ de Franche-Comté, from Oct 2021, HDR]
- Matthieu Rambaud [Institut Telecom ex GET Groupe des Écoles des Télécommunications]
- Guénaël Renault [Secrétariat Général de la Défense et de la Sécurité Nationale]
- Luca de Feo [Univ de Versailles Saint-Quentin-en-Yvelines, HDR]

2 Overall objectives

2.1 Scientific foundations

Grace combines expertise and deep knowledge in algorithmic number theory and algebraic geometry, to build and analyse (public-key) cryptosystems, design new error correcting codes, with real-world concerns like cybersecurity or blockchains (software and hardware implementations, secure implementations in constrained environments, countermeasures against side channel attacks, white box cryptography).

The foundations of Grace therefore lie in algorithmic number theory (fundamental algorithms primality, factorization), number fields, the arithmetic geometry of curves, algebraic geometry and the theory of algebraic codes.

Arithmetic Geometry is the meeting point of algebraic geometry and number theory: the study of geometric objects defined over arithmetic number systems. In our case, the most important objects are curves and their Jacobians over finite fields; these are fundamental to our applications in both coding theory and cryptology. Jacobians of curves are excellent candidates for cryptographic groups when constructing efficient instances of public-key cryptosystems, of which Diffie–Hellman key exchange is an instructive example.

Coding Theory studies originated with the idea of using redundancy in messages to protect them against noise and errors. While the last decade of the 20th century has seen the success of so-called iterative decoding methods, we see now many new ideas in the realm of algebraic coding, with the foremost example being list decoding, (zero knowledge or not) proofs of computation.

Part of the activities of the team are oriented towards post-quantum cryptography, either based on elliptic curves (isogenies) or code-based. Also the team study relevant cryptography for the blockchain arena.

The group is strongly invested in cybersecurity: software security, secure hardware implementations, privacy, etc.

3 Research program

3.1 Algorithmic Number Theory

Participants: Luca De Feo, François Morain, Benjamin Smith, Mathilde de la Morinerie, Antonin Leroux, Guénaël Renault.

Algorithmic Number Theory is concerned with replacing special cases with general algorithms to solve problems in number theory. In the Grace project, it appears in three main threads:

- fundamental algorithms for integers and polynomials (including primality and factorization);
- algorithms for finite fields (including discrete logarithms);
- algorithms for algebraic curves.

Clearly, we use computer algebra in many ways. Research in cryptology has motivated a renewed interest in Algorithmic Number Theory in recent decades—but the fundamental problems still exist *per se*. Indeed, while algorithmic number theory application in cryptanalysis is epitomized by applying factorization to breaking RSA public key, many other problems, are relevant to various area of computer science. Roughly speaking, the problems of the cryptological world are of bounded size, whereas Algorithmic Number Theory is also concerned with asymptotic results.

3.2 Arithmetic Geometry: Curves and their Jacobians

Participants: Luca De Feo, François Morain, Benjamin Smith, Mathilde de la Morinerie, Antonin Leroux.

Theme: Arithmetic Geometry: Curves and their Jacobians *Arithmetic Geometry* is the meeting point of algebraic geometry and number theory: that is, the study of geometric objects defined over arithmetic number systems (such as the integers and finite fields). The fundamental objects for our applications in both coding theory and cryptology are curves and their Jacobians over finite fields.

An algebraic *plane curve* $\mathcal{X}$ over a field

$\mathbf{K}$ is defined by an equation

$$\mathcal{X} : F_{\mathcal{X}}(x, y) = 0 \quad \text{where } F_{\mathcal{X}} \in \mathbf{K}[x, y].$$

(Not every curve is planar—we may have more variables, and more defining equations—but from an algorithmic point of view, we can always reduce to the plane setting.) The *genus* $g_{\mathcal{X}}$ of $\mathcal{X}$ is a non-negative integer classifying the essential geometric complexity of $\mathcal{X}$; it depends on the degree of $F_{\mathcal{X}}$ and on the number of singularities of $\mathcal{X}$. The curve $\mathcal{X}$ is associated in a functorial way with an algebraic group $J_{\mathcal{X}}$, called the *Jacobian* of $\mathcal{X}$. The group $J_{\mathcal{X}}$ has a geometric structure: its elements correspond to points on a $g_{\mathcal{X}}$-dimensional projective algebraic group variety. Typically, we do not compute with the equations defining this projective variety: there are too many of them, in too many variables, for this to be convenient. Instead, we use fast algorithms based on the representation in terms of classes of formal sums of points on $\mathcal{X}$.

The simplest curves with nontrivial Jacobians are curves of genus 1, known as *elliptic curves*; they are typically defined by equations of the form $y^2 = x^3 + Ax + B$. Elliptic curves are particularly important given their central role in public-key cryptography over the past two decades. Curves of higher genus are important in both cryptography and coding theory.

3.3 Curve-Based cryptology

Participants: Luca De Feo, François Morain, Benjamin Smith, Mathilde de la Morinerie, Antonin Leroux.

Theme: Curve-Based Cryptology

Jacobians of curves are excellent candidates for cryptographic groups when constructing efficient instances of public-key cryptosystems. Diffie–Hellman key exchange is an instructive example.

Suppose Alice and Bob want to establish a secure communication channel. Essentially, this means establishing a common secret *key*, which they will then use for encryption and decryption. Some decades ago, they would have exchanged this key in person, or through some trusted intermediary; in the modern, networked world, this is typically impossible, and in any case completely unscalable. Alice and Bob may be anonymous parties who want to do e-business, for example, in which case they cannot securely meet, and they have no way to be sure of each other's identities. Diffie–Hellman key exchange solves this problem. First, Alice and Bob publicly agree on a cryptographic group G with a generator P (of order N); then Alice secretly chooses an integer a from $[1..N]$, and sends aP to Bob. In the meantime, Bob secretly chooses an integer b from $[1..N]$, and sends bP to Alice. Alice then computes $a(bP)$, while Bob computes $b(aP)$; both have now computed abP, which becomes their shared secret key. The security of this key depends on the difficulty of computing abP given P, aP, and bP; this is the Computational Diffie–Hellman Problem (CDHP). In practice, the CDHP corresponds to the Discrete Logarithm Problem (DLP), which is to determine a given P and aP.

This simple protocol has been in use, with only minor modifications, since the 1970s. The challenge is to create examples of groups G with a relatively compact representation and an efficiently computable group law, and such that the DLP in G is hard (ideally approaching the exponential difficulty of the DLP in an abstract group). The Pohlig–Hellman reduction shows that the DLP in G is essentially only as hard as the DLP in its largest prime-order subgroup. We therefore look for compact and efficient groups of prime order.

The classic example of a group suitable for the Diffie–Hellman protocol is the multiplicative group of a finite field $\mathbf{F}_q$. There are two problems that render its usage somewhat less than ideal. First, it has too much structure: we have a subexponential Index Calculus attack on the DLP in this group, so while it is very hard, the DLP falls a long way short of the exponential difficulty of the DLP in an abstract group. Second, there is only one such group for each q: its subgroup treillis depends only on the factorization of $q-1$, and requiring $q-1$ to have a large prime factor eliminates many convenient choices of q.

This is where Jacobians of algebraic curves come into their own. First, elliptic curves and Jacobians of genus 2 curves do not have a subexponential index calculus algorithm: in particular, from the point of view of the DLP, a generic elliptic curve is currently *as strong as* a generic group of the same size. Second, they provide some diversity: we have many degrees of freedom in choosing curves over a fixed $\mathbf{F}_q$, with a consequent diversity of possible cryptographic group orders. Furthermore, an attack which leaves one curve vulnerable may not necessarily apply to other curves. Third, viewing a Jacobian as a geometric object rather than a pure group allows us to take advantage of a number of special features of Jacobians. These features include efficiently computable pairings, geometric transformations for optimised group laws, and the availability of efficiently computable non-integer endomorphisms for accelerated encryption and decryption.

3.4 Algebraic Coding Theory

Participants: Daniel Augot, Alain Couvreur, Françoise Levy-Dit-Vehel, Maxime Roméas, Sarah Bordage, Isabella Panaccione.

Theme: Coding theory

Coding Theory studies originated with the idea of using redundancy in messages to protect against noise and errors. The last decade of the 20th century has seen the success of so-called iterative decoding methods, which enable us to get very close to the Shannon capacity. The capacity of a given channel is the best achievable transmission rate for reliable transmission. The consensus in the community is that this capacity is more easily reached with these iterative and probabilistic methods than with algebraic codes (such as Reed–Solomon codes).

However, algebraic coding is useful in settings other than the Shannon context. Indeed, the Shannon setting is a random case setting, and promises only a vanishing error probability. In contrast, the algebraic Hamming approach is a worst case approach: under combinatorial restrictions on the noise, the noise can be adversarial, with strictly zero errors.

These considerations are renewed by the topic of list decoding after the breakthrough of Guruswami and Sudan at the end of the nineties. List decoding relaxes the uniqueness requirement of decoding, allowing a small list of candidates to be returned instead of a single codeword. List decoding can reach a capacity close to the Shannon capacity, with zero failure, with small lists, in the adversarial case. The method of Guruswami and Sudan enabled list decoding of most of the main algebraic codes: Reed–Solomon codes and Algebraic–Geometry (AG) codes and new related constructions "capacity-achieving list decodable codes". These results open the way to applications against adversarial channels, which correspond to worst case settings in the classical computer science language.

Another avenue of our studies is AG codes over various geometric objects. Although Reed–Solomon codes are the best possible codes for a given alphabet, they are very limited in their length, which cannot exceed the size of the alphabet. AG codes circumvent this limitation, using the theory of algebraic curves over finite fields to construct long codes over a fixed alphabet. The striking result of Tsfasman–Vladut–Zink showed that codes better than random codes can be built this way, for medium to large alphabets. Disregarding the asymptotic aspects and considering only finite length, AG codes can be used either for longer codes with the same alphabet, or for codes with the same length with a smaller alphabet (and thus faster underlying arithmetic).

From a broader point of view, wherever Reed–Solomon codes are used, we can substitute AG codes with some benefits: either beating random constructions, or beating Reed–Solomon codes which are of bounded length for a given alphabet.

Another area of Algebraic Coding Theory with which we are more recently concerned is the one of Locally Decodable Codes. After having been first theoretically introduced, those codes now begin to find practical applications, most notably in cloud-based remote storage systems.

3.5 Post-quantum cryptography

Participants: Gustavo Banegas, Maxime Bombar, Luca De Feo, Mathilde de la Morinerie, Alain Couvreur, Thomas Debris-Alazard, Antonin Leroux, Benjamin Smith.

Theme: Cryptography

A huge amount of work is being put into developing an efficient quantum computer. But even if the advent of such a computer may wait for decades, it is urgent to deploy post-quantum cryptography (PQC), *i.e:* solutions on our current devices that are quantum-safe. Indeed, an attacker could store encrypted sessions and wait until a quantum computer is available to decrypt. In this context the National Institute of Standard Technology (NIST) has launched in 2017 (see this website) a call for standardizing public-key PQC schemes (key exchanges and signatures). Among the mathematical objects to design post quantum primives, one finds error correcting codes, Euclidean lattices and isogenies.

We are currently in the final step of the standardization of the NIST and most of the selected solutions are based on codes and lattices. These preliminary results tend to show that codes and lattices will be in a near future at the ground of our numerical security. If isogenies are less represented, they remain of deep interest since they appear to be the post quantum solution providing the smallest key sizes. The purpose of our research program is to bring closer these solutions for a post-quantum security in order to improve their efficiency, diversity and to increase our trust in these propositions.

4 Application domains

4.1 Application Domain: cybersecurity

Participants: Guénaël Renault, Benjamin Smith, François Morain, Alexis Challande, Simon Montoya, Maxime Anvari, Gustavo Banegas.

We are interested in developing some interactions between cryptography and cybersecurity. In particular, we develop some researches in embedded security (side channels and fault attack), software security (finding vulnerability efficiently) and privacy (security of TOR).

4.2 Application Domain: blockchains

Participants: Daniel Augot, Lucas Benmouffok, Sarah Bordage, Youssef El Housni, François Morain, Matthieu Rambaud.

The huge hype about blockchains attracted the attention of many companies towards advanced cryptographic protocols. While basic and standard blockchain ideas rely, on the cryptographic side, on very basic and standard cryptographic primitives like signature and hash functions, more elaborate techniques from crypto could alleviate some shortcomings of blockchain, like the poor bandwith and the lack of privacy.

Team Grace is investigating two topics in these areas: secure multiparty computation and verifiable computation.

Secure multiparty computation enables several participants to compute a common function of data they each secretly own, without each participant revealing his data to the other participants. This area has seen great progress in recent years, and the cryptogaphic protocols are now mature enough for practical use. This topic is new to project-team Grace, and we will investigate it in the context of blockchains. Daniel Augot is involved in blockchains from the point of view of cryptography for better blockchains, mainly for improving privacy. A PhD student has been enrolled at IRT System-X, to study pratical use cases of Secure Multiparty Computtiton in the context of blockchains.

The topic of verifiable computation consists in verifying heavy computations done by a remote computer, using a lightweight computer which is not able to do the computation. The remore computer, called the prover, is allowed to provided a proof aside the result of the computation. This proof must be very short and fast to verify. It can also be made zero-knowledge, where the prover hides some inputs to the computation, and yet prove the result is correct.

There are two competing propositions which provide a mathematical and algorithmic background for these proof techniques: one based on a line of research dating back to the celebrated PCP theorem (from algorithmic complexity theory, using error correcting codes), and one base on the discrete logarithm problem and pairing based protocols (algorithmic number theory and elliptic curves over finite fields). Daniel Augot is advising Sarah Bordage on the first topic, also known as "STARKS" (Scalable Transparent Arguments of Knowledge), and François Morain is advising Youssef El Housni on the second topic, known as "SNARKS" (Succint Non Interactive Arguments of Knowledge).

These proofs allows to move computation off chain, pushing the burden to off chain servers, who then post results onchain, accompanied by short and easy to verify proofs onchain. This is one of the promising paths for scalability. Also, including zero-knowledge in these proofs provides privacy.

Also Daniel Augot, together with Julien Prat (economist, ENSAE), is co-leading a Polytechnique teaching and research "chair", called *Blockchain and B2B plaforms*, funded by CapGemini, Caisse des dépots and NomadicLabs, for blockchains in the industry, B2B platforms, supply chains, etc.

4.3 Cloud storage

Participants: Françoise Levy-Dit-Vehel, Maxime Roméas.

The team is concerned with several aspect of reliability and security of cloud storage, obtained mainly with tools from coding theory. On the privacy side, we build protocols for so-called Private Information Retrieval which enable a user to query a remote database for an entry, while not revealing his query. For instance, a user could query a service for stock quotes without revealing with company he is interested in. On the availability side, we study protocols for proofs of retrievability, which enable a user to get assurance that a huge file is still available on a remote server, with a low bandwith protocol which does not require to download the whole file. For instance, in a peer-to-peer distributed storage system, where nodes could be rewarded for storing data, they can be audited with proof of retrievability protocols to make sure they indeed hold the data.

We investigate these problems with algebraic coding theory for the effective constuction of protocols. To this respect, we mainly use locally decodable codes and in particular high-rate lifted codes.

Maxime Roméas is a PhD student of the team. (PhD grant from IP Paris/Ecole Polytechnique for a 3-year doctorate, Oct 2019-Sept 2022). The subject of his thesis is "The Constructive Cryptography paradigm applied to Interactive Cryptographic Proofs".

The Constructive Cryptography framework, introduced by Maurer in 2011, redefines basic cryptographic primitives and protocols starting from discrete systems of three types (resources, converters, and distinguishers). This not only permits to construct them effectively, but also lighten and sharpen their security proofs. One strength of this model is its composability. The purpose of the PhD is to apply this model to rephrase existing interactive cryptographic proofs so as to assert their genuine security, as well as to design new proofs. The main concern here is security and privacy in Distributed Storage settings. Another axis of the PhD is to augment the CC model by, e.g., introducing new functionalities to a so-called Server Memory Resource.

5 Highlights of the year

5.1 Awards

- T. Debris–Alazard received the Gilles Kahn award for his PhD Thesis *Cryptographie fondée sur les codes : nouvelles approches pour constructions et preuves; contribution en cryptanalyse* [54].

- M. Bombar and A. Couvreur obtained the *Best Paper Award* for their article *Decoding supercodes of Gabidulin codes and applications to cryptanalysis* [21] at the conference *Post Quantum Cryptography* 2021.

- A. Leroux received an *accessit to the Doctorant STIC 2021 Award* for his work *SQISign: Compact Post-quantum Signatures from Quaternion and isogenies* on [53]

5.2 PhD Defenses

- M. Chenu de la Morinerie defended her PhD on december 17, 2021 [32].

- I. Panaccione defended her PhD on december 3rd, 2021 [33].

5.3 Accepted Grants

- T. Debris–Alazard obtained an ANR grant *Jeunes chercheuses, Jeunes chercheurs.* Project name : COLA;

- A. Couvreur obtained an ANR grant *Projet de recherche collaborative.* Project name : BARRACUDA.

6 New results

6.1 Post quantum cryptography

6.1.1 Decoding Supercodes of Gabidulin Codes and Applications to Cryptanalysis

Participants: Maxime Bombar, Alain Couvreur.

Besides the Hamming metric, other metrics have been considered for building error correcting codes. In particular, rank metric codes, and more specifically the so-called Fqm-linear codes, have found their way to code-based cryptography because they allow a more compact description and therefore smaller keys for comparable efficiency. Gabidulin codes, which are the rank-metric analogue of Reed-Solomon codes, come with a strong algebraic structure and efficient algorithms to decode uniquely up to half the minimum distance. However, contrary to their Hamming metric counterpart, they lack from a list-decoding algorithm, and therefore it is considered as a hard problem to decode beyond this bound. Based on this hard problem, two somehow dual encryption schemes with short keys had been recently proposed: LIGA and RAMESSES.

In [21], we analyse the security of these two cryptosystems, and show that in both cases the ciphertext could also be seen as a codeword from a bigger code corrupted by a small error. We then extend a decoding algorithm for Gabidulin codes to any code *containing* a Gabidulin code, at the cost of a decrease in the decoding radius, which was enough to recover the plaintext from the ciphertext and public data. We furthermore propose an implementation of our algorithm and of the attack on LIGA in SageMath.

6.1.2 Quantum reduction

Participants: Thomas Debris-Alazard.

We give a quantum reduction from finding short codewords in a random linear code to decoding for the Hamming metric. This is the first time such a reduction (classical or quantum) has been obtained. Our reduction adapts to linear codes Stehlé-Steinfield-Tanaka- Xagawa's re-interpretation of Regev's quantum reduction from finding short lattice vectors to solving the Closest Vector Problem. The Hamming metric is a much coarser metric than the Euclidean metric and this adaptation has needed several new ingredients to make it work. For instance, in order to have a meaningful reduction it is necessary in the Hamming metric to choose a very large decoding radius and this needs in many cases to go beyond the radius where decoding is unique. Another crucial step for the analysis of the reduction is the choice of the errors that are being fed to the decoding algorithm. For lattices, errors are usually sampled according to a Gaussian distribution. However, it turns out that the Bernoulli distribution (the analogue for codes of the Gaussian) is too much spread out and can not be used for the reduction with codes. Instead we choose here the uniform distribution over errors of a fixed weight and bring in orthogonal polynomials tools to perform the analysis and an additional amplitude amplification step to obtain the aforementioned result.

The result is presented in the preprint [44].

6.1.3 LLL like algorithm for codes

Participants: Thomas Debris-Alazard.

In [14], we have proposed an adaptation of the algorithmic reduction theory of lattices to binary codes. This includes the celebrated LLL algorithm (Lenstra, Lenstra, Lovasz, 1982), as well as adaptations of associated algorithms such as the Nearest Plane Algorithm of Babai (1986). Interestingly, the adaptation of LLL to binary codes can be interpreted as an algorithmic version of the bound of Griesmer (1960) on the minimal distance of a code. Using these algorithms, we demonstrate —both with a heuristic analysis and in practice— a small polynomial speed-up over the Information-Set Decoding algorithm of Lee and Brickell (1988) for random binary codes. This appears to be the first such speed-up that is not based on a time-memory trade-off. The above speed-up should be read as a very preliminary example of the potential of a reduction theory for codes, for example in cryptanalysis.

6.1.4 Wavelet: Code-based postquantum signatures with fast verification on microcontrollers

Participants: Gustavo Banegas, Thomas Debris-Alazard, Ben Smith.

This work [37] has presented the first full implementation of Wave, a postquantum code-based signature scheme. We define Wavelet, a concrete Wave scheme at the 128-bit classical security level (or NIST postquantum security Level 1) equipped with a fast verification algorithm targeting embedded devices. Wavelet offers 930- byte signatures, with a public key of 3161 kB. We include implementation details using AVX instructions, and on ARM Cortex-M4, including a solution to deal with Wavelet's large public keys, which do not fit in the SRAM of a typical embedded device. Our verification algorithm is approximately 4.65 times faster then the original, and verifies in 1 087 538 cycles using AVX instructions, or 13 172 ticks in an ARM Cortex-M4.

6.1.5 Quantum-resistant software update security on low-power networked embedded devices

Participants: Gustavo Banegas, Ben Smith.

Bringing practical post-quantum security to low-end IoT devices is a pressing challenge. In [38] we evaluate a range of pre- and post-quantum secure signature schemes in the context of SUIT software updates (specified by the IETF), on three popular, off-the-shelf microcontroller boards (ARM Cortex-M4, ESP32, and RISC-V) that are representative of the 32-bit landscape. We show that upgrading to postquantum security is practical now, and reflect on the best choices for various use cases. This work has been selected for presentation at Real World Crypto 2022.

6.1.6 Attack on LAC Key Exchange in Misuse Situation

Participants: Guenael Renault, Simon Montoya.

LAC is a Ring Learning With Error based cryptosystem that has been proposed to the NIST call for post-quantum standardization and passed the first round of the submission process. It did not pass to the third round but it is selected as the chinese standard for key exchange. The particularity of LAC is to use an error-correction code ensuring a high security level with small key sizes and small ciphertext sizes. LAC team proposes a CPA secure cryptosystem, LAC-CPA, and a CCA secure one, LAC-CCA, obtained by applying the Fujisaki-Okamoto transformation on LAC-CPA.

Together with Aurelien Greuet (IDEMIA), we study in [57] the security of LAC Key Exchange (KE) mechanism, using LAC-CPA, in a misuse context: when the same secret key is reused for several key exchanges and an active adversary has access to a *mismatch oracle*. This oracle indicates information on the possible mismatch at the end of the KE protocol. In this context, we show that an attacker needs at most 8 queries to the oracle to retrieve one coefficient of a static secret key. This result has been experimentally confirmed using the reference and optimized implementations of LAC. Since our attack can break the CPA version in a misuse context, the Authenticated KE protocol, based on the CCA version, is not impacted. However, this research provides a tight estimation of LAC resilience against this type of attacks.

6.1.7 Post-quantum Public Key Encryption from Isogenies

Participants: Luca De Feo, Antonin Leroux.

Together with Cyprien Delpech de Saint Guilhem (KU Leuven), Tako Boris Fouotsa (Universit‘a Degli Studi Roma Tre), Peter Kutas (University of Birmingham), Christophe Petit (Université Libre de Bruxelles), Javier Silva (Universitat Pompeu Fabra)and Benjamin Wesolowski (Institut Mathématiques de Bordeaux), Luca de Feo and Antonin Leroux have introduced a new post-quantum public key encryption scheme that uses constructively the torsion point attack against the SIDH key exchange. The publication includes an implementation in C of this new construction. Another contribution of this work is the "uber-isogeny assumption" which aims at generalizing some computational assumption encountered in various scheme of the literature.

6.1.8 CTIDH: high-speed constant-time isogeny-based key exchange

Participants: Gustavo Banegas, Ben Smith.

Together with Daniel J. Bernstein, Fabio Campos, Tung Chou, Tanja Lange, Michael Meyer, and Jana Sotáková, this work [7] implements the fastest implementation of commutative supersingular isogeny-based key exchange (CSIDH) with basic side-channel protection to date. This new speed record is partly due to a redesign of the private key space, while maintaining compatibilty with existing CSIDH software. This work was published in TCHES 2021.

6.1.9 HD-CSIDH: higher-degree generalizations of commutative isogeny-based key exchange

Participants: Mathilde Chenu, Ben Smith.

CSIDH—Commutative Supersingular Isogeny Diffie–Hellman—is a post-quantum non-interactive key exchange (NIKE) algorithm based on the action of a certain ideal class group on the set of supersingular elliptic curves defined over $\mathbb{F}_p$. In [10], we show that CSIDH is just one protocol in a family of more general group actions parameterized by positive squarefree integers d, with CSIDH corresponding to the case $d = 1$.

6.1.10 Quantum Equivalence of the DLP and CDHP for Group Actions

Participants: Ben Smith.

The classical equivalence of the Computational Diffie–Hellman and Discrete Logarithm Problems is a long-standing problem at the foundations of group-based public-key cryptography. Moving to the post-quantum paradigm of group actions, where CSIDH takes the place of Diffie–Hellman, it is important to understand the relationship between the analogues of the DLP and CDHP. With Steven Galbraith, Lorenz Panny, and Frederik Vercauteren, we show in [16] that there is a polynomial-time quantum equivalence between these problems.

6.2 Verifiable computation

Participants: Daniel Augot, Sarah Bordage, Youssef El Housni, François Morain, Jade Nardi.

Suppose a user of a small device requires a powerful computer to perform a heavy computation for him. The computation can not be performed by the device. After completion of the computation, the powerful computer reports a result. Suppose now that the user has not full confidence that the remote computer performs correctly or behaves honestly. How can the user be assured that the correct result has been returned to him, given that he can not redo the computation ?

The topic of verifiable computation deals with this issue. Essentially it is a cryptographic protocol where the prover (i.e. the remote computer) provides a proof to the verifier (i.e. the user) that a computation is correct. The protocol may be interactive, in which case there may be one or more rounds of interactions between the prover and the verifier, or non interactive, in which case the prover sends a proof that the computation is correct.

These protocols incorporate zero-knowledge variants, where the scenario is different. A service performs a computation on date, part of which remaining private (for instance statistics on citizen's incomes). It is possible for the service to prove the correctness of the result without revealing the data (which has to be committed anyway).

The two main venues for building these protocols are the setting of discrete logarithms (and pairings) in elliptic curves and a coding theoretical setting (originating to the PCP theorem). Both variants admit a zero-knowledge version, and the core of the research is more on provable computation than the zero-knowledge aspect, which comes rather easily in comparison.

6.2.1 Verifiable computation based on coding theory

Participants: Daniel Augot, Sarah Bordage, Jade Nardi.

In the coding theoretic setting, these protocols are made popular, in particular in the blockchain area, under the name of (ZK-)STARKS, *Scalable Transparent Arguments of Knowledge*, introduced in 2018. In theoretical computer science, these proofs are derived for protocols which are called IOPs *Interactive Oracle Proofs*, which are combination of IPs *Interactive Proofs* and PCPs *Probabilistically Checkable Proofs*, for combining the best of both worlds, and making PCPs pratical.

At the core of these protocols lies the following coding problem: how to decide, with high confidence, that a very long ambient word is close to a given code, while looking at very few coordinates of it.

These protocols were originally designed for the simplest algebraic codes, Reed-Solomon codes. Daniel Augot and Sarah Bordage provided a generalization of these protocols to multivariate codes, i.e. product of Reed-Solomon codes and Reed-Muller codes. The performance does not degrade badly with respect to the basic Reed-Solomon case [36]. It remains to assert the revelance of these codes for building proof systems and to compare to litterature, where product of Reed-Solomon codes have been studied for more than twenty years.

A very important issue is have a smaller alphabet, and this can be done using algebraic-geometric codes. This was done by Sarah Bordage and Jade Nardi [40], using curves with a resoluble automorphims group, which enable to build codes which are foldable in way similar to the Reed-Solomon codes with are folded in the "FRI" protocol [52]. Their protocol has very good perfomance, akin to the Reed-Solomon case.

6.2.2 Verifiable computation based on elliptic curves

Participants: Daniel Augot, Youssef El Housni, François Morain.

Verifiable computation can also be built using the theory of ellitpic curves, the hardness of the discrete logarithms, and pairings, as introduced in [58] and made practical in [60]. These proofs are much more shorter than the ones provided by the STARKS, with a higher cost for the prover. Furthermore, these systems are not post-quantum, and there are important issues in the setting of the proof system, where a trusted third party is required.

The verifiable computation problems leads to several new questions in elliptic curves cryptographic, since the required operations depart from the standard ones used for instance in signature algorithms.

A very interesting topic is the notion of "proof of proofs". Essentially, verifying a proof is a computation, and a proof that a proof has been verified can be given. The same idea applies for verifying hundreds of proofs. A single proof can report that hundred of proofs have been checked.

This is very strong in the elliptic curve setting because the size of a proof is a constant (a few hundred bytes, only depending on the security parameter, not the computation). This means that the above hundred of statements admits a very short proof. In the blockchain world, this translates into a very short proof that many offchain transactions are correct.

To achieve this goal, this requires an ellitpic curve for proving computations done over an other elliptic curve. The problem is that there is an arithmetic mismatch: the statement which is to be proved is defined over $\mathbb{F}_r$, for a prime r which is a size of a cyclic group provided by an elliptic curve defined over $\mathbb{F}_q$. Verifying the proof requires to do computations over $\mathbb{F}_q$, and thus, for the above recursion, one needs another curve over $\mathbb{F}_{q'}$ providing a group of prime order q. Furthermore both curves must be pairing-friendly. This raises quite challenging questions, which are solved using the theory of complex multiplication.

In collaboration with Aurore Guillevic, Youssef El Housni provided curves which are very efficient for this recursion [56, 45]. These curves beat the competition, an implementation has been provided here. Some other blockchain players CELO, Consensys also have used these curves in their implentations of verifiable computation and zero-knowledge proofs.

6.3 Machine learning on private data using multiplication

Participants: Daniel Augot, Angelo Saadeh.

In collaboration with Matthieu Rambaud (Télécom Paris), Daniel Augot is advising Angelo Saadeh. The issue which is adressed is the following. Two parties each hold privately some distinct slices of common data. compute a logistic regression on the whole set of data, without each party revealing its data to the other party.

Computing a common output from inputs of several participants in the above is done in cryptography using MPC *Secure Multiparty Computation*, as introduced by Yao [61], and made recently practical, with several implementations. Yet, as classically observed in MPC, the actual result, when learned, may leak information about the secret inputs. The same problem occurs here, where the model may leak information about the data.

Thus it is natural to investigate the use of ϵ-differential privacy, introduced by [55] on top of MPC. This raises the concern of obtaining a reasonnable accuracy, since noise has been introduced with differential privacy. Preliminary tests have been done, using the functional mechanism of [62], that Angelo Saadeh implemented in PySyft, which is a library of cryptographic primitives building on the PyTorch machine learning platform and the obtained accuracy is actually good. A publication is in preparation.

6.4 Secure multiparty computation in blockchains

Participants: Daniel Augot, Lucas Benmouffok.

The topic of MPC enables several participants to obtain a common result of a computation of each one's data, while not revealing data of others participants, without any trusted third party. This seems quite related to the blockchain philosophy, where decentralisation and trustless environments are at the core of the claimed properties of blockchains.

Actually, this is not so clear, since MPC deals with privacy and secret data, while blockchains typically imply transparency and public data. A PhD, funded by System-X, studies this possible interactions, and a model is under design. We take the idea that blockchains can enable to allocate jobs to "workers", provide them a reward for doing so, and notarize the result in the ledger. MPC would complement this by having "MPC workers" which, under the security models of MPC, could do jobs on private data submitted by clients (this could be called MPC-as-a-service). In [19], we showed that an implementation of these ideas are pratical, bsed on the work of Benhamouda et al [59], with improvements with respect to the hyperledger/fabric blockchain platform, and integrating into it the Scale-Mamba MPC library.

6.5 Cloud storage

Participants: Françoise Levy-Dit-Vehel, Maxime Roméas.

We revisit the issue of efficient and secure Proofs of Retrievability (PoR). To do so, we build upon the work of Maurer et al. on Constructive Cryptography (CC) to give a clearer and more usable security framework for PoR protocols. We propose a scheme based of Locally Correctable Codes (LCC), and assert its security by giving an explicit formula for the probability of an adversary to fool the client who outsourced his data on the remote server. Our scheme has reduced storage overhead and communication complexity, compared to a previous scheme of Lavauzelle and Levy-dit-Vehel, which was also based on LCCs. We achieve better parameters by introducing a new definition and construction of so-called "authentic Server Memory Resource" (aSMR) in the CC context. It has to be noted that our aSMR can be used as an intermediate step in all code-based protocols for outsourced storage. We also model LCCs in a composable framework. Doing so, we show that the exact failure probability of the local decoder depends not only on the number of corrupted symbols, but also on their locations. For the important class of lifted Reed-Solomon codes, we prove that this failure probability can be computed in polynomial time in the length of the lifted code. A paper on this work has been submitted to STACS 2022.

6.6 Fast Cornacchia algorithm

Participants: François Morain.

Cornacchia's algorithm is an important building block of CM elliptic curve cryptography. Sharing many properties with fast integer gcd algorithms, we worked on a fast version for this tool. A paper is to be submitted at ISSAC'2022 and the code is to be available on gitlab.

6.7 Pre-quantum factoring using elliptic curves

Participants: François Morain.

One of the most powerful factoring algorithm is ECM that uses elliptic curves. To improve it, families of curves are traditionally built over the rationals. In this work, number fields are used to treat the special numbers $b^n \pm 1$. See the preliminary results in [48].

6.8 Reed-Muller codes in the rank metric

Participants: Daniel Augot, Alain Couvreur.

There does not exist Reed-Muller codes for the rank matric over finite fields, due the simple cyclic structure of Galois group of finite fields. However when the Galois does not have a cyclic structure, for instance for some extension fields of the rational numbers, and using the langage of skew polynomials, it is possible to build rank-matrix analogues of classical Reed-Muller codes [6], with rank minimum distance similar to the one of classical Reed-Muller codes.

6.9 Trustless unknown-order groups

Participants: Ben Smith.

Groups of unknown order are a classic setting for asymmetric cryptosystems—RSA being the most famous example. In recent times, unknown-order groups have returned to prominence as a setting for new, advanced cryptosystems including accumulators and VDFs (Verifiable Delay Functions). In these applications, *trustless setup* becomes critical: not even the constructor of the group should know its order. In [15] (joint work with Samuel Dobson and Steven Galbraith), we re-evaluate the security of ideal class groups—the most popular source of trustless unknown-order groups—and show that generally accepted parameters do not meet claimed security levels. We also propose a more efficient alternative: Jacobians of genus-3 hyperelliptic curves.

7 Bilateral contracts and grants with industry

7.1 Bilateral contracts with industry

Participants: Daniel Augot, Sarah Bordage, François Morain, Guénaël Renault, Azam Soleimanian.

- Through École polytechnique, D. Augot is leader of a teaching and research chair on Blockchains "Blockchains and B2B platforms", funded by CapGemini, under the French patronage laws. This chair aims at fostering teaching and doing research in topics related to blockchains, from the points of view of both computer science and economics. This chair has a co-leader, Julien Prat from the department of economics. This started in 2018, for a five years duration. Another mission of the chair is networking and outreach, (see this website). Sarah Bordage (PhD since 2019) and Azam Soleimanian (Post-doctoral fellow since 2021) funded by this chair since January 2019.

- IRT System-X funds and hosts a PhD student, L. Benmouffok for Secure Multiparty Computation in blockchains. System-X is an organisation connecting industry and research, where research topics are built in close collaboration with industrial partners. The thesis started in October 2018. System-X launched a larger initiative, called BART, with INRIA and Télécom as partners, "blockchain advanced research and topics" (see this website) which hosts L. Benmouffok's thesis.

- Since October 2019, D. Augot and F. Morain are providing PhD advisorship to one of the employees of Ernst& Young, Y. El Housni, on the topic of zero-knowledge proofs. Then Y. El Housni moved to Consensys, still doing a PhD under F. Morain and D. Augot guidance. A contract has been establised for Daniel Augot and François Morain advisorship of Y. El Housni.

- Since October 2019, Idemia funds a CIFRE PhD student, Simon Montoya on the secure implementation in constrained environement of post-quantum cryptosystems.

- Since October 2019, Quarkslab funds a CIFRE PhD student, Alexis Challande, on the analysis of malware code.
- Since November 2019, French Min. Arm. funds a PhD student, Maxime Anvari, on the analysis of the ToR network.
- Since October 2020, Orange funds a CIFRE PhD student, Anaïs Barthoulot on Advanced encryption for Sensitive data sharing.

8 Partnerships and cooperations

8.1 International research visitors

Visit of Giuseppe Cotardo

Status PhD student.

Institution of origin: University College Dublin.

Country: Ireland

Dates: From September 1st to december 31st, 2021.

Context of the visit: Giuseppe visited us during his PhD in order to work in collaboration on algebraic problems on rank metric codes.

8.2 European initiatives

8.2.1 FP7 & H2020 projects

SPARTA

Participants: Gustavo Banegas, Ben Smith.

SPARTA is a European H2020 competence network: *re-imagining the way cybersecurity research, innovation, and training are performed in Europe.*

Website: sparta.eu

We have participated in the **HAII-T** Program (High-Assurance Intelligent Infrastructure Toolkit), developing high-performance, high-assurance cryptographic software for IoT devices, especially in the context of the free, open-source RIOT operating system. While SPARTA will end in early 2022, this work is continuing in the framework of the Inria *Défi* **RIOT-FP**, which aims to provide proven, future-proof—and, in particular, post-quantum—security for RIOT-OS and its users.

8.3 National initiatives

8.3.1 ANR CIAO

Participants: Benjamin Smith, Luca De Feo, Antonin Leroux, Mathilde Chenu.

ANR **CIAO** (Cryptography, Isogenies, and Abelian varieties Overwhelming) is a JCJC 2019 project, led by Damien Robert (Inria EP LFANT). This project, which started in October 2019, will examine applications of higher-dimensional abelian varieties in isogeny-based cryptography.

8.3.2 ANR CBCRYPT

Participants: Alain Couvreur, Olivier Blazy.

ANR **CBCRYPT** (Code–based Cryptography) This is a project from (*Appel à projets générique, Défi 9, Liberté et sécurité de l'Europe, de ses citoyens et de ses résidents, Axe 4 ; Cybersécurité*). This project, starting in october 2017 led by Jean-Pierre Tillich (Inria, EP Cosmiq) focusses on the design and the security analysis of code–based primitives, in the context of the current NIST competition.

8.3.3 ANR COLA

Participants: Alain Couvreur, Thomas Debris–Alazard.

ANR **COLA** (An interface between COde and LAttice-based cryptography) is a project from (*Appel à projets générique, Défi 9, Liberté et sécurité de l'Europe, de ses citoyens et de ses résidents, Axe 4 ; Cybersécurité*). This project (ANR JCJC), starting in october 2021 led by Thomas Debris-Alazard focusses on bringing closer post-quantum solutions based on codes and lattices to improve our trust in cryptanalysis and to open new perspectives in terms of design.

8.3.4 ANR BARRACUDA

Participants: Daniel Augot, Alain Couvreur, Françoise Levy-dit-Vehel.

BARRACUDA is a collaborative ANR project accepted in 2021 and led by A. Couvreur.
Website : `barracuda.inria.fr`

The project gathers specialists of coding and cryptology on one hand and specialists of number theory and algebraic geometry on the other hand. The objectives concern problems arising from modern cryptography which require the use of advanced algebra based objects and techniques. It concerns for instance mathematical problems with applications to distributed storage, multi-party computation or zero knowledge proofs for protocols.

8.3.5 ANR SANGRIA

Participants: Olivier Blazy.

SANGRIA is a collaborative ANR project accepted in 2021.
Website : `lip6.fr/Damien.Vergnaud/projects/sangria/`

The main scientific challenge of the SANGRIA (Secure distributed computAtioN - cryptoGRaphy, combinatorIcs and computer Algebra) project are (1) to construct specific protocols that take into account practical constraints and prove them secure, (2) to implement them and to improve the efficiency of existing protocols significantly. The SANGRIA project (for Secure distributed computAtioN: cryptoGRaphy, combinatorIcs and computer Algebra) aims to undertake research in these two aspects while combining research from cryptography, combinatorics and computer algebra. It is expected to impact central problems in secure distributed computation, while enriching the general landscape of cryptography.

8.3.6 ANR MobiS5

Participants: Olivier Blazy.

MobiS5 is a collaborative ANR project accepted in 2018.

Website : mobis5.limos.fr/

MobiS5 will aim to foresee and counter the threats posed in 5G architectures by the architectural modifications suggested in TR 22.861-22.864. Concretely, we will provide a provably-secure cryptographic toolbox for 5G networks, validated formally and experimentally, responding to the needs of 5G architectures at three levels:

* Challenge 1: security in the network infrastructure and end points: including core network security and attack detection and prevention; * Challenge 2: cryptographic primitives and protocols, notably : a selection of basic primitives, an authenticated key-exchange protocol, tools to compute on encrypted data, and post-quantum cryptographic countermeasures * Challenge 3: mobile applications, specifically in the use-case of a secure server that aids or processes outsourced computation; and the example of a smart home.

8.3.7 ANR CryptiQ

Participants: Olivier Blazy.

CryptiQ is a collaborative ANR project accepted in 2018.

The goal of the CryptiQ project is to major changes due to Quantum Computing by considering three plausible scenarios, from the closest to the furthest foreseeable future, depending on the means of the adversary and the honest parties. In the first scenario, the honest execution of protocols remains classical while the adversary may have oracle access to a quantum computer. This is the so-called post-quantum cryptography, which is the best known setting. In the second scenario (quantum-enhanced classical cryptography), we allow honest parties to have access to quantum technologies in order to achieve enhanced properties, but we restrict this access to those quantum technologies that are currently available (or that can be built in near-term). The adversary is still allowed to use any quantum technology. Finally, in the third scenario (cryptography in a quantum world), we allow the most general quantum operations to an adversary and we consider that anybody can now have access to both quantum communication and computation.

9 Dissemination

Participants: Daniel Augot, Olivier Blazy, Alain Couvreur, Thomas Debris-Alazard, Françoise Levy-dit-Vehel, François Morain, Guenael Renault, Benjamin Smith.

9.1 Promoting scientific activities

9.1.1 Scientific events: organisation

General chair, scientific chair

- A. Couvreur was president of the program committee of the *Journées scientifiques Inria* 2021.

Member of the organizing committees

- A. Couvreur was member of the organisation committee of the *Journées scientifiques Inria* 2021;
- O. Blazy was a co-organizer of the *Journées REDOCS 2021*.

- D. Augot is a member of the scientific committee of the triannual or quadriannual French C2 seminar

9.1.2 Scientific events: selection

Member of the conference program committees

- A. Couvreur was member of the program committee of the conference CBCrypto 2021;
- O. Blazy was a member of the program committee of the conference CT-RSA 2022;
- O. Blazy was a member of the program committee of the conference Eurocrypt 2022;
- O. Blazy was a member of the program committee of the conference WCC 2022.
- B. Smith served on the program committee of the International Conference on Post-Quantum Cryptography PQCrypto 2021
- B. Smith served on the program committee of the 18th IMA International Conference on Coding and Cryptography
- B. Smith served on the program committee of Selected Areas in Cryptography: SAC 2021
- D. Augot was a member of the program committee of the conference 5th International Workshop on Cryptocurrencies and Blockchain Technology - CBT 2021.
- D. Augot was a member of the program committee of the conference IEEE International Conference on Blockchain and Cryptocurrency.
- D. Augot was a member of the program committee of the conference 5th Workshop on Trusted Smart Contracts

Reviewer

- B. Smith was a reviewer for Eurocrypt 2021, Crypto 2021, TCS 2021, STACS 2022, and CT-RSA 2022.
- A. Couvreur was reviewer for ISIT 2021.
- T. Debris–Alazard was reviewer for Eurocrypt 2021, PQCrypto 2021, CT-RSA 2021, ISIT 2021, LatinCrypt 2021, IMACC 2021, ITW 2021, and Crypto 2021

9.1.3 Journal

Member of the editorial boards

- A. Couvreur is member of the editorial board of the *Publications Mathématiques de Besançon*;
- O. Blazy is a member of the editorial board of the Computer Law & Security Review journal.

Reviewer - reviewing activities

- B. Smith was a reviewer for Journal of Algebra; Finite Fields and Applications; Transactions on Mathematical Software; Moscow Mathematical Journal; Mathematical Cryptology; Theoretical Computer Science.
- A. Couvreur was reviewer for *Advances in Mathematics of Communication, Finite Fields Appl., IEEE Trans. Inform. Theory, Journal of Algebra, Journal of Algebra and its Applications.*
- T. Debris–Alazard was reviewer for *Advances in Mathematics of Communication* and *Designs, Codes, and Cryptography.*

9.1.4 Invited talks

- A. Couvreur gave an invited talk at the conference *Curves over finite fields, past present and future*

9.1.5 Leadership within the scientific community

- O. Blazy and A. Couvreur lead the CNRS' *Groupe de travail Codage et Cryptographie* of *Groupes de recherche Sécurité Informatique* and *Informatique Mathématique*.

9.1.6 Scientific expertise

- A. Couvreur was referee for the PhD of Dang Truong Mac (Université de Limoges);
- A. Couvreur was referee for the PhD of Ba-Duc Pham (Université Rennes 1);
- O. Blazy was referee for the PhD of Mirko Koscina (Université PSL);
- T. Debris–Alazard was reviewer for the ANR.

9.1.7 Research administration

- A. Couvreur is elected member of Inria's *Commission d'évaluation*
- Until September 30th 2021, A. Couvreur was appointed member (*membre nommé*) of the french *Conseil National des universités* (CNU) in 25th section (*Mathematics*).
- A. Couvreur is member of the *Comité scientifique du programme Maths et IA* of the *Labex Mathématiques Jacques Hadamard*.
- B. Smith is a member of the *Commission Recherche et Innovation* of LabEx DigiCosme.
- B. Smith is a member of the *Commission Scientifique* at Inria Saclay.
- T. Debris–Alazard is a contact for LIX PhD students

9.2 Teaching - Supervision - Juries

9.2.1 Teaching

- Licence : F. Morain, Lectures for INF361: "Introduction à l'informatique", 15h (equiv TD), 1st year (L3), École polytechnique. Coordinator of this module (350 students).
- Licence : T. Debris–Alazard, Exercises for INF361: "Introduction à l'informatique", 15h (equiv TD), 1st year (L3), École polytechnique.
- Licence : B. Smith: *CSE101: Introduction to Computer Programming*, 42h, L1, École polytechnique, France
- Licence : O. Blazy: *CSE101: Introduction to Computer Programming* (Tutorials), 58h, L1, École polytechnique, France
- Master : T. Debris–Alazard, Lectures for "Post-quantum cryptography", 8h, 4th year, ENS Lyon,
- Master : A. Couvreur : *MPRI 2-13-2: Error Correcting codes and applications to cryptography.*
- Master A. Couvreur : *Master QDCS Calcul quantique avancé et codes correcteurs. 10h.*
- Master: D. Augot: lectures and labs on crypto in blockchains, 24h, M2, École polytechnique, France.
- Master: D. Augot designed with Julien Prat the cursus of a course in blockchains and economics, and made lectures on zero-knowledge.

- Master : F. Morain is the scientific leader of the Master of Science and Technology *Cybersecurity: Threats and Defense* of École Polytechnique.
- Master : F. Morain, INF558, *Introduction to cryptology*, 36h, M1, École Polytechnique. This special year included video making of all his courses.
- Master : T. Debris–Alazard, Lectures on INF558, *Introduction to cryptology*, 36h, M1, École Polytechnique.
- Master : B. Smith: *INF568: Advanced Cryptography*, 45h, M1, École polytechnique, France
- Master : B. Smith and F. Morain: *MPRI 2-12-2: Algorithmes Arithmétiques pour la Cryptologie*, 22.5h, M2, Master Parisien de Recherche en Informatique, France. The lectures were all given in live video.
- Master : F. Levy-dit-Vehel, Lectures on discrete maths, 21h, M1, ENSTA.
- Master : T. Debris–Alazard, Exercices on discrete maths, 21h, M1, ENSTA.
- Master : F. Levy-dit-Vehel, Lectures on cryptography, 24h, M2, ENSTA.
- Master Cybersecurity: D. Augot, cryptography in blockchains, 24h, M2.
- Master : G. Renault: Lectures and Labs for *INF565: Information Systems Security*, 60h, M1, École polytechnique, France
- Master : G. Renault: Lectures and Labs for *INF648: Embedded security: side-channel attacks; javacard*, 60h, M2, École polytechnique, France
- Master : G. Renault: Coordinator for *INF637: Reverse engineering vs Obfuscation*, 2h, M2, École polytechnique, France
- Professionnal training: D. Augot gave a two hours lecture at System-X.

9.2.2 Juries

- D. Augot was member of the PhD jury of Isabella Panaccione (Institut Polytechnique de Paris);
- D. Augot was president of the PhD jury of Édouard Rousseau (Institut Polytechnique de Paris);
- A. Couvreur was member of the PhD jury of Valentin Vasseur (Université de Paris);
- A. Couvreur was member of the PhD jury of Matthieu Lequesne (Sorbonne Université);
- A. Couvreur was member of the PhD jury of Dang Truong Mac (Université de Limoges);
- O. Blazy was member of the PhD jury of Mirko Koscina (Université PSL);
- O. Blazy was president of the PhD jury of Dang Truong Mac (Université de Limoges);
- A. Couvreur was member of the PhD jury of Ba-Duc Pham (université Rennes 1);
- A. Couvreur was president of the PhD jury of Nilesh Vyas (Institut Polytechnique de Paris);
- B. Smith was a member of the PhD jury of Dimitri Koshelev (Université Paris-Saclay)
- B. Smith was a member of the the PhD jury of Sudarshan Shinde (Sorbonne Université)
- T. Debris–Alazard was member of the Gilles Kahn PhD award jury.

9.2.3 Recruiting juries

- A. Couvreur was member of the recruiting jury for *chargés de recherche* and *ISFP* of the centre of Nancy.

- A. Couvreur was member of a recruiting jury for a *Maître de conférence position* in pure mathematics at *Université Toulouse Jean Jaurès*;

- D. Augot was member of a recruiting jury for a *Professor position* at École polytechnique;

- O. Blazy was member of a recruiting jury for a *Maître de conférence position* in cybersecurity/cryptographie at *Telecom Paris*;

- O. Blazy was member of a recruiting jury for a *Maitre de Conférence position* in computer science at *Insa de Bourges*.

9.3 Popularization

9.3.1 Internal or external Inria responsibilities

- A. Couvreur is the *référent médiation scientifique* of Saclay's research center.
  - He organised the *Rendez-vous des Jeunes Mathématiciennes et Informaticiennes* on February 25 and 26th 2021. The event happened online due to the pandemic.
  - He participated to the organisation of *Fête de la science* 2021.
  - He has been involved in the development of vulgarisation videos for the on-line *Fête de la science* of Université Paris-Saclay.

- T. Debris–Alazard gave a plenary talk at Inria Saclay's *Rendez-vous des Jeunes Mathématiciennes et Informaticiennes* 2021.

- T. Debris–Alazard was plenary speaker for the ceremony award of the *Olympiades de Mathématiques de l'Académie de Créteil*

9.3.2 Articles and contents

- O. Blazy wrote an article in Polethis about ethics in computer science;

- O. Blazy gave various interviews about trending privacy/security topics like a cyberattack (La tribune), blockchains and NFT (Science & Vie, Science & Vie Junior), age control technologies for websites (La Croix)

- D. Augot was interviewed by University Paris-Saclay, by Science & Vie on blockchains.

9.3.3 Interventions

- A. Couvreur and T. Debris–Alazard were volunteers for the fête de la science 2021 at École polytechnique.

10 Scientific production

10.1 Major publications

[1] E. Barelli and A. Couvreur. 'An efficient structural attack on NIST submission DAGS'. In: ASIACRYPT 2018. Vol. 11272. Advances in Cryptology – ASIACRYPT 2018. Brisbane, Australia, 2nd Dec. 2018. DOI: 10.1007/978-3-030-03326-2_4. URL: https://hal.archives-ouvertes.fr/hal-01796338.

[2] D. J. Bernstein, L. De Feo, A. Leroux and B. Smith. 'Faster computation of isogenies of large prime degree'. In: *ANTS-XIV - 14th Algorithmic Number Theory Symposium*. Ed. by S. Galbraith. Vol. 4. Proceedings of the Fourteenth Algorithmic Number Theory Symposium (ANTS-XIV). Auckland, New Zealand: Mathematical Sciences Publishers, June 2020, pp. 39–55. DOI: 10.2140/obs.2020.4.39. URL: https://hal.inria.fr/hal-02514201.

[3] A. Couvreur, P. Lebacque and M. Perret. 'Toward good families of codes from towers of surfaces'. In: *Contemporary Mathematics*. Arithmetic, Geometry, Cryptography and Coding Theory. Vol. 770. Contemporary Mathematics. Marseille, France: American Mathematical Society, 2021. DOI: 10.1090/conm/770. URL: https://hal.archives-ouvertes.fr/hal-02470343.

[4] L. De Feo, D. Kohel, A. Leroux, C. Petit and B. Wesolowski. 'SQISign: compact post-quantum signatures from quaternions and isogenies'. In: *ASIACRYPT 2020 - 26th Annual International Conference on the Theory and Application of Cryptology and Information Security*. Daejeon (virtual), South Korea: Association for Computing Machinery, Dec. 2020. URL: https://hal.archives-ouvertes.fr/hal-03038004.

[5] T. Debris-Alazard, L. Ducas and W. P. Van Woerden. 'An Algorithmic Reduction Theory for Binary Codes: LLL and more'. In: *IEEE Transactions on Information Theory* (14th Jan. 2022). DOI: 10.1109/TIT.2022.3143620. URL: https://hal.inria.fr/hal-03529739.

10.2 Publications of the year

International journals

[6] D. Augot, A. Couvreur, J. Lavauzelle and A. Neri. 'Rank-metric codes over arbitrary Galois extensions and rank analogues of Reed-Muller codes'. In: *SIAM Journal on Applied Algebra and Geometry* 5.2 (2021), pp. 165–199. DOI: 10.1137/20M1348583. URL: https://hal.archives-ouvertes.fr/hal-02882019.

[7] G. Banegas, D. J. Bernstein, F. Campos, T. Chou, T. Lange, M. Meyer, B. Smith and J. Sotáková. 'CTIDH: Faster constant-time CSIDH'. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2021.4 (11th Aug. 2021). DOI: 10.46586/tches.v2021.i4.351-387. URL: https://hal.inria.fr/hal-03229428.

[8] O. Blazy, L. Brouilhet, C. Chevalier, P. Towa, I. Tucker and D. Vergnaud. 'Hardware security without secure hardware: How to decrypt with a password and a server'. In: *Theoretical Computer Science* 895 (Dec. 2021), pp. 178–211. DOI: 10.1016/j.tcs.2021.09.042. URL: https://hal.archives-ouvertes.fr/hal-03378464.

[9] S. Bordage and J. Lavauzelle. 'On the privacy of a code-based single-server computational PIR scheme'. In: *Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences* (24th Mar. 2021). DOI: 10.1007/s12095-021-00477-z. URL: https://hal.inria.fr/hal-03181082.

[10] M. Chenu and B. Smith. 'Higher-degree supersingular group actions'. In: *Mathematical Cryptology* (2021). URL: https://hal.inria.fr/hal-03288075.

[11] J.-J. Chi-Domínguez, F. Rodríguez-Henríquez and B. Smith. 'Extending the GLS endomorphism to speed up GHS Weil descent using Magma'. In: *Finite Fields and Their Applications* 75 (June 2021). DOI: 10.1016/j.ffa.2021.101891. URL: https://hal.inria.fr/hal-03233803.

[12] A. Couvreur and M. Lequesne. 'On the security of subspace subcodes of Reed-Solomon codes for public key encryption'. In: *IEEE Transactions on Information Theory* 68.1 (15th Oct. 2021), pp. 632–648. DOI: 10.1109/TIT.2021.3120440. URL: https://hal.archives-ouvertes.fr/hal-02938812.

[13] N. Coxon. 'Fast transforms over finite fields of characteristic two'. In: *Journal of Symbolic Computation* 104 (2021), pp. 824–854. DOI: 10.1016/j.jsc.2020.10.002. URL: https://hal.archives-ouvertes.fr/hal-01845238.

[14] T. Debris-Alazard, L. Ducas and W. P. Van Woerden. 'An Algorithmic Reduction Theory for Binary Codes: LLL and more'. In: *IEEE Transactions on Information Theory* (14th Jan. 2022). DOI: 10.1109/TIT.2022.3143620. URL: https://hal.inria.fr/hal-03529739.

[15] S. Dobson, S. Galbraith and B. Smith. 'Trustless unknown-order groups'. In: *Mathematical Cryptology* (2021). URL: https://hal.inria.fr/hal-02882161.

[16] S. Galbraith, L. Panny, B. Smith and F. Vercauteren. 'Quantum Equivalence of the DLP and CDHP for Group Actions'. In: *Mathematical Cryptology* 1.1 (2021), pp. 40–44. URL: https://hal.inria.fr/hal-01963660.

[17] J. Lavauzelle, R. Tajeddine, R. Freij-Hollanti and C. Hollanti. 'Private Information Retrieval Schemes with Product-Matrix MBR Codes'. In: *IEEE Transactions on Information Forensics and Security* 16 (2021), pp. 441–450. DOI: 10.1109/TIFS.2020.3003572. URL: https://hal.archives-ouvertes.fr/hal-01951956.

[18] F. Morain, G. Renault and B. Smith. 'Deterministic factoring with oracles'. In: *Applicable Algebra in Engineering, Communication and Computing* (16th Sept. 2021). DOI: 10.1007/s00200-021-00521-8. URL: https://hal.inria.fr/hal-01715832.

International peer-reviewed conferences

[19] L. Benmouffok, K. Singh, N. Heulot and D. Augot. 'Privacy-Preserving Initial Public Offering using SCALE-MAMBA and Hyperledger Fabric'. In: ChainTech'2021 is a track of WETICE : the 31st IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises. Basque Coast, Bayonne, France, 27th Oct. 2021. URL: https://hal.inria.fr/hal-03345605.

[20] L. Bettale, S. Montoya and G. Renault. 'Safe-Error Analysis of Post-Quantum Cryptography Mechanisms'. In: FDTC 2021 - Fault Diagnosis and Tolerance in Cryptographie. Virtual event, France, 17th Sept. 2021. URL: https://hal.inria.fr/hal-03330189.

[21] M. Bombar and A. Couvreur. 'Decoding supercodes of Gabidulin codes and applications to cryptanalysis'. In: Post-Quantum Cryptography 2021. Vol. 12841. Post-Quantum Cryptography. PQCrypto 2021. Daejeon, South Korea: Springer, July 2021, pp. 3–22. DOI: 10.1007/978-3-030-81293-5_1. URL: https://hal.inria.fr/hal-03256980.

[22] A. Chailloux, T. Debris-Alazard and S. Etinski. 'Classical and Quantum Algorithms for Generic Syndrome Decoding Problems and Applications to the Lee Metric'. In: *Post-Quantum Cryptography*. PQCrypto 2021 - Post-Quantum Cryptography 12th International Workshop. Vol. 12841. Lecture Notes in Computer Science. Daejeon, South Korea: Springer International Publishing, 15th July 2021, pp. 44–62. DOI: 10.1007/978-3-030-81293-5_3. URL: https://hal.inria.fr/hal-03529777.

[23] A. Challande, R. David and G. Renault. 'Exploitation du graphe de dépendance d'AOSP à des fins de sécurité'. In: SSTIC 2021 - Symposium sur la sécurité des technologies de l'information et des communications. Rennes, France, 2nd June 2021. URL: https://hal.inria.fr/hal-03329791.

[24] K. Eldefrawy, T. Lepoint and A. Leroux. 'Communication-Efficient Proactive MPC for Dynamic Groups with Dishonest Majorities'. In: *ACNS 2022*. ACNS 2022. Rome, Italy, 2021. URL: https://hal.inria.fr/hal-03471927.

[25] E. Florit and B. Smith. 'Automorphisms and isogeny graphs of abelian varieties, with applications to the superspecial Richelot isogeny graph'. In: Arithmetic, Geometry, Cryptography, and Coding Theory 2021. Arithmetic, Geometry, Cryptography, and Coding Theory. Luminy, France: American Mathematical Society, 31st May 2021. URL: https://hal.inria.fr/hal-03094375.

[26] A. Greuet, S. Montoya and G. Renault. 'On Using RSA/ECC Coprocessor for Ideal Lattice-Based Key Exchange'. In: COSADE 2021. Lugano, Switzerland, 25th Oct. 2021. URL: https://hal.inria.fr/hal-03330066.

[27] E. Guerrini, R. Lebreton and I. Zappatore. 'Polynomial Linear System Solving with Random Errors: New Bounds and Early Termination Technique'. In: ISSAC 2021 - 46th International Symposium on Symbolic and Algebraic Computation. Saint Petersburg, Russia: ACM, 18th July 2021, pp. 171–178. DOI: 10.1145/3452143.3465548. URL: https://hal.archives-ouvertes.fr/hal-03386106.

Scientific book chapters

[28] C. Brunetta, G. Tsaloli, B. Liang, G. Banegas and A. Mitrokotsa. 'Non-interactive, Secure Verifiable Aggregation for Decentralized, Privacy-Preserving Learning'. In: *Information Security and Privacy*. Vol. 13083. Lecture Notes in Computer Science. Springer International Publishing, 4th Nov. 2021, pp. 510–528. DOI: 10.1007/978-3-030-90567-5_26. URL: https://hal.inria.fr/hal-03454325.

[29] A. Couvreur and H. Randriambololona. 'Algebraic geometry codes and some applications'. In: *A Concise Encyclopedia of Coding Theory*. A Concise Encyclopedia of Coding Theory. Chapman and Hall/CRC, 26th Mar. 2021, p. 998. URL: https://hal.archives-ouvertes.fr/hal-02931167.

[30] L. De Feo, C. Delpech de Saint Guilhem, T. B. Fouotsa, P. Kutas, A. Leroux, C. Petit, J. Silva and B. Wesolowski. 'Séta: Supersingular Encryption from Torsion Attacks'. In: *Advances in Cryptology – ASIACRYPT 2021*. Vol. 13093. Lecture Notes in Computer Science. Springer International Publishing, 1st Dec. 2021, pp. 249–278. DOI: 10.1007/978-3-030-92068-5_9. URL: https://hal.inria.fr/hal-03471926.

[31] G. Tsaloli, B. Liang, C. Brunetta, G. Banegas and A. Mitrokotsa. 'DEVA: Decentralized, Verifiable Secure Aggregation for Privacy-Preserving Learning'. In: *Information Security*. Vol. 13118. Lecture Notes in Computer Science. Springer International Publishing, 27th Nov. 2021, pp. 296–319. DOI: 10.1007/978-3-030-91356-4_16. URL: https://hal.inria.fr/hal-03456382.

Doctoral dissertations and habilitation theses

[32] M. Chenu. 'Supersingular Group Actions and Post-quantum Key Exchange'. Ecole Polytechnique, 17th Dec. 2021. URL: https://hal.inria.fr/tel-03508143.

[33] I. Panaccione. 'On decoding algorithms for algebraic geometry codes beyond half the minimum distance'. Institut Polytechnique de Paris, 3rd Dec. 2021. URL: https://hal.inria.fr/tel-03512261.

Reports & preprints

[34] S. Abelard, E. Berardini, A. Couvreur and G. Lecerf. *Computing Riemann-Roch spaces via Puiseux expansions*. 8th July 2021. URL: https://hal.inria.fr/hal-03281757.

[35] S. Abelard, A. Couvreur and G. Lecerf. *Efficient computation of Riemann-Roch spaces for plane curves with ordinary singularities*. 14th Jan. 2021. URL: https://hal.archives-ouvertes.fr/hal-03110135.

[36] D. Augot, S. Bordage and J. Nardi. *Efficient multivariate low-degree tests via interactive oracle proofs of proximity for polynomial codes*. 11th Aug. 2021. URL: https://hal.inria.fr/hal-03454113.

[37] G. Banegas, T. Debris-Alazard, M. Nedeljković and B. Smith. *Wavelet: Code-based postquantum signatures with fast verification on microcontrollers*. Oct. 2021. URL: https://hal.inria.fr/hal-03403225.

[38] G. Banegas, K. Zandberg, A. Herrmann, E. Baccelli and B. Smith. *Quantum-Resistant Security for Software Updates on Low-power Networked Embedded Devices*. 10th June 2021. URL: https://hal.inria.fr/hal-03255844.

[39] M. Bombar and A. Couvreur. *Right-hand side decoding of Gabidulin codes and applications*. 15th Dec. 2021. URL: https://hal.archives-ouvertes.fr/hal-03481406.

[40] S. Bordage and J. Nardi. *Interactive Oracle Proofs of Proximity to Algebraic Geometry Codes*. 16th Feb. 2021. URL: https://hal.archives-ouvertes.fr/hal-03142459.

[41] A. Canteaut, A. Couvreur and L. Perrin. *Recovering or Testing Extended-Affine Equivalence*. 2nd Mar. 2021. URL: https://hal.inria.fr/hal-03156177.

[42] A. Challande, R. David and G. Renault. *Patch Detection using Binary Only Semantic Signatures*. 13th Dec. 2021. URL: https://hal.archives-ouvertes.fr/hal-03477882.

[43] A. Couvreur. *How arithmetic and geometry make error correcting codes better*. 25th Oct. 2021. URL: https://hal.inria.fr/hal-03400779.

[44] T. Debris-Alazard, M. Remaud and J.-P. Tillich. *Quantum Reduction of Finding Short Code Vectors to the Decoding Problem*. 17th Jan. 2022. URL: https://hal.inria.fr/hal-03529802.

[45] Y. El Housni and A. Guillevic. *Families of SNARK-friendly 2-chains of elliptic curves*. 8th Oct. 2021. URL: https://hal.inria.fr/hal-03371573.

[46] E. Florit and B. Smith. *An atlas of the Richelot isogeny graph*. 4th Jan. 2021. URL: https://hal.inria.fr/hal-03094296.

[47] F. Levy-dit-Vehel and M. Roméas. *A Composable Look at Updatable Encryption*. 18th Jan. 2022. URL: https://hal.inria.fr/hal-03531837.

[48] F. Morain. *SOME FACTORS OF NUMBERS OF THE FORM b^n ± 1 FOUND USING ECM WITH NEW CLASSES OF CURVES*. 20th Nov. 2021. URL: https://hal.inria.fr/hal-03437714.

[49] J. Nardi. *Projective toric codes*. 16th Feb. 2021. URL: https://hal.archives-ouvertes.fr/hal-03142469.

[50] I. Panaccione. *Attaining Sudan's decoding radius with no genus penalty for algebraic geometry codes*. 7th Apr. 2021. URL: https://hal.inria.fr/hal-03177569.

Other scientific publications

[51] D. Augot, S. Bordage, Y. El Housni, G. Fedak and A. Simonet. *Zero-Knowledge : trust and privacy on an industrial scale*. 5th Jan. 2022. URL: https://hal.inria.fr/hal-03512005.

10.3 Cited publications

[52] E. Ben-Sasson, I. Bentov, Y. Horesh and M. Riabzev. 'Fast Reed-Solomon Interactive Oracle Proofs of Proximity'. In: *45th International Colloquium on Automata, Languages, and Programming, ICALP 2018, July 9-13, 2018, Prague, Czech Republic*. 2018, 14:1–14:17.

[53] L. De Feo, D. Kohel, A. Leroux, C. Petit and B. Wesolowski. 'SQISign: compact post-quantum signatures from quaternions and isogenies'. In: *ASIACRYPT 2020 - 26th Annual International Conference on the Theory and Application of Cryptology and Information Security*. Daejeon (virtual), South Korea: Association for Computing Machinery, Dec. 2020. URL: https://hal.archives-ouvertes.fr/hal-03038004.

[54] T. Debris-Alazard. 'Cryptographie fondée sur les codes : nouvelles approches pour constructions et preuves ; contribution en cryptanalyse'. Theses. Sorbonne Universites, UPMC University of Paris 6, Dec. 2019. URL: https://hal.inria.fr/tel-02424234.

[55] C. Dwork, F. McSherry, K. Nissim and A. Smith. 'Calibrating Noise to Sensitivity in Private Data Analysis'. In: *Theory of Cryptography*. Ed. by T. Halevi Shaiand Rabin. Berlin, Heidelberg, 2006, pp. 265–284.

[56] Y. El Housni and A. Guillevic. 'Optimized and secure pairing-friendly elliptic curves suitable for one layer proof composition'. In: *CANS 2020 - 19th International Conference on Cryptology and Network Security*. Ed. by H. Shulman and S. Vaudenay. Vol. 12579. Lecture Notes in Computer Science. Vienna / Virtual, Austria: Springer, Dec. 2020, pp. 259–279. URL: https://hal.inria.fr/hal-02962800.

[57] A. Greuet, S. Montoya and G. Renault. 'Attack on LAC Key Exchange in Misuse Situation'. In: *CANS 2020 - 19th International conference on Cryptology and Network Security*. Vienna, Austria, Dec. 2020. URL: https://hal.inria.fr/hal-03046345.

[58] J. Groth. 'Short Pairing-Based Non-interactive Zero-Knowledge Arguments'. In: *Advances in Cryptology - ASIACRYPT 2010*. Ed. by M. Abe. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 321–340.

[59] T. Halevi, F. Benhamouda, A. D. Caro, S. Halevi, C. Jutla, Y. Manevich and Q. Zhang. ‘Initial Public Offering (IPO) on Permissioned Blockchain Using Secure Multiparty Computation’. In: *2019 IEEE International Conference on Blockchain (Blockchain)*. 2019, pp. 91–98. DOI: 10.1109/Blockchain.2019.00021.

[60] B. Parno, J. Howell, C. Gentry and M. Raykova. ‘Pinocchio: Nearly Practical Verifiable Computation’. In: *Commun. ACM* 59.2 (Jan. 2016), pp. 103–112.

[61] A. C.-C. Yao. ‘Protocols for Secure Computations (Extended Abstract)’. In: *FOCS*. IEEE Computer Society, 1982, pp. 160–164.

[62] J. Zhang, Z. Zhang, X. Xiao, Y. Yang and M. Winslett. ‘Functional mechanism: regression analysis under differential privacy’. In: *arXiv preprint arXiv:1208.0219* (2012).