RESEARCH CENTRE

Inria Nancy - Grand Est Center

IN PARTNERSHIP WITH:

Université de Lorraine, CNRS

2022

ACTIVITY REPORT

Project-Team

CARAMBA

Cryptology, arithmetic : algebraic methods for better algorithms

IN COLLABORATION WITH: Laboratoire lorrain de recherche en informatique et ses applications (LORIA)

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Algorithmics, Computer Algebra and Cryptology

Inria

Contents

Project-Team CARAMBA

Creation of the Project-Team: 2016 September 01

Keywords

Computer sciences and digital sciences

A1.1.2. – Hardware accelerators (GPGPU, FPGA, etc.)

A4.3.1. – Public key cryptography

A4.3.2. – Secret key cryptography

A4.8. – Privacy-enhancing technologies

A6.2.7. – High performance computing

A7.1. – Algorithms

A7.1.4. – Quantum algorithms

A8.4. – Computer Algebra

A8.5. – Number theory

A8.10. – Computer arithmetic

Other research topics and application domains

B8.5. – Smart society

B9.5.1. – Computer science

B9.5.2. – Mathematics

B9.10. – Privacy

1 Team members, visitors, external collaborators

Research Scientists

- Emmanuel Thomé [Team leader, INRIA, Senior Researcher, HDR]
- Xavier Bonnetain [INRIA, Researcher]
- Pierrick Gaudry [CNRS, Senior Researcher, HDR]
- Aurore Guillevic [INRIA, Researcher]
- Virginie Lallemand [CNRS, Researcher]
- Cécile Pierrot [INRIA, Researcher]
- Pierre Jean Spaenlehauer [INRIA, Researcher]
- Paul Zimmermann [INRIA, Senior Researcher, interim team leader until July 2022, HDR]

Faculty Members

- Sébastien Duval [UL, Associate Professor]
- Marine Minier [UL, Professor, HDR]

Post-Doctoral Fellow

- Loïc Rouquette [UL]

PhD Students

- Haetham Al Aswad [INRIA]
- Hamid Boukkerou [UL, ATER]
- Antoine Leudière [INRIA]
- Ana Rodriguez Cordero [UL]
- Quentin Yang [INRIA]

Administrative Assistants

- Anne Chrétien [CNRS]
- Emmanuelle Deschamps [INRIA]

2 Overall objectives

Our research addresses the broad application domain of cryptography and cryptanalysis from the algorithmic perspective. We study all the algorithmic aspects, from the top-level mathematical background down to the optimized high-performance software implementations. Several kinds of mathematical objects are commonly encountered in our research. Some basic ones are truly ubiquitous: integers, finite fields, polynomials, real and complex numbers. We also work with more structured objects such as number fields, algebraic curves, or polynomial systems. In all cases, our work is geared towards making computations with these objects effective and fast.

The two facets of cryptology—cryptography and cryptanalysis—are central to our research. The key challenges are the assessment of the classical and quantum security of proposed cryptographic

primitives (both public- and secret-key), as well as the introduction of new cryptographic primitives, or the performance improvement of existing ones.

Our research connects to both symmetric and asymmetric key cryptography. While the basic principles of these domains are rather different—indeed their names indicate different handlings of the key—research in both domains is led by the same objective of finding the best trade-offs between efficiency and security. In addition to this, both require to study design and analysis together as these two aspects nurture each other.

Our research topics can be listed either with broad applications domains in mind (a very coarse-grain view would have us list them under cryptography and cryptanalysis), or more thematically (see Figure 1). Either way, we also identify a set of *tools* that we sometimes develop *per se*, but most often as ingredients towards goals that are set in the context of other themes. Following the "vertical" reading direction in Figure 1, our research topics are as follows.

- Extended NFS family. A common algorithmic framework, called the Number Field Sieve (NFS), addresses both the integer factorization problem as well as the discrete logarithm problem over finite fields. We have numerous algorithmic contributions in this context, and develop software to illustrate them.

  We plan to improve on the existing state of the art in this domain by researching new algorithms, by optimizing the software performance, and by demonstrating the reach of our software with highly visible computations.

- Algebraic curves and their Jacobians. We develop algorithms and software for computing essential properties of algebraic curves for cryptology, eventually enabling their widespread cryptographic use.

  Closely related to the Tower Number Field Sieve are pairing-friendly curves. Pairings are bilinear maps $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ available on dedicated elliptic curves. The target group $\mathbb{G}_T$ is an extension $\mathrm{GF}(p^n)$ of small degree ($1 \le n \le 54$ in practice) where the TNFS algorithm and its variants apply. We study the security of these curves w.r.t. the TNFS algorithm, and we are interested in making recommendations of key-sizes, elliptic curve choices, and providing faster implementation of pairings.

  Questions more recently studied include the development of cryptosystems based on isogenies.

- Symmetric key cryptography. This topic has emerged in the team with several new hires since 2016. We are interested in particular in automatic tools for new paradigms of cryptanalysis, going beyond the classical linear and differential cryptanalysis techniques. Newer, more intricate techniques are rather hard to apply and are error-prone. The idea is then to automate the analysis process by developing tools implemented in constraint programming (CP) , satisfability (SAT) or mixed integer linear programming (MILP). We plan to pay special attention to the recent advances in cryptanalysis and to study recently proposed lightweight ciphers.

  In addition, we also study new designs. The challenge of the lightweight world (Embedded systems, Internet of Things) pushes symmetric cryptography to be ever more efficient while guaranteeing the same level of security as before. It is thus very important to scrutinize each building block of the symmetric key primitives to be convinced of their security.

- Quantum cryptanalysis. Cryptanalysis is at the core of security assessments. With the current progress of quantum computing, we need to know the security of cryptosystems against a quantum computer, especially for long-term security. Hence, we study quantum cryptanalysis. We focus on quantum algorithms that are the most distinct from classical algorithms, like the algorithms for the hidden subgroup problem, and on quantum variants of our classical cryptanalyses.

- Tools. Several mathematical objects are pervasive in our research. We sometimes study them *per se*, but they most often play a key role in the work related to the topics above. In particular, we study computer arithmetic, polynomial systems, linear algebra. In the context of symmetric cryptography, the mathematical objects we deal with are rather different: we are mainly interested in small (4 or 8 bits) non-linear permutations (the so-called S-boxes) and in linear transformations based on coding theory (Maximum Distance Separable (MDS) matrices or quasi-MDS matrices).

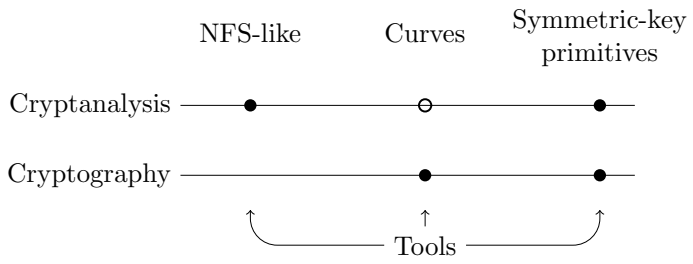

Figure 1: Visual representation of the thematic organization of CARAMBA. Solid dots: major interaction; clear dots: minor interaction.

Our goals with all these basic objects include a strong commitment to providing high-quality software that can be used as a dependable building block in our research.

As a complement to the last point, we consider that the impact of our research on cryptology in general owes a lot to the publication of concrete practical results. We are strongly committed to making our algorithms available as software implementations. We thus have several long-term software development projects that are, and will remain, part of our research activity.

3 Research program

3.1 The Extended Family of the Number Field Sieve

The Number Field Sieve (NFS) has been the leading algorithm for factoring integers for more than 25 years, and its variants have been used to set records for discrete logarithms in finite fields. It is reasonable to understand NFS as a framework that can be used to solve various sorts of problems. Factoring integers and computing discrete logarithms are the most prominent for the cryptographic observer, but the same framework can also be applied to the computation of class groups.

The state of the art with NFS is built from numerous improvements of its inner steps. In terms of algorithmic improvements, the recent research activity on the NFS family has been rather intense. Several new algorithms have been discovered since 2014, notably for non-prime fields, and their practical reach has been demonstrated by actual experiments.

The algorithmic contributions of the CARAMBA members to NFS would hardly be possible without access to a dependable software implementation. To this end, members of the CARAMBA team have been developing the Cado-NFS software suite since 2007. Cado-NFS is now the most widely visible open-source implementation of NFS, and is a crucial platform for developing prototype implementations for new ideas for the many sub-algorithms of NFS. Cado-NFS is free software (LGPL) and follows an open development model, with a publicly accessible development repository and regular software releases. Competing free software implementations exist, such as `msieve`, developed by J. Papadopoulos (whose last commit is from August 2018). T. Kleinjung develops his own code base, which is unfortunately not public.

The work plan of CARAMBA on the topic of the Number Field Sieve algorithm and its cousins includes the following aspects:

- Pursue the work on NFS, which entails in particular making it ready to tackle larger challenges. Several of the important computational steps of NFS that are currently identified as stumbling blocks will require algorithmic advances and implementation improvements. We will illustrate the importance of this work by computational records.
- Work on the specific aspects of the computation of discrete logarithms in finite fields.
- As a side topic, the application of the broad methodology of NFS to the treatment of “ideal lattices” and their use in cryptographic proposals based on Euclidean lattices is also relevant.

3.2 Algebraic Curves for Cryptology

The challenges associated with algebraic curves in cryptology are diverse, because of the variety of mathematical objects to be considered. These challenges are also connected to each other. On the cryptographic side, efficiency matters, while cryptanalysis looks at the hardness of the discrete logarithm problem.

Several members have expertise in multiple facets of curve-based cryptology, but recent work in the team has been concentrated on a few precise topics. One of them is pairing-based cryptography. Pairing-friendly curves were introduced in 2001 in (constructive) cryptography and should be designed with a very precise application goal in mind, contrary to the widespread curves such as x25519 or x448 in TLS, or the NIST curves, which can be used much more generically. The bilinear pairing has two aspects. First a destructive side: it transfers a discrete logarithm computation from the group of points of the curve (where the DLP is known to be hard, of exponential complexity in the size of the group), to a finite field extension GF(p^n) where better variants of the NFS algorithm apply. Hence pairing-friendly curves and in particular, wrong choices of parameters provide a large range of targets for record computations with the TNFS algorithm. Second, a constructive side: the pairing allows multiplying in the exponents two hidden values (two secret scalars) without knowing them explicitly, thanks to the formula $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$. We are looking for new curves that ensure a given security level, taking into account the latest advances in DL computation in GF(p^n), together with the development of faster pairing computation on these curves. Another growing area of interest for efficient pairings is zero-knowledge Succinct Non-interactive ARgument of Knowledge (zk-SNARK). Dedicated pairing-friendly curves are required and the team is interested in finding new such curves, while ensuring a security margin w.r.t. the TNFS algorithm.

We also investigate the practical security (e.g. against physical attacks) of elliptic curves and their implementations. Our focus here is more on the connection of such problems with Euclidean lattice theory, for example.

With NIST's competition on post-quantum cryptographic primitives, the new area of isogenies on elliptic curves is developing. Efficient implementation of isogenies is an active area of research nowadays, together with better parameter selection. The elliptic curves suitable for isogenies require different properties: they are supersingular contrary to the ordinary curves in classical cryptography. Selecting parameters is a difficult task, and in some cases, it requires a large computational effort of a class number computation.

The research objectives of CARAMBA on the topic of algebraic curves for cryptology are as follows:

- Ban obsolete parameters of pairing-friendly curves thanks to new discrete logarithm record computations. Investigate new parameter selections and build new cryptographic recommendations of pairing-friendly elliptic curves.
- Develop a full library of elliptic curves with their pairing computations in SageMath in the spirit of the Elliptic Curve Formula Database to bridge the gap between theoretical papers and efficient software library developments.

3.3 Symmetric Cryptography

In symmetric key cryptology, we are tackling problems related to both design and analysis. A large part of our recent research has been motivated by the Lightweight Cryptography Standardization Process of NIST [1] that embodies a crucial challenge of the last decade: finding ciphers that are suitable for resource-constrained devices.

On a general note, the working program of CARAMBA in symmetric cryptography is defined as follows:

- Develop automatic tools based on constraint programming to help find optimum attack parameters. The effort will be focused on the AES standard and on recent lightweight cipher proposals.
- Contribute to the security and performance analysis effort required to sort out the candidates for the NIST Lightweight Cryptography Standardization Process.
- Study how to protect services execution on dedicated platforms using white-box cryptography and software obfuscation methods.

[1] National Institute of Standard and Technology.

3.4 Computer Arithmetic

Computer arithmetic is part of the common background of all team members, and is naturally ubiquitous in our application domains. However involved the mathematical objects considered may be, dealing with them first requires to master more basic objects: integers, finite fields, polynomials, and real and complex floating-point numbers. Libraries such as GNU MP, GNU MPFR, GNU MPC do an excellent job for these, both for small and large sizes.

Most of our involvement in subjects related to computer arithmetic is to be understood in connection to our applications to the Number Field Sieve and to Abelian varieties. As such, much of the research work we envision will appear as side-effects of developments in these contexts. On the topic of arithmetic work *per se*:

- We will seek algorithmic and practical improvements to the most basic algorithms. That includes for example the study of advanced algorithms for integer multiplication, and their practical reach.

- We will continue to work on the arithmetic libraries in which we have crucial involvement, such as GNU MPFR, GNU MPC, GF2X, MPFQ, and also GMP-ECM.

4 Application domains

4.1 Better Awareness and Avoidance of Cryptanalytic Threats

Our study of the Number Field Sieve family of algorithms aims at showing how the threats underlying various supposedly hard problems are real. Our record computations, as well as new algorithms, contribute to having a scientifically accurate assessment of the feasibility limit for these problems, given academic computing resources. The data we provide in this way is a primary ingredient for government agencies whose purpose includes guidance for the choice of appropriate cryptographic primitives. For example the French ANSSI [2], German BSI, or the NIST [3] in the United States base their recommendations on such computational achievements.

The software we make available to achieve these cryptanalytic computations also allows us to give cost estimates for potential attacks to cryptographic systems that are taking the security/efficiency/legacy compatibility trade-offs too lightly. Attacks such as LogJam [36] are understood as being serious concerns thanks to our convincing proof-of-concepts. In the LogJam context, this impact has led to rapid worldwide security advisories and software updates that eventually defeat some potential intelligence threats and improve confidentiality of communications.

4.2 Promotion of Better Cryptography

We also promote the switch to algebraic curves as cryptographic primitives. Those offer nice speed and excellent security, while primitives based on elementary number theory (integer factorization, discrete logarithm in finite fields), which underpin e.g., RSA, are gradually forced to adopt unwieldy key sizes so as to comply with the desired security guarantees of modern cryptography. Our contributions to the ultimate goal of having algebraic curves eventually take over the cryptographic landscape lie in our contributions to fast arithmetic, our contributions to the point counting problem, and more generally our expertise on the diverse surrounding mathematical objects, or on the special cases where the discrete logarithm problem is not hard enough and should be avoided.

We also promote cryptographically sound electronic voting, for which we develop the Belenios prototype software (licensed under the AGPL). It depends on research made in collaboration with the PESTO team, and provides stronger guarantees than current state of the art.

[2] In [37], the minimal recommended RSA key size is 2048 bits for usage up to 2030. See also Annex B, in particular Section B.1 “Records de calculs cryptographiques”.

[3] The work [39] is one of only two academic works cited by NIST in the initial version (2011) of the report [40].

4.3 Key Software Tools

The vast majority of our work is eventually realized as software. We can roughly categorize it in two groups. Some of our software covers truly fundamental objects, such as the GNU MPFR, GNU MPC, GF2X, or MPFQ packages. To their respective extent, these software packages are meant to be included or used in broader projects. For this reason, it is important that the license chosen for this software allows proper reuse, and we favor licenses such as the LGPL, which is not restrictive. We can measure the impact of this software by the way it is used in e.g., the GNU Compiler Collection (GCC), in Victor Shoup's Number Theory Library (NTL), or in the Sage computer algebra system. The availability of these software packages in most Linux distributions is also a good measure for the impact of our work.

We also develop more specialized software. Our flagship software package is Cado-NFS[42], and we also develop some others with various levels of maturity, such as GMP-ECM, CMH, or Belenios, aiming at quite diverse targets. Within the lifespan of the CARAMBA project, we expect more software packages of this kind to be developed, specialized towards tasks relevant to our research targets: important mathematical structures attached to genus 2 curves, generation of cryptographically secure curves, or tools for attacking cryptographically hard problems. Such software both illustrates our algorithms, and provides a base on which further research work can be established. Because of the very nature of these specialized software packages as research topics in their own right, needing both to borrow material from other projects, and being possible source of inspiring material for others, it is again important that these be developed in a free and open-source development model.

5 Highlights of the year

5.1 Awards

- Gabrielle de Micheli who did her PhD in the team under the supervision of Pierrick Gaudry and Cécile Pierrot won the "Gilles Kahn" award for her PhD thesis in January 2022.

- The article [22] about the CORE-MATH project by Sibidanov, Zimmermann and Glondu was published at the ARITH conference and received the Best Paper Award.

5.2 Other highlights

- On November 23, 2022, Cécile Pierrot, Pierrick Gaudry, Paul Zimmermann, and their historian colleague Camille Desenclos (Amiens) gave a press conference on their work on deciphering an encrypted letter written by the emperor Charles Quint in 1547. This work produced a lot of feedback in different national and international media.

- In July 2022, Virginie Lallemand co-organized Cyber in Nancy, the summer school in Cybersecurity of the “GDR Sécurité Informatique”.

5.3 Research environment

Over the last few years, and even more so in 2022, Inria's institutional positioning and communication policy have been the source of increasing trouble, which is harmful to our research environment. Bodies such as the CNRS national committee rightly pointed out the detrimental effect of Inria's ambition on the research ecosystem, especially in joint labs such as Loria. Lastly, Inria's top management has embarked on a preposterous crusade against its own evaluation body (the Evaluation Committee), which contributes in no way to a healthy research environment.

6 New software and platforms

6.1 New software

6.1.1 Belenios

Name: Belenios - Verifiable online voting system

Keyword: E-voting

Functional Description: Belenios is an open-source online voting system that provides vote confidentiality and verifiability. End-to-end verifiability relies on the fact that the ballot box is public (voters can check that their ballots have been received) and on the fact that the tally is publicly verifiable (anyone can recount the votes). Vote confidentiality relies on the encryption of the votes and the distribution of the decryption key (no one detains the secret key).

Belenios supports various kind of elections. In the standard mode, Belenios supports simple elections where voters simply select one or more candidates. It also supports arbitrary counting functions at the cost of a slightly more complex tally procedure for the authorities. For example, Belenios supports Condorcet, STV, and Majority Judgement, where voters rank candidates and grade them.

Belenios is available in several languages for the voters as well as the administrators of an election. More languages can be freely added by users.

News of the Year: In 2022, our platform was used to run about 1400 elections, with about 50,000 ballots counted.

This year we released a major update of Belenios (2.0) that introduces a new election format where election events (e.g., ballot submission) are chained to each other. This sets the stage for a future release where the server will be able to commit to the actual content of an election. We have also improved the monitoring of the server (eg by making the voting authority code constant) and we have initiated compliance with the CNIL recommendations. We have hardened the security of Belenios by linking a voter to the public part of their voting code from the setup phase. To ensure better availability, Belenios is now hosted on OVH servers. Finally, we have pursued the development of the REST API in preparation of a major overhaul of the election administration interface.

URL: https://www.belenios.org/

Contact: Stephane Glondu

Participants: Pierrick Gaudry, Stephane Glondu, Véronique Cortier

Partners: CNRS, Inria

6.1.2 CADO-NFS

Name: Crible Algébrique: Distribution, Optimisation - Number Field Sieve

Keywords: Cryptography, Number theory

Functional Description: CADO-NFS is a complete implementation in C/C++ of the Number Field Sieve (NFS) algorithm for factoring integers and computing discrete logarithms in finite fields. It consists in various programs corresponding to all the phases of the algorithm, and a general script that runs them, possibly in parallel over a network of computers.

News of the Year: In 2022, Cado-NFS evolved in the form of preparatory work for further computations. In particular, work has been done in order to make it possible to run Cado-NFS on small Docker containers, which is a useful first step towards easy deployment on various kinds of cloud-scale computing infrastructures, using engines such as Kubernetes, for example.

Furthermore, work towards some of the ideas in the context of the Kleptomaniac ANR project is ongoing within Cado-NFS, and will continue in 2023.

URL: https://cado-nfs.inria.fr/

Contact: Emmanuel Thomé

Participants: Pierrick Gaudry, Emmanuel Thomé, Paul Zimmermann

6.1.3 Drinfeld modules in SageMath

Keywords: Computer algebra, Number theory

Functional Description: This project is an implementation, starting from scratch, of Drinfeld modules in SageMath. This module shall be integrated into SageMath.

Drinfeld modules are mathematical objects similar to elliptic curves, but in another setting, which is that of function fields.

The aim of this implementation is to provide researchers with all basic computational tools for Drinfeld modules, and to build a reliable basis for future, more sophisticated algorithms.

URL: https://trac.sagemath.org/ticket/33713

Author: Antoine Leudière

Contact: Antoine Leudière

6.1.4 snark-2-chains

Name: Families of SNARK-friendly 2-chains of elliptic curves

Keywords: Cryptography, Cryptocurrency, Blockchain

Functional Description: This library implements finite field and elliptic curve arithmetic for BN curves (Barreto-Naehrig), BLS (Barreto-Lynn-Scott), KSS (Kachisa-Schaefer-Scott), and 2-chains made of BW6 (Brezing-Weng curves of embedding degree 6), CP8, CP12 (Cocks-Pinch curves of embedding degree 8 and 12) for use with zk-snarks (zero-knowledge succinct non-interactive argument of knowledge). The cryptographic applications are: pairing, scalar multiplication on the curves, hashing on the curves. The code is a proof of concept tied to two papers and is not optimized.

News of the Year: The library was first released in October 2021 as companion code of the EUROCRYPT'2022 paper. In 2022, state-of-the-art pairing computation on KSS16 and KSS18 curves was developed (known as "optimal-ate" pairing), together with state-of-the-art final exponentiation, according to the latest preprints on the topic. Support for BN curves, BLS 21 and BLS27, FST 6.4 (curves with embedding degrees 20 and 28 and j-invariant 1728) was developed. Formulas from Costello, Lange and Naehrig at PKC'2010 were implemented for cubic twists and quartic twists. Testing and documentation were extended. As companion code of the survey paper at DCC, it now includes faster final exponentiation for outer curves BW6 of 2-chains made of an inner BN, BLS12 or BLS24 curve. Finally it provides a basic support for Remi Clarisse curves BW13 and BW19 of prime embedding degree.

URL: https://gitlab.inria.fr/zk-curves/snark-2-chains

Publications: hal-03667798, hal-03371573

Contact: Aurore Guillevic

6.1.5 TNFS-alpha

Name: alpha for the Tower Number Field Sieve algorithm

Keyword: Cryptography

Functional Description: This library implements a simulation tool for the tower number field sieve algorithm computing discrete logarithms in extension fields of small degree (tested up to 54). The library contains an implementation of the exact computation of alpha, the bias between the expected smoothness of an integer and the expected smoothness of a norm of an algebraic integer in a number field made of two extensions. The algorithm is a generalization to extensions of the exact implementation of alpha in the software CADO-NFS. The software contains an implementation of the E-function of B. A. Murphy (Murphy's E) which estimates the quality of the polynomial selection step in TNFS through a simulation of the yield of the relation collection in the TNFS algorithm. Finally it contains a database of pairing-friendly curve seeds with the estimated level of security w.r.t a discrete logarithm computation in the corresponding finite field.

News of the Year: In 2022 support was included to generate sparse seeds of pairing-friendly curves with many more curve families, and with specific needs for SNARKs such as a large power of 2 dividing the predecessor of the characteristic, or dividing the predecessor of the order, or both conditions at the same time. Now it supports BN curves, all BLS curves, all KSS curves, Aurifeuillean curves, Fotiadis-Martindale curves, Freeman-Scott-Teske curves and allows generating seeds producing FFT-friendly fields. Galbraith-McKee-Valença curves were included as special cases of MNT curves. The security level of these curves was estimated for the DCC survey paper. For TNFS simulation, precomputed tables of sparse irreducible polynomials of degree 18, 20, 24 were released to estimate the security of KSS18, BLS24, and FST6.4 k=20 curves.

URL: https://gitlab.inria.fr/tnfs-alpha/alpha

Publications: hal-03667798, hal-03371573, hal-02263098, hal-02396352

Contact: Aurore Guillevic

6.1.6 CORE-MATH

Name: CORE-MATH

Keywords: Arithmetic code, Floating-point, Correct Rounding

Functional Description: CORE-MATH Mission: provide on-the-shelf open-source mathematical functions with correct rounding that can be integrated into current mathematical libraries (GNU libc, Intel Math Library, AMD Libm, Newlib, OpenLibm, Musl, Apple Libm, llvm-libc, CUDA libm, ROCm)

News of the Year: In 2022, a full set of C99 single precision functions was designed, and in addition single precision functions from the new C23 standard. Also, a few double precision functions are already available: acos, asin, cbrt, exp, exp2, hypot, log and rsqrt.

URL: https://core-math.gitlabpages.inria.fr/

Publication: hal-03721525

Contact: Paul Zimmermann

6.1.7 GNU-MPFR

Keywords: Multiple-Precision, Floating-point, Correct Rounding

Functional Description: GNU MPFR is an efficient arbitrary-precision floating-point library with well-defined semantics (copying the good ideas from the IEEE 754 standard), in particular correct rounding in 5 rounding modes. It provides about 100 mathematical functions, in addition to utility functions (assignments, conversions...). Special data (Not a Number, infinities, signed zeros) are handled like in the IEEE 754 standard. GNU MPFR is based on the mpn and mpz layers of the GMP library.

News of the Year: In November 2022, a minor version (4.1.1) was released, with 13 bug fixes with respect to 4.1.0 (released in 2020), various internal changes due to the switch from Subversion to Git and a complete review of the typography of the manual. In early January 2023, a major version (4.2.0) was released, which in particular implements missing functions from the new ISO C23 standard.

URL: https://www.mpfr.org/

Publications: hal-01394289, hal-01502326, inria-00069930, inria-00070174, inria-00103655, inria-00000026

Contact: Vincent Lefèvre

Participants: Guillaume Hanrot, Paul Zimmermann, Philippe Théveny, Vincent Lefèvre

7 New results

7.1 Algebraic curves for cryptology

7.1.1 Computing a Group Action from the Class Field Theory of Imaginary Hyperelliptic Function Fields

Participants: Antoine Leudière, Pierre-Jean Spaenlehauer.

In this work [29] we expand the algorithmic toolbox for finite Drinfeld modules by designing algorithms and complexity bounds for the manipulation of isogenies of ordinary Drinfeld modules. This paper is an expanded version of a previous preprint which focused on cryptographic applications. Benjamin Wesolowski found a way to attack our proposed cryptographic applications, this is why this new version of the paper focuses more on purely algorithmic aspects and on effective number theory.

7.1.2 Families of SNARK-friendly 2-chains of elliptic curves

Participants: Aurore Guillevic.

This work [19] is a generalization of [35] published at CANS'2020, with Youssef El Housni, PhD student in the GRACE team at Inria Saclay, and ConsenSys. This paper considers chains of two pairing-friendly elliptic curves for SNARKs (Succinct Non-interactive ARguments of Knowledge). In the previous work, one 2-chain was investigated: the curves BLS12-381 and BW6-761. This work considers 2-chains of curves where the first (inner) curve can be a BN (Barreto–Naehrig), or a BLS12 or BLS24 (Barreto–Lynn–Scott) curve. The second (outer) curve is obtained with the Brezing–Weng construction (BW6 curves). Our comparison shows that it is faster than curves obtained with the Cocks-Pinch method. The aim is to provide other trade-offs in terms of size, and arithmetic and pairing efficiency. The companion code is referenced in Section 6.1.4, and a full Golang implementation is developed in the library GNARK. The preprint appeared in the 2021 report and was published in the proceedings of the EUROCRYPT conference in 2022.

7.1.3 Co-factor clearing and subgroup membership testing on pairing-friendly curves

Participants: Aurore Guillevic.

The paper [19] improved the group operations on BLS curves. These curves are not of prime order, and two important cryptographic operations are: *co-factor clearing*, that is multiplying a point on the curve by the cofactor so that the point has prime order, and *membership testing*, that is testing if the point is in the subgroup of prime order. In [20] with Youssef El Housni and Thomas Piellard (Consensys), we generalized our results for these two operations for all known pairing-friendly curves: the speed-up applies to many curves except the KSS curves. It was presented at the AFRICACRYPT'2022 conference.

7.1.4 A survey of elliptic curves for proof systems

Participants: Aurore Guillevic.

On October 21, 2021, A. Guillevic received an invitation from Carla Ràfols to submit a survey paper on *Elliptic curves for zero-knowledge proofs* to the special issue *Mathematics of Zero-Knowledge* of the DCC journal. This survey paper [10] written with Diego Aranha (Aarhus University) and Youssef El Housni presents the area and the state of the art for 2-chains and cycles, the known constructions, and the known impossibility results on finding cycles. It also lists the open-source implementations of such curves available in 2022. The 2-chain constructions from [19] were generalized to BN curves.

7.2 Factorization and discrete logarithm

7.2.1 State of the art

Participants: Pierrick Gaudry, Aurore Guillevic, Emmanuel Thomé, Paul Zimmermann.

In the invited article [32] in IEEE Security & Privacy, we review the current state of the art of cryptanalysis for three number-theoretic problems using classical (nonquantum) computers, including, in particular, our most recent computational records for integer factoring and prime-field discrete logarithms. This work is connected to our earlier work on factoring and discrete logarithm records, which we put in perspective in the broader context of the assessment of the security of the classical public-key cryptographic primitives. Despite the hype about the future transition to post-quantum cryptographic algorithms, everyone is fully aware of the fact that classical algorithms are here to stay, at least for a long while. It is of utmost importance to properly assess the possible security risk that arises from their continued use.

7.2.2 Algorithmic aspects of elliptic bases in finite field discrete logarithm algorithms

Participants: Cécile Pierrot.

The article [13] published in Advances in Mathematics of Communications 2022 investigates the practicality of heuristic algorithms based on elliptic bases, for the computation of discrete logarithms in small characteristic finite fields. Elliptic curve representation is already used to achieve provable quasi-polynomial time but the idea here is to use a different model of the elliptic curve used for the elliptic basis that allows for a relatively simple adaptation of the techniques used with former Frobenius representation algorithms. Our experiments with the field $GF(3^{1345})$ indicate that switching to elliptic representations might be possible with performances comparable to the current best practical methods.

7.2.3 Individual Discrete Logarithm with Sublattice Reduction

Participants: Haetham Al Aswad, Cécile Pierrot.

The work [26] deals with the splitting step in the number field sieve for finite fields of composite extension degree. The splitting step consists in finding an element R with a smooth norm and such that the logarithm of the target T can be easily deduced from the logarithm of R. The current state of the art takes advantage of lattice-reduction algorithms, such as LLL and BKZ in order to find such an element R. In this work, the authors explore the use of sublattices of the lattices usually used and perform experiments to validate this idea. Moreover, the authors give an asymptotic analysis of the individual logarithm step in NFS when LLL or BKZ are used as lattice-reduction in this new algorithm.

7.3 Floating-point arithmetic

7.3.1 The CORE-MATH project

Participants: Stéphane Glondu, Paul Zimmermann.

The aim of the CORE-MATH project is to provide on-the-shelf open-source mathematical functions with correct rounding that will be integrated into current mathematical libraries (GNU libc, Intel Math Library, AMD Libm, Newlib, OpenLibm, Musl, Apple Libm, llvm-libc, CUDA libm, ROCm). These functions are implemented in the C language and target the three IEEE 754 binary formats (single precision, double precision, quadruple precision), and also the extended double precision (significand of 64 bits). This project is motivated by the fact that current mathematical libraries are far from giving the best possible results, as demonstrated in [28].

In 2022, with the help of Stéphane Glondu, some tools were set up to assess the correctness of the CORE-MATH functions, and to measure their speed (both reciprocal throughput and latency). These tools are also able to test other mathematical libraries.

In 2022, a full set of C99 single precision (binary32) functions was implemented. In addition, binary32 functions from the new C23 standard were also implemented. The article [22] detailing this work got the Best Paper Award at the Arith'2022 conference. A few double precision (binary64) functions are now available: `acos`, `asin`, `cbrt`, `exp`, `exp2`, `hypot`, `log`, `rsqrt`. During his M1 internship, Tom Hubrecht designed an efficient `pow` function in double precision, which is in review before inclusion into CORE-MATH.

The development of CORE-MATH forced us to revisit some classical algorithms, for example FastTwoSum in the context of directed roundings [31].

Monthly video-conferences are organized with the LLVM developers who also develop correctly-rounded routines, and use the CORE-MATH tools to check their correctness and efficiency.

7.3.2 Search for worst cases

Participants: Paul Zimmermann.

To design correctly-rounded functions as in the CORE-MATH project, it is of utmost importance to know "worst cases" of mathematical functions, i.e., inputs x such that $f(x)$ has many zeros or ones after the rounding bit. During her M1 internship, Lauriane Turelier extended the SLZ algorithm to bivariate functions, and designed a SageMath implementation of this extension [30].

7.4 Symmetric cryptology

7.4.1 Automatic Search of Rectangle Attacks on Feistel Ciphers: Application to WARP

Participants: Virginie Lallemand, Marine Minier, Loïc Rouquette.

The research presented in [14] studies how to build an automated tool that searches for good boomerang characteristics and boomerang attacks for Feistel ciphers, and how to apply these to the ciphers Warp, LBlock-S and Twine. By relying on the findings by Delaune and coauthors [38] (for the distinguisher search) together with the work by Qin and co-authors [41] for the inclusion of the key-recovery cost, we produce a new model that directly looks for an optimization of the boomerang attack as a whole. For the recent cipher Warp, this model returns a 26-round rectangle attack of time complexity equivalent to 2^{116} cipher encryptions, which at the time was the best known attack on Warp (other techniques later presented were able to attack more rounds).

7.4.2 Benchmarking of lightweight cryptographic algorithms for wireless IoT networks

Participants: Marine Minier.

Cryptographic algorithms that can provide both encryption and authentication are increasingly required in modern security architectures and protocols (e.g. TLS v1.3). Many authenticated encryption systems have been proposed in the past few years, which has resulted in several contributions to research in cryptanalysis. In this same direction, the National Institute of Standards and Technology (NIST) is coordinating a large effort to find a new standard authenticated encryption algorithm to be used by resource-constrained and limited devices. In this paper, 12 algorithms of the 33 candidates of the Round 2 phase from NIST competition are being benchmarked on a real IoT test-bed. In [11], these 33 ciphers implement authenticated encryption with associated data which aims at preserving integrity, privacy and authenticity at the same time. In this work, we ported the 12 algorithms to different hardware platforms (an x86_64 PC, an AVR ATmega128, an MSP430F1611 and the IoT-LAB platform) and made a fair comparison between their performance. We adapted these algorithms to the Contiki operating system to evaluate the latency and efficiency of each algorithm on IoT applications deployed on a national experimental platform which is IoT-LAB. In addition, we used the FELICS-AE benchmark to quantify locally the RAM, execution time and code size of each algorithm. This work provides practical results of their performance in an IoT scenario, which pave the way for further research on other algorithms, platforms or OS.

7.4.3 And Rijndael? Automatic Related-key Differential Analysis of Rijndael

Participants: Loïc Rouquette, Marine Minier.

Finding optimal related-key differential characteristics for a given cipher is a problem that hardly scales. For the first time, in [21] we study this problem against the 25 instances of the block cipher Rijndael, which are the little brothers of AES. To achieve this, we adapt and improve an existing approach for AES which is based on Constraint Programming. The attacks presented here surpass all the previous cryptanalytic results of Rijndael. Among all our results, we obtain a 12-round (out of 13 rounds) related-key differential attack for Rijndael with a block size equal to 128 bits and a key size equal to 224 bits. We also obtain an 11-round related-key differential characteristic distinguisher for Rijndael with a block size equal to 160 bits and a key size equal to 256 bits leading to an attack on 12 rounds (out of 14 rounds).

7.4.4 Non-triangular self-synchronizing stream ciphers

Participants: Paul Huynh, Marine Minier.

In [12], we propose an instantiation, called Stanislas, of a dedicated Self-Synchronizing Stream Cipher (SSSC) involving an automaton with finite input memory using non-triangular state transition functions. Previous existing SSSCs are based on automata with shifts or triangular functions (T–functions) as state transition functions. Our algorithm Stanislas admits a matrix representation deduced from a general and systematic methodology called Linear Parameter Varying (LPV). This particular representation comes from control theory, more specifically from a special property of dynamical systems called flatness. Hardware implementations and comparisons with some state-of-the-art stream ciphers on Xilinx FPGAs are presented. It turns out that Stanislas provides bigger throughput than the considered stream ciphers (synchronous and self-synchronizing) when straightforward implementations are considered. Moreover, its synchronization delay is much smaller than the SSSC Moustique (40 clock cycles instead of 105) and the standard approach CFB1-AES128 (40 clock cycles instead of 128).

7.4.5 Towards a new design of ciphers to secure CPS: the role of control theory

Participants: Hamid Boukerrou, Marine Minier.

Among several solutions to face the unprecedented increase of attacks against Cyber Physical Systems, encryption plays a central role. In the form of a Proof of Concept and in [24], this contribution gives a new methodology for designing self-synchronizing automata, having in mind their use in symmetric cryptography, namely the Self-Synchronizing Stream Ciphers. The contribution of the paper is to recast the design as control theoretical issues. It calls for a graph-based approach and results borrowed from control theory and dynamical systems, in particular LPV systems. The design leads to not necessarily T -functions as state transition functions of the automata involved in the ciphering and deciphering sides. It is a consideration that is important for the sake of security. Another asset of the approach is that the resulting ciphers admit possibly vectorial inputs to enhance the throughput.

7.4.6 Beyond quadratic speedups in quantum attacks on symmetric schemes

Participants: Xavier Bonnetain.

We report in [15] the first quantum key-recovery attack on a symmetric block cipher design, using classical queries only, with a more than quadratic time speedup compared to the best classical attack.

We study the 2XOR-Cascade construction of Gaži and Tessaro (EUROCRYPT 2012). It is a key length extension technique which provides an n-bit block cipher with 5n/2 bits of security out of an n-bit block cipher with 2n bits of key, with a security proof in the ideal model. We show that the offline-Simon algorithm of Bonnetain et al. (ASIACRYPT 2019) can be extended to, in particular, attack this construction in quantum time $O(2^n)$, providing a 2.5−th power quantum speedup over the best classical attack.

Regarding post-quantum security of symmetric ciphers, it is commonly assumed that doubling the key sizes is a sufficient precaution. This is because Grover's quantum search algorithm, and its derivatives, can only reach a quadratic speedup at most. Our attack shows that the structure of some symmetric constructions can be exploited to overcome this limit. In particular, the 2XOR-Cascade cannot be used to generically strengthen block ciphers against quantum adversaries, as it would offer only the same security as the block cipher itself.

7.5 E-voting

7.5.1 General audience book on e-voting

Participants: Pierrick Gaudry.

Together with Véronique Cortier (PESTO Team), Pierrick Gaudry wrote a general audience book [33] on various aspects of electronic voting, with an emphasis on security aspects. Written in French, this book was published by Odile Jacob and received a nice press coverage, including an article in Le Monde.

7.5.2 Coercion-resistance

Participants: Pierrick Gaudry, Quentin Yang.

In a first work [18], we explore the possibility of revealing only the result of an election, without decrypting the individual ballots, or any side-information. The result must be computed in a way such that everyone can verify that it indeed corresponds to the (public) ballot box. Also, even the trust parties who possess the shares of the decryption key should not learn anything more than the winner of the election.

We propose a multi-party computation toolbox dedicated to this kind of problems, and show that it allows us to tackle all well-known tally functions, including the most complicated, like the Condorcet-Schulze, D'Hondt, STV, or Majority Judgement. We also explain how the classical ElGamal encryption (typically based on elliptic curves) can be used, instead of the Paillier scheme that is often chosen in theoretical papers, but is far less frequent in standard crypto libraries.

In [27], we show that the JCJ e-voting protocol that is the basis of many coercion-resistant systems is flawed, in the sense that the tally phase leaks more information than what it should. In some specific scenarios, this can give an advantage to a coercer. We therefore propose a new version of JCJ, that we call CHide, and that relies on the multi-party toolbox that we designed in the previous article. We also refine the existing formal definitions of coercion-resistance, in order to highlight the flaw, and prove that CHide fixes the problem.

7.5.3 Features and usage of Belenios in 2022

Participants: Pierrick Gaudry, Stéphane Glondu.

This short paper [17] was written with V. Cortier and describes the list of features that have been added to the Belenios software in the past few years.

7.5.4 Themis: an on-site voting system with systematic cast-as-intended verification and partial accountability

Participants: Pierrick Gaudry.

In collaboration with members of the PESTO team and members of the Idemia company, we proposed a new voting system. The goal is to offer better guarantees in a context of on-site voting. The main advantages of our system is that it offers the cast-as-intended property, *i.e.* the machines used by the voters can not cheat when preparing the electronic ballot. This comes with a thorough study of accountability, that is the possibility to blame the right entity, when a problem is detected. Formal proofs of security are provided, using the ProVerif tool.

8 Bilateral contracts and grants with industry

8.1 Bilateral contracts with industry

8.1.1 Consulting with Swiss Post

Participants: Pierrick Gaudry.

Together with the PESTO team, we had a consulting contract with Swiss Post. The topic was e-voting in general, and more precisely various topics (short-term and long-term design evolution, security analysis) related to their solution.

8.1.2 Verifiability during the French legislative elections

Participants: Pierrick Gaudry, Stéphane Glondu.

Together with the PESTO team, we had a contract with the French Ministry of Foreign Affairs (MEAE), in the context of the legislative elections, for which the French citizens from abroad had the possibility to vote over Internet. We played the role of external third-party, as required by the CNIL recommendations for such high-stake elections. While the contract was signed with the MEAE, it also involved interactions with the vendor of the solution (Voxaly), and the ANSSI who was the security advisor for the MEAE.

9 Partnerships and cooperations

9.1 Visits to international teams

9.1.1 Sabbatical programme

Aurore Guillevic

- **Visited institution:** Aarhus University (Denmark)
- **Dates of the stay:** From August 1, 2021 to July 31, 2022
- **Summary of the stay:** A. Guillevic visited the Cryptography and Security Group led by Pr. Ivan Damgård and collaborated with Diego F. Aranha on pairing-friendly curves and pairing implementation. During her stay, she took part in the weekly group meetings and seminars, and joined the monthly faculty meetings of the Computer Science department led by Pr. Kaj Grønbæk. With Diego F. Aranha she taught Pr. Johan Hansen's former course Elliptic Curves, Number Theory and Cryptography. 12 students from the CS department and the Math department enrolled in the course which ran 15 weeks, 4 hours per week. A. Guillevic attended the conference EUROCRYPT'2022 in Trondheim, Norway, like many cryptographers of the Aarhus team. Youssef El Housni, PhD student in the GRACE team (Inria Saclay) co-advised by A. Guillevic, visited her one week, May 9–13 in 2022. With D. F. Aranha and Youssef El Housni, they wrote a survey paper on elliptic curves for SNARKs [10]. The one-year sabbatical stay ended with the Aarhus crypto days, two days of talks and presentations organised by the group at the CS department where cryptographers from Denmark and Sweden (Lund University) attend. An ongoing project is continuing with D. F. Aranha and G. Fotiadis on secure and fast pairing-friendly curves.

Emmanuel Thomé

- **Visited institution:** University of California San Diego
- **Dates of the stay:** From August 1, 2021 to July 31, 2022

- **Summary of the stay:** Emmanuel Thomé was on Inria sabbatical at the University of California San Diego, and supported by a Fulbright grant. The latter was also co-funded by the Région Grand-Est. Much of the work done there was in connection with the preparation of future factoring projects, and in particular the adaptation of the CADO-NFS to cloud environments. As a visiting professor at UCSD, Emmanuel Thomé also participated in teaching at the graduate and undergraduate level.

9.1.2 Research stays abroad

Haetham Al Aswad

- **Visited institution:** University of California San Diego
- **Country:** United States
- **Dates:** From May 01, 2022 to June 30, 2022
- **Summary of the stay:** Haetham Al Aswad was a student visitor at the University of California San Diego, under the supervision of Nadia Heninger. The work consisted on working on a multiple variant of the number field sieve. Haetham Al Aswad worked there with Emmanuel Thomé and Nadia Heninger. Haetham Al Aswad also attended a graduate course about Cryptography given by Nadia Heninger.
- **Mobility program/type of mobility:** This stay was funded by the program *Dream* of Université de Lorraine.

Quentin Yang

- **Visited institution:** Université Catholique de Louvain
- **Country:** Belgium
- **Dates:** From May 30, 2022 to August 05, 2022
- **Summary of the Stay:** Quentin Yang was a visiting researcher at the Université Catholique de Louvain, under the supervision of Olivier Pereira. In collaboration with Thomas Peters and Henri Devillez, he worked on a traceable encryption primitive and its application to end-to-end verifiable receipt-free electronic voting. This work resulted in the writing of a paper which was submitted to Security and Privacy.

9.2 National initiatives

9.2.1 PEPR Quantique, project PQ-TLS

Participants: Xavier Bonnetain, Pierre-Jean Spaenlehauer.

- Program: PEPR Quantique
- Project acronym: PQ-TLS
- Duration: 01/2022 - 12/2026
- Coordinator: Université de Rennes 1
- Other partners: Université de Limoges, Université de Rouen, Université de Bordeaux, Université de Saint-Quentin-en Yvelines, Université de Saint-Étienne, ENS de Lyon, Inria (GRACE, CARAMBA, COSMIQ, PROSECCO), CEA (Grenoble LETI), CNRS Labstic (Lorient).

Since 1996 and the discovery of Shor's algorithm, new quantum threats emerged against classical security protocols and cryptographic primitives. The objective of the PQ-TLS project is to design a quantum-safe version of the security layer of web protocols, via the integration of post-quantum cryptographic primitives and the quantum cryptanalysis of existing systems. The project also aims at developping new techniques to compare existing primitives from the quantum viewpoint and at promoting arising solutions from the academic and industrial research. The goal is to develop a large toolbox whose targets range from the mathematical foundations of post-quantum cryptography to its concrete implementations.

Xavier Bonnetain is the national coordinator of the work package 5 "Quantum cryptanalysis".

Pierre-Jean Spaenlehauer is the local scientific coordinator for the CARAMBA team.

9.2.2 Projet ANR KLEPTOMANIAC

Participants: Pierrick Gaudry, Cécile Pierrot, Pierre-Jean Spaenlehauer, Emmanuel Thomé, Paul Zimmermann.

- Program: ANR AAPG
- Project acronym: KLEPTOMANIAC
- Duration: 01/2022 - 12/2025
- Coordinator: Inria Nancy
- Other partners: ANSSI, LIP6

The RSA cryptosystem and the Diffie-Hellman key exchange protocol in finite fields were the first invented primitives of public-key cryptography.

It is hard to estimate the time and resources that are needed to factor an integer, and thereby how hard it is to break RSA. All regulatory bodies recommend that people either avoid RSA, or prefer large RSA key sizes for safety, above 2048 bits at least. In environments where computing power is plentiful, this recommendation is most often followed. Yet, it is a fact that we do rely on cryptography that uses smaller key sizes.

We plan to employ our expertise to provide solid hardness assessments for key sizes that are relevant today, and for which accuracy in the prediction is important. Our targets for accurate assessment are RSA-1024 and DH-1024 as well as specific discrete logarithm-related problems that arise in the blockchain context. We also intend to develop simulation software that would enable more accurate estimates.

In 2022, the work on the "double matrix" subtask was initiated, in collaboration with Charles Bouillaguet (Sorbonne University). This work is integrated in a branch of Cado-NFS.

9.2.3 ANR Decrypt

Participants: Marine Minier, Virginie Lallemand.

- Program: ANR
- Project acronym: DECRYPT
- Duration: 01/2019 - 12/2023
- Coordinator: Caramba Team, LORIA
- Other partners: LIRIS (Lyon), LIMOS (Clermont-Ferrand), IRISA (Rennes), TASC (Nantes).

This project aims to propose a declarative language dedicated to cryptanalytic problems in symmetric key cryptography using constraint programming (CP) to simplify the representation of attacks, to improve existing attacks and to build new cryptographic primitives that withstand these attacks. We also want to compare the different tools that can be used to solve these problems: SAT and MILP where the constraints are homogeneous and CP where the heterogeneous constraints can allow a more complex treatment.

One of the challenges of this project will be to define global constraints dedicated to the case of symmetric cryptography.

Concerning constraint programming, this project will define new dedicated global constraints, will improve the underlying filtering and solution search algorithms, and will propose dedicated explanations generated automatically. See the web site for more information.

9.3 Regional initiatives

9.3.1 Impact Project LUE DigiTrust

Participants: Marine Minier.

- Program: LUE
- Project acronym: DigiTrust
- Duration: 04/2019 - 12/2022
- Scientific Leader: Marine Minier

The Citizen Trust in the Digital World (acronym DigiTrust) project is part of the latest wave of IMPACT projects within the Lorraine University of Excellence (LUE) initiative proposed under the PIA2 IDEX/I call for tenders -SITE. It was launched in April 2019 and its ambition is to build citizens' trust in the digital world around four areas of research.

The digital revolution has a fundamental impact on daily life, particularly on the way citizens get information, communicate and organize themselves. This revolution also changed the manufacturing and supply of goods and energy, the design of cities, transportation infrastructure, and even administration and politics. New paradigms such as smart cities, manufacturing or the use of connected objects (IoT) rely on permanently connected communication at all scales, which further increases the dependence of modern society on digital technologies. See the web site for more information.

10 Dissemination

Participants: Haetham Al Aswad, Xavier Bonnetain, Pierrick Gaudry, Stéphane Glondu, Aurore Guillevic, Virginie Lallemand, Antoine Leudière, Marine Minier, Cécile Pierrot, Pierre-Jean Spaenlehauer, Emmanuel Thomé, Quentin Yang, Paul Zimmermann.

10.1 Promoting scientific activities

10.1.1 Scientific events: organisation

- Haetham Al Aswad and Ana Rodriguez Cordero created the Ph.D. seminar at Loria, Nancy, which is a monthly seminar held and done by Ph.D. students for PhD students.
- Pierre-Jean Spaenlehauer is a member of the organization committee of the Journées Nationales du Calcul Formel 2022 and 2023.
- Virginie Lallemand co-organized Cyber in Nancy, the summer school in Cybersecurity of the "GDR Sécurité Informatique".

10.1.2 Scientific events: selection

Member of conference program committees

- Marine Minier was program committee member of SPACE 2022, Africacrypt 2022, Indocrypt 2022, RESSI 2022 (national event, teaching track).
- Xavier Bonnetain and Virginie Lallemand are program committee members of the conference ACNS 2023.
- Aurore Guillevic was program committee member of SAC 2023.

10.1.3 Journal

Member of editorial boards

- Xavier Bonnetain is member of the editorial board of IACR Transactions on Symmetric Cryptology (ToSC) Journal and IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES) Journal for 2022. These journals are the open-access journals associated respectively to the International Conference on Fast Software Encryption (FSE) and the International Conference on Cryptographic Hardware and Embedded Systems (CHES).
- Emmanuel Thomé is a member of the editorial board of the Journal of Algebra, dealing with the section on computational algebra.

Reviewer - reviewing activities Members of the project-team did their share in reviewing submissions to renowned conferences and journals. Actual publications venues are not disclosed for anonymity reasons.

10.1.4 Invited talks

- Antoine Leudière was invited to give a talk on Drinfeld modules in cryptography at the INRIA GRACE team seminar, Saclay, France, in May.
- Antoine Leudière was invited to give a talk on the algorithmics of Drinfeld modules at the INRIA LFANT team seminar, Bordeaux, France, in June.
- Antoine Leudière was invited to give a talk on Drinfeld modules in cryptography at the *Géométrie et algèbre effectives* team seminar, Rennes, France, in September.
- Cécile Pierrot was an invited speaker at the conference Application of Computer Algebra (ACA 2022), August 2022, Istanbul, Turkey.
- Marine Minier was invited to give a talk at “Journées du GDR sécurité” 2022, Paris, France, in June.
- Marine Minier was invited to give a talk at the CISPA/LORIA seminar 2022, Saarbrücken, Germany, in November.
- Xavier Bonnetain was invited to give a talk at the CISPA/LORIA seminar 2022, Saarbrücken, Germany, in October.
- Xavier Bonnetain was invited to give a talk during the FRISIACRYPT 2022 invitation-only seminar.
- Xavier Bonnetain was invited to give a talk for the “Journée de la Sécurité Informatique en Normandie” in Rouen.
- Paul Zimmermann was invited to give a talk on the IEEE 754 standard to the French “Groupe Calcul”, in February (virtual talk).
- Paul Zimmermann was invited to give a talk on CORE-MATH to the FPBench Community Meeting, in March (virtual talk).

- Paul Zimmermann was invited to give a talk on CORE-MATH at the RAIM 2022 (13èmes Rencontres Arithmétique de l'Informatique Mathématique), in November.
- Emmanuel Thomé was invited to give a talk at the Cryptography seminar in Rennes.

10.1.5 Leadership within the scientific community

- Cécile Pierrot is a member of the steering committee of the French working group Code and Cryptography.
- Pierrick Gaudry is a member of the Conseil Scientifique of GdR IM.
- Marine Minier is co-supervisor with Antoine Joux of the virtual cybersecurity center between CISPA and LORIA (2020-2023).

10.1.6 Scientific expertise

- Pierrick Gaudry was a member of a jury for the Innoviris LAUNCH program, whose goal is to fund start-ups created on the basis of academic work.

10.1.7 Research administration

- Pierrick Gaudry is a member of the steering committee of the LHS – Laboratoire Haute Sécurité of LORIA.
- Pierrick Gaudry was a member of the hiring committee for a Professor in computer science and mathematics (26/27) at Ensimag, Grenoble.
- Marine Minier is a member of the steering committee of the LHS – Laboratoire Haute Sécurité of LORIA.
- Marine Minier was a member of the hiring committee for an assistant professor in computer science and mathematics (26/27) at University of Grenoble-Alpes.
- Marine Minier was a member of the hiring committee for a Professor in computer science (27) at University of Nancy.
- Marine Minier was president of the hiring committee for a Professor in computer science (27) at University of Nancy, Télécom.
- Marine Minier was a member of the hiring committee for an assistant professor in computer science (27) for an exchange of positions between University of Nancy and University of Nice.
- Cécile Pierrot was a member of the hiring committee for research scientists "Chargé de Recherche" at Inria Nancy, May 2022.
- Pierre-Jean Spaenlehauer is a member of the Commission des Développements Technologiques of the Inria Nancy – Grand Est research center.
- Paul Zimmermann is member of the scientific committee of the EXPLOR computing center (Université de Lorraine).
- Cécile Pierrot created and leads the working group Intégration Locale at Loria/Inria Nancy. She created the English Coffee Time too, dedicated for all the non-French speakers in the lab.
- Cécile Pierrot is a member of Bureau du Comité des Projets, Inria Nancy.
- Cécile Pierrot is a member of Comité de Centre of Inria Nancy.
- Cécile Pierrot is a member of the working group about remote working at Inria.

10.2 Teaching - Supervision - Juries

10.2.1 Teaching

Marine Minier obtains this year an half Inria Delegation.

- Bachelor
  - Sébastien Duval, *Algorithmique et Programmation 2*, 38h eq. TD, L1 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Sébastien Duval, *Algorithmique et Programmation 3*, 26h eq. TD, L2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Sébastien Duval, *Mathématiques Discrètes 2*, 16h eq. TD, L2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Sébastien Duval, *Introduction à la sécurité et à la cryptographie*, 20h eq. TD, L3 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Aurore Guillevic, *Intégration Web* (R112) and *Suivi de projet* (SAE-105), 64h eq. TD, IUT 1A, Université de Lorraine, IUT Charlemagne, Nancy, France.
  - Marine Minier, *Introduction à la sécurité et à la cryptographie*, 35h eq. TD, L3, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Emmanuel Thomé, *Introduction to Modern Cryptography*, 25h, University of California San Diego, USA.
  - Quentin Yang, *Algorithmique et Programmation 3*, 28h eq. TD, L2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
- Master
  - Sébastien Duval, *Analyse et Conception de Logiciels*, 16h eq. TD, M1 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Sébastien Duval, *Introduction à la cryptographie*, 12h eq. TD, M1 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Sébastien Duval, *Sécurité des Systèmes d'Information*, 35h eq. TD, M2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Sébastien Duval, *Sécurité des Applications Web*, 32h eq. TD, M2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Aurore Guillevic, *Elliptic Curves - Number Theory and Cryptography*, 72h eq. TD, Master Mathématiques et Master Informatique, Aarhus University, Aarhus, Danemark.
  - Pierre-Jean Spaenlehauer, *Théorie analytique des nombres, géométrie algébrique, et applications à la cryptographie*, 24h eq. TD, M2 Mathématiques Fondamentales et Appliquées, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Marine Minier, *Contrôle d'accès*, 40h eq. TD, M2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Marine Minier, *Intégration Méthodologique*, 36h eq. TD, M2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Marine Minier *Sécurité Informatique*, 18h eq. TD, M2 droit, Université de Lorraine.
  - Marine Minier is head of the M2 SIRAV, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Emmanuel Thomé, *The Number Field Sieve* (CSE 291-14, graduate course), 25h, University of California San Diego, USA.
- Engineering school

- Cécile Pierrot, *Introduction to Cryptography*, 54h eq. TD, Mastère spécialisé de cybersécurité, École des Mines de Nancy, France.
- Haetham AL ASWAD, *Programming languages*, 22h eq. TD, Second year of Engineering, École des Mines de Nancy, France.
- Antoine Leudière, *Programming and Data Structures: Python*, 22h eq. TD, First year of Engineering, École des Mines de Nancy, France.
- Antoine Leudière, *Algorithms and complexity*, 22h eq. TD, First year of Engineering, École des Mines de Nancy, France.
- Antoine Leudière, *Database essentials*, 18h eq. TD, Second year of Engineering, École des Mines de Nancy, France.
- Ana Margarita Rodríguez Cordero, *Programming and Data Structures: Python*, 22h eq. TD, First year of Engineering, École des Mines de Nancy, France.

10.2.2 Supervision

- Ph.D. in progress: Hamid Boukerrou, *Synthèse de nouveaux automates à états finis décrits par une représentation matricielle: application à la cryptographie*, since Oct. 2019, Marine Minier and Gilles Millerioux. Defence is planed for the 4th of April 2023.
- Ph.D. in progress: Haetham Al Aswad, *Number field sieve for discrete logarithm*, since Oct. 2021, Cécile Pierrot and Emmanuel Thomé.
- Ph.D. completed: Youssef El Housni, *The Arithmetic of Pairing-Based Proof Systems*, November 2019–November 2022, co-advised by François Morain and Daniel Augot (HDR, GRACE team, doctoral school ED-IPP), and Aurore Guillevic.
- Ph.D. in progress: Antoine Leudière, *Isogenies of Drinfeld modules and post-quantum cryptography*, since Oct. 2021, Pierre-Jean Spaenlehauer and Emmanuel Thomé.
- Ph.D. in progress: Ana Rodriguez Cordero, *Design and Cryptanalysis of New Symmetric Key Cryptographic Primitives*, since Oct. 2021, Virginie Lallemand and Marine Minier.
- Ph.D. in progress: Quentin Yang, *Design and analysis of e-voting protocols*, since Oct. 2020, Pierrick Gaudry and Véronique Cortier (PESTO team).

10.2.3 Juries

- Pierrick Gaudry was reviewer of the PhD thesis *Efficient protocols for testing proximity to algebraic codes* defended by Sarah Bordage, June 2022, École polytechnique.
- Aurore Guillevic was member of the PhD defense committee of Youssef El Housni, *The Arithmetic of Pairing-Based Proof Systems*, defended on November 18, 2022, at École Polytechnique, Palaiseau.
- Cécile Pierrot was a jury member during the PhD defense of Andy Russon, January 2022, Rennes.
- Marine Minier was a reviewer and the president of the jury of the PhD defense of Tanguy Gernot, November 2022, Caen.
- Marine Minier was a reviewer of the PhD defense of Paul Frixons, November 2022, Paris.
- Marine Minier was president of the jury of the PhD defense of Mohamed Traoré, May 2022, Grenoble-Alpes.
- Marine Minier was president of the jury of the PhD defense of Bizhan Alipour, March 2022, Nancy.
- Marine Minier was member of the jury of the HDR defense of Marc Pouget, June 2022, Nancy.
- Marine Minier was member of the jury of the HDR defense of Charles Bouillaguet, March 2022, Paris.

- Marine Minier was member of the jury of the PhD defense of Loïc Rouquette, November 2022, Lyon.
- Marine Minier was member of the jury of the PhD defense of Victor Mollimard, January 2022, Rennes.
- Pierre-Jean Spaenlehauer was a jury member for the PhD defense of Maxime Bros, December 2022, Limoges.
- Emmanuel Thomé was a jury member for the PhD defense of Olivier Bernard, June 2022, Rennes.

10.3 Popularization

- Cécile Pierrot, Pierrick Gaudry, Paul Zimmermann, and Camille Desenclos from Amiens, held a press conference to present their joint work on the decryption of a letter from Charles Quint. This was followed by many articles and interviews, in France and abroad (Le Monde, France 2, Ouest France, The Guardian, BBC, to name but a few).
- Pierrick Gaudry participated in *Le Livre sur La Place*, in order to present his book on e-voting, together with Véronique Cortier (PESTO team).

10.3.1 Internal or external Inria responsibilities

- Marine Minier is assistant director of the LORIA laboratory (450 persons) since September 2021.
- Marine Minier is responsible of the axis CyberSecurity for the LORIA Lab.

10.3.2 Articles and contents

- Cécile Pierrot and Marine Minier made a few-minutes video about women in science, with the help of the Loria laboratory.

10.3.3 Education

- Cécile Pierrot, Pierre-Jean Spaenlehauer and Paul Zimmermann participated in the Math-En-Jeans project. They supervised a group of teenagers from the Lycée Français Vauban du Luxembourg.
- Cécile Pierrot gave a talk for the association Science Ouverte dedicated to high school students from disadvantaged backgrounds. April 2022, Sorbonne Université, Paris.
- Aurore Guillevic participated in the 1 scientifique 1 classe chiche program and presented her work as researcher in computer science to 1st year high school teenagers at Verdun and Longwy.
- Quentin Yang participated in *La fête de la science*, where he held a workshop to present the security of electronic protocols, together with Elise Klein and Maïwenn Racouchot (PESTO team).
- Sébastien Duval participates to the organisation of *Cyber Humanum Est*, a 3-day-long exercise simulating a cyber war, for students of multiple origins (specialised bachelor, masters 1 and 2, engineering schools in computer science, and masters 1 and 2 in social sciences).

10.3.4 Interventions

- Pierre-Jean Spaenlehauer and Paul Zimmermann are involved in the animation of a MATh. en. JEANS activity at the Lycée Vauban, Luxembourg.
- In November, Paul Zimmermann initiated to cryptography two classes of “troisième” of a “collège” at Is-sur-Tille, and helped a few selected students to (re)decrypt the letter from Charles Quint.

11 Scientific production

11.1 Major publications

[1] X. Bonnetain, G. Leurent, M. Naya-Plasencia and A. Schrottenloher. 'Quantum Linearization Attacks'. In: ASIACRYPT 2021 - 27th Annual International Conference on the Theory and Application of Cryptology and Information Security. Vol. 13090. Lecture Notes in Computer Science. Singapore / Virtual, Singapore: Springer International Publishing, 1st Dec. 2021, pp. 422–452. DOI: 10.1007/978-3-030-92062-3_15. URL: https://hal.inria.fr/hal-03516730.

[2] X. Bonnetain, A. Schrottenloher and F. Sibleyras. 'Beyond quadratic speedups in quantum attacks on symmetric schemes'. In: *Lecture Notes in Computer Science*. EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques. Vol. LNCS-13277. Advances in Cryptology – EUROCRYPT 2022 Part III. Trondheim, Norway: Springer International Publishing, 25th May 2022, pp. 315–344. DOI: 10.1007/978-3-031-07082-2_12. URL: https://hal.inria.fr/hal-03926591.

[3] F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé and P. Zimmermann. 'The State of the Art in Integer Factoring and Breaking Public-Key Cryptography'. In: *IEEE Security and Privacy Magazine* 20.2 (Mar. 2022), pp. 80–86. DOI: 10.1109/MSEC.2022.3141918. URL: https://hal.science/hal-03691141.

[4] V. Cortier and P. Gaudry. *Le vote électronique - les défis du secret et de la transparence*. Odile Jacob, 25th May 2022. URL: https://hal.inria.fr/hal-03740465.

[5] G. De Micheli, P. Gaudry and C. Pierrot. 'Lattice Enumeration for Tower NFS: a 521-bit Discrete Logarithm Computation'. In: Asiacrypt 2021. Vol. 13090. ASIACRYPT. Virtual, Singapore: Springer, 2021, pp. 67–96. DOI: 10.1007/978-3-030-92062-3_3. URL: https://hal.inria.fr/hal-03242324.

[6] Y. El Housni and A. Guillevic. 'Families of SNARK-friendly 2-chains of elliptic curves'. In: *LNCS*. Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques. Vol. 13276. EUROCRYPT 2022. Trondheim / Hybrid, Norway: Springer, 30th May 2022, pp. 367–396. DOI: 10.1007/978-3-031-07085-3_13. URL: https://hal.inria.fr/hal-03371573.

[7] J. Francq, L. Besson, P. Huynh, P. Guillot, G. Millérioux and M. Minier. 'Non-triangular self-synchronizing stream ciphers'. In: *IEEE Transactions on Computers* 71.1 (Jan. 2022), pp. 134–145. DOI: 10.1109/TC.2020.3043714. URL: https://hal.science/hal-03081725.

[8] V. Lallemand, M. Minier and L. Rouquette. 'Automatic Search of Rectangle Attacks on Feistel Ciphers: Application to WARP'. In: *IACR Transactions on Symmetric Cryptology* 2022.2 (10th June 2022), pp. 113–140. DOI: 10.46586/tosc.v2022.i2.113-140. URL: https://hal.science/hal-03760280.

[9] A. Sibidanov, P. Zimmermann and S. Glondu. 'The CORE-MATH Project'. In: ARITH 2022 - 29th IEEE Symposium on Computer Arithmetic. virtual, France, 12th Sept. 2022. URL: https://hal.inria.fr/hal-03721525.

11.2 Publications of the year

International journals

[10] D. F. Aranha, Y. El Housni and A. Guillevic. 'A survey of elliptic curves for proof systems'. In: *Designs, Codes and Cryptography*. Special Issue: Mathematics of Zero-Knowledge (21st Dec. 2022), p. 46. DOI: 10.1007/s10623-022-01135-y. URL: https://hal.inria.fr/hal-03667798.

[11] S. Blanc, A. Lahmadi, K. Le Gouguec, M. Minier and L. Sleem. 'Benchmarking of lightweight cryptographic algorithms for wireless IoT networks'. In: *Wireless Networks* 28.8 (Nov. 2022), pp. 3453–3476. DOI: 10.1007/s11276-022-03046-1. URL: https://hal.inria.fr/hal-03850763.

[12] J. Francq, L. Besson, P. Huynh, P. Guillot, G. Millérioux and M. Minier. 'Non-triangular self-synchronizing stream ciphers'. In: *IEEE Transactions on Computers* 71.1 (Jan. 2022), pp. 134–145. DOI: 10.1109/TC.2020.3043714. URL: https://hal.archives-ouvertes.fr/hal-03081725.

[13] A. Joux and C. Pierrot. 'Algorithmic aspects of elliptic bases in finite field discrete logarithm algorithms'. In: *Advances in Mathematics of Communications* (2022). URL: https://hal.sorbonne-universite.fr/hal-02173688.

[14] V. Lallemand, M. Minier and L. Rouquette. 'Automatic Search of Rectangle Attacks on Feistel Ciphers: Application to WARP'. In: *IACR Transactions on Symmetric Cryptology* 2022.2 (10th June 2022), pp. 113–140. DOI: 10.46586/tosc.v2022.i2.113-140. URL: https://hal.archives-ouvertes.fr/hal-03760280.

International peer-reviewed conferences

[15] X. Bonnetain, A. Schrottenloher and F. Sibleyras. 'Beyond quadratic speedups in quantum attacks on symmetric schemes'. In: *Lecture Notes in Computer Science*. EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques. Vol. LNCS-13277. Advances in Cryptology – EUROCRYPT 2022 Part III. Trondheim, Norway: Springer International Publishing, 25th May 2022, pp. 315–344. DOI: 10.1007/978-3-031-07082-2_12. URL: https://hal.inria.fr/hal-03926591.

[16] M. Bougon, H. Chabanne, V. Cortier, A. Debant, E. Dottax, J. Dreier, P. Gaudry and M. Turuani. 'Themis: an On-Site Voting System with Systematic Cast-as-intended Verification and Partial Accountability'. In: CCS 2022 - The ACM Conference on Computer and Communications Security. Los Angeles, United States: ACM, 2022. DOI: 10.1145/3548606.3560563. URL: https://hal.inria.fr/hal-03763294.

[17] V. Cortier, P. Gaudry and S. Glondu. 'Features and usage of Belenios in 2022'. In: The International Conference for Electronic Voting (E-Vote-ID 2022). Bregenz / Hybrid, Austria, 4th Oct. 2022. URL: https://hal.inria.fr/hal-03791757.

[18] V. Cortier, P. Gaudry and Q. Yang. 'A toolbox for verifiable tally-hiding e-voting systems'. In: ESORICS 2022 - 27th European Symposium on Research in Computer Security. Copenhague, Denmark, 26th Sept. 2022. URL: https://hal.inria.fr/hal-03367930.

[19] Y. El Housni and A. Guillevic. 'Families of SNARK-friendly 2-chains of elliptic curves'. In: *LNCS*. Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques. Vol. 13276. EUROCRYPT 2022. Trondheim / Hybrid, Norway: Springer, 30th May 2022, pp. 367–396. DOI: 10.1007/978-3-031-07085-3_13. URL: https://hal.inria.fr/hal-03371573.

[20] Y. El Housni, A. Guillevic and T. Piellard. 'Co-factor clearing and subgroup membership testing on pairing-friendly curves'. In: AFRICACRYPT 2022 - 13th International Conference on Cryptology. Vol. 13503. LNCS. Fes, Morocco: Springer, 6th Oct. 2022, pp. 518–536. DOI: 10.1007/978-3-031-17433-9_22. URL: https://hal.inria.fr/hal-03608264.

[21] L. Rouquette, D. Gerault, M. Minier and C. Solnon. 'And Rijndael? Automatic Related-key Differential Analysis of Rijndael'. In: *Progress in Cryptology - AFRICACRYPT 2022, 13th International Conference on Cryptology in Africa, Fes, Morocco, July 18–20, 2022 Proceedings*. AfricaCrypt 2022 - 13th International Conference on Cryptology AfricaCrypt. Vol. LNCS-13503. LNCS. Fes, Morocco: Springer, 2022, pp. 150–175. DOI: 10.1007/978-3-031-17433-9_7. URL: https://hal.archives-ouvertes.fr/hal-03671013.

[22] A. Sibidanov, P. Zimmermann and S. Glondu. 'The CORE-MATH Project'. In: ARITH 2022 - 29th IEEE Symposium on Computer Arithmetic. virtual, France, 12th Sept. 2022. URL: https://hal.inria.fr/hal-03721525.

[23] S. Vivien. 'Parallel integer multiplication'. In: *30th Euromicro International Conference on Parallel, Distributed andNetwork-based Processing (PDP 2022)*. PDP 2022 - 30th Euromicron International Conference on Parallel, Distributed, and Network-Based Processing. Valladoid, Spain, 2022. DOI: 10.1109/PDP55904.2022.00024. URL: https://hal.archives-ouvertes.fr/hal-03541726.

Conferences without proceedings

[24] H. Boukerrou, G. Millérioux and M. Minier. 'Towards a new design of ciphers to secure CPS: the role of control theory'. In: 26th International Conference on System Theory, Control and Computing, ICSTCC 2022. Sinaia, Romania, 19th Oct. 2022. DOI: 10.1109/ICSTCC55426.2022.9931873. URL: https://hal.archives-ouvertes.fr/hal-03893003.

[25] V. Cortier, A. Debant and P. Gaudry. 'A privacy attack on the Swiss Post e-voting system'. In: RWC 2022 - Real World Crypto Symposium. Amsterdam (NETHERLANDS), Netherlands, 24th Nov. 2021. URL: https://hal.inria.fr/hal-03446801.

Reports & preprints

[26] H. Al Aswad and C. Pierrot. *Individual Discrete Logarithm with Sublattice Reduction*. 25th July 2022. URL: https://hal.science/hal-03737874.

[27] V. Cortier, P. Gaudry and Q. Yang. *Is the JCJ voting system really coercion-resistant?* 4th Apr. 2022. URL: https://hal.inria.fr/hal-03629587.

[28] V. Innocente and P. Zimmermann. *Accuracy of Mathematical Functions in Single, Double, Extended Double and Quadruple Precision*. 27th Sept. 2022. URL: https://hal.inria.fr/hal-03141101.

[29] P.-J. Spaenlehauer and A. Leudière. *Computing a Group Action from the Class Field Theory of Imaginary Hyperelliptic Function Fields*. 7th Apr. 2022. URL: https://hal.inria.fr/hal-03633990.

[30] L. Turelier. *Extension of the SLZ algorithm to bivariate functions*. INRIA Nancy, 29th July 2022. URL: https://hal.inria.fr/hal-03740209.

[31] P. Zimmermann. *Note on FastTwoSum with Directed Roundings*. 8th Oct. 2022. URL: https://hal.inria.fr/hal-03798376.

Other scientific publications

[32] F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé and P. Zimmermann. 'The State of the Art in Integer Factoring and Breaking Public-Key Cryptography'. In: *IEEE Security and Privacy Magazine* 20.2 (Mar. 2022), pp. 80–86. DOI: 10.1109/MSEC.2022.3141918. URL: https://hal.archives-ouvertes.fr/hal-03691141.

11.3 Other

Scientific popularization

[33] V. Cortier and P. Gaudry. *Le vote électronique - les défis du secret et de la transparence*. Odile Jacob, 25th May 2022. URL: https://hal.inria.fr/hal-03740465.

Softwares

[34] [SW] G. Hanrot, P. Zimmermann, V. Lefèvre, P. Pélissier and P. Théveny, *GNU MPFR* version 4.2.0, 6th Jan. 2023. LIC: GNU General Public License. HAL: ⟨hal-03940504⟩, URL: https://hal.inria.fr/hal-03940504, VCS: https://gitlab.inria.fr/mpfr/mpfr, SWHID: ⟨swh:1:rel:b5e308c5dd459a81d8523e1dcb84c19dbc47b51b;origin=https://gitlab.inria.fr/mpfr/mpfr;visit=swh:1:snp:15595615280f9f91d107c1f4e9fa915fda0076dc⟩.

11.4 Cited publications

[35] 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. Vienna, Austria: https://cans2020.at/, 14th Dec. 2020. URL: https://hal.inria.fr/hal-02962800.

[36] D. Adrian, K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, J. Alex Halderman, N. Heninger, D. Springall, E. Thomé, L. Valenta, B. VanderSloot, E. Wustrow, S. Zanella-Béguelin and P. Zimmermann. 'Imperfect Forward Secrecy: How Diffie-Hellman fails in practice'. In: *CCS '15: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. Denver, Colorado, United States: ACM, Oct. 2015, pp. 5–17. DOI: 10.1145/2810103.2813707. URL: https://hal.inria.fr/hal-01184171.

[37] Agence nationale de la sécurité des systèmes d'information. *Référentiel général de sécurité, annexe B1*. Version 2.04. 2021. URL: https://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-mecanismes_crypto-2.04.pdf.

[38] S. Delaune, P. Derbez and M. Vavrille. 'Catching the Fastest Boomerangs Application to SKINNY'. In: *IACR Trans. Symmetric Cryptol.* 2020.4 (2020), pp. 104–129. DOI: 10.46586/tosc.v2020.i4.104-129. URL: https://doi.org/10.46586/tosc.v2020.i4.104-129.

[39] T. Kleinjung, K. Aoki, J. Franke, A. K. Lenstra, E. Thomé, J. Bos, P. Gaudry, A. Kruppa, P. L. Montgomery, D. A. Osvik, H. te Riele, A. Timofeev and P. Zimmermann. 'Factorization of a 768-bit RSA modulus'. In: *CRYPTO 2010*. Ed. by T. Rabin. Vol. 6223. Lecture Notes in Comput. Sci. Proceedings. Springer–Verlag, 2010, pp. 333–350.

[40] National Institute of Standards and Technology. *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*. First revision. 2011. DOI: 10.6028/NIST.SP.800-131A.

[41] L. Qin, X. Dong, X. Wang, K. Jia and Y. Liu. 'Automated Search Oriented to Key Recovery on Ciphers with Linear Key Schedule Applications to Boomerangs in SKINNY and ForkSkinny'. In: *IACR Trans. Symmetric Cryptol.* 2021.2 (2021), pp. 249–291. DOI: 10.46586/tosc.v2021.i2.249-291. URL: https://doi.org/10.46586/tosc.v2021.i2.249-291.

[42] The CADO-NFS Development Team. *CADO-NFS, An Implementation of the Number Field Sieve Algorithm*. Release 2.3.0. 2017. URL: https://hal.inria.fr/hal-02099620.