14 th International Conference on Cryptology
19 to 21 July 2023

Program

AfricaCrypt 2023

WEDNESDAY 19 JULY 2023

08:00 – 09:00: Registration
Conference venue
09:00 – 09:30: Opening Ceremony
09:30 – 10:30: Keynote speaker: Koray Karabina
Fuzzy Extractors: Applications and Challenges

Fuzzy extractors are among the primary methods that enable the use of noisy secrets in cryptographic applications, such as biometric authentication, record linkage, and physically unclonable function-based key generation. In a nutshell, a fuzzy scheme can extract a cryptographic key from its input in such a way that the key can be regenerated even if some noise is introduced to the original input. In this presentation, we will explore various schemes that can effectively tolerate noise across different metrics, including Hamming distance, set difference, and L1-distance. We will also discuss the security of these schemes and the underlying computational problems from coding theory, number theory and lattices. Finally, we will delve into some challenges involved in implementing these schemes in real-life applications.

10:30 – 11:00: Coffee Break

SESSION 1: IMPLEMENTATION

11:00 – 11:25: Title: Fast Falcon Signature Generation and Verification Using ARMv8 NEON Instructions.
Authors: Duc Tri Nguyen and Kris Gaj

Abstract: We present our speed records for Falcon signature generation and verification on ARMv8- architecture. Our implementations are benchmarked on Apple M1 'Firestorm', Raspberry Pi 4 Cortex-A72, and Jetson AGX Xavier.
Our optimized signature generation is 2×slower, but signature verification is 3–3.9× faster than the state-of-the art CRYSTALS-Dilithium implementation on the same platforms. Faster signature verification may be particularly useful for the client side on constrained devices. Our Falcon implementation outperforms the previous work targeting Jetson AGX Xavier by the factors 1.48× for signing in falcon512 and falcon1024, 1.52× for verifying in falcon512, and 1.70× for verifying in falcon1024.We achieve improvement in Falcon signature generation by supporting a larger subset of possible parameter values for FFT-related functions and applying our compressed twiddle-factor table to reduce memory usage.We also demonstrate that the recently proposed signature scheme Hawk, sharing optimized functionality with Falcon, has 3.3× faster signature generation and 1.6–1.9× slower signature verification when implemented on the same ARMv8 processors as Falcon.

11:25 – 11:50: Title: Benchmarking and Analysing the NIST PQC Lattice-Based Signature Schemes Standards on the ARM Cortex M7
Authors: James Howe and Bas Westerbaan

Abstract: This paper presents an analysis of the two lattice-based digital signature schemes, Dilithium and Falcon, which have been chosen by NIST for standardisation, on the ARM Cortex M7 using the STM32F767ZI NUCLEO-144 development board. This research is motivated by the ARM Cortex M7 device being the only processor in the Cortex-M family to offer a double precision (i.e., 64-bit) floating-point unit, making Falcon's implementations, requiring 53 bits of double precision able to fully run native floating-point operations without any emulation. When benchmarking natively, Falcon shows significant speed-ups between 6.2–8.3x in clock cycles, 6.2-11.8x in runtime, and Dilithium does not show much improvement other than those gained by the slightly faster processor. We then present profiling results of the two schemes on the ARM Cortex M7 to show their respective bottlenecks and operations where the improvements are and can be made. This demonstrates, for example, that some operations in Falcon's procedures observe speed-ups by an order of magnitude. Finally, since Falcon's use of floating points is so rare in cryptography, we test the native FPU instructions on 4 different STM32 development boards with the ARM Cortex M7 and also a Raspberry Pi 3 which is used in some of Falcon's official benchmarking results. We find constant-time irregularities in all of these devices, which makes Falcon insecure on these devices for applications where signature generation can be timed by an attacker.

12:00 – 14:00: Lunch break

Session 2: Blockchain

14:00 – 14:25: Title: The curious case of the half-half Bitcoin ECDSA nonces.
Authors: Dylan Rowe, Joachim Breitner and Nadia Heninger

Abstract: We report on a new class of ECDSA signature vulnerability observed in the wild on the Bitcoin blockchain that results from a signature nonce generated by concatenating half of the bits of the message hash together with half of the bits of the secret signing key. We give a lattice-based attack for efficiently recovering the secret key from a single signature of this form. We then search the entire Bitcoin blockchain for such signatures, and identify and track the activities of an apparently custom ECDSA/Bitcoin implementation that has been used to empty hundreds of compromised Bitcoin addresses for many years.

14:25 – 14:50: Title: Maravedí: A Secure and Practical Protocol to Trade Risk for Instantaneous Finality.
Authors: Mario Larangeira and Maxim Jourenko

Abstract: The efficiency of blockchain systems is often compared to popular credit card networks with respect to the transactions per second rate. This seems to be an unfair comparison since these networks do not complete a transaction from beginning to end. Rather they buy the risk and settle it much later. Typically transactions have only two players, the payer and the payee, and the settlement of this transaction requires time since it depends on basic properties of the consensus protocol. In practice, the payee, very often, needs to wait for confirmation in order to ship the traded goods. Alternatively, the payee, or merchant, can ship it in faith that the transaction will be confirmed. Our contribution, the Maravedí Protocol, introduces a third player to minimize the risk of the payee to be left without the payment even without the consensus layer confirmation. The main idea is that the third player can work similarly to a credit card company. That is, it buys the risk from the merchant, by a small discount, and allows the third player to pay it instantaneously via a payment-channel like protocol. In parallel, the third player receives the regular payment transaction from the payer that can be settled on the chain, thus, after waiting the consensus/blockchain required time. Moreover, the on-chain transaction pays the full amount, allowing the third player to cash in the discount. Hence, on the side of the merchant, our protocol puts forth instantaneous finality in a novel way to the best of our knowledge.

14:50 – 15:20: Poster Presentations

15:20 – 15:50: Coffee Break

Session 3: Symmetrie Cryptography

15:50 – 16:15: Title: Poseidon2: A Faster Version of the Poseidon Hash Function.
Authors: Lorenzo Grassi, Dmitry Khovratovich and Markus Schofnegger

Abstract: Zero-knowledge proof systems for computational integrity have seen a rise in popularity in the last couple of years. One of the results of this development is the ongoing effort in designing so-called arithmetization-friendly hash functions in order to make these proofs more efficient. One of these new hash functions, Poseidon, is extensively used in this context, also thanks to being one of the first constructions tailored towards this use case. Many of the design principles of Poseidon have proven to be efficient and were later used in other primitives, yet parts of the construction have shown to be expensive in real-word scenarios.

In this paper, we propose an optimized version of Poseidon, called Poseidon2. The two versions differ in two crucial points. First, Poseidon is a sponge hash function, while Poseidon2 can be either a sponge or a compression function depending on the use case. Secondly, Poseidon2 is instantiated by new and more efficient linear layers with respect to Poseidon.

These changes allow to decrease the number of multiplications in the linear layer by up to 90% and the number of constraints in Plonk circuits by up to 70%. This makes Poseidon2 the currently fastest arithmetization-oriented hash function without lookups. Besides that, we address a recently proposed algebraic attack and propose a simple modification that makes both Poseidon and Poseidon2 secure against this approach.

16:15 – 16:40: Title: Universal hashing based on field multiplication and (near-) MDS matrices.
Authors: Koustabh Ghosh,Joan Daemen, Parisa Eliasi and Jonathan Fuchs

Abstract: In this paper we propose a new construction for building universal hash functions, a specific instance called multi-265, and provide proofs for their universality. Our construction follows the key-then-hash parallel paradigm. In a first step it adds a variable length input message to a secret key and splits the result in blocks. Then it applies a fixed-length public function to each block and adds their results to form the output. The innovation presented in this work lies in the public function: we introduce the multiply-transform-multiply-construction that makes use of field multiplication and linear transformations. We prove upper bounds for the universality of key-then-hash parallel hash functions making use of a public function with our construction provided the linear transformation are maximum-distance-separable (MDS). We additionally propose a concrete instantiation of our construction multi-265, where the underlying public function uses a near-MDS linear transformation and prove it to be 2^{-154}-universal. We also make the reference code for multi-265 available.

16:40 – 17:05: Title: Invertible Quadratic Non-Linear Functions over $\mathbb{F}_p^n$ via Multiple Local Maps.

Authors: Ginevra Giordani, Lorenzo Grassi, Silvia Onofri and Marco Pedicini

Abstract: The construction of invertible non-linear layers over $\mathbb{F}_p^n$ that minimize the multiplicative cost is crucial for the design of symmetric primitives targeting Multi Party Computation (MPC), Zero-Knowledge(ZK), and Fully Homomorphic Encryption (FHE). At the current state of the art, only few non-linear functions are known to be invertible over $\mathbb{F}_p$ as the power maps $x \mapsto x^d$ for gcd(d; p-1) = 1. When working over $\mathbb{F}_p^n$ for $n \geq 2$ a possible way to construct invertible non-linear layers S over $\mathbb{F}_p^n$ is by making use of a local map $F : \mathbb{F}_p^m \rightarrow \mathbb{F}_p$ for $m \leq n$ that is, $S_F(x_0, x_1, \ldots, x_{n-}) = y \| y_1 \| \ldots \| y_{n-1}$ where $y_i = F(x_i, x_{i+1}, \ldots, x_{i\ m-1})$. This possibility has been recently studied by Grassi, Onofri, Pedicini and Sozzi at FSE/ToSC 2022. Given a quadratic local map $F : \mathbb{F}_p^m \rightarrow \mathbb{F}_p$ for $m \in \{1\ 2\ 3\}$, they proved that the shift-invariant non-linear function S_F over $\mathbb{F}_p^n$ defined as before is never invertible for any $n \geq 2.m - 1$.

In this paper, we face the problem by generalizing such construction. Instead of a single local map, we admit multiple local maps, and we study the creation of nonlinear layers that can be efficiently verified and implemented by a similar shift-invariant lifting. After formally defining the construction, we focus our analysis on the case $S_{F_0, F_1}(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1}$ for $F_0, F_1 : \mathbb{F}_p^2 \rightarrow \mathbb{F}_p$ of degree at most 2. This is a generalization of the previous construction using two alternating functions $F_0\ F_1$ instead of a single F. As main result, we prove that (i) if $n \geq 3$, then S_{F_0,F_1} , is never invertible if both F_0 and F_1 are quadratic, and that (ii) if $n \geq 4$, then S_{F_0,F_1} invertible if and only if it is a Type-II Feistel scheme.

17:05 – 17:30: Title: From Unbalanced to Perfect: Implementation of Low Energy Stream Ciphers.

Authors: Jikang Lin, Jiahui He, Yanhong Fan and Meiqin Wang

Abstract: Low energy is an important aspect of hardware implementation. For energy-limited battery-powered devices, low energy stream ciphers can play an important role. In IACR ToSC 2021, Caforio et al proposed the Perfect Tree energy model for stream cipher that links the structure of combinational logic circuits with state update functions to energy consumption. In addition, a metric given by the model shows a negative correlation with energy consumption, i.e., the higher the balance of the perfect tree, the lower the energy consumption. However, Caforio et al. didn't give a method that eliminate imbalances of the unrolled strand tree for the existing stream ciphers. In this paper, based on the Perfect Tree energy model, we propose a new redundant design model that improve the balances of the unrolled strand tree for the purpose of reducing energy consumption. In order to obtain the redundant design, we propose a search algorithm for returning the corresponding implementation scheme. For the existing stream ciphers, the proposed model and search method can be used to provide a lowpower redundancy design scheme. To verify the effectiveness, we apply our redundant model and search method in the stream ciphers (e.g.,Trivium and Kreyvium) and conducted a synthetic test. The results of the energy measurement demonstrate that the proposed model and search method can obtain lower energy consumption.

THURSDAY 20 JULY 2023

08:00 – 09:00: Registration

09:00 – 10:00: Keynote speaker: Anne Canteaut

The Unbearable Lightness of Symmetric Primitives

Lightweight symmetric cryptography emerged thirty years ago with the proliferation of applications with very limited resources, such as energy-harvesting devices, like RFID tags. These platforms actually imposed severe constraints on the algorithms that they can embed, and standardized cryptographic algorithms appeared to be too expensive in such contexts. This situation led the industry to design proprietary ciphers for wireless access control or public transport ticketing systems, which met the implementation requirements, typically a very small hardware footprint and very low power consumption. Some examples include KeeLoq used for car keyless entry systems or Crypto-1 integrated in the MIFARE Classic RFID contactless smart cards. However, designing a symmetric cipher, even a lightweight variant of an existing cipher, is not a trivial task: all these early attempts were severely broken, which was a major concern for such widely deployed devices.

It then became clear that lightweight cryptography needed to take advantage of the expertise of the cryptography community, especially of the comprehension of symmetric algorithm design that was gained during several public competitions.

A new research direction then emerged, related to lightweight primitives, resulting in several new design principles and in many algorithms. The multiplication of proposals and the need for reliable primitives which received an in-depth security evaluation led to the inclusion of a lightweight category in several design competitions such as eSTREAM (2004-08) for stream ciphers and CAESAR (2014-19) for authenticated encryption. More recently, a dedicated standardization effort launched by NIST in 2019 led to the selection of Ascon as a future standard.

Session 4: Protocols

10:00 – 10:25: Title: Applications of Timed-release Encryption with Implicit Authentication.

Authors: Angelique Faye Loe, Liam Medley, Christian O'Connell and Elizabeth Quaglia

Abstract: A whistleblower is a person who leaks sensitive information on a prominent individual or organization engaging in an unlawful or immoral activity. Whistleblowing has the potential to mitigate corruption and fraud by identifying the misuse of capital. In extreme cases whistleblowing can also raise awareness about unethical practices to individuals by highlighting dangerous working conditions. Obtaining and sharing the sensitive information associated with whistleblowing can carry great risk to the individual or party revealing the data. In this paper we extend the notion of timed-release encryption to include a new security property which we term implicit authentication, with the goal of making the practice of whistleblowing safer.

We formally define the new primitive of timed-release encryption with implicit authentication (TRE-IA), providing rigorous game-base definitions. We then build a practical TRE-IA construction that satisfies the security requirements of this primitive, using repeated squaring in an RSA group, and the RSA-OAEP encryption scheme. We formally prove our construction secure and provide a performance analysis of our implementation in Python along with recommendations for practical deployment and integration with an existing whistleblowing tool SecureDrop.

10:25 – 10:50: Title: Impossibilities in Succinct Arguments:Black-box Extraction and More.

Authors: Matteo Campanelli, Chaya Ganesh, Hamidreza Khoshakhlagh and Janno Siim

Abstract: The celebrated result by Gentry and Wichs established a theoretical barrier for succinct non-interactive arguments (SNARGs), showing that for (expressive enough) hard-on-average languages, we must assume non-falsifiable assumptions. We further investigate those barriers by showing new negative and positive results related to the proof size.

1. We start by formalizing a folklore lower bound for the proof size of black-box extractable arguments based on the hardness of the language. This separates knowledge-sound SNARGs (SNARKs) in the random oracle model (that can have black-box extraction) and those in the standard model.
2. We find a positive result in the non-adaptive setting. Under the existence of non-adaptively sound SNARGs (without extractability) and from standard assumptions, it is possible to build SNARKs with blackbox extractability for a non-trivial subset of NP.
3. On the other hand, we show that (under some mild assumptions) all NP languages cannot have SNARKs with black-box extractability even in the non-adaptive setting.
4. The Gentry-Wichs result does not account for the preprocessing model, under which fall several efficient constructions. We show that also, in the preprocessing model, it is impossible to construct SNARGs that rely on falsifiable assumptions in a black-box way.

Along the way, we identify a class of non-trivial languages, which we dub “trapdoor languages”, that can bypass these impossibility results.

10:50 – 11:20: Coffee Break

11:20 – 11:35: CTF Prizes

Session 5: Quantum and Post-Quantum Cryptography

11:35 – 12:00: Title: The special case of cyclotomic fields in quantum algorithms for unit groups**.**

Authors: Razvan Barbulescu and Adrien Poulalion

Abstract: Unit group computations are a cryptographic primitive for which one has a fast quantum algorithm, but the required number of qubits is $\tilde{O}(m^5)$. In this work we propose a modification of the algorithm for which the number of qubit is $\tilde{O}(m^2)$ in the case of cyclotomic fields. Moreover, under a recent conjecture on the size of the class group of $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ the quantum algorithm is much simpler because it is a hidden subgroup problem (HSP) algorithm rather than its error estimation counterpart: continuous hidden subgroup problem (CHSP). We also discuss the (minor) speed-up obtained when exploiting Galois automorphisms thanks to the Buchmann-Pohst algorithm over $\mathcal{O}_K$-lattices.

12:00 – 12:25: Title: MinRank in the Head: Short Signatures from Zero - Knowledge Proofs**.**

Authors: Gora Adj, Luis Rivera-Zamarripa and Javier Verbel

Abstract: In recent years, many digital signature scheme proposals have been built from the so-called MPC-in-the-head paradigm. This has shown to be an outstanding way to design efficient signatures with security based on hard problems. MinRank is an NP-complete problem extensively studied due to its applications to cryptanalysis since its introduction in 1999. However, only a few schemes base their security on its intractability, and their signature size is large compared with other proposals based on NP problems. This paper introduces the first MinRank-based digital signature scheme that uses the MPC-in-the-head paradigm, allowing to achieve small signature sizes and running times. For NIST's category I parameter set, we obtain signatures of 6.5KB, which is competitive with the shortest proposals in the literature that are based on non-structured problems.

12:25 – 13:00: Title: Take your MEDS: Digital Signatures from Matrix Code Equivalence.

Authors: Tung Chou, Ruben Niederhagen, Edoardo Persichetti, Tovohery Hajatiana Randrianarisoa, Krijn Reijnders, Simona Samardjiska and Monika Trimoska

Abstract: In this paper, we show how to use the Matrix Code Equivalence (MCE) problem as a new basis to construct signature schemes.

This extends previous work on using isomorphism problems for signature schemes, a trend that has recently emerged in post-quantum cryptography. Our new formulation leverages a more general problem and allows for smaller data sizes, achieving competitive performance and great flexibility. Using MCE, we construct a zero-knowledge protocol which we turn into a signature scheme named Matrix Equivalence Digital Signature (MEDS). We provide an initial choice of parameters for MEDS, tailored to NIST's Category 1 security level, yielding public keys as small as 2.8 kB and signatures ranging from 18 kB to just around 6.5 kB, along with a reference implementation in C.

13:00 – 14:30: Lunch Break

15:00 – 19:30: Excursion

20:00 : Gala Dinner

FRIDAY 21 JULY 2023

08:00 – 09:00: Registration

09:00 – 10:00: Keynote speaker: Ward Beullens
Making Sense of the Additional Signature Submissions to the NIST PQC Standardization Process

The National Institute of Standards and Technology (NIST) is running a public process to select quantum-resistant public-key cryptographic algorithms for standardization. After three rounds of analysis, NIST selected Kyber, Dilithium, Falcon, and SPHINCS+ for standardization, but the process is far from over. There is a fourth round for Key Encapsulation Mechanisms, and NIST called for additional digital signature proposals to be considered in the PQC standardization process. In this invited talk, Ward Beullens will present an overview of the new batch of digital signature submissions to the NIST competition and the underlying mathematics. Ward will compare how the different (families of) submissions perform according to the evaluation criteria set out by NIST, such as security, efficiency, key sizes, and signature sizes, and attempt to highlight some of the key advancements and trends observed in the submitted proposals.

Session 6: Lattice-based cryptography

10:00 – 10:25: Title: Finding and Evaluating Parameters for BGV
Authors: Johannes Mono, Chiara Marcolla, Georg Land, Tim Güneysu and Najwa Aaraj

Abstract: Fully Homomorphic Encryption (FHE) is a groundbreaking technology that allows for arbitrary computations to be performed on encrypted data. State-of-the-art schemes such as Brakerski Gentry Vaikuntanathan (BGV) are based on the Learning with Errors over rings (RLWE) assumption where each ciphertext has an associated error that grows with each homomorphic operation. For correctness, the error needs to stay below a certain threshold, requiring a trade-off between security and error margin for computations in the parameters. Choosing the parameters accordingly, for example, the polynomial degree or the ciphertext modulus, is challenging and requires expert knowledge specific to each scheme. In this work, we improve the parameter generation across all steps of its process. We provide a comprehensive analysis for BGV in the Double Chinese Remainder Theorem (DCRT) representation providing more accurate and better bounds than previous work on the DCRT, and empirically derive a closed formula linking the security level, the polynomial degree, and the ciphertext modulus. Additionally, we introduce new circuit models and combine our theoretical work in an easy-to-use parameter generator for researchers and practitioners interested in using BGV for secure computation.
Our formula results in better security estimates than previous closed formulas while our DCRT analysis results in reduced prime sizes of up to 42% compared to previous work.

10:25 – 10:50: Title: ComBo: a Novel Functional Bootstrapping Method for Efficient Evaluation of Nonlinear Functions in the Encrypted Domain
Authors: Pierre-Emmanuel Clet, Aymen Boudguiga, Renaud Sirdey, and Martin Zuber

Abstract: The application of Fully Homomorphic Encryption (FHE) to privacy issues arising in inference or training of neural networks has been actively researched over the last few years. Yet, although practical performances have been demonstrated on certain classes of neural networks, the inherent high computational cost of FHE operators has prevented the scaling capabilities of FHE-based encrypted domain inference to the large and deep networks used to deliver advanced classification functions such as image interpretation tasks. To achieve this goal, a new hope is coming from TFHE functional bootstrapping which, rather than being just used for refreshing ciphertexts (i.e., reducing their noise level), can be used to evaluate operators which are difficult to express as low complexity arithmetic circuits, at no additional cost. In this work, we first propose ComBo (Composition of Bootstrappings) a new full domain functional bootstrapping method with TFHE for evaluating any function of domain and codomain the real torus T by using a small number of bootstrappings. This result improves on previous approaches: like them, we allow for evaluating any functions, but with error rates reduced by a factor of up to 280. This claim is supported by a theoretical analysis of the error rate of other functional bootstrapping methods from the literature. The paper is concluded by extensive experimental results demonstrating that our method achieves better performances in terms of both time and precision, in particular for the Rectified Linear Unit (ReLU) function, a nonlinear activation function commonly used in neural networks. As such, this work provides a fundamental building-block towards scaling the homomorphic evaluation of neural networks over encrypted data.

10:50 – 11:20: Coffee Break + Poster Presentations

Session 6 Bis: Lattice-based cryptography

11:20 – 11:45: Title: Concrete Security from Worst-Case to Average-Case Lattice Reductions

Author: Joel Gärtner

Abstract: A famous reduction by Regev shows that random instances of the Learning With Errors (LWE) problem are asymptotically at least as hard as a worst-case lattice problem. As such, by assuming that standard lattice problems are hard to solve, the asymptotic security of cryptosystems based on the LWE problem is guaranteed. However, it has not been clear to which extent, if any, this reduction provides support for the security of present concrete parametrizations. In this work we therefore use Regev's reduction to parametrize a cryptosystem, providing a reference as to what parameters are required to actually claim security from this reduction. This requires us to account for the concrete performance of this reduction, allowing the first parametrization of a cryptosystem that is provably secure based only on a conservative hardness estimate for a standard lattice problem. Even though we attempt to optimize the reduction, our system still requires significantly larger parameters than typical LWE-based cryptosystems, highlighting the significant gap between parameters that are used in practice and those for which worst-case reductions actually are applicable.

11:45 – 12:10: Title: Quantum Search-to-Decision Reduction for the LWE Problem

Authors: Kyohei Sudo, Masayuki Tezuka, Keisuke Hara and Yusuke Yoshida

Abstract: The learning with errors (LWE) problem is one of the fundamental problems in cryptography and it has many applications in post-quantum cryptography. There are two variants of the problem, the decisional-LWE problem, and the search-LWE problem. LWE search-todecision reduction shows that the hardness of the search-LWE problem can be reduced to the hardness of the decisional-LWE problem. The efficiency of the reduction can be regarded as the gap in difficulty between the problems.
We initiate a study of quantum search-to-decision reduction for the LWE problem and propose a reduction that satisfies sample-preserving. In sample-preserving reduction, it preserves all parameters even the number of instances. Especially, our quantum reduction invokes the distinguisher only 2 times to solve the search-LWE problem, while classical reductions require a polynomial number of invocations. Furthermore, we give a way to amplify the success probability of the reduction algorithm. Our amplified reduction works with fewer LWE samples compared to the classical reduction that has a high success probability. Our reduction algorithm supports a wide class of error distributions and also provides a searchto- decision reduction for the learning parity with noise problem.
In the process of constructing the search-to-decision reduction, we give a quantum Goldreich-Levin theorem over $\mathbb{Z}_q$where q is prime. In short, this theorem states that, if a hardcore predicate $a.s$ (mod q) can be predicted with probability distinctly greater than $1/q$ with respect to a uniformly random $a \in \mathbb{Z}_q^n$, then it is possible to determine $s \in \mathbb{Z}^n$.

12:10 – 14:00: Lunch Break

Session 7: Cryptanalysis

14:00 – 14:25: Title: On the Post-Quantum Security of Classical Authenticated Encryption Schemes.
Authors: Nathalie Lang and Stefan Lucks

Abstract: We study the post-quantum security of authenticated encryption (AE) schemes, designed with classical security in mind. Under superposition attacks, many CBC-MAC variants have been broken, and AE modes employing those variants, such as EAX and GCM, thus fail at authenticity. As we show, the same modes are IND-qCPA insecure, i.e., they fail to provide privacy under superposition attacks.
However, a constrained version of GCM is IND-qCPA secure, and a nonce-based variant of the CBC-MAC is secure under superposition queries. Further, the combination of classical authenticity and classical chosen-plaintext privacy thwarts attacks with superposition chosen-ciphertext and classical chosen-plaintext queries – a security notion that we refer to as IND-qdCCA. And nonce-based key derivation allows generically turning an IND-qdCCA secure scheme into an IND-qCCA secure scheme.

14:25 – 14:50: Title: Efficient computation of $(3^n, 3^n)$-isogenies.
Authors: Thomas Decru and Sabrina Kunzweiler

Abstract: The parametrization of (3 , 3)-isogenies by Bruin, Flynn and Testa requires over 37 . 500 multiplications if one wants to evaluate a single isogeny in a point. We simplify their formulae and reduce the amount of required multiplications by 94%. Further we deduce explicit formulae for evaluating (3 , 3)-splitting and gluing maps in the framework of the parametrization by Br¨oker, Howe, Lauter and Stevenhagen. We provide implementations to compute $(3^n, 3^n)$-isogenies between principally polarized abelian surfaces with a focus on cryptographic application. Our implementation can retrieve Alice's secret isogeny in 11 seconds for the SIKEp751 parameters, which were aimed at NIST level 5 security

15:00 – 15:45: Coffee Break + Poster Presentations

Session 7 Bis: Cryptanalysis

15:45 – 16:10: Title: A Side-Channel Attack against Classic McEliece when loading the Goppa Polynomial

Authors: Boly Seck, Pierre-Louis Cayrel, Vlad-Florin Dragoi, Idy Diop, Morgan Barbier, Jean Belo Klamti, Vincent Grosso and Brice Colombier

Abstract: :The NIST Post-Quantum Cryptography (PQC) standardization challenge was launched in December 2016 and recently, has released its first results. The whole process has given a considerable dynamic to the research in post-quantum cryptography, in particular to practical aspects, such as the study of the vulnerabilities of post-quantum algorithms to side-channel attacks. In this paper, we present a realistic template attack against the reference implementation of Classic McEliece which is a finalist of the 4th round of NIST PQC standardization. This profiled attack allowed us to accurately find the Hamming weight of each coefficient of the Goppa polynomial. With only one decryption, this result enables us first, to find directly the Goppa polynomial in the case of weak keys with the method of Loidreau and Sendrier (P. Loidreau and N. Sendrier, ”Weak keys in the McEliece public-key cryptosystem”, IEEE Trans. Inf. Theory, 2001). Then, in the case of “slightly less weak keys”, we also find this polynomial with an exhaustive search with low complexity. Finally, we propose the best complexity reduction for exhaustive Goppa polynomial search on F2m. We attack the constant-time implementation of Classic McEliece proposed by Chen et al.. This implementation, which follows the NIST specification, is realized on a stm32f4-Discovery microcontroller with a 32-bit ARM Cortex-M4.

16:10 – 16:35: Title: Improved Cryptanalysis of the Multi-Power RSA Cryptosystem Variant

Authors: Abderrahmane Nitaj and Maher Boudabra

Abstract: The multi-power RSA cryptosystem is a variant of RSA where the modulus is in the form $N = p^r q^s$ with $max(r, s) \geq 2$. In the multi-power RSA variant, the decryption phase is much faster than the standard RSA. While RSA has been intensively studied, the security of the multi-power RSA variant needs to be deeply investigated.
In this paper, we consider a multi-power RSA cryptosystem with a modulus $N = p^r q^s$ and propose a method to solve the modular polynomial equations of the form $F(x) \equiv 0$ (mod$W$ $p^u q^v$) where $F(x)$ is a polynomial with integer coefficients, W is a positive integer, and u,v are integers satisfying $0 \leq u \leq r, 0 \leq v \leq s$, and $su - rv \neq 0$.
Our method is based on Coppersmith's method and lattice reduction techniques.
We show that the new results retrieve or supersede the former results.
Moreover, we apply the new method to study various instances of the multi-power RSA cryptosystem, especially when the private exponent is small, when the prime factors have a specific form, and when the least significant or the most significant bits of the private exponent are known.

16:35 – 17:00: Concluding Remarks

Poster Sessions

Title: Multidimensional scalar multiplication.
Author: Walid Haddaji (MDN)

Abstract: Multidimensional scalar multiplication (d - mul) consists in the computation of [a1]P1+.....+ [a2]Pd where d is an integer and P1, P2,...,Pd are points of an elliptic curve. This operation, i.e., d-mul is increasingly used in cryptography in particular in elliptic curve-based cryptographic algorithms. For example, it is used in the verification algorithm of the digital signature (ECDSA), in proving and verification algorithms such as the Succinct Non-interactive ARgument of Knowledge (SNARK) protocol, and in isogenies-based post-quantum cryptosystems. There are several methods in the literature that allows as to compute efficiently the d-mul,(e.g., the bucket method, the method of Karabina et al.,...)
This poster aims to present the most recent and efficient methods for computing the d-mul with a comparison between them (complexity, memory consumption). I will also present my work in progress in the optimization of the d-mul.

Title: SQISign: A View from the Embedded World.

Author: Komal Kumari (Technical University of Munich, Germany, TUM School of Computation, Information and Technology) and Patrick Karl (Technical University of Munich, Germany, TUM School of Computation, Information and Technology).

Abstract: SQISign (Short Quaternion and Isogeny Signature) is an isogeny-based post-quantum signature scheme that shows promising resistance against quantum attacks.
Recent advancements by Luca De Feo, Antonin Leroux, and Benjamin Wesolowski have resulted in significant improvements to the cryptosystem, reducing the combined size of the signature and public key to a fraction of signature schemes in the NIST standardization process.
Due to the attractive sizes, it holds great importance for both research and practical applications, particularly for resource constrained embedded devices. However, current implementations make use of large arithmetic libraries that exceed the memory requirements of embedded devices. This master thesis aims to develop an efficient implementation of SQISign on resource constrained devices. The focus will be on carefully selecting and implementing key components, taking into account the latest optimizations proposed by De Feo, Leroux, Wesolowski and Longa. To achieve that goal, a first step is the assessment of memory requirements of the implementation for target devices such as Electronic Control Units (ECUs).

The primary hurdle lies in integrating the Pari/GP and GMP libraries, essential for efficient arithmetic operations and instrumental in enhancing the speed of SQISign. However, the resource-intensive nature of these libraries presents a formidable challenge when attempting to incorporate them into a device with limited resources. It is worth noting that the Pari/GP and GMP library alone can consume up to 800 MB of memory, further complicating the integration process.
The work therefore aims to contribute to the understanding and practical implementation of the SQISign cryptosystem. The findings will shed light on the feasibility of deploying this cryptographic scheme on resource-limited embedded devices, thus paving the way for secure and efficient post-quantum cryptographic solutions in real-world applications.

Title: Efficient and Secure Authentication for Resource-Constrained IoT Devices using Non-Interactive Zero-Knowledge Protocols.

Author: Firas Hamila (Technical University of Munich), Mohammad Hamad (Technical University of Munich), Daniel Costa Salgado (Exxeta AG) and Sebastian Steinhorst (Technical University of Munich).

Abstract: With the rapid expansion of IoT devices and their applications, there is an increasing demand for efficient and secure authentication mechanisms to protect against unauthorized access. Traditional authentication mechanisms face limitations regarding computational speed, communication costs, and vulnerability to cyber-attacks. Zero-Knowledge Proof (ZKP) protocols have emerged as an effective solution for achieving secure and efficient authentication in such environments without revealing sensitive information. Among ZKP protocols, Σ-protocols, a class of interactive ZKP protocols, have been employed for their efficiency and security. However, their interactive nature necessitates multiple rounds of communication between the prover and the verifier, which can reduce efficiency and increase communication overhead for resource-constrained devices. In this work, we propose an approach for transforming Σ-protocols into noninteractive zero-knowledge (NIZK) protocols based on the Fiat-Shamir transformation (FST), yielding significant enhancements in efficiency, communication overhead reduction, and elimination of interaction. Our proposed protocol enables the completion of the authentication process in a single request while also strengthening the soundness of Σ-protocols in comparison to the traditional FST by requiring two authentication factors instead of one. Additionally, our protocol introduces a session key agreement mechanism, leveraging our NIZK transformation, to ensure secure end-to-end communication. By reducing the required interaction for sharing an ephemeral session key to just one, our proposed solution outperforms traditional protocols and offers notable improvements. To demonstrate the robustness of our approach against various attacks, we conducted a comprehensive formal security analysis employing the Tamarin prover. Moreover, our performance analysis showcased a remarkable enhancement in comparison to traditional Σ-protocols, with our proposed protocol outperforming them by 100% in the worst case. The adoption of our protocol enables the realization of an efficient authentication mechanism for resource-constrained devices operating in insecure networks.

AfricaCrypt
TUNISIA 2023

Lecture Notes in Computer Science

Technology Innovation Institute

Tunisia

TABC

tuntrust

TOPNET

Next Step

SECURE-iC

Symbolic Software

INSTITUT FRANÇAIS

www.africacrypt2023.tn

Designed by : Amal Samti