AMS-UMI International
Joint Meeting 2024
Palermo, July 23–26, 2024

# Post-quantum Group-based Cryptography Special Session B24

*Delaram Kahrobaei*
The City University of New York, Queens College, USA

*Antonio Tortora*
Università della Campania "Luigi Vanvitelli", ITALY

*Maria Tota*
Università di Salerno, ITALY

This session is scheduled on July 25-26. We bring cryptographers, group theorists, quantum computational theorists to discuss various aspects of post-quantum group-based cryptography. Group-based cryptography is a relatively new family of classes of post-quantum primitives with great potential. Due to the diversity of backgrounds of the speakers, we are aiming to create interdisciplinary areas for collaborations. The topics of talks could generate new mathematical questions for group theorists as well as for cryptographers striking applying new mathematical objects and problems for the cryptographic schemes. This meeting is designed to exchange the new results in this direction and well as creating national and international collaborations among the speakers and attendees.

**Schedule and Abstracts**

July 25, 2024

**11:30–12:15 Automaton group-based cryptography**
**Marialaura Noce, (Università di Salerno, ITALY)**

*Abstract.* In cryptography most famous protocols (RSA, Diffie-Hellman, and elliptic curve methods) depend on the structure of commutative groups and they are related to the difficulty to solve integers factorization and discrete logarithms. In 1994 Shor provided a quantum algorithm that solves these problems in polynomial time. As a consequence, researchers are now interested in finding alternative methods in cryptography that are secure in a post-quantum world. Some of the candidates have been known for years, while others are still emerging. Group theory, and in particular non-abelian groups, offers a rich supply of complex and varied problems for cryptography.

In this talk, we present an overview of the current state-of-the-art in post-quantum group-based cryptography. We will describe in particular the class of automaton groups as suitable platfrom for cryptography, and we present new results and some open problems.

**12:30–12:50 Hash functions with special linear groups**
**Ramón Flores, (University of Seville, SPAIN)**

*Abstract.* In this talk new families of Tillich-Zémor hash functions are defined, using higher dimensional special linear groups over finite fields as platforms. We will show that the Cayley graphs of these groups combine fast mixing properties and high girth, which together give rise to good preimage and collision resistance of the corresponding hash functions.

**13:00–14:30 Lunch Break**

**14:30–14:50 Secret sharing schemes using representation theory of finite $p$-groups**
**Keivan Mallahi-Karai, (Jacobs University, Bremen, GERMANY)**

*Abstract.* In this talk, I will describe a new approach toward constructing secret sharing schemes that is based on the representation theory of finite $p$-groups. I will explain connections to the Kirillov's orbit method, and a number of other works that aim at characterizing minimal faithful representations of p-groups. This is based on a joint work with Delaram Kahrobaei.

**15:00–15:20 A Guide to the Design of Digital Signatures based on Cryptographic Group Actions**

**Federico Pintore, (Università di Trento, ITALY)**

*Abstract.* Recent years have witnessed a revival of cryptography based on group actions, mainly due to its role in post-quantum cryptography, i.e. the branch of cryptography whose goal is designing cryptosystems believed to be secure even in the presence of quantum attackers. For instance, several works have proposed digital signature schemes based on group actions, as well as a variety of techniques aimed at improving their performance and efficiency. Most of these techniques can be explained as transforming one Sigma protocol into another, while essentially preserving security. In this talk, we present a unified taxonomy of such techniques. In particular, we describe all techniques in a single fashion, show how they impact the performance of the resulting protocols and analyse how different techniques can be combined for optimal performance. This analysis is meant to provide a flexible tool which is easy to adapt and employ in the design of future schemes.

**15:30–15:50 On the security of some group-based key exchange protocols**

**António Malheiro, (NOVA University of Lisbon, PORTUGAL)**

*Abstract.* In this talk we will discuss the security of some group-based key exchange protocols with emphasis on the semantic security and its connection with well-known group-theoretic decidability problems. We will make considerations on how this analysis can affect the choice of platform groups, presenting concrete examples.

**16:00–16:20 Quantum-Safe Data Aggregation Solution for Smart Meter Networks**

**Maria Ferrara, (Università della Campania "Luigi Vanvitelli", ITALY)**

*Abstract.* *Smart meters* have replaced traditional electricity meters in recent years, marking a significant advancement in energy management. Italy is the nation in Europe that first expressed interest in first-generation smart meters and is currently replacing them with second-generation ones.

These digital devices offer several advantages, enabling daily consumption monitoring and support for real consumption-based billing. By continuously monitoring, it is possible to identify consumption peaks and enhance network stability at different levels of aggregation. In this context, it is crucial to have a cryptographic scheme that preserves consumers' privacy.

This talk aims to describe a protocol that enables an unreliable data aggregator to compute the sum of several plaintexts working only with the corresponding ciphertexts. Our proposal, unlike other solutions to this problem, does not require communication between smart meters and is quantum-safe.

**16:30–17:00 Coffee Break**

**17:00–17:20 Navigating in graphs of elliptic curves**

**Daniele Taufer, (KU Leuven, BELGIUM)**

*Abstract.* Many past and current cryptographic challenges are based on the difficulty of efficiently navigating in graphs whose vertices represent elliptic curves from certain families. A relevant instance is given by isogeny graphs between supersingular elliptic curves, which have been proposed as valid postquantum candidates. Although some of these protocols did not pass the test of time, others are still alive and keep motivating the fundamental research of these curves. In this talk, such graphs and their difficulty assumptions will be reviewed. Furthermore, other families of graphs naturally arising from elliptic curves over finite fields will be presented, highlighting differences and possible connections. It will be noted how this topic is linked to several distinct fields, highlighting the group actions underlying the considered graphs. It is based on two ongoing works, joint with Eleni Agathocleous, Antoine Joux, Marzio Mula and Federico Pintore.

### 17:30–17:50 Automorphisms of bibraces and their applications to symmetric-key cryptography

**Roberto Civino, (Università dell'Aquila, ITALY)**

*Abstract.* In a XOR-based alternating block cipher the plaintext is masked by a sequence of layers each performing distinct actions: a highly nonlinear permutation, a linear transformation, and the bitwise key addition. When assessing resistance against *classical* differential attacks (where differences are computed with respect to XOR), the cryptanalysts must only take into account differential probabilities introduced by the nonlinear layer, this being the only one whose differential transitions are not deterministic. The temptation of computing differentials with respect to another difference operation runs into the difficulty of understanding how differentials propagate through the XOR-affine levels of the cipher. In this talk we introduce a special family of *braces* that enable the derivation of a set of differences whose interaction with *every* layer of an XOR-based alternating block cipher can be understood. We show that such braces can be described also in terms of alternating binary algebras of nilpotency class two. Additionally, we present a method to compute the automorphism group of these structures through an equivalence between bilinear maps. By doing so, we characterise the XOR-linear permutations for which the differential transitions with respect to the new difference are deterministic, facilitating an alternative differential attack.

#### References

[1] R. Civino, C. Blondeau, and M. Sala, *Differential attacks: using alternative operations*, Designs, Codes and Cryptography, 87(2):225-247 (2019).

[2] M. Calderini, R. Civino, and M. Sala, *On properties of translation groups in the affine general linear group with applications to cryptography*, Journal of Algebra, 569:658-680 (2021).

[3] R. Civino and V. Fedele, *Binary bi-braces and applications to cryptography*, preprint (2024).

### 18:00–18:20 Applications of varieties over finite fields to the differential uniformity of polynomials

**Daniele Bartoli, (Università di Perugia, ITALY)**

*Abstract.* Algebraic curves over finite fields hold significance not only in theory but also establish profound links with various branches of mathematics and combinatorics. They serve as crucial instruments in tackling topics such as APN functions, planar functions, APcN functions, and APN permutations. In this presentation, I'll delve into the applications of algebraic curves in exploring the aforementioned concepts.

July 26, 2024

### 11:30–12:15 Cryptanalysis of Xifrat1-Sign.I quasigroup-based digital signature scheme

**Dmytro Savchuk, (University of South Florida, USA )**

*Abstract.*We propose a new cryptanalysis of the `Xifrat1-Sign.I DDS` digital signature scheme proposed by Jianfang "Danny" Niu in 2023 as a candidate to NIST's post-quantum Cryptography Standardization project [1]. The scheme is based on a quasigroup $Q$ of order 16 satisfying restrictive commutativity property, stating that $(ab)(cd) = (ac)(bd)$ for all elements $a, b, c, d \in Q$. The scheme, using multiplication in the quasigroup and several rounds of mixing, constructs a 768-bit shared secret key. We study properties of the underlying quasigroup and expose a vulnerability that allows us to recover the key from public data within seconds in all tested cases. Another attack on the scheme was proposed in July 2023 by Lorenz Panny using the linearization. Our attack takes much less time to recover the secret key. The implementation of the attack in GAP and statistical analysis of the scheme are given in [2].

#### References

[1] Jingfang Niu, *NIST Submission: Xifrat1-Sign.I DSS*, `https://csrc.nist.gov/projects/pqc-dig-sig/round-1-additional-signatures`.

[2] Kianna Cabral, Dmytro Savchuk *Cryptanalysis of `Xifrat1-Sign.I DSS` quasigroup-based digital signature scheme*, `https://github.com/kiki1123/xifrat-cryptanalysis`.

### 12:30–12:50 A new primitive for multivariate schemes arising from Boolean functions theory

**Irene Villa, (Università di Genova, ITALY)**

*Abstract.* Multivariate public-key cryptography is one of the families of post-quantum cryptography. Most of the schemes belonging to this family can be seen as applying an affine transformation to a quadratic map from $\mathbb{F}_q^n$ to $\mathbb{F}_q^m$, where $n, m$ are positive integers, $q$ is a power of a prime and $\mathbb{F}_q$ is a finite field with $q$ elements. In this talk, we will consider a more general notion of equivalence relation, the CCZ-transformation, borrowed from the area of cryptographically relevant Boolean functions. To allow a generic CCZ-transformation, we make use of the *twisting*, introduced by Canteaut and Perrin in [1].

**Definition 1.** Two functions $F, G : \mathbb{F}_q^n \to \mathbb{F}_q^m$ are equivalent via $t$-twist, for $0 \leq t \leq \min(n, m)$, if $F(x, y) = (T(x, y), U(x, y)) = (T_y(x), U_x(y))$ and $G(x, y) = (T_y^{-1}(x), U_{T_y^{-1}(x)}(y))$, where $T : \mathbb{F}_q^t \times \mathbb{F}_q^{n-t} \to \mathbb{F}_q^t$, $U : \mathbb{F}_q^t \times \mathbb{F}_q^{n-t} \to \mathbb{F}_q^{m-t}$, and $T_y(x)$ is a bijection for any fixed $y \in \mathbb{F}_q^{n-t}$.

Using the twisting, we define the following pair of public and secret keys.
For $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ a $t$-twistable function, we consider the equivalent function via $t$-twist $G$. For random $A_1, A_2$ affine bijections of $\mathbb{F}_q^m$ and $\mathbb{F}_q^n$ respectively, we set $G_{pub} = A_1 \circ G \circ A_2$. Then, the public key is $\texttt{pk} = G_{pub}$ and the secret key is the tuple $\texttt{sk} = \langle F, A_1, A_2 \rangle$.

We present an encryption scheme and a signature scheme using the above cryptographic primitive. We provide further specifications on the map $F$, hence on the choice of quadratic $T$ and $U$, and we call it the UOV-CCZ scheme. Focusing on the latter, we study its structure and its properties. Finally, we study whether and how some known attacks to multivariate cryptographic schemes can be applied to our proposal. For example, the *linearization attack*, proposed by Patarin in [2], works only under some restriction on the choice of parameters.

#### References

[1] A. Canteaut, L. Perrin, *On CCZ-equivalence, extended-affine equivalence, and function twisting*, Finite Fields and Their Applications, 56 (2019), 209–246.

[2] J. Patarin, *Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt 88*, in CRYPTO 1995, Lecture Notes in Computer Science, 963 (Springer, Berlin, 1995), 248-–261.

### 13:00–14:30 Lunch Break

### 14:30–14:50 Security Analysis of ZKPoK based on MQ problem

**Martina Vigorito, (Università di Salerno, ITALY)**

*Abstract.* In this talk I will investigate the security of a new Zero-Knowledge Proof-of Knowledge scheme based on Multivariate Quadratic problem, presented in [1, 2]. The security of this new scheme is related to a new hard problem: the so-called DMQH.

I will present a new efficient probabilistic algorithm for solving the DMQH. The algorithm solves DMQH in polynomial time if $m - n \in O(1)$. For more details see [3].

#### References

[1] L. Bidoux, P. Gaborit, *Compact post-quantum signatures from proofs of knowledge leveraging structure for the sfpkp, sfsd and sfrsd problem*, In S. E. Hajji, S. Mesnager, and E. M. Souidi, editors, Codes, Cryptology and Information Security - 4th International Conference, C2SI 2023, Rabat, Morocco, May 29-31, 2023, Proceedings, volume 13874 of Lecture Notes in Computer Science, pages 10–42. Springer, 2023.

[2] L. Bidoux, P. Gaborit, *Shorter signatures from proofs of knowledge for the sd, mq, pkp and rsd problems*, arXiv, Initial version, April 2022.

[3] D. Kahrobaei, L. Perret, M. Vigorito, *Security Analysis of ZKPoK based on MQ problem in the Multi-Instance Setting*, submitted.

### 15:00–15:20 Conjugacy Search Problem in Contracting Self-similar Groups Arsalan Akram Malik, (University of South Florida, USA)

*Abstract.* We propose self-similar contracting groups as a new platform for cryptographic schemes based on simultaneous conjugacy search problem (SCSP). The class of these groups contains extraordinary examples like Grigorchuk group, which is known to be non-linear, and groups in this class admit a natural normal form based on the notion of a portrait. While for some groups in the class the conjugacy search problem has been studied, there are many groups for which no such algorithms are known. We discuss benefits and drawbacks of using these groups in cryptography and provide computational analysis of variants of the length based attack on SCSP for some groups in the class, including Grigorchuk group.

### 15:30–15:50 Some group-theoretical results on block ciphers in a long-key scenario Riccardo Aragona, (Università dell'Aquila, ITALY)

*Abstract.* Most modern block ciphers belong to two families of symmetric cryptosystems, i.e. Substitution-Permutation Networks (SPN) and Feistel Networks. Typically, in both cases, each encryption function is a composition of key-dependent permutations of the plaintext space, called *round functions*, designed in a such way to provide both *confusion* and *diffusion*. Confusion is provided applying public non-linear vectorial Boolean functions, called S-boxes, whereas diffusion is obtained by means of public linear maps, called diffusion layers. The private component of the cipher, i.e. the *key*, is derived from the user-provided information by means of a public procedure known as *key-schedule*. When the round functions are made in such a way the confusion and diffusion layers are followed by the XOR-addition with the so-called *round-key*, where the round-key is every possible vector in the message space, the cipher is a *long-key cipher*.

Since the seventies, many researchers have studied the relationship between some algebraic properties of the confusion/diffusion layers and some algebraic weaknesses of the corresponding ciphers, using a permutation-group-theoretical approach. In 1975, Coppersmith and Grossman considered a set of permutations which can be used to define a block cipher and, by studying the permutation group that they generate, they linked some properties of this group and the security of the corresponding cipher. From this work a new branch of research was born, which focuses on group-theoretical properties that can be exploited to attack encryption methods. Kaliski, Rivest and Sherman proved that if the permutation group generated by the encryption functions of a cipher is too small, then the cipher is vulnerable to birthday-paradox attacks. Calderini, Civino and Sala proved that if such group is isomorphic to a subgroup of the affine group of the plaintext space, induced by a sum different to the classical bitwise XOR, then it is possible to embed a dangerous trapdoor on it. More relevant, Paterson built a DES-like cipher whose encryption functions generate an imprimitive group and showed how the knowledge of this trapdoor can be turned into an efficient attack to the cipher. For this reason, showing that the group generated by the encryption functions of a given cipher is primitive and not of affine type became a relevant branch of research. In 2016, Bannier, Bodin and Filiol generalized the imprimitive attack shown by Paterson by means of a trapdoor which consists in mapping a partition of the plaintext space into a (different) partition of the ciphertext space. The authors also proved that only *linear* partitions can propagate round-by-round in a long-key SPN.

In this talk, first we present some conditions ensuring that linear partitions cannot propagate in a long-key SPN [2]. Then, we study some properties of the linear-partition propagation under the action of a long-key Feistel Network. In particular, we will see that also in a Feistel-Network-like long-key framework, if the cipher allows partition propagation, then the partitions are linear ones. Moreover, we provide a partial generalisation in the Feistel Network case [1] of the results given in the SPN case.

#### References

[1] R. Aragona, M. Calderini, R. Civino, *Some group-theoretical results on Feistel Networks in a long-key scenario*, Adv. Math. Commun., 14 (2020), 727–743.

[2] M. Calderini, *Primitivity of the group of a cipher involving the action of the key-schedule*, J. Algebra Appl., 20 (2021), Nr. 2150084.

**16:00–16:20 Using regular subgroups in block cipher cryptanalysis**
**Marco Calderini, (Università di Trento, ITALY)**

*Abstract.* In the context of iterated block ciphers classical cryptanalysis techniques and their generalizations exploit linear relations between the inputs (plaintexts) and outputs (ciphertexts) of an encryption function. Usually the plaintext and ciphertext space is given by an $n$ dimensional vector space over the binary field $\mathbb{F}_2$, $V = \mathbb{F}_2^n$, and the operation which is exploited in the linear relations is the XOR sum $(+)$.

Alternative operations $\circ$ can be defined over the space $V$ in order to obtain that $(V, \circ)$ is still a vector space. Such operations come from the elementary abelian regular subgroups of $\mathrm{Sym}(V)$, that are the conjugates to the usual translation group $T_+(V)$. In this talk, we will focus on the properties of the elementary abelian regular subgroups contained in the general affine group. We will give a characterizations of such groups and we will discuss how they can be exploited in order to implement possible attacks to block ciphers.

**16:30–17:00 Coffee Break**

**17:00–17:20 Subsets of groups in public-key cryptography**
**André Carvalho, (University of Porto, PORTUGAL)**

*Abstract.* Subsets of groups defined by language-theoretic conditions (rational, algebraic, context-free,...) are an interesting object of study in group theory and algorithmic problems when defined on subsets are in general harder than when defined on finitely generated subgroups.

In this talk, we suggest the usage of algebraic subsets instead of subgroups in public-key cryptography, playing the role of subgroups in some classical key exchange protocols. We also introduce new group theoretic problems arising from this work.

This is joint work with António Malheiro and the results can be found in the preprint [1].

### References

[1] A. Carvalho and A. Malheiro, *Subsets of groups in public-key cryptography*, arXiv:2311.15039.

**17:30–17:50 Exploring problems and platforms in group-based cryptography**
**Carmine Monetta, (Università di Salerno, ITALY)**

*Abstract.* Group-based cryptography is mainly concerned with the study of cryptographic protocols which rely on problems within nonabelian Group Theory. These problems typically manifest as search variants stemming from decision-type problems.

Once a cryptographic system is established, the primary challenge lies in identifying an appropriate platform, whether it is a singular group or a class of groups, endowed with favorable algorithmic properties. Indeed, this platform should render the underlying problems sufficiently complex to effectively withstand attacks.

This presentation aims to investigate various decision problems in Group Theory from two distinct perspectives. Firstly, we will explore their application in proposed cryptographic systems. Subsequently, we will embark on a comprehensive discussion regarding the advantages and disadvantages of various suggested platforms.

E–mail: `mtota@unisa.it`.