IMAR

Simion Stoilow Institute of Mathematics
Romanian Academy

Doctoral School of Mathematical Sciences and Informatics

Surrey Centre for Cyber Security
University of Surrey, UK

spring 2025
WSTC

Workshop on Selected Topics in Cryptography
Spring 2025 Edition, May 30-31, Iași, Romania

This is the short version of the booklet for print use.
Full abstracts and presentations with all authors, references, and figures can be found at:
https://www.wstc.flt-info.eu/spring-2025

Contents

About WSTC

Scope

WSTC aims to provide an appropriate and interactive environment to:

1. encourage and strengthen scientific cooperation and communication in cryptography and related fields;
2. focus discussions on research topics and problem statements;
3. offer feedback on research papers/ideas to help authors prepare better versions of their work.

To achieve these objectives, the thematic palette of each workshop session will be limited and a prior established by the workshop organizers. It will be announced in due course on the workshop's web page.

How WSTC works

How WSTC works will differ from typical cryptography conferences in some ways:

- The participants will be invited to contribute through presentations within workshop topics. These may include specific problems on which there is the hope of making some progress during the workshop, as well as more ambitious problems that may influence the future activity of the field;
- WSTC will invite talks and lectures by specialists to familiarize the participants with the background material leading up to specific problems;
- The schedule will include discussion and parallel working sessions.

Contact

Organizers

Ferucio Laurențiu Țiplea, Ph.D.
Department of Computer Science
Alexandru Ioan Cuza University, Iasi, Romania;
Simion Stoilow Institute of Mathematics of the Romanian Academy, Bucharest, Romania

Ioana Boureanu, Ph.D.
Surrey Centre for Cyber Security
University of Surrey, UK

Constantin Cătălin Drăgan, Ph.D.
Surrey Centre for Cyber Security
University of Surrey, UK

Local Organizers

Sorin Iftene, Ph.D.
Department of Computer Science
Alexandru Ioan Cuza University of Iasi, Romania

Anca-Maria Nica, Ph.D.
Department of Computer Science
Ioan Cuza University, Iasi, Romania

Dana Savu, Ec.
Simion Stoilow Institute of Mathematics of the Romanian Academy, Bucharest, Romania

Spring Edition 2025

The Spring 2025 edition gathered 15 contributed talks in the following fields:

- code-based cryptography,
- lattice-based cryptography,
- residuosity-based cryptography,
- privacy and authentication in information security,
- multilinear-maps,
- secret sharing,
- anonymous signatures, and
- searchable encryption.

The participants were from “Simion Stoilow” Institute of Mathematics of the Romanian Academy (Bucharest, Romania), Advanced Technologies Institute (Bucharest, Romania), “Alexandru Ioan Cuza” University (Iași, Romania), Bitdefender (Iasi, Romania), and Surrey Centre for Cyber Security, University of Surrey (UK).

Timetable

CT: Contributed Talk

Friday, 30th of May

9:00–9:20	**Welcome**		
9:20–10:00	CT	**Olimpia Ţiclos[1,2], Ioana Boureanu[2], and Cătălin Drăgan[2]** [1]IMAR, RO; [2]SCCS, UK	Bridging the Gap: From ISD to ISIS through Generalised Inverses
10:00–10:40	CT	**Patricia Safriuc** UAIC, RO	Permutation-based Optimization in GI Decoding
10:40–11:00	**Coffee break**		
11:00–11:40	CT	**Nada El Kassem** SCCS, University of Surrey, UK	Post-Quantum Direct Anonymous Attestation (PQ-DAA)
11:40–12:20	CT	**Callum London** SCCS, University of Surrey, UK	Lattice based Isomorphism problem and applications
12:20–14:20	**Lunch break**		
14:20–15:00	CT	**Victor Talif** IMAR, RO	Graded Encoding Systems: A summary of implementations and attacks
15:00–15:40	CT	**Alexandru-Valentin Bașagă and Sorin Iftene** UAIC, RO	Ideal Compartmented Secret Sharing Scheme Based on the Chinese Remainder Theorem for Polynomial Rings
15:40–16:00	**Coffee break**		
16:00–16:40	CT	**Oana Tătaru** UAIC, RO	NP-Completeness of SVP for Binary Lattices
16:40–17:00	**Discussions**		

Saturday, 31th of May

9:20–10:00	CT	**Long Meng** SCCS, University of Surrey, UK	FEASE: Fast and Expressive Asymmetric Searchable Encryption
10:00–10:40	CT	**Yalan Wang** SCCS, University of Surrey, UK	Anonymous signature from hash functions
10:40–11:00	**Coffee break**		
11:00–11:40	CT	**Anca-Maria Nica** UAIC, RO	Authentication in IoT
11:40–12:20	CT	**Manuela Horduna** IMAR, RO	Shaping Privacy Models in Searchable Encryption
12:20–14:20	**Lunch break**		
14:20–15:00	CT	**Maria Coteanu** Bitdefender, RO	On Strong Privacy in Vaudenay's RFID Model
15:00–15:40	CT	**Ferucio Laurențiu Țiplea** UAIC, RO	Weak, Weak-insider, and Randomized Weak Privacy in the HPVP model for RFID
15:40–16:00	**Coffee break**		
16:00–16:40	CT	**Paul Cotan** IMAR, RO	Algorithms for Rational Conics on Finite Fields
16:40–17:20	CT	**George Teșeleanu** ATI, RO	A Generalized Wiener-type Attack Against an RSA-like Cryptosystem
17:20–18:00	**Discussions**		

List of Abstracts – Talks

Ideal Compartmented Secret Sharing Scheme Based on the Chinese Remainder Theorem for Polynomial Rings

Alexandru-Valentin Bașagă and Sorin Iftene **CT**

Department of Computer Science, "Alexandru Ioan Cuza" University of Iaşi, Romania

A secret sharing scheme starts with a secret and then derives from it certain shares (or shadows) which are distributed to users. The secret may be recovered only by certain predetermined groups. In case of compartmented secret sharing, the set of users is partitioned into compartments and the secret can be recovered only if the number of participants from any compartment is greater than or equal to a fixed compartment threshold and the total number of participants is greater than or equal to a global threshold. In this paper we use the Chinese Remainder Theorem for Polynomial Rings in order to construct an ideal compartmented secret sharing scheme, inspired by the work from [1].

References

[1] Yang, J., S.-T. Xia, X. Wang, J. Yuan and F.-W. Fu, *A perfect ideal hierarchical secret sharing scheme based on the CRT for polynomial rings*, in: 2024 IEEE International Symposium on Information Theory (ISIT), 2024, pp. 321–326

Algorithm for Rational Conics on Finite Fields

Paul Cotan **CT**

"Simion Stoilow" Institute of Mathematics of the Romanian Academy, Bucharest, Romania

Starting from the space-efficient IBE cryptosystem introduced by Boneh, Gentry and Hamburg, we will focus our attention on the most challenging step of it, namely the synchronization between the sender's and receiver's parameters. This talk will present a family of algorithms for rational conics on finite fields which manage to solve the main problem.

On Strong Privacy in Vaudenay's RFID Model

Maria Coteanu **CT**

Bitdefender, Iași, România

Radio Frequency Identification (RFID) systems have become essential tools in modern technology, facilitating efficient solutions in areas like contactless payments, access control, and asset tracking. To address the privacy risk inherent in RFID technology, a formal model of privacy has been proposed that categorised privacy into different levels. Vaudenay's model is one such formal of privacy that differentiates between 4 levels of privacy: weak, forward, destructive and strong. This paper revisits Vaudenay's strong privacy level and examines his proof of impossibility based on the public algorithm for setting an illegitimate tag. We show that strong privacy is possible in Vaudenay's model using the permitted oracle and the strong impossibility proof was misguided. Our findings inspire a new definition of the RFID privacy model and the adversary's capabilities.

Post-Quantum Direct Anonymous Attestation (PQ-DAA)

Nada El Kassem **CT**

Surrey Centre for Cyber Security, University of Surrey, UK

Direct Anonymous Attestation (DAA) is a group-type anonymous signature scheme that allows users in a group to sign messages such that the signatures can be verified using a group public key, and the actual signers' identities are not revealed (beyond the fact that they belong to the group). DAA was initially designed to support anonymous attestation using a Trusted Platform Module (TPM), a hardware component embedded in a host computer platform. A unique feature of DAA is that a group signer's role is split into two entities, a principal signer and an assistant signer; the former is the TPM, and the latter is the host platform.

Currently, standardised DAA schemes rely on the security of factoring and discrete logarithm problems. Should a quantum computer become available in the next few decades, these schemes will be broken. Therefore, there is a need to start developing post-quantum DAA schemes. Our research into quantum-resistant DAA has resulted in several Lattice-based schemes. The security of our schemes is proved in the Universally Composable (UC) security model under the hardness assumptions of the Ring Inhomogeneous Short Integer Solution (Ring-ISIS) and Ring Learning with Errors (Ring-LWE) problems.

Shaping Privacy Models in Searchable Encryption

Manuela Horduna **CT**

"Simion Stoilow" Institute of Mathematics of the Romanian Academy, Bucharest, Romania

Searchable encryption lets users run fast queries on data stored with untrusted providers—without ever revealing the raw content. Nevertheless, striking the right balance among privacy, dynamic updates, and performance is challenging. Recent security incidents show that merely preventing unauthorized access is not enough; systems must also hide side- channel signals (like the queries issued or the patterns of data access or search) that could quietly expose sensitive information. The matter presented hereafter will establish the roadmap forward for reinforcing the privacy foundations of searchable encryption by sharpening the distinction between security and privacy. Afterwards will be presented a systematic mapping from privacy classes to the leakage they allow illustrating how one scheme can operate in different privacy "modes" under different threat models. Moreover, the privacy properties will be refined and it will be formalized four granular privacy models, each paired with a purpose-built illustrative privacy game tailored to its expected leakage profile.

Lattice Isomorphism Problem: Variants and Applications

Callum London **CT**

Surrey Centre for Cyber Security, University of Surrey, UK

The Lattice Isomorphism Problem (LIP) is a promising hard problem in the post-quantum space which underpins the HAWK signature scheme by Ducas et. al, currently a second round candidate in the NIST standardisation project Post Quantum Cryptography: Additional Digital Signature Schemes. It can offer significant performance improvements over standard lattice assumptions due to its improved decoding, however, only a small number of primitives have been constructed from it. Compared with other lattice assumptions such as SIS or LWE, LIP is not as well-understood. For example, LIP does not have a known search-to-distinguish reduction. To better understand the implications of LIP, we introduce related problems which we call approximate-LIP and image-hinted-LIP. These variant problems may be used to design more exotic cryptographic primitives benefitting from the efficiency improvements offered by LIP. In particular, we show how an existing LIP-based signature scheme may be extended to a blind signature scheme provided that either of these variant problems is hard.

FEASE: Fast and Expressive Asymmetric Searchable Encryption

Long Meng **CT**

Surrey Centre for Cyber Security, University of Surrey, UK

Asymmetric Searchable Encryption (ASE) is a promising cryptographic mechanism that enables a semi-trusted cloud server to perform keyword searches over encrypted data for users. To be useful, an ASE scheme must support expressive search queries, which are expressed as conjunction, disjunction, or any Boolean formulas. In this paper, we propose a fast and expressive ASE scheme that is adaptively secure, called FEASE. It requires only 3 pairing operations for searching any conjunctive set of keywords independent of the set size and has linear complexity for encryption and trapdoor algorithms in the number of keywords. FEASE is based on a new fast Anonymous Key-Policy Attribute-Based Encryption (A-KP-ABE) scheme as our first proposal, which is of independent interest. To address optional protection against keyword guessing attacks, we extend FEASE into the first expressive Public-Key Authenticated Encryption with Keyword Search (PAEKS) scheme. We provide implementations and evaluate the performance of all three schemes, while also comparing them with the state of the art. We observe that FEASE outperforms all existing expressive ASE constructions and that our A-KP-ABE scheme offers anonymity with efficiency comparable to the currently fastest yet non-anonymous KP-ABE schemes FAME (ACM CCS 2017) and FABEO (ACM CCS 2022).

Authentication in Internet of Things (IoT)

Anca-Maria Nica **CT**

Department of Computer Science, “Alexandru Ioan Cuza” University, Iaşi, Romania

As Marc Goodman says, “when everything is connected, everyone is vulnerable”[1]. The Internet of Things (IoT) comes with undoubtable facilities coming aside with some important disadvantages like security and privacy lakes, a high percentage of those due to authentication process. In this presentation we will address different facets regarding authentication in IoT, such as complexity aspects, current and future methods along with possible attacks, centralized vs. decentralized architectures, one-way vs. mutual authentication. We will also cover some domain specific issues on IoT authentication.

Permutation-based Optimization in GI Decoding

Patricia Safriuc **CT**

Department of Computer Science, "Alexandru Ioan Cuza" University of Iaşi, Romania

Generalized Inverse based Decoding is a technique of decoding linear codes introduced recently, with applications in finding solutions to hard problems, such as The Low Weight COdeword Problem. We build upon the algorithm proposed by Prange, that is Information Set Decoding, focusing on one of its downfalls: relying solely on randomness when choosing a permutation matrix. We introduce a new way of navigating the set of such permutation matrices by performing shifts on the rows and constantly taking into consideration the improvement one matrix brings to the final solution.

Graded Encoding Systems: A summary of implementations and attacks

Victor Talif **CT**

"Simion Stoilow" Institute of Mathematics of the Romanian Academy, Bucharest, Romania

Multilinear maps represent an important primitive in cryptography, with a vast array of applications. Amidst the candidates for the general case, graded encoding systems offer a valid structure to support N-linear maps, for $N > 2$. However, attacks were presented for most implementations, exploring weaknesses such as weak DL and zero-testing faults. In this presentation, we aim to highlight the source of the faults, then abstract and compare them across constructions and suggest ways around them, based on other existing implementations or insight. The goal is to provide a comprehensive overview of the existing research and use it to hint at its future development.

NP-Completeness of SVP for Binary Lattices

Oana Tătaru **CT**

Department of Computer Science, "Alexandru Ioan Cuza" University, Iaşi, Romania

The Shortest Vector Problem (SVP) is a fundamental challenge in lattice theory, with wide-ranging applications in number theory, coding theory, and particularly in cryptography. Its assumed intractability underlies the security of lattice-based cryptographic schemes, which are among the leading candidates for post-quantum cryptography. While SVP has been studied extensively in general settings, its exact complexity in restricted cases—such as binary lattices—remains less understood. In this paper, we prove that SVP is NP-complete when restricted to binary lattices, via a polynomial-time reduction from the NP-complete Decisional Minimum Distance Decoding (MDD) problem for binary codes. We formalize SVP as an NP optimization problem, show that it lies in NP using a nondeterministic algorithm, and construct a structure-preserving R-reduction that maintains solution equivalence under Hamming and Euclidean norms. We hope these results strengthen the complexity-theoretic foundations of SVP and highlight its continued importance in cryptographic applications.

A Generalized Wiener-type Attack Against an RSA-like Cryptosystem

George Teşeleanu **CT**

Advanced Technologies Institute, Bucharest, Romania

Let $N = pq$ be the product of two balanced prime numbers p and q. In 2023, Cotan and Teşeleanu introduced a family of RSA-like cryptosystems based on the key equation $ed - k(p^n - 1)(q^n - 1) = 1$, where $n \geq 1$. Note that when $n = 1$, we obtain the classical RSA system, while $n = 2$ yields the variant proposed by Elkamchouchi, Elshenawy, and Shaban. In this paper, we present a novel attack that combines continued fractions with lattice-based methods for the case $n = 8$. This represents a natural continuation of previous research, which successfully applied similar techniques for $n = 1, 2, 4$.

Bridging the Gap: From ISD to ISIS through Generalised Inverses

Olimpia Ţiclo**ș*[1,2], ***Ioana Boureanu[2] ***and Cătălin Drăgan***[2] **CT**

[1] "Simion Stoilow" Institute of Mathematics of the Romanian Academy, Bucharest, Romania
[2] Surrey Centre for Cyber Security, University of Surrey, UK

This presentation explores the connection between Information Set Decoding (ISD) and the Inhomogeneous Short Integer Solution (ISIS) problem in lattice-based cryptography. By adapting classical ISD and Ball-Collision Decoding (BCD) algorithms, we extend their application to solving ISIS over Fq with binary solutions through a unified Generalized Inverses (GI) framework. Our implementation and analysis demonstrate that ISD-style approaches remain competitive, suggesting their relevance in both theoretical and practical settings. This work contributes to bridging the gap between code-based and lattice-based post-quantum cryptography.

Weak, Weak-insider, and Randomized Weak Privacy in the HPVP model for RFID

Ferucio Laurenţiu Ţiplea **CT**

Department of Computer Science, "Alexandru Ioan Cuza" University of Iaşi, Romania

RFID schemes that provide weak privacy or similar privacy forms are useful in any domain where the adversary cannot mount a corruption attack. In addition, these schemes can be constructed using only symmetric cryptography and can provide time-efficient identification. This paper focuses on RFID schemes that provide weak privacy in the Hermans-Pashalidis-Vercauteren-Preneel (HPVP) model based on tag indistinguishability. We first show that no adversary can have a non-negligible advantage in distinguishing between keys of a pseudo-random function. We then use this result to highlight RFID schemes that provide weak, weak-insider, and randomized weak privacy in the model above.

Anonymous signature from hash functions

Yalan Wang **CT**

Surrey Centre for Cyber Security, University of Surrey, UK

Anonymous signatures, such as group signatures, Direct Anonymous Attestation (DAA) and Enhanced Privacy ID (EPID) have been widely used in privacy-sensitive scenarios such as anonymous authentication and attestation. Considering the transition to post-quantum cryptographic primitives, we focus on post-quantum anonymous signatures. Using only hash functions makes the scheme less prone to unknown attacks than basing the design on newly proposed hard problems whose security is less well-understood. However, hash functions do not have rich algebraic properties, and this makes it extremely challenging to design anonymous signatures on top of them. It is even more challenging if we want an anonymous signature scheme suitable for real-world applications, one that can support large groups and require few trust assumptions. Our scheme is based on Multi-Party Computation in-the-head (MPC-in-the-head) non-interactive zero-knowledge proofs, and we specifically design novel hash-based anonymous signature schemes, which is rooted in the SPHINCS+ signature scheme but with various modifications to make it MPC friendly. These proposed anonymous signature schemes can contain a large number of members, 2^60 and are well-proved.