IMAR MSCS

IMAR workshops on Mathematical Structures in Computer Science

spring 2022

WSTC

Workshop on Selected Topics in Cryptography

Spring 2022 Edition, March 21-25, Sinaia, 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/spring2022

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.
Alexandru Ioan Cuza University, Iași

Vlad-Florin Drăgoi, Ph.D.
Aurel Vlaicu University, Arad

Local Organizers

Anca-Maria Nica, Ph.D.
Alexandru Ioan Cuza University, Iași

Cristian Hristea, Ph.D.
Institute for Advanced Technologies, Bucharest

Spring Edition 2022

The Spring 2022 edition focuses on topics such as, Algebraic variants of Learning With Errors (LWE), Code-based cryptography, Functional encryption, Private set intersection, Residuosity based cryptography, Attribute-based encryption, Security protocols.

Invited talks: Prof. Ayoub Otmani, LITIS lab. University of Rouen, Normandy, France.

There were 13 contributed talks, of which 3 in code-based cryptography, 3 in lattice-based cryptography, 3 in number theoretic-based cryptography, 2 in security models/proofs, 1 in attribute-based encryption, and 1 in PRNGs.

The Spring edition gathered participants from Bitdefender (Bucharest, Romania), Advanced Technologies Institute (Bucharest, Romania), Polytechnic University (Bucharest, Romania), Alexandru Ioan Cuza University (Iași, Romania), Aurel Vlaicu University (Arad, Romania), University of Normandy (Rouen, France).

Timetable

CT: Contributed Talk, IS: Invited Speaker

Monday, 21st of March

9:00–9:30	**Welcome**		
9:30–10:30	CT	**George Teşeleanu** *Advanced Technologies Institute, Bucharest, Romania*	The Impact of Small Primes on Partially Homomorphic Schemes
10:30–11:00	**Discussions - Coffee break**		
11:00–12:00	CT	**Diana Maimuț** *Advanced Technologies Institute, Bucharest, Romania*	Black-Box, Gray-Box and White-Box Cryptography
12:00–12:30	**Discussions**		
12:30–14:00	**Lunch**		
14:00–15:00	CT	**Paul Cotan** *Advanced Technologies Institute, Bucharest, Romania*	A Mathematical Overview of Higher Order Residuosity
15:00–16:00	**Coffee break**		
16:00–18:30	**Work session**		

Tuesday, 22nd of March

9:30–10:30	CT	**Cristian Hristea** *Advanced Technologies Institute, Bucharest, Romania*	Security and Privacy Proofs in Vaudenay's RFID Model: An Introduction
10:30–11:00	**Discussions - Coffee break**		
11:00–12:00	CT	**Alexandru Ioniță** *Alexandru Ioan Cuza University of Iaşi*, Romania	Key-policy Attribute-Based Encryption with Hidden Attributes
12:00–12:30	**Discussions**		
12:30–14:00	**Lunch**		
14:00–15:00	CT	**Vlad-Florin Drăgoi** *Aurel Vlaicu University, Arad, Romania*	Code-based Public-key Encryption Schemes
15:00–15:30	**Coffee break**		
15:30–18:30	**Excursion**		

Wednesday, 23rd of March

9:30–10:30	CT	**Miruna Roşca** *Bitdefender, Bucharest, Romania*	Algebraic Variants of Learning With Errors
10:30–11:00	**Discussions - Coffee break**		
11:00–12:00	CT	**Mădălina Bolboceanu** *Bitdefender, Bucharest, Romania*	Private Set Intersection
12:00–12:30	**Discussions**		
12:30–14:00	**Lunch**		
14:00–15:00	CT	**Radu Ţiţiu** *Bitdefender, Bucharest, Romania*	Inner-Product Functional Encryption from Lattice Assumptions
15:00–16:00	**Coffee break**		
16:00–18:30	**Work session**		

Thursday, 24th of March

9:30–10:30	CT	**Ferucio Laurenţiu Ţiplea** *Alexandru Ioan Cuza University of Iaşi, Romania*	Generalized Inverse Based Decoding
10:30–11:00	**Discussions - Coffee break**		
11:00–11:30	CT	**Andreea Szöcs** *Aurel Vlaicu University, Arad, Romania*	Structural Properties of Self-Dual Monomial Codes with Application to Code-Based Cryptography
11:30–12:00	CT	**Anca-Maria Nica** *Alexandru Ioan Cuza University of Iaşi, Romania*	On Anonymization of Cocks' Identity-based Encryption Scheme
12:00–12:30	**Discussions**		
12:30–14:00	**Lunch**		
14:00–15:00	CT	**Emil Simion** *Polytechnic University of Bucharest, Romania*	New Results on Statistical Testing of Random Number Generators
15:00–15:30	**Coffee break**		
15:30–18:30	**Excursion**		

Friday, 25th of March

9:30–11:00	**WSTC meeting**		
11:00–12:00	IS	**Ayoub Otmani** *LITIS, University of Normandy, France*	Code-based Cryptography: Past, Present and Future
12:00–12:30	**Discussions**		
12:30–13:00	**Closing remarks**		

List of Abstracts – Talks

Private Set Intersection

Mădălina Bolboceanu, Cryptography Researcher **CT**

Bitdefender, Bucharest, Romania

Private Set Intersection (PSI) is an interactive protocol between a client and a server. Here, the client wants to compute the intersection of its set of items and of the set of items of the server. By the end of a PSI protocol, the client learns only this intersection and nothing else about the server's items, while the server learns nothing about the client's items.

Firstly, I will show some applications that motivate our interest in PSI such as private contact discovery for Whatsapp or measuring ads efficiently privately. Secondly, I will talk about Homomorphic Encryption and how to build a PSI protocol based on it. Finally, I will present some optimizations towards the efficiency of this protocol.

This talk is based on this paper [1], its followup [2] and on our implementation [3].

References

[1] `https://eprint.iacr.org/2017/299.pdf`
[2] `https://eprint.iacr.org/2018/787.pdf`
[3] `https://github.com/bit-ml/Private-Set-Intersection`

A Mathematical Overview of Higher Order Residuosity

Paul Cotan, PhD Student **CT**

Simion Stilow Institute of Mathematics of the Romanian Academy, Bucharest, Romania

The most prominent and applicable domain of the mathematical residuosity symbols (2nd order) is, probably, the identity based encryption (IBE). This field has regained the public eye in the last few years due to a series of papers which generalized Clifford Cocks' IBE. In order to provide additional generalizations, it is necessary to understand the higher order residues.

Code-based Public-key Encryption Schemes

Vlad-Florin Drăgoi*[1,2], *Associate Professor **CT**

[1]Faculty of Exact Sciences, Aurel Vlaicu University, Arad, Romania
[2]LITIS Lab, Université de Rouen, Avenue de l'Universitée, 76800 Saint-Étienne-du-Rouvray, France

The evolution of the McEliece encryption framework is a long and thrilling research process. The code families supposed to securely reduce the key size of the original scheme were often cryptanalyzed and thus the future of the code-based cryptography was many times doubted. Yet from this long evolution emerged a great comprehension and understanding of the main difficulties and advantages that coding theory can offer to the field of public key cryptography. Nowadays code-based cryptography has become one of the most promising solutions to post-quantum cryptography. We analyze in this presentation the evolution of the main encryption variants coming from this field.

Security and Privacy Proofs in Vaudenay's RFID Model: An Introduction

Cristian Hristea*, *PhD Student **CT**

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

Given the wireless nature of RFID technology and its high potential for unauthorised tracking, security and privacy are a central component in the design of RFID authentication protocols. However, the manner in which protocols are analysed is equally important, as informal reasoning about these properties is prone to incorporating well known design flaws and to producing insecure protocols. Vaudenay's model is a leading RFID security and privacy model and could be considered the most influential. It contains a thorough description of the adversary's capabilities and establishes eight classes of privacy. The presentation aims to provide an introduction into the process of constructing rigorous security and privacy proofs in this model.

Key-policy Attribute-Based Encryption with Hidden Attributes

Alexandru Ioniță*[1,2]*, PhD Student **CT**

[1]Simion Stoilow Institute of Mathematics of the Romanian Academy, Bucharest, Romania
[2]Department of Computer Science, "Alexandru Ioan Cuza" University, Iaşi, Romania

This paper focuses on hiding attributes in ciphertexts of KP-ABE schemes. In order to acomplish this, we use methods such as Private Set Intersection [1], or ABE access structures with wildcards [2]. Based on the security achievements, we can define three security levels, as follows:

1. simple hidden attributes - this type of HKP-ABE presumes that an attribute A_i from a ciphertext can simply be revealed by any key that contains this attribute, even if the key cannot decrypt the respective ciphertext.
   Problems: Users with multiple decryption keys could query about any attribute available on any of it's key.

2. secure hidden attributes - this type of HKP-ABE presumes that an attribute A_i from a ciphertext can be revealed only by keys that contain this attribute and the key is allowed to decrypt the ciphertext.
   Problems: Users with multiple decryption keys that can decrypt some ciphertext could find out information about more attributes than a minimal set required to decrypt.

3. blind decryption - this type of HKP-ABE presumes that a ciphertext could be decrypted without revealing anything about the attributes, except the fact that they satisfy some access policy linked to the decryption key.

References

[1] Ioniță, A.: Private set intersection: Past present and future. In: Proceedings of the 18th International Conference on Security and Cryptography-SECRYPT. pp. 680-685 (2021).
[2] Cheung, L., Newport, C.: Provably secure ciphertext policy abe. In: Proceedings of the 14th ACM conference on Computer and communications security. pp. 456-465 (2007).

Black-Box, Gray-Box and White-Box Cryptography

Diana-Ştefania Maimuţ, Cryptography Researcher **CT**

Advanced Technologies Institute, Bucharest, Romania

The standard security model considered in cryptography used to be (and still is at least in the case of theoretical cryptography) the black-box model. However, things changed during the last decades: the gray-box model appeared, especially together with the development of side-channel attacks. Research went further and the white-box model started being regarded as the most realistic scenario. The previously mentioned concepts are to be discussed during the talk. Moreover, case studies will be tackled for every model.

On Anonymization of Cocks' Identity-based Encryption Scheme

Anca-Maria Nica, Assistant Professor **CT**

"Alexandru Ioan Cuza" University, Iaşi, Romania

Cocks' identity-based encryption (IBE) scheme is the first IBE scheme that avoids the use of bilinear maps. Based on quadratic residues and due to its simplicity, the scheme gained much attention from researchers. Unfortunately, the scheme is not anonymous in the sense that the cryptotexts may reveal the identities for which they have been computed. Several anonymous variants of it have then been proposed. In this paper we revise Joye's approach to the anonymization of the Cocks' IBE scheme. Due to some recent results on the distribution of quadratic residues, we present a very simple and direct approach that leads to Joye's scheme.

Code-based Cryptography: Past, Present and Future

Ayoub Otmani, Professor **IS**

LITIS lab., University of Rouen, Normandy, France

This talk will be a survey about the most important results in code-based cryptography. The journey will begin with the breakthrough made by McEliece who built the first trapdoor function that rely on the hardness of decoding a linear code. It will then recall the main challenges posed by the scheme immediately after its introduction, and the major failures to solve them. Next we will look at the recent advances and finally we will terminate by relevant questions that are still unanswered.

Algebraic Variants of Learning With Errors

Miruna Roşca, Cryptography Researcher **CT**

Bitdefender, Bucharest, Romania

Lattice-based cryptography relies in great parts on the use of the Learning With Errors (LWE) problem as hardness foundation. However, the LWE-based cryptographic primitives are relatively inneficient. In the last years, new variants of LWE have been introduced (Polynomial-LWE, Ring-LWE, Module-LWE, Middle-Product-LWE, etc.). These variants (which we call algebraic) make use of the algebraic structure of the objects involved (rings, modules, etc.) in order to improve the efficiency of the LWE-based cryptographic schemes.

In this talk, I will describe the most known algebraic variants of LWE, present relationships between them and state some related open problems.

New results on statistical testing of random number generators

Emil Simion, Associate Professor **CT**

Department of Mathematics, Faculty of Applied Sciences, Polytechnic University of Bucharest, Bucharest, Romania

The purpose of the communication is to present a series of improvements to the decision-making process of the statistical tests used in the validation of pseudorandom generators. Improvements refer to the calculation of the probability of accepting a false hypothesis in various circumstances, with the exemplification on the standardized statistical testing procedures.

Structural properties of self-dual monomial codes with application to code-based cryptography

Andreea Szöcs, Msc Student **CT**

Aurel Vlaicu University, Arad, Romania

This presentation focuses on the self-dual monomial codes that have an underlying structure of decreasing/weakly decreasing monomial codes. Having such a property permits an in-depth analysis of their structure: The permutation group of a subclass is (significantly) bigger than the affine group. Upon looking at higher powers of the code, we see that its third power is the entire space, but the dual of the square code gives information helpful for decoding. Using operations such as shortening, puncturing and taking the discrete derivative, we extract the subcode generated by the multiples of a certain variable.

Recently, self-dual monomial codes have been proposed for a McEliece public key encryption scheme. They seem to possess strong security features - they have a large permutation group, they are self-dual, there are exponentially many of them by counting the possible monomial bases used in their construction. A more detailed analysis allows us to identify subclasses where the square code and shortening methods yield non-trivial results; in these cases, the security is dominated by the complexity of the Information Set Decoding, which is exponential in the square root of the length of the code. This is a solid argument for the security of the McEliece variant based on self-dual monomial codes.

The results presented here were in part published in the proceedings of the IMACC 2021 [1].

References

[1] Drăgoi V.F., Szöcs A. (2021) Structural Properties of Self-dual Monomial Codes with Application to Code-Based Cryptography. In: Paterson M.B. (eds) Cryptography and Coding. IMACC 2021. Lecture Notes in Computer Science, vol 13129. Springer, Cham.

The Impact of Small Primes on Partially Homomorphic Schemes

George Teşeleanu, Cryptography Researcher **CT**

Advanced Technologies Institute, Bucharest, Romania

In this talk we will discuss the effects of using multiple prime moduli instead of two prime moduli in the case of partially homomorphic encryption schemes based on factoring. We study the impact of this change on the underlying security assumptions and also the performance improvements achieved by using small primes.

Generalized Inverse Based Decoding

Ferucio Laurenţiu Ţiplea*, *Professor **CT**

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

The concept of Generalized Inverse based Decoding (GID) is introduced, as an algebraic framework for the syndrome decoding problem (SDP) and low weight codeword problem (LWP). The framework has ground on two characterizations by generalized inverses (GIs), one for the null space of a matrix and the other for the solution space of a system of linear equations over a finite field. Generic GID solvers are proposed for SDP and LWP. It is shown that information set decoding (ISD) algorithms, such as Prange, Lee-Brickell, Leon, and Stern's algorithms, are particular cases of GID solvers. All of them search GIs or elements of the null space under various specific strategies. However, as the paper shows the ISD variants do not search through the entire space, while our solvers do even when they use just one Gaussian elimination. Apart from these, our GID framework clearly shows how each ISD algorithm, except for Prange's solution, can be used as an SDP or LWP solver. A tight reduction from our problems, viewed as optimization problems, to the MIN-SAT problem is also provided. Experimental results show a very good behavior of the GID solvers. The domain of easy weights can be reached by a very few iterations and even enlarged.

Inner-Product Functional Encryption from Lattice Assumptions

Radu Ţiţiu*, *Cryptography Researcher **CT**

Bitdefender, Bucharest, Romania

In this presentation I will give a brief introduction on Functional Encryption (FE) and provide some context. Then I will focus on FE for the particular functionality class of linear functions, also known as Inner-Product FE (IPFE). More precisely, I will discuss the construction from [1] whose security (Adaptive Indistinguishability (AD-IND)) is based on the Learning With Errors (LWE) problem. This construction can be adapted to achieve the stronger security notion of Adaptive Simulation (AD-SIM) [2,3] or to make it more practical by using algebraic variants of LWE [4].

References

[1] `https://eprint.iacr.org/2015/608.pdf`
[2] `https://eprint.iacr.org/2020/209.pdf`
[3] `https://tel.archives-ouvertes.fr/tel-03116774/document`
[4] `https://eprint.iacr.org/2021/046.pdf`

Useful Information

Presentations and working sessions will be held at the conference room of **Casa Iris Hotel** (`https://www.casa-iris.ro/facilitati.html`).

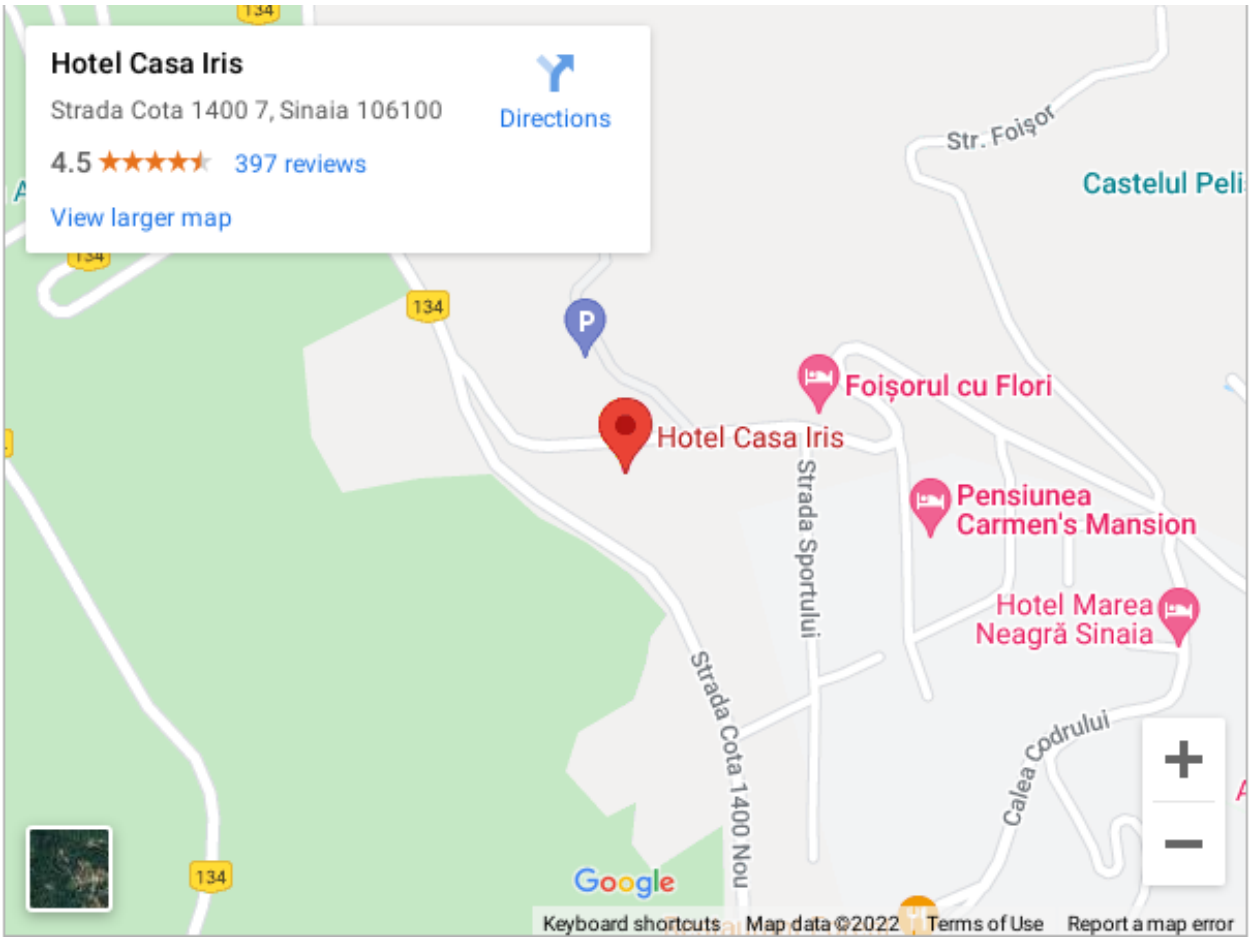
Coffee breaks and lunches will be offered in the hotel's restaurant `https://www.casa-iris.ro/facilitati.html`

Wi-Fi will be available during the conference.

How to get to the Casa Iris Hotel

Casa Iris is in Sinaia, 125 km North of Bucharest, on Valea Prahovei, one of the most visited place in Romania.

- **Address:** Drumul Cota 1400 nr.7, Sinaia, Prahova, Romania
- **Site:** `https://www.casa-iris.ro/`


Hotel Casa Iris
Strada Cota 1400 7, Sinaia 106100
4.5
397 reviews
Directions
View larger map
Str. Foișor
Castelul Peli
134
P
Foișorul cu Flori
Hotel Casa Iris
Strada Sportului
Pensiunea Carmen's Mansion
Hotel Marea Neagră Sinaia
Strada Cota 1400 Nou
Calea Codrului
Google
Keyboard shortcuts
Map data ©2022
Terms of Use
Report a map error

Once arrived in Sinaia, you can get the Hotel by bus, on the yellow, orange or green route and stop at *Piateta Foisor* bus station: