ERCIM Alain Bensoussan Fellowship Programme

ABCDE

MARIE CURIE ACTIONS

Scientific Report

First name / Family name	Dr. Dimitrios Simos
Nationality	Greek
Name of the *Host Organisation*	INRIA Paris-Rocquencourt
First Name / family name of the *Scientific Coordinator*	Dr. Nicolas Sendrier
Period of the fellowship	01/03/2012 to 28/02/2013

I – SCIENTIFIC ACTIVITY DURING YOUR FELLOWSHIP

The first period of the ERCIM fellowship was within Project-Team SECRET of INRIA Paris-Rocquencourt, located in France. SECRET Team is a follow-up of CODES research-team since January 1st, 2008. The team is led by senior researchers, Dr. Anne Canteaut who serves as the head of the team and Dr. Nicolas Sendrier which is the vice-leader of the team and also was the scientific coordinator and (principal) collaborator during my fellowship.

I am especially grateful, to the hospitality of the team, and in particular to the friendly and family spirit that enables junior researchers, as myself, to be entirely devoted on their line of research interests.

My research work within SECRET team was mostly devoted in the design and analysis of cryptographic algorithms, especially through the study of the involved discrete structures. In particular, my research was primarily focused on the field of code-based cryptography. In this application-domain of cryptography the cryptographic primitives studied exploit some problems coming from coding theory and they provide a good alternative to the commonly used systems based on number theory. These are usually named post-quantum cryptosystems since they would not be broken by the coming up of the quantum computer.

The security of code-based cryptosystems is based on decoding and structural attacks. Our research was focused on the latter attacks, which are based on the idea of an adverdsary trying to distinguish the given code (public-key) from a random code. This idea can be formulated as an instance of the **code equivalence problem**, that is given generator matrices of two linear codes, to decide whether or not these are equivalent over a finite field. The computational version of the later problem is to recover the equivalence transformation. More specifically, our efforts were concentrated on a generalization of the support-splitting algorithm (SSA), originally developed by Nicolas Sendrier, which in practice solves the code equivalence problem in time polynomial for all but an exponentially small proportion of the instances when the code alphabet is the binary field. In the case of non-binary fields we successfully extended SSA for the ternary and quaternary field, and similarly solve all but an exponentially small proportion of the instances in polynomial time. However, for any finite field with more than five elements, the computational and the decisional problem seems to be intractable for almost all instances [3,5].

The latter results, appear to have an impact on the design of zero-knowledge protocols in code-based cryptography. In particular, Girault's zero-knowledge protocol was severely weakened and could no longer be used with random codes in the binary case. We repaired Girault's zero-knowledge protocol when the finite fields has more than five elements and showed that random codes are again a viable option. Moreover, the context of the framework built in recent papers related to coding theory and quantum mechanics suggest that codes with large automorphism groups resist quantum Fourier sampling over the binary field. We also examined whether it is possible to extend these results, for non-binary fields [4].

The research activity described so far, was in accordance with work package 1 of the ERCIM training programme and the related results have been published in [3,4,5].

Moreover, I have worked on extending and publishing some results of my PhD research, related to symmetric cryptography [1,2] and secret-sharing cryptography [6]. This research fell within scope of the work package 2 of the ERCIM training programme.

During my ERCIM fellowship, I was a member of the **editorial board** of three international peer-reviewed journals,

- Applied Mathematics & Information Sciences (AMIS)
- International Journal of Contemporary Advanced Mathematics (IJCM)
- Information Sciences Letters (ISL)

and on the basis of my publications, I was also named a **Fellow of the Institute of Combinatorics and its Applications (FTICA)** on March, 2012.
In addition, I have been involved in the organization and/or program committee of several international scientific events:

- **International Program Committee (IPC) Member**. *The International Workshop on "Nature-Inspired Computing and Metaheuristics for Web Intelligence"*, December 4-7, 2012, Venetian, Macau, China
- **Program Committee (PC) Member.** *The 7th International Conference on "Availability, Reliability and Security" (ARES '12)*, University of Economics, August 20-24, 2012, Prague, Czech Republic.
- **Program Committee (PC) Chair.** *The 1s International Workshop on "Modern Cryptography and Security Engineering" (MoCrySEn '12),* University of Economics, August 20-24, 2012, Prague, Czech Republic.
- **Program Committee (PC) Member.** *The 1st International Workshop on "Security of Mobile Applications" (IWSMA '12),* University of Economics, August 20-24, 2012, Prague, Czech Republic.

In particular, MoCrySEn workshop was a joint initiative between SECRET team and SBA Research institute (the second host of the ERCIM fellowship) to encourage collaboration between hosts (related to work package 3 of the ERCIM training programme) and aimed to bring together researchers working in theoretical aspects of modern cryptography with proffesionals working on applied aspects of security engineering. The workshop was organized with the assistance of SBA Research and the invited speaker, was Nicolas Sendrier from SECRET team. Finally, a second workshop is planned on September, 2013.

II – PUBLICATION(S) DURING YOUR FELLOWSHIP

In total, the first period of the ERCIM fellowship at INRIA has led to 5 scientific publications, including 2 journal papers, 1 workshop paper and 2 extended abstracts. One additional submission is currently under review, and one more is in preparation.

Journal Papers

[1] Christos Koukouvinos and **Dimitris E. Simos**. ``Encryption schemes based on Hadamard matrices with circulant cores." to appear in *J. Appl. Math & Bioinformatics*.

Abstract: *In this paper, we propose two encryption schemes based on Hadamard matrices with one and two circulant cores, which are classes of combinatorial designs. A cryptanalysis of the proposed schemes against some popular attacks, brute force, plaintext attacks and ciphertext attacks is explored and our study shows that these attacks does not compromise the security of the system. Furthermore, we make use of the Kronecker product to strengthen our encryption schemes while maintaining the private key size in reasonable lengths.*

[2] Christos Koukouvinos and **Dimitris E. Simos**. ``Encryption schemes from Williamson matrices,” *J. Inf. Assur. Secur.*, vol. 7, pp. 252-258, 2012.

Abstract: *In this paper, we propose an encryption scheme based on the famous Williamson construction for Hadamard matrices. The proposed cipher belongs to the class of symmetric cryptography. A cryptanalysis of the proposed scheme against some popular attacks, such as plaintext attacks and ciphertext attacks is explored and our study shows that these attacks does not compromise the security of the system. Furthermore, we make use of the Kronecker product to strengthen the proposed cipher while maintaining the private key size in reasonable lengths.*

Conference & Workshop Papers

[3] Nicolas Sendrier and **Dimitris E. Simos**, “How easy is code equivalence over $\mathbb{F}_q$?,” to appear in *WCC '13: Proceedings of the 8th International Workshop on Coding and Cryptography*, Bergen, Norway, 2013.

Abstract: *The linear code equivalence problem is to decide whether two linear codes over $\mathbb{F}_{q}$ are identical up to a linear isometry of the Hamming space. The support splitting algorithm \cite{S2000:IEEE} runs in polynomial time for all but a negligible proportion of all linear codes, and solves the latter problem by recovering the isometry when it is just a permutation of the code support. While for a binary alphabet isometries are exactly the permutations, this is not true for $q\ge3$. We explore in this paper, a generalization of the support splitting algorithm where we aim to retrieve any isometry between equivalent codes. Our approach is twofold; first we reduce the problem of deciding the equivalence of linear codes to an instance of permutation equivalence. To this end, we introduce the notion of the closure of a code and give some of its properties. In the aftermath, we exhibit how this algorithm can be adapted for $q\in\{3,4\}$, where its complexity is polynomial for almost all of its instances. Although the aforementioned reduction seems attractive, when $q\ge 5$ the closure reduces the instances of the linear code equivalence problem to exactly those few instances of permutation equivalence that were hard for the support splitting algorithm. Finally, we argue that for $q \ge 5$ the linear code equivalence problem might be hard for almost all instances.*

Note: An extended journal version of this paper, is currently under preparation.

[4] Nicolas Sendrier and **Dimitris E. Simos**, “The hardness of code equivalence over $\mathbb{F}_q$ and its application to code-based cryptography,” submitted for publication.

Abstract: *The code equivalence problem is to decide whether two linear codes over $\mathbb{F}_{q}$ are identical up to a linear isometry of the Hamming space. In this paper, we review the hardness of code equivalence over $\mathbb{F}_q$ due to some recent negative results and argue on the possible implications in code-based cryptography. In particular, we present an improved version of the three-pass identification scheme of Girault and discuss on a connection between code equivalence and the hidden subgroup problem.*

Extended Abstracts

[5] Nicolas Sendrier and **Dimitris E. Simos**, “How easy is code equivalence over GF(q)?,” in *C2 '12: Abstracts of Presentations of Journees Codage et Cryptographie*, Dinard, France, 2 pg., 2012.

[6] Dimitris E. Simos and Zlatko Varbanov, “MDS codes, NMDS codes and their secret-sharing schemes,” in *ACA '12: Abstracts of Presentations of the 18th International Conference on Applications of Computer Algebra*, Sofia, Bulgaria, 2 pg., 2012.

III – ATTENDED SEMINARS, WORKHOPS, CONFERENCES

During the first period of the ERCIM fellowship at INRIA, I have participated in the following conferences, workshops and seminars as a contributed or invited speaker.

Conferences & Workshops

- **Contributed Talk.** “How easy is code equivalence over GF(q)?”, *Journees Codage et Cryptographie (C2 ‘12)*, Manoir de la Vicomte, October 7-12, 2012, Dinard, France (**Note**: joint work with Nicolas Sendrier).
- **Contributed Talk.** “The support-splitting algorithm and its application to code-based cryptography”, *Code-based Cryptography Workshop (CBC ‘12)*, Technical University of Denmark, May 9-11, 2012, Lyngby, Denmark (**Note**: joint work with Nicolas Sendrier)
- **Invited Talk.** “Families of block ciphers from combinatorial designs”, *Colloquium in “Cryptography and its Applications in the Armed Forces” (CAIAF ‘12)*, Hellenic Military Academy (HMA) “Evelpidon”, April 6, 2012, Vari, Greece (**Note**: joint work with Christos Koukouvinos)

Seminars

- **Invited Talk.** “Symbolic computation for orthogonal designs”, *PolSys Seminar*, LIP6, Universite Pierre et Marie Curie 06 (UPMC), February 15, 2013, Paris, France (**Note**: joint work with Christos Koukouvinos and Zafeirakis Zafeirakopoulos)
- **Invited Talk.** “On the hardness of code equivalence over $\mathbb{F}_q$”, *Combinatorics and Algorithms Seminar,* LITIS, University of Rouen, Campus du Madrillet, February 14, 2013, Rouen, France (**Note**: joint work with Nicolas Sendrier)
- **Participant.** *ERCIM ABCDE Seminar II*, INRIA Sophia-Antipolis, October 24-25, 2012, Alpes-Maritimes, France

IV – RESEARCH EXCHANGE PROGRAMME (REP)

N/A.