Scientific Report

First name / Family name	Dr. Dimitrios Simos
Nationality	Greek
Name of the *Host Organisation*	SBA Research
First Name / family name of the *Scientific Coordinator*	Dr. Edgar Weippl
Period of the fellowship	01/03/2013 to 28/02/2015

I – SCIENTIFIC ACTIVITY DURING YOUR FELLOWSHIP

The second period of the ERCIM fellowship was within SBA Research, located in Austria. SBA Research is aresearch center for IT-Security founded by the Vienna University of Technology, Graz University of Technology and University of Vienna. In its second research phase from 2010 to 2017, the Vienna University of Economics and Business has joined the center as a fourth full academic partner. SBA Research aims to become the premiere research center for IT security in Austria. SBA Research brings together the best national academic institutions and corporations and cooperates with leading universities and research institutions in our field of expertise all over the world. Its research addresses large corporations as well as small and medium-sized enterprises and private individuals. The research center is led by Dr. Edgar Weippl which is also the scientific coordinator for the ERCIM fellowship.

I am especially grateful, to the hospitality of the researchers and all administrative personnel of SBA Research, and in particular to the friendly and family spirit that enables researchers, as myself, to be entirely devoted on their line of research interests. The institute offers certain lines of flexibility to forge your own path in academia or industry.
My line of research within SBA Research was mostly devoted on the application of discrete mathematics to the various application domains of information security. It was an extremely productive period as it has matured me to a level that I am currently a principal researcher within the same institute continuing and expanding the projects I have sought as part of the original ERCIM project with SBA Research.
In particular, my theoretical background on discrete mathematics, and especially on combinatorial designs and codes gave me the opportunity to bridge two very different fields of research: fundamental mathematics with information security. I have devoted most of my time during the past two years of the ERCIM fellowship at SBA Research on modelling and optimizing software testing procedures via combinatorial designs, a field that is known as combinatorial testing. The latter field, is focused on the reduction of the test suite sizes while at the same time being able to reveal flaws or errors that depend on a few parameters of the system under test. I have achieved pioneering results in the field of penetration testing, a subdomain of software testing, where in particular the mathematical constructs managed to reveal security flaws in various cases of web application security [5,6,7,8,15] as well as kernel software [9]. As part of an ERCIM expert group on security and privacy. I have also initiated a large scale testing of the W3C portal with great success[1]. Within this activity, I initiated various collaborations with prestigious institutes, such as IST/ TU Graz and US NIST. In particular, these two institutes are currently supporting my vision for combinatorial security testing which I currently pursue at SBA Research.
At the same time, I have published many results on the theoretical analysis and construction of combinatorial designs [1,2,3,4,14] that subsequently were used to the application domains of software testing. Moreover, due to my experience from the first period of the ERCIM fellowship, at the cryptographic team of INRIA/SECRET I have been involved in various activities for evaluating the correctness of industrial patents and prototypes for cloud computing and mobile banking [12, 16]. In this domain, I have also researched authentication methods with QR codes and how these benefit from visual cryptography schemes [10]. Last but not least, I have achieved some results on database reduction using combinatorial designs [11]. Finally, some papers from the first ERCIM period were published on post-quantum cryptography [13].

[1] http://www.w3.org/blog/2014/12/rxss-security-audit-results/

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:

- **ESORICS2015 Program Committee (PC) Member**. The 20th European Symposium on *"Research in Computer Security"*, Vienna University of Technology, Vienna, September 21–25, 2015, Austria
- **BalkanCryptSec2015 Program Committee (PC) Member**. The 2nd Annual International Conference on *"Cryptography and Information Security",* University of Primorska, Koper, September 3–4, 2015, Slovenia
- **AReS2015 Program Committee (PC) Member**. The 10th International Conference on *"Availability, Reliability and Security"* Universite Paul Sabatier, Toulouse, August 24–28, 2015, France
- **IWCT2015 Program Committee (PC) Member**. The 4th International Workshop on *"Combinatorial Testing"* Graz University of Technology, Graz, April 13, 2015, Austria
- **BalkanCryptSec2014 Program Committee (PC) Member**. The 1st Annual International Conference on *"Cryptography and Information Security"* Istanbul Technical University, Istanbul, October 16–17, 2014, Turkey
- **AReS2014 Program Committee (PC) Member**. The 9th International Conference on *"Availability, Reliability and Security"* University of Fribourg, Fribourg, September 8–12, 2014, Switzerland
- **OPTI2014 Co-Organizer**. Minisymposium on *"Metaheuristic Algorithms for Combinatorial Problems and Engineering Applications"* International Conference on Engineering and Applied Sciences Optimization, Kos Island, June 4–6, 2014, Greece
- **IWSMA2014 Program Committee (PC) Member**. The 3rd International Workshop on *"Security of Mobile Applications"* University of Fribourg, Fribourg, September 8–12, 2014, Switzerland
- **MoCrySEn2013 Workshop Chair**. The 2nd International Workshop on *"Modern Cryptography and Security Engineering"* University of Regensurg, Regensburg, September 2–6, 2013, Germany
- **AReS2013 Program Committee (PC) Member**. The 8th International Conference on *"Availability, Reliability and Security"* University of Regensurg, Regensburg, September 2–6, 2013, Germany

In particular, MoCrySEn workshop was a joint initiative between INRIA/SECRET team (the first host of the ERCIM fellowship) and SBA Research institute to encourage collaboration between hosts 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 program co-chairs, were Nicolas Sendrier from SECRET team and Edgar Weippl from SBA Research.

II – PUBLICATION(S) DURING YOUR FELLOWSHIP

In total, the second period of the ERCIM fellowship at SBA Research has led to 16 scientific publications, including 1 book chapter, 2 journal papers, 10 conference and workshop papers and 3 extended abstracts. One additional submission is currently under review, and three more are in preparation.

Book Chapters

[1] D. E. Simos, "Genetic algorithms for the construction of 2^2 and 2^3-level response surface designs," in *OPT-i '14: Engineering and Applied Sciences Optimization, Computational Methods in Applied Sciences*, vol. 1, pp. xx–xx, 2015

Journal Papers

[2] C. Parpoula, C. Koukouvinos, D. E. Simos, and S. Stylianou, "Supersaturated plans for variable selection in large databases," *Stat., Optim. Inf. Comput.*, vol. 2, pp. 161–175, 2014.

[3] P. Angelopoulos, C. Koukouvinos, D. E. Simos, and A. Skountzou, "Mixed-level response surface designs via a hybrid genetic algorithm," *J. Stat. Appl. Pro.*, vol. 2, pp. 1–7, 2013.

Conference and Workshop Papers

[4] I. Kotsireas, T. Kutsia, and D. E. Simos, "Constructing orthogonal designs in powers of two: Groebner bases meet equational unification," in *RTA '15: Prooceedings of the 26th International Conference on Rewriting Techniques and Applications*, pp. xx–xx, 2015.

[5] J. Bozic, B. Garn, D. E. Simos, and F. Wotawa, "Evaluation of the ipo-family algorithms for test case generation in web security testing," in *IWCT '15: Proceedings of the 4th International Workshop on Combinatorial Testing, collocated with ICST '15: 8th IEEE International Conference on Software Testing, Verification and Validation, pp. xx–xx, 2015.*

[6] B. Garn, I. Kapsalis, D. E. Simos, and S. Winkler, "On the applicability of combinatorial testing to web application security testing: A case study," in *JAMAICA 14: Proceedings of the 2nd International Workshop on Joining AcadeMiA and Industry Contributions to Test Automation and Model-based Testing, collocated with ISSTA '14: International Symposium on Software Testing and Analysis, ACM*, pp. 16–21, 2014.

[7] J. Bozic, D. E. Simos, and F. Wotawa, "Attack pattern-based combinatorial testing," in *AST '14: Proceedings of the 9th International Workshop on Automation of Software Test, collocated with ICSE '14: 36th ACM/IEEE International Conference on Software Engineering, ACM*, pp. 1–7, 2014.

[8] A. Bernauer, J. Bozic, D. E. Simos, S. Winkler, and F. Wotawa, "Retaining consistency for knowledge-based security testing," in *IEA/AIE '14: Proceedings of the 27th International Conference on Industrial, Engineering & Other Applications of Applied Intelligent Systems, Lecture Notes in Computer Science*, vol. 8482, pp. 88–97, 2014.

[9] B. Garn and D. E. Simos, "Eris: A tool for combinatorial testing of the linux system

call interface," in *IWCT '14: Proceedings of the 3rd International Workshop on Combinatorial Testing,collocated with ICST '14: 7th IEEE International Conference on Software Testing, Verificationand Validation*, pp. 58–67, 2014.

[10] S. Falkner, P. Kieseberg, D. E. Simos, C. Traxler, and E. Weippl, "E-voting authentication with QR-codes," in *HAS '14: Proceedings of the 2nd International Conference on Human Aspects of Information Security, Privacy, and Trust, collocated with HCI '14: 16th International Conference on Human-Computer Interaction, Lecture Notes in Computer Science*, vol. 8533, pp. 149–159, 2014.

[11] C. Koukouvinos, C. Parpoula, and D. E. Simos, "Genetic algorithm and data mining techniques for design selection in databases," in *RAMSS '13: Proceedings of the 1st International Workshop on Statistical Methods in Reliability Assessment of Complex Industrial Multi-state Systems,collocated with ARES '13: 8th International Conference on Availability, Reliability and Security*, pp. 743–746, 2013.

[12] A. Hudic, E. Revell, and D. E. Simos, "A generation method of cryptographic keys for enterprise communication systems," in *FARES '13: Proceedings of the 8th International Workshop on Frontiers in Availability, Reliability, and Security, collocated with ARES '13: 8th International Conference on Availability, Reliability and Security*, pp. 406–411, 2013.

[13] N. Sendrier and D. E. Simos, "The hardness of code equivalence over F*q* and its application to code-based cryptography," in *PQCrypto '13: Proceedings of the Fifth International Conference on Post-Quantum Cryptography, Lecture Notes in Computer Science*, vol. 7932, pp. 203–216, 2013.

Extended Abstracts

[14] C. Koukouvinos, D. E. Simos, and Z. Zafeirakopoulos, "A grobner bases method for complementary sequences," in *ACA '13: Book of Proceedings of the 19th Conference on Applications of Computer Algebra*, pp. 255–259, 2013.

[15] D. E. Simos and S. Winkler, "An approach to penetration testing via combinational designs,"in *ASQT '13: Proceedings of the 11th User Conference for Software Quality, Test and Innovation, Austrian Computer Society (OCG), to appear*.

[16] A. Hudic, E. Revell, and D. E. Simos, "A custom classification of communication flow in a client-server model," in *ASQT '13: Proceedings of the 11th User Conference for Software Quality,Test and Innovation, Austrian Computer Society (OCG), to appear*.

III – ATTENDED SEMINARS, WORKHOPS, CONFERENCES

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

Conferences and Workshops

Presentation, Analysis of Quantum Bit Error Estimation with Different Combinatorial

Designs**.** 4th International Conference on Quantum Cryptography (QCRYPT), Telecom ParisTech, September 1–5, 2014, Paris, France

Contributed Talk, On the Applicability of Combinatorial Testing to Web Application Security Testing: A Case Study**.** 2nd workshop on Joining AcadeMiA and Industry Contributions to Test Automation and Model-based Testing (JAMAICA). International Symposium on Software Testing and Analysis (ISSTA), Hilton San Jose, July 21–25, 2014, Bay Area, California, USA

Contributed Talk, E-voting Authentication with QR-Codes**.** 2nd International Conference on Human Aspects of Information Security, Privacy and Trust (HAS), Creta Maris, June 22–27, 2014, Heraklion, Crete, Greece

Lightning Talk, Combinatorial Testing for Web Application Security**.** IMPACT event SBA Research, May 22, 2014, Vienna, Austria

Contributed Talk, An Approach to Penetration Testing via Combinatorial Designs**.** 11th User Conference for Software Quality, Test and Innovation (ASQT), Technical University of Graz, September 19–20, 2013, Graz, Austria

Contributed Talk, Genetic Algorithm and Data Mining Techniques for Design Selection in Databases**.** 1st International Workshop on Statistical Methods in Reliability Assessment of Complex Industrial Multi-state Systems (RAMSS), University of Regensburg, September 2, 2013, Regensburg, Germany

Contributed Talk, The Hardness of Code Equivalence over F*q* and its Application to Code-based Cryptography**.** 5th International Conference on Post-Quantum Cryptography (PQCrypto), Xlim, June 4–7, 2013, Limoges, Haute-Vienne, France

Contributed Talk, How Easy is Code Equivalence over F*q*?**.** 8th International Workshop on Coding Theory and Cryptography (WCC), Grand Terminus, April 14–19, 2013, Bergen, Norway

Invited Talk, The Mathematics behind an Automated Penetration Testing Framework**.** Security Forum Hagenberg 2014, University of Applied Sciences Upper Austria, April 9, 2014, Hagenberg Campus, Austria

Seminars

Presentation, Position Statement on Automotive Security and Security Testing**.** ERCIM Expert Group Meeting on Security & Privacy, Wroclaw University of Technology, September 9, 2014, Wroclaw, Poland

Presentation, Recent Results and Related Problems for Code-based and Secret-Sharing Cryptography**. C**ryptography Meeting (Kryptostammtisch), Austrian Computer Society (OCG), October 11, 2013, Vienna, Austria

Invited Talk, An Overview of Code-based Cryptography**.** Cryptography Seminar, Austrian Institute of Technology (AIT), Safety and Security Department, Optical Quantum Technology Group, December 5, 2013, Vienna, Austria

Invited Talk, A Bird's-Eye View of Code-based Cryptography**.** Cryptography Seminar,

Institute for Applied Information Processing and Communications (IAIK), Technical University of Graz, September 18, 2013, Graz, Austria

Presentation, A Novel Approach to Automated Software Testing using Combinatorial Designs**.** Information Security Seminar, SBA Research, March 21, 2013, Vienna, Austria

IV – RESEARCH EXCHANGE PROGRAMME (REP)

N/A