Constantin Cătălin DRĂGAN

Address: LORIA,
Equipe Pesto,
Campus scientifique, BP 239,
Postal Cod 54506,
Vandoeuvre, France

Email: catalin.dragan@loria.fr
Skype: dragancc
Phone: (+33)646271189

Nationality: Romanian
Date of birth: 14.03.1986
Place of birth: Iaşi, Romania

Professional Experience

Post-Doc (Jan. 2017 – present)

INRIA, Delegation Centre Est, Nancy, France
Project: SPOOC – Automated security proofs of cryptographic protocols
Supervisor: Véronique Cortier

Post-Doc (Nov. 2014 – Dec. 2016)

Loria & CNRS, Delegation Centre Est, Nancy, France
Project: ProSecure – Provably secure systems: foundations, design, and modularity
Supervisor: Véronique Cortier

Collaborator Teaching Assistant (2011 – 2014)

Faculty of Computer Science, Alexandru Ioan Cuza University of Iaşi, Romania

Education

PhD in Computer Science (2010 – 2013)

Faculty of Computer Science, Alexandru Ioan Cuza University of Iaşi, Romania
PhD Thesis: "Security of Secret Sharing Schemes based on the Chinese Remainder Theorem."
Supervisor: Prof. Dr. Ferucio Laurentiu Tiplea
Diploma degree: excellent (*summa cum laude*)

Master in Software Engineering (2008 – 2010)

Faculty of Computer Science, Alexandru Ioan Cuza University of Iaşi, Romania
Master Thesis: "Secret Sharing Schemes. Interactive Management."
Supervisor: Prof. Dr. Ferucio Laurentiu Tiplea
Overall average grade (credit-weighted average): 9.33
Diploma degree: 10

Bachelor in Computer Science (2005-2008)

Faculty of Computer Science, Alexandru Ioan Cuza University of Iaşi, Romania
Undergraduate Thesis: "Cryptosystems based on lattice theory."
Overall average grade (credit-weighted average): 8.80
Diploma degree: 9.37

Teaching Experience:

Faculty of Computer Science, Alexandru Ioan Cuza University of Iasi, Romania

- Taught seminars on *Information Security* and *Introduction to Cryptography*

Relevant Skills

Experience with formal method tools:

- EasyCrypt

Foreign languages:

- Romanian – mother tongue • English –fluent • German –beginner • French–beginner.

Programming skills:

- C++ • Java

Research Interests

Formal verification of protocols and cryptographic primitives:

- Electronic Voting

Design and analysis of protocols

- Electronic Voting
- Secret Sharing Schemes
- Attribute-based Encryption

Applications of number theory in computer science

Hobbies:

- Reading: science fiction or/and fantasy books
- Travelling

References

Prof. Ferucio Laurenţiu ŢIPLEA, PhD
Faculty of Computer Science, Alexandru Ioan Cuza University of Iaşi, Romania
Email: adress available on request
Véronique Cortier, PhD
French National Scientific Research Center (CNRS), at the LORIA laboratory, Nancy, France
Email: adress available on request
Bogdan Warinschi, PhD
Computer Science Department, University of Bristol, United Kingdom
Email: adress available on request

List of publications

Most relevant:

- V. Cortier, **C.C. Drăgan**, F. Dupressoir, B. Schmidt, P-Y. Strub, B. Warinschi. *Machine-Checked Proofs of Privacy for Electronic Voting Protocols.* IEEE Sym. on Security and Privacy 2017

- V. Cortier, **C.C. Drăgan**, F. Dupressoir, P-Y. Strub, B. Warinschi. *Machine-Checked Proofs of Verifiability for Electronic Voting Protocols.* (in preparation)

- M. Barzu, F.L. Ţiplea, **C.C. Drăgan**. *Compact sequences of co-primes and their applications to the security of CRT-based threshold schemes*. Information Sciences, vol 240: 161-172, 2013.
    - DOI: dx.doi.org/10.1016/j.ins.2013.03.062

Journals:

- **C.C. Drăgan**, F.L. Ţiplea. *On the Asymptotic Idealness of the Asmuth-Bloom Threshold Secret Sharing Scheme*. Information Sciences (accepted in April 2017)

- **C.C. Drăgan**, F.L. Ţiplea. *Distributive Weighted Threshold Secret Sharing Schemes*. Information Sciences, vol 339: 85-97, 2016
    - DOI: dx.doi.org/10.1016/j.ins.2016.01.019
- F.L. Ţiplea, **C.C. Drăgan**. *A Necessary and Sufficient Condition for the Asymptotic Idealness of the GRS Threshold Secret Sharing Scheme*. Information Processing Letters, vol 114(6): 299-303, 2014.
    - DOI: dx.doi.org/10.1016/j.ipl.2014.01.008
- M. Barzu, F.L. Ţiplea, **C.C. Drăgan**. *Compact sequences of co-primes and their applications to the security of CRT-based threshold schemes*. Information Sciences, vol 240: 161-172, 2013.
    - DOI: dx.doi.org/10.1016/j.ins.2013.03.062

Conferences and Talks:

- V. Cortier, **C.C. Drăgan**, F. Dupressoir, B. Schmidt, P-Y. Strub, B. Warinschi. *Machine-Checked Proofs of Privacy for Electronic Voting Protocols.* IEEE Sym. on Security and Privacy 2017

- F.L. Ţiplea, **C. C. Drăgan**. *Key-policy Attribute-based Encryption for General Boolean Circuits from Bilinear Maps*, BalkanCryptSec 2014, LNCS 9024, pp 175-193.
    - DOI: dx.doi.org/ 10.1007/978-3-319-21356-9_12

- **C. C. Drăgan**, F.L. Ţiplea. *Key-Policy Attribute-Based Encryption for General Boolean Circuits from Secret Sharing and Multi-linear Maps,* BalkanCryptSec 2015, LNCS 9540, pp 112-133.
    - DOI: dx.doi.org/10.1007/978-3-319-29172-7_8

- **C. C. Drăgan**. *Interactive Secret Share Management*. SECRYPT 2009, International Conference on Security and Cryptography SECRYPT 2009, ed. E. Fernández-Medina, M. Malek and J. Hernando, pp. 266-269, Milan, Italy, 2009.

- **C.C. Drăgan**, F.L. Ţiplea. *CRT-based Secret Sharing Schemes: Design and Security*, BalkanCrypt Kickoff Meeting and Workshop, Sofia, Bulgaria, Nov. 2013
    - balkancrypt.uist.edu.mk

PhD Thesis:

- **C. C. Drăgan**. *Security of CRT-based Secret Sharing Schemes*. PhD thesis, Alexandru Ioan Cuza University of Iaşi, Romania, Department of Computer Science, Sept. 2013.
    - https://www.iacr.org/phds/index.php?p=detail&entry=981

DBLP

- http://dblp.uni-trier.de/pers/hd/d/Dragan:Constantin_Catalin