Benoît-Michel Cogliati

Cryptographer

Stuhlsatzenhaus 5, Saarland Informatics Campus
66123 Saarbrücken
Germany
☎ *+33 6 78 98 63 41*
✉ *benoit.cogliati@gmail.com*
benoitcogliati.bitbucket.io

Positions

2020– **Research Group Leader**, *CISPA Helmholtz Center for Information Security*, Saarbrücken, Germany.

2016–2019 **Postdoctoral researcher**, *University of Luxembourg*, Esch-sur-Alzette, Luxembourg.

2013–2016 **Ph.D. student**, *Versailles Saint-Quentin-en-Yvelines University*, Versailles, France.

Education

2013–2016 **Ph.D. in Computer Science**, *Versailles Saint-Quentin-en-Yvelines University*, Versailles, France.
Title: The Tweakable Even-Mansour construction: security proofs with the H-coefficients technique.
Supervision: Jacques Patarin.

2012–2013 **Master's degree in Mathematics**, *Versailles Saint-Quentin-en-Yvelines University*, Versailles, France.
Dissertation: Study of the indistinguishability of the XOR of multiple permutations.

Journal publications.

DCC **Multi-user security bound for filter permutators in the random oracle model**, *Designs, Codes and Cryptography*, to appear.
B. Cogliati, T. Tanguy.

DCC **Tweaking a Block Cipher: Multi-user Beyond-Birthday-Bound Security in the Standard Model**, *Designs, Codes and Cryptography*, 2018.
B. Cogliati.

DCC **Analysis of the Single-Permutation Encrypted Davies-Meyer Construction**, *Designs, Codes and Cryptography*, 2018.
B. Cogliati, Y. Seurin.

IACR ToSC **New Constructions of MACs from (Tweakable) Block Ciphers**, *IACR Transactions on Symmetric Cryptology*, 2017.
B. Cogliati, J. Lee, Y. Seurin.

Conference publications.

Crypto 2018 **Provable Security of (Tweakable) Block Ciphers Based on Substitution-Permutation Networks**.
B. Cogliati, Y. Dodis, J. Katz, J. Lee, J. Steinberger, A. Thiruvengadam, Z. Zhang.

FSE 2016 **Strengthening the Known-Key Security Notion for Block Ciphers**.
B. Cogliati, Y. Seurin.

Crypto 2016 **EWCDM: An Efficient, Beyond-Birthday Secure, Nonce-Misuse Resistant MAC**.
B. Cogliati, Y. Seurin.

Eurocrypt 2015 **On the Provable Security of the Iterated Even-Mansour Cipher against Related-Key and Chosen-Key Attacks**.
B. Cogliati, Y. Seurin.

Crypto 2015 **Tweaking Even-Mansour Ciphers**.
B. Cogliati, R. Lampe, Y. Seurin.

Asiacrypt 2015 **Beyond-Birthday-Bound Security for Tweakable Even-Mansour Ciphers with Linear Tweak and Key Mixing**.
B. Cogliati, Y. Seurin.

FSE 2014 **The Indistinguishability of the XOR of k Permutations**.
B. Cogliati, R. Lampe, J. Patarin.

SAC 2014 **Security Amplification for the Composition of Block Ciphers: Simpler Proofs and New Results**.
B. Cogliati, J. Patarin, Y. Seurin.

Seminars

2017 **Early Symmetric Crypto ESC 2017**, *Canach*, Luxembourg.

2016 **Dagstuhl Seminar 16021**, *Schloss Dagstuhl*, Germany.
Topic: authenticated encryption and Even-Mansour designs.

Supervision

2018 **Supervision of a Bachelor project (first year)**.
Topic: *Develop a tool that encrypts and hides data in PNG files.*

2017 **Supervision of an ENSEEIHT intern (Master I)**.
Topic: *Study of the FLIP family of stream ciphers.*

2017 **Supervision of a Bachelor project (first year)**.
Topic: *The AES Block Cipher.*

Teaching

2016–2019 **Teaching activity**, *University of Luxembourg*.
Courses: Introduction to Programming, Bachelor of Science and Engineering, first year (15 hours of lectures and practical exercises in 2016/2017).
Security I, Bachelor of Science and Engineering, second year (12 hours of lectures in 2018/2019 and 2019/2020).

2015–2016 **Optional teaching activity**, *Versailles Saint-Quentin-en-Yvelines University*.
64 hours of practical exercises.
Courses: Introduction to Cryptography, Master of Mathematics, first year.
Introduction to Programming, Bachelor of Science, first year.

2013–2014 **Optional teaching activity**, *Versailles Saint-Quentin-en-Yvelines University*.
64 hours of practical exercises.
Course: Introduction to Cryptography, Master of Mathematics, first year.

Dissemination

2016 **Researcher's Days**, *Esch-sur-Alzette*, Luxembourg.
Animation of a group activity about onion routing for children aged 8 to 18.