# Pascal JUNOD

*"I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me..."*

from *The Conscience of a Hacker* by The Mentor

## Personal Information

Born in Bienne (Switzerland) on November 14, 1976. Married, two children, Swiss citizen.

## Contact Information


| | |
|---|---|
| E-mail | pascal@junod.info |
| Web Page | crypto.junod.info |
| Twitter | @cryptopathe |
| LinkedIn | www.linkedin.com |

## Employment

| | |
|---|---|
| 2022 - | **Founder and Director** of modulo p SA, Switzerland |
| 2017 - | **External Lecturer**, at University of Applied Sciences and Arts Western Switzerland (HES-SO), Lausanne, Switzerland |
| 2017 - 2021 | **Senior Manager Security Technology**, at Snap Switzerland Sàrl, Yverdon-les-Bains, Switzerland |
| 2016 - 2021 | **Co-Founder and Chairman of the Board** of strong.codes SA, a startup active in the domain of software protection |
| 2008 - 2017 | **Full Professor** ("Professeur HES ordinaire") in the domain of information security, at HEIG-VD, a school of the University of Applied Sciences and Arts Western Switzerland (HES-SO), Yverdon-les-Bains, Switzerland |
| 2005 - 2008 | **Cryptography Expert**, at Nagravision SA (Kudelski Group), Cheseaux-sur-Lausanne, Switzerland |
| 2000 - 2005 | **Research and Teaching Assistant**, at the Security and Cryptography Laboratory (LASEC), École Polytechnique Fédérale de Lausanne (EPFL), Switzerland |
| 2000 | **Security Engineer**, at Europay AG, Wallisellen, Switzerland |

## Education

| | |
|---|---|
| 2012 | Teaching certificate delivered by the HES-SO (15 training days in the domain of university pedagogy) |
| 2000 - 2004 | PhD in Communication Systems at EPF Lausanne (Switzerland). Thesis: "*Statistical Cryptanalysis of Block Ciphers*", supervised by Prof. Serge Vaudenay |
| 2000 - 2001 | Pre-doctoral school, School of Communication and Computer Sciences, EPF Lausanne (Switzerland) |
| 1995 - 2000 | Master in Computer Science, ETH Zurich (Switzerland). Thesis: "*Linear Cryptanalysis of DES*", supervised by Prof. Ueli Maurer and Prof. Serge Vaudenay |

## Awards

| | |
|---|---|
| 2019 | IACR Test-of-Time Award for "*How Far Can We Go Beyond Linear Cryptanalysis*", presented at Asiacrypt'04 and co-written with Thomas Baignères and Serge Vaudenay |
| 2019 | Nominated as one of the 100 Swiss Digital Shapers for 2019. |
| 2016 | strong.codes SA nominated in the 2016 edition of the TOP100 Swiss startups ranking |
| 2016 | Venture Kick stage 2 won by strong.codes SA |
| 2015 | Venture Kick stage 1 won by strong.codes SA |
| 2005 | Best paper award for "*Distinguishing Attacks on T-Functions*", presented at Mycrypt'05 and co-written with Simon Künzli and Willi Meier |
| 2005 | Frost and Sullivan's *Excellence in Technology Award* for the IDEA-NXT block cipher, via MediaCrypt AG |

## PhD Thesis Committees

| | |
|---|---|
| 2017 | Pierre Lestringant, *Identification d'Algorithmes Cryptographiques dans du Code Natif*, Université de Rennes 1, Rennes (France). |
| 2017 | Ninon Eyrolles, *Obfuscation par Expressions Mixtes Arithmético-Booléennes : Reconstruction, Analyse et Outils de Simplification*, Université de Versailles Saint-Quentin-en-Yvelines, Versailles (France). |
| 2016 | Maxime Augier, *Trustworthy Cloud Storage*, École Polytechnique Fédérale, Lausanne (Suisse). |
| 2015 | Michel Dubois, *Analyse combinatoire des schémas de chiffrement par bloc et application à l'Advanced Encryption Standard*, École Polytechnique, Palaiseau (France). |
| 2013 | Christophe Grenier, *Confidential Title*, École Polytechnique, Palaiseau (France). |
| 2010 | Benoît Gérard, *Cryptanalyses Statistiques des Algorithmes de Chiffrement à Clef Secrète*, Université Pierre et Marie Curie, Paris (France). |
| 2009 | Francesco Regazzoni, *A Design Flow and Evaluation Framework for DPA-Resistant Embedded Systems*, Università della Svizzera italiana, Lugano (Switzerland). |

## Standardization

| | |
|---|---|
| 2005 - 2007 | Digital Video Broadcasting (DVB), Technical Module - Common Scrambling Algorithm (TM-CSA) |

# Research Projects

Grants: the first figure is the project overall budget; if available, the second one is the budget allocated to my research group.

| | |
|---|---|
| 2015-2017 | CRYPTACUS - *Cryptanalysis of Ubiquitous Computing Systems*. ICT COST Action IC1403 funded by the European Cooperation in Science and Technology. Representative of Switzerland and website manager. See www.cryptacus.eu. |
| 2015-2016 | FIT Grant Innovaud - *strong.codes* (CHF 150k/150k). **Principal investigator**. |
| 2013-2016 | H2B2VS - *HEVC Hybrid Broadcast Broadband Video Services*. Funded by the EUREKA-Celtic-Plus initiative (CHF 24.3M/325k), in cooperation with 19 partners in France, Switzerland, Spain, Finland and Turkey. |
| 2011-2014 | Obfuscator - *Exploring the Blind Spots of White-Box Adversaries*. Funded by the Hasler foundation (CHF 160k/80k), in cooperation with the BFH (Switzerland). **Principal investigator**. |
| 2010-2013 | QCRYPT - *Secure High-Speed Communication based on Quantum Key Distribution*. Funded by SNF Nano-Terra (CHF 4M/65k), and performed in cooperation with the University of Geneva, Id Quantique SA, EPF Lausanne, ETH Zürich and HES-SO. See www.nano-tera.ch. |
| 2011-2012 | Obfuscator - *Développement d'un Outil de Protection Logicielle*. Funded by HES-SO (CHF 161k/81k), and performed in cooperation with EIA-FR. **Principal Investigator**. |
| 2009-2010 | SwissQuantum - *Réseau Sécurisé avec des Clés Quantiques*. Funded by HES-SO, and performed in cooperation with the University of Geneva, Id Quantique SA, hepia and EIA-FR. |

Several confidential consulting mandates in the domain of cryptography and information security with both local and global companies.

## Academic Services

Program chair of the *Application Security Forum Western Switzerland (ASFWS)* in 2014.

Member of the program committees of IACR *Eurocrypt* in 2021 (area chair for real-world cryptography); *IEEE/ACM Workshop on Software Protection* in 2019, 2016 and 2015; *BlackAlps* in 2017; *GreHack* in 2017; IACR *Fast Software Encryption (FSE)* in 2016, 2012, 2011, 2008 and 2007; *LightSec* in 2016, 2015, 2014 and 2013; *Selected Areas in Cryptography (SAC)* in 2014, 2011, 2007 and 2006; *Application Security Forum Western Switzerland (ASFWS)* in 2012; IACR *Cryptographic Hardware and Embedded Systems (CHES)* in 2011; *Workshop on Coding and Cryptography (WCC)* in 2011; *Indocrypt*, in 2009; *SECRYPT*, in 2008 and 2007; *Africacrypt*, in 2008; *Vietcrypt*, in 2006.

Regular external reviewer for the *Journal of Cryptology*, the *European Transactions on Telecommunications*, *Theoretical Computer Science A*, the *IEEE Transactions on Information Theory*, the *IEEE Transactions on Dependable and Secure Computing*, *Designs, Codes and Cryptography*, *IET Information Security*, the *Signal Processing Journal*, the *Computer Journal*, the *Information Processing Letters*, the *Journal of Computational and Applied Mathematics*, *Discrete Applied Mathematics*, the *Journal of Systems and Software*, *Cryptography and Communications*, the *IEICE Transactions*, and the *Mathematical Reviews*, as well as for the *Crypto*, *Eurocrypt*, *Asiacrypt*, *FSE*, *PKC*, *CHES*, *SAC*, *RSA-CT*, *ACNS*, *ACM-CCS*, *IEEE ICC*, *IEEE Globecom*, *WISA*, *ICISC*, *ACISP*, *Cardis*, *Indocrypt*, *ISC*, *ISIT*, *ProvSec*, *WCC* conferences and workshops.

## Academic Impact Factor

| | |
|---|---|
| Citations count | **2156** |
| H-index | **20** |
| i10-index | **27** |

Data gathered through Google Scholar on June 16, 2022.

Most publications are available online as PDF files on my personnal website crypto.junod.info.

## Books

[B1] Gildas Avoine, Pascal Junod, Philippe Oechslin, and Sylvain Pasini. *Sécurité Informatique - Cours et Exercices Corrigés*. Vuibert, October 2015. Third edition.

[B2] Pascal Junod and Anne Canteaut, editors. *Advanced Linear Cryptanalysis of Block and Stream Ciphers*, volume 7 of *Cryptology and Information Security Series*. IOS Press, 2011.

[B3] Gildas Avoine, Pascal Junod, and Philippe Oechslin. *Sécurité Informatique - Cours et Exercices Corrigés*. Vuibert, 2010. Second edition.

[B4] Gildas Avoine, Pascal Junod, and Philippe Oechslin. *Computer Systems Security*. EPFL Press, 2007.

[B5] Thomas Baignères, Pascal Junod, Yi Lu, Jean Monnerat, and Serge Vaudenay. *A Classical Introduction to Cryptography - Exercise Book*. Springer-Verlag, 2006.

[B6] Gildas Avoine, Pascal Junod, and Philippe Oechslin. *Sécurité Informatique - Exercices Corrigés*. Vuibert, 2004. First edition.

[B7] Douglas R. Stinson. *Cryptographie: Théorie et Pratique*. Vuibert, 2003. French translation by Gildas Avoine, Pascal Junod and Serge Vaudenay.

## Publications in Journals

[J1] Jeremy Constantin, Raphaël Houlmann, Nicholas Preyss, Nino Walenta, Hugo Zbinden, Pascal Junod, and Andreas Burg. An FPGA-based 4 Mbps secret-key distillation engine for quantum key distribution systems. *Journal of Signal Processing Systems*, 86(1):1--15, January 2017.

[J2] Rodrigue Oeuvray and Pascal Junod. A practical approach to semideviation and its time scaling in a jump-diffusion process. *Quantitative Finance*, 15(5):809--827, 2015.

[J3] Nino Walenta, Andreas Burg, Dario Caselunghe, Jeremy Constantin, Nicolas Gisin, Olivier Guinnard, Raphael Houlmann, Pascal Junod, Boris Korzh, Natalia Kuleszaand Matthieu Legré, Charles Ci Wen Lim, Tommaso Lunghi, Laurent Monat, Christopher Portmann, Mathilde Soucarros, Patrick Trinkler, Gregory Trolliet, Fabien Vannel, and Hugo Zbinden. A fast and versatile QKD system with hardware key distillation and wavelength multiplexing. *New Journal of Physics*, 16(1):013047, 2014.

[J4] Damien Stucki, Matthieu Legré, François Buntschu, Christoph Clausen, Norbert Felber, Nicolas Gisin, Luca Henzen, Pascal Junod, Gérald Litzistorf, Patrick Monbaron, Laurent Monat, Jeff B. Page, Didier Perroud, Grégoire Ribordy, Alexis Rochas, Samuel Robyr, José Tavares, Rob Thew, Patrick Trinkler, Stefano Ventura, Raphaël Voirol, Nino Walenta, and Hugo Zbinden. Long term performance of the SwissQuantum quantum key distribution network in a field environment. *New Journal of Physics*, 13:123001, 2011.

[J5] Gildas Avoine, Pascal Junod, and Philippe Oechslin. Characterization and improvement of time-memory trade-off based on perfect tables. *ACM Transactions on Information and System Security*, 11(4):no 17, 2008.

## Publications in Peer-Reviewed Conferences

[C1] Benjamin Wesolowski and Pascal Junod. Ciphertext-policy attribute-based broadcast encryption scheme with small keys. In Soonhak Kwon and Aaram Yun, editors, *Information Security and Cryptology - ICISC 2015 - 18th International Conference, Seoul, South Korea, November 25-27, 2015, Revised Selected Papers*, volume 9558 of *Lecture Notes in Computer Science*, pages 53--68. Springer-Verlag, 2016.

[C2] Pascal Junod, Julien Rinaldini, Johan Wehrli, and Julie Michielin. Obfuscator-LLVM -- software protection for the masses. In Brecht Wyseur, editor, *Proceedings of the IEEE/ACM 1st International Workshop on Software Protection, SPRO'15, Firenze, Italy, May 19th, 2015*, pages 3--9. IEEE, 2015.

[C3] Hugo Zbinden, Nino Walenta, Olivier Guinnard, Raphael Houlmann, Charles Lim Ci Wen, Boris Korzh, Tommaso Lunghi, Nicolas Gisin, Andreas Burg, Jeremy Constantin, Matthieu Legré, Patrick Trinkler, Dario Caselunghe, Natalia Kulesza, Gregory Trolliet, Fabien Vannel, Pascal Junod, Olivier Auberson, Yoan Graf, Gilles Curchod, Gilles Habegger, Etienne Messerli, Christopher Portmann, Luca Henzen, Christoph Keller, Christian Pendl, Michael Mühlberghuber, Christoph Roth, Norbert Felber, Frank Gürkaynak, Daniel Schöni, and Beat Muheim. Continuous QKD and high speed data encryption. In *Proceedings of SPIE 8899, October 29, Dresden, Germany*, 2013.

[C4] Damien Stucki, Matthieu Legré, Laurent Monat, Samuel Robyr, Patrick Trinkler, Grégoire Ribordy, Rob Thew, Nino Walenta, Nicolas Gisin, François Buntschu, Didier Perroud, Gérald Litzistorf, Stefano Ventura, Pascal Junod, Raphaël Voirol, and Patrick Monbaron. Performance of the SwissQuantum network over 21 months. In *Proceedings of SPIE 8189, September 19, Prague, Czech Republic*, 2011.

[C5] Pascal Junod and Alexandre Karlov. An efficient public-key attribute-based broadcast encryption scheme allowing arbitrary access policies. In *Proceedings of the 10th ACM Workshop on Digital Rights Management (DRM 2010), October 4, 2010, Chicago, Illinois, USA*, pages 13--24, 2010.

[C6] Pascal Junod and Marco Macchetti. Revisiting the IDEA philosophy. In Orr Dunkelman, editor, *Fast Software Encryption, 16th International Workshop, FSE 2009, Leuven, Belgium, February 22-25, 2009, Revised Selected Papers*, volume 5665 of *Lecture Notes in Computer Science*, pages 277--295. Springer-Verlag, 2009.

[C7] Pascal Junod, Alexandre Karlov, and Arjen K. Lenstra. Improving the Boneh-Franklin traitor tracing scheme. In Stanislaw Jarecki and Gene Tsudik, editors, *Public Key Cryptography - PKC 2009, 12th International Conference on Practice and Theory in Public Key Cryptography, Irvine, CA, USA, March 18-20, 2009. Proceedings*, volume 5443 of *Lecture Notes in Computer Science*, pages 88--104. Springer-Verlag, 2009.

[C8] Graham Turner, Corinne Le Buhan Jordan, Robin Wilson, and Pascal Junod. The influence of network evolution, cryptography advances, and the need for flexible entitlement models in DCAS design. In *Proceedings of the 58th Annual IEEE Broadcast Symposium, Alexandria, VA, USA*. IEEE, 2008.

[C9] Gildas Avoine, Pascal Junod, and Philippe Oechslin. Time-memory trade-offs: False alarm detection using checkpoints. In Subhamoy Maitra, C. E. Veni Madhavan, and Ramarathnam Venkatesan, editors, *Progress in Cryptology - INDOCRYPT 2005, 6th International Conference on Cryptology in India, Bangalore, India, December 10-12, 2005, Proceedings*, volume 3797 of *Lecture Notes in Computer Science*, pages 183--196. Springer-Verlag, 2005.

[C10] Simon Künzli, Pascal Junod, and Willi Meier. Distinguishing attacks on T-functions. In Ed Dawson and Serge Vaudenay, editors, *Progress in Cryptology - Mycrypt 2005, First International Conference on Cryptology in Malaysia, Kuala Lumpur, Malaysia, September 28-30, 2005, Proceedings*, volume 3715 of *Lecture Notes in Computer Science*, pages 2--15. Springer-Verlag, 2005.

[C11] Pascal Junod. New attacks against reduced-round versions of IDEA. In Henri Gilbert and Helena Handschuh, editors, *Fast Software Encryption: 12th International Workshop, FSE 2005, Paris, France, February 21-23, 2005, Revised Selected Papers*, volume 3557 of *Lecture Notes in Computer Science*, pages 384--397. Springer-Verlag, 2005.

[C12] Thomas Baignères, Pascal Junod, and Serge Vaudenay. How far can we go beyond linear cryptanalysis? In Pil Joong Lee, editor, *Advances in Cryptology - ASIACRYPT 2004, 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, December 5-9, 2004, Proceedings*, volume 3329 of *Lecture Notes in Computer Science*, pages 432--450. Springer-Verlag, 2004.

[C13] Pascal Junod and Serge Vaudenay. FOX: a new family of block ciphers. In Helena Handschuh and M. Anwar Hasan, editors, *Selected Areas in Cryptography, 11th International Workshop, SAC 2004, Waterloo, Canada, August 9-10, 2004, Revised Selected Papers*, volume 3357 of *Lecture Notes in Computer Science*, pages 114--129. Springer-Verlag, 2004.

[C14] Pascal Junod and Serge Vaudenay. Perfect diffusion primitives for block ciphers -- building efficient MDS matrices. In Helena Handschuh and M. Anwar Hasan, editors, *Selected Areas in Cryptography, 11th International Workshop, SAC 2004, Waterloo, Canada, August 9-10, 2004, Revised Selected Papers*, volume 3357 of *Lecture Notes in Computer Science*, pages 84--99. Springer-Verlag, 2004.

[C15] Pascal Junod. On the optimality of linear, differential, and sequential distinguishers. In Eli Biham, editor, *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*, volume 2656 of *Lecture Notes in Computer Science*, pages 17--32. Springer-Verlag, 2003.

[C16] Pascal Junod and Serge Vaudenay. Optimal key ranking procedures in a statistical cryptanalysis. In Thomas Johansson, editor, *Fast Software Encryption, 10th International Workshop, FSE 2003, Lund, Sweden, February 24-26, 2003, Revised Papers*, volume 2887 of *Lecture Notes in Computer Science*, pages 235--246. Springer-Verlag, 2003.

[C17] Pascal Junod. On the complexity of Matsui's attack. In Serge Vaudenay and Amr M. Youssef, editors, *Selected Areas in Cryptography, 8th Annual International Workshop, SAC 2001 Toronto, Ontario, Canada, August 16-17, 2001, Revised Papers*, volume 2259 of *Lecture Notes in Computer Science*, pages 199--211. Springer-Verlag, 2001.

## Patents

[P1] Pierre Sarda and Pascal Junod. Management of broadcast encrypted digital multimedia data receivers. EP/15169696, May 2015.

[P2] Pascal Junod. Method for generating software code. EP/20100162997, May 2010.

[P3] Pascal Junod and Alexandre Karlov. Method for public-key attribute-based encryption with respect to a conjunctive logical expression. WO/2011/061285, November 2009.

[P4] Pascal Junod. Method for authenticating access to a secured chip by a test device. WO/2010/130709, May 2009.

[P5] Alexandre Karlov and Pascal Junod. Method to enforce by a management center the access rules for a broadcast product. WO/2010/031781, September 2008.

[P6] Pascal Junod and Olivier Brique. Method for updating security data in a security module and security module for implementing this method. EP 2129115, May 2008.

[P7] Alexandre Karlov and Pascal Junod. Method to generate a private key in a Boneh-Franklin scheme. WO/2009/071639, December 2007.

[P8] Alexandre Karlov and Pascal Junod. Method to trace traceable parts of original private keys in a public-key cryptosystem. WO/2009/080683, December 2007.

[P9] Pascal Junod, Alexandre Karlov, and Nicolas Fischer. System for traceable decryption of bandwidth-efficient broadcast of encrypted messages and security module revocation method used for securing broadcasted messages. US 8548167, August 2006.

[P10] Pascal Junod. Method of revocation of security modules used to secure broadcast messages. WO/2008/020041, August 2006.

[P11] Thierry Lelégard and Pascal Junod. Method for encrypting and decrypting a conditional access content. WO/2007/068720, December 2005.

[P12] Pascal Junod and Serge Vaudenay. Method for generating pseudo-random sequence. WO/2005/025123, September 2003.

[P13] Pascal Junod and Serge Vaudenay. Device and method for encrypting and decrypting a block of data. WO/2004/105305, May 2003.

## ≺ Reports ≻

[R1] Jean-Philippe Aumasson, Steve Babbage, Daniel J. Bernstein, Carlos Cid, Joan Daemen, Orr Dunkelman, Kris Gaj, Shay Gueron, Pascal Junod, Adam Langley, David McGrew, Kenny Paterson, Bart Preneel, Christian Rechberger, Vincent Rijmen, Matt Robshaw, Palash Sarkar, Patrick Schaumont, Adi Shamir, and Ingrid Verbauwhede. Challenges in authenticated encryption. Technical report, ECRYPT - CSA, 2017.

## ≺ Vulgarization ≻

[V1] Pascal Junod. Cryptographie et standardisation. *Market.ch*, December 2009.

[V2] Pascal Junod. Les fonctions de hachage sortiraient-elles de l'ombre ? *Multi-System and Internet Security Cookbook (MISC)*, 18, March-April 2005.

[V3] Pascal Junod and Frédéric Raynal. Dix dangers qui guettent le programmeur de cryptographie. *Multi-System and Internet Security Cookbook (MISC)*, 12, March-April 2004.

[V4] Pascal Junod. Problèmes d'implémentation de la cryptographie: les attaques par effet de bord. *Multi-System and Internet Security Cookbook (MISC)*, 4, November-December 2002.

[V5] Gildas Avoine and Pascal Junod. PGP: Comment éviter les mauvaises surprises ? *Multi-System and Internet Security Cookbook (MISC)*, 3, July 2002.

[V6] Pascal Junod. Six façons différentes de casser DES. *Flash Informatique Spécial Été EPFL*, 2000.

## ≺ Theses ≻

[T1] Pascal Junod. *Statistical Cryptanalysis of Block Ciphers*. PhD thesis, École Polytechnique Fédérale de Lausanne (EPFL), Switzerland, 2005. No 3179.

[T2] Pascal Junod. *Linear Cryptanalysis of DES*. Master Thesis, Eidgenössische Technische Hochschule (ETH) Zürich, Switzerland, Computer Science Department, 2000.

---

## ≺ Invited Talks ≻

2017 *Confessions d'un Cyber-Serrurier*, Association Vaudoise des Banques, November 2nd, 2017, Lausanne-Palace, Lausanne (Switzerland)

2016 *Towards Developer-Proof Cryptography*, Summer Research Institute, June 20th, 2016, School of Computer and Communication Sciences, EPFL, Lausanne (Switzerland)

2016 *Secure Software Development and Beyond*, Fri Software Days, February 1st, 2016, Fribourg (Switzerland)

2015 *The Long Journey from Papers to Software: Crypto APIs*, IACR Cryptology School on Design and Security of Cryptographic Algorithms and Devices, October 23rd, 2015, Chia, Sardinia (Italy)

2015 *A Secure Development Lifecycle*, DEVCON 2015, October 6th, 2015, European Broadcasting Union (EBU), Geneva, (Switzerland)

2015 *SSL/TLS: Still Alive?*, Tech Meetings, Colab, March 27th, Fribourg (Switzerland)

2014 *Cyber-Sécurité en 2014: Bienvenue au Far-West!*, Keynote, InnovaudConnect@AppSec, November 5th, Yverdon-les-Bains (Switzerland)

2013 *LLVM and Code Obfuscation*, Université Catholique de Louvain, June 26th, Louvain-la-Neuve (Belgium)

2013 *Playing Hide-and-Seek with Hash-DoS*, Insomni'Hack 2013, March 22nd, Geneva (Switzerland)

2011 *Bridging Theory and Practice in Cryptography*, ECRYPT Workshop on Lightweight Cryptography, November 28-29, Louvain-la-Neuve (Belgium)

2011 *Advanced Block Cipher Design*, ECRYPT II Summer School, May 31st, Albena (Bulgaria)

2011 *Cryptography: How to Break it in Practice if you Must ?*, Swiss Cyber Storm, May 12th, Rapperswil (Switzerland)

2011 *Cryptographie: de la Théorie à la Pratique*, CLUSIS, March 8th, Genève (Switzerland)

2011 *La Cryptographie*, Insomni'Hack 2011, March 4th, Genève (Switzerland)

2009 *Exploitation de l'Identité Numérique*, Journée sur l'identité numérique et la sphère privée, June 16th, Hôtel Royal Savoy, Lausanne (Switzerland)

2003 *FOX – une Nouvelle Famille d'Algorithmes de Chiffrement par Bloc*, November 24th, Université Joseph Fourier, Grenoble (France)

2003 *A Brief Outlook at Block Ciphers*, Summer School "Cryptologie, Sécurité et Applications", September 8-12, Rabat (Morocco).

## Regular Talks

2019 *Computing on Encrypted Data: a Survey*, BlackAlps'19, November 7th, 2019, Yverdon-les-Bains (Switzerland)

2018 *Looking into the White Box*, area41, June 15th, 2018, Zürich (Switzerland)

2016 *Are Crypto APIs Good Friends of Developers?*, area41, June 10th, 2016, Zürich (Switzerland)

2015 *Ciphertext-Policy Attribute-Based Broadcast Encryption with Small Keys*, ICISC'15, November 25th, Seoul (South Korea)

2015 *Obfuscator-LLVM — Software Protection for the Masses*, SPRO'15, May 19th, Firenze (Italy)

2014 *Obfuscator-LLVM — Software Obfuscation for the Masses*, area41, June 2nd, Zürich (Switzerland)

2013 *Sécurité Informatique: Késako?*, September 14th, La Chaux-de-Fonds (Switzerland)

2013 *QCrypt: Implementing a Next-Generation Quantum Key Distillation Engine in Practice*, ESC'13, January 18th, Mondorf-les-Bains (Luxembourg)

2012 *Obfuscator*, final project workshop, November 7th, Yverdon-les-Bains (Switzerland)

2011 *Software Obfuscation: Quid Novi?*, ASFWS'11, October 27th, Yverdon-les-Bains (Switzerland)

2011 *Software Obfuscation: Quid Novi?*, 0sec, October 14th, Bern (Switzerland)

2011 *Cryptographie: de la Théorie à la Pratique*, CLUSIS, March 8th, Geneva (Switzerland)

2010 *Open-Source Cryptographic Libraries and Embedded Platforms*, Hashdays 2010, November 5th, Luzern (Switzerland)

2010 *IDEA - Past, Present and Future*, ESC'10, January 14th, Remich (Luxembourg)

2005 *Yet another Proof of the PRP/PRF Switching lemma*, EUROCRYPT'05 (rump session), May 24th, Aarhus (Denmark)

2005 *New Attacks against Reduced-Round Versions of IDEA*, FSE'05, February 23rd, Paris, (France)

| | |
|---|---|
| 2005 | *Attacks against TSC*, FSE'05 (rump session), February 21st, Paris (France) |
| 2005 | *Statistical Cryptanalysis of Block Ciphers*, Journées Codes et Cryptographie, February 2nd, 2005, Aussois (France) |
| 2004 | *FOX: a New Family of Block Ciphers*, SAC'04, August 9th, Waterloo (Canada) |
| 2004 | *Perfect Diffusion Primitives for Block Ciphers – Building Efficient MDS Matrices*, SAC'04, August 9th, Waterloo (Canada) |
| 2003 | *On the Optimality of Linear, Differential and Sequential Distinguishers*, EUROCRYPT'03, May 5th, Warsaw, (Poland) |
| 2003 | *Optimal Key Ranking Procedures in a Statistical Cryptanalysis*, FSE'03, February 25th, Lund (Sweden) |
| 2001 | *On the Complexity of Matsui's Attack*, SAC'01, August 16th, Toronto (Canada) |
| 2001 | *On the Complexity of Matsui's Attack*, Workshop on Cryptographic Protocols, March 22nd, Monte-Verita ( Switzerland) |
| 2000 | *On the Complexity of Matsui's Attack*, ASIACRYPT'00 (rump session), December 5th, Kyoto (Japan) |

## Teaching

| | |
|---|---|
| 2016 - | *Software Reverse Engineering and Protection*, master level, HES-SO. |
| 2014 - 2017 | *Industrial Cryptography*, master level, HES-SO. |
| 2012 - 2013 | *Sécurité des Systèmes d'Exploitation*, bachelor level, HEIG-VD. |
| 2011 - 2017 | *Cryptographie*, bachelor level, HEIG-VD. |
| 2010 - 2014 | *Ethical Hacking and Computer Forensics*, master level, HES-SO. |
| 2009 - 2017 | *Cryptography and Coding Theory*, master level, HES-SO. |
| 2009 - 2014 | *Software Security*, master level, HES-SO. |
| 2008 - 2010 | *Sécurité des Systèmes Informatiques*, bachelor level, HEIG-VD. |

# ≺ Supervised Student Works ≻

2017 Sébastien Henneberger, *Intégration d'ELCARD au sein de Windows*, bachelor thesis, HEIG-VD

2017 Lucie Steiner, *Confidential Title*, bachelor thesis, HEIG-VD

2017 Yolan Romailler, *Automated Testing of Cryptographic Implementations*, master thesis, HES-SO

2017 Julie Michielin, *Leveraging Intel Software Guard Extensions to implement Time-Lock Encryption*, master thesis, HES-SO

2017 Philippe Bonvin, *Analyse de Performance et de Sécurité des Applications MyCity*, master thesis, HES-SO

2015 Alexandre Perez, *Multi-Device Application*, master thesis, HES-SO

2015 Gaël Jobin, *Software Protection with Obfuscator-LLVM*, master thesis, HES-SO

2014 Johan Wehrli, *Obfuscator - Integrating Code Tamper-proofing into an LLVM Pass*, master thesis, HES-SO

2014 Julien Rinaldini, *Obfuscator - Integrating Functions Merging into an LLVM Pass*, master thesis, HES-SO

2014 Florian Valentino, *Confidential Title*, bachelor thesis, HEIG-VD

2014 Yves Marti, *Création de Boîtiers de Télémaintenance Sécurisés*, bachelor thesis, HEIG-VD

2014 Yassine Mansri, *Virtual Patching Automatisé des Applications Web*, bachelor thesis, HEIG-VD

2013 Stéphane Ongagna Ntobe, *Obfuscator - Obfuscation de Code avec LLVM*, bachelor thesis, HEIG-VD

2013 Guillaume Camenzind, *Découverte d'APT par Observation du Trafic DNS*, bachelor thesis, HEIG-VD

2012 Cédric Rais, *Application Android et Application Web Permettant la Saisie et le Traitement des Pénalités lors d'un Slalom de Canoë-Kayak*, bachelor thesis, HEIG-VD

2012 Thierry Hayoz, *HIDEA – Famille de Fonctions de Hachage basée sur le Chiffrement par Bloc IDEA*, bachelor thesis, HEIG-VD

2012 Julie Michielin, *Intégration de Techniques de Protection Logicielle dans l'Outil Obfuscator*, bachelor thesis, HEIG-VD

2012 Denis Elsig, *Conception et Réalisation d'un Outil d'Analyse et de Visualisation d'Avatars Numérique sur l'Internet*, master thesis, HES-SO

2012 Grégory Ruch, *Safe Browsing*, master thesis, HES-SO

2012 Andrien Giner, *Scanning at Wire Speed*, master thesis, HES-SO

2011 Alberto Certo, *Démonstrateur pour Metasploit*, bachelor thesis, HEIG-VD

2011 Alexandre Kovar, *Recherche de Méthodes de Décryptage pour Accéder aux Systèmes de Fichiers des Consoles de Jeux*, bachelor thesis, HEIG-VD

| | |
|---|---|
| 2010 | Sébastien Bischof, *Rootkits – Kernel Exploitation for Fun and Profit*, master thesis, HES-SO |
| 2010 | Pierre Steiner, *PC d'Examen II*, bachelor thesis, HEIG-VD |
| 2009 | Christophe Lugon, *PC d'Examen*, bachelor thesis, HEIG-VD |
| 2006 | Alexandre Karlov, *Confidential Title*, master thesis, Nagravision SA |