ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

C4DT Research Portfolio

Heads of Research Groups Active in Digital Trust

This document compiles all research, technology transfer and teaching activities at EPFL **on the topic of digital trust**.

Karl Aberer	Semantic information processing in distributed systems
Katerina Argyraki	Network security
David Atienza	Embedded Systems, Hardware Design
Edouard Bugnion	Datacenter systems
George Candea	Reliability and security in large-scale systems
Pierre Collin-Dufresne	Asset pricing
Giovanni De Micheli	Integrated circuits, quantum systems
Touradj Ebrahimi	Media Security
Rüdiger Fahlenbrach	Corporate finance, initial coin offerings (ICO)
Babak Falsafi	Cloud computing
Boi Faltings	Artificial Intelligence
Jacques Fellay	Health and genomic information management
Damir Filipović	Quantitative finance and risk management
Bryan Ford	Decentralized and blockchain systems
Matthias Grossglauser	Data mining and machine learning
Rachid Guerraoui	Distributed algorithms and consensus
Jean-Pierre Hubaux	Privacy and Security
Julien Hugonnier	Asset pricing and mathematical Finance
Paolo Ienne	Processor architecture and electronic design automation
Martin Jaggi	Machine Learning
Dimitar Jetchev	Mathematical cryptography
Viktor Kunčak	Formal software verification
James Larus	Very large scale systems
Jean-Yves Le Boudec	Cyber physical systems
Martin Odersky	Programming languages
Mario Paolone	Power systems (smart grids)
Mathias Payer	Software and systems security
Marcel Salathé	Digital epidemiology and personalized health
Sabine Süsstrunk	Image understanding and conceptualization
Carmela Troncoso	Privacy enhancing technologies
Serge Vaudenay	Cryptography
Robert West	Data Science and Privacy

Karl Aberer

Professor of Computer and Communication Sciences

Aberer is a worldwide leading researcher on semantic information processing in distributed systems (h-index: 58), notably with applications to trust and privacy.

Selected scientific publications:

- K. Aberer and Z. Despotovic. "Managing Trust in a Peer-2-Peer Information System." Ninth International Conference on Information and Knowledge Management (CIKM 2001), Atlanta, Georgia, 2001. (1356 citations on Google Scholar)
- H. Harkous and K. Aberer. "If You Can't Beat them, Join them: A Usability Approach to Interdependent Privacy in Cloud Apps." Outstanding Paper Award at the Seventh ACM on Conference on Data and Application Security and Privacy. ACM, 2017.

In the past years, Aberer has focused on **data analytics of web and social media content to evaluate their influence, credibility and trustworthiness**. This work has been done in collaboration with end users in humanitarian action, health and nutrition.

Notable engagements:

- Advisory Board on Cyber-Security of the Swiss Department of Defense.
- Scientific Advisory Board of the Leistungszentrum "Digitale Vernetzung" Berlin.

Software:

- PriBot (pribot.org): PriBot is the first question-answering chatbot for privacy policies. It takes a previously unseen privacy policy and uses it to answer user questions that are posed in free form. It further simplifies the policy with high-level summaries generated from the legalese text.
- PrivySeal (privyseal.epfl.ch): PrivySeal is a web app that tells users what apps can needlessly know about them from their cloud data. Through machine learning and visualization techniques, our "Far-reaching Insights" scheme was twice as effective in deterring users from installing misbehaving apps as the current model.

Current digital trust projects with non-academic partners:

- CTI project: collaboration with Privatley on developing their Oyoty service (oyoty.com). The service enables detection and protection for children of undesired contents.

Katerina Argyraki

Professor of Computer and Communication Sciences

Katerina Argyraki heads the Network Architecture Lab. She received her PhD (2007) in Electrical Engineering from Stanford University, with a dissertation on **Denial-of-Service Attacks and Defences**. During her graduate-student years, she spent time in several startup companies: – a summer in Kealia (now part of Sun), another one in BlueArc, and, finally, a year in Arista Networks. Her research focuses on **network verification and troubleshooting**, on the one hand, and ways to **define and monitor network neutrality,** on the other. She has received best paper awards at the ACM Symposium on Operating Systems Principles (2009), the USENIX Symposium on Networked Systems Design and Implementation (2014), and the ACM SIGCOMM Workshop on Kernel-bypass Networks (2017). She has also received a Starting Grant from the Swiss National Science Foundation (2015) and the EuroSys Jochen Liedke Young Researcher Award (2016).

Selected scientific publications:

- Arseniy Zaostrovnykh, Solal Pirelli, Luis Pedrosa, Katerina Argyraki, George Candea. "A Formally Verified NAT." The ACM SIGCOMM Conference, August 2017.
- Mihai Dobrescu and Katerina Argyraki. "Software Data-plane Verification." The USENIX Symposium on Networked Systems Design and Implementation (NSDI), April 2014. Recipient of the best-paper award.

Software:

- VigNAT: A Formally Verified, Performant NAT (https://vignat.github.io)
- The LINE Network Emulator (https://github.com/nal-epfl/line)

Teaching related to digital trust:

- Principles of Computer Systems (MS/PhD)

David Atienza

Professor of Electrical and Computer Engineering, School of Engineering (STI)

My research interests focus on system-level design co-methodologies to design secure high-performance multiprocessor system-on-chip (MPSoC) and low-power Internet-of-Thing (ioT) systems, including ultra-low power embedded systems architectures. Among others, Prof. Atienza received the 2018 ACM/IEEE/ESDA Design Automation Conference (DAC) Under-40 Innovators Award for notable impact in the field of design and automation of electronics, the IEEE TCCPS Mid-Career Award for sustained contributions to the design of medical wearables, and he was named IEEE Fellow for his contributions to design methods and tools for MPSoC.

Selected scientific publications

- Soumya Basu, Loris Duch, Ruben Braojos, Giovanni Ansaloni, Laura Pozzi, David Atienza, "An Inexact Ultra-Low Power Bio-Signal Processing Architecture With Lightweight Error Recovery", *ACM Transactions on Embedded Computing Systems (TECS)*, ISSN: 1539–9087, Vol. 16, Issue: 5s (Article No. 159), pp. 159:1-159:19, September 2017.
- Shivani Raghav, Christian Pinto, Martino Ruggiero, Andrea Marongiu, David Atienza, Luca Benini, "GPU Acceleration for simulating massively parallel many-core platforms", *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, ISSN: 10459219, Vol. 26, Issue/Nr: 5, pp. 1336–1349, IEEE Computer Society, May 2015.
- Mohamed Sabry, David Atienza, Francky Catthoor, "OCEAN: An Optimized HW/SW Reliability Mitigation Approach for Scratchpad Memories in Real-Time SoCs", *ACM Transactions on Embedded Computing Systems (TECS)*, ISSN. 1539–9087, Vol. 13, Issue/Nr: 4s, Article No. 138, pp. 1–26, ACM Press, April 2014.

Targeting to enable digital trust, we target in my Embedded Systems Lab (ESL) to enable novel ways to design secure edge computing and embedded machine learning, while optimizing jointly both hardware and low-level software aspects of MPSoCs and IoT objects related to operating system functionality, memory hierarchy and processing elements (cores and accelerators) potential vulnerabilities.

Notable engagement

- President, IEEE Council on Electronic Design Automation (CEDA), period 2018–2019
- Executive Board Member, European Design Automation Association (EDAA), Since 2015

Software

- https://esl.epfl.ch/3D-ICE: "3D-ICE: 3D Interlayer Cooling Emulator". It is a Linux-based Thermal Emulator Library written in C, which can perform transient thermal analyses of vertically stacked 3D integrated circuits and MPSoCs.
- https://esl.epfl.ch/SIMinG.html: "SIMinG: GPU-accelerated full system simulation of heterogeneous many-core platforms". SIMinG is an open-source, fast, scalable and parallel simulator which is used for design space exploration and software development for future heterogeneous platforms with thousands of cores.

Teaching and advocacy:

- "Lab on app development for tablets and smartphones", MSc course, Section of Electrical Engineering (SEL), EPFL
- "Internet of Things (IoT) – Smart connected technologies: latest trends, challenges and opportunities," 3-day course targeting professionals and engineering, Continuous Education Unit UNIL-EPFL, since 2016.

Edouard Bugnion

Professor of Computer and Communication Sciences

Edouard Bugnion joined EPFL in 2012, where his focus is on datacenter systems. His areas of interest include operating systems, data center infrastructure (systems and networking), and computer architecture. Edouard Bugnion is a Fellow of the ACM. Together with his colleagues, he received the ACM Software System Award for VMware 1.0 in 2009.

Selected scientific publications:

- E. Bugnion, S. Devine, K. Govil, and M. Rosenblum. "Disco: Running Commodity Operating Systems on Scalable Multiprocessors." *ACM Transactions on Computer Systems*, vol. 15, No. 4, November 1997, pp. 412–447. Best paper award and entered into the ACM SIGOPS Hall of Fame Award in 2008.
- A. Belay, G. Prekas, A. Klimovic, S. Grossman, C. Kozyrakis, and E. Bugnion. "IX: A Protected Dataplane Operating System for High Throughput and Low Latency." In *Proceedings of the 11th USENIX Symposium on Operating Systems Design and Implementation*, 2014, 49–65. Best Paper Award.

Before joining EPFL, Edouard spent 18 years in the US, where he studied at Stanford and co-founded two startups: VMware and Nuova Systems (acquired by Cisco). At VMware from 1998 until 2005, he played many roles including CTO. At Nuova/Cisco from 2005 until 2011, he helped build the core engineering team and became the VP/CTO of Cisco's Server, Access, and Virtualization Technology Group, a group that brought to market Cisco's Unified Computing System (UCS) platform for virtualized data centers.

Notable engagements:

- Prof. Bugnion is Vice-President of EPFL for Information Systems and as such responsible for the integrity and the trust put by students, faculty, collaborators and partners into EPFL's IT systems.

Teaching related to digital trust:

- Principles of Computer Systems (MS/PhD)

George Candea

Professor of Computer and Communication Sciences

George Candea heads the Dependable Systems Lab, where he conducts research on both the fundamentals and the practice of achieving **trust (security and reliability) in complex software systems**. His main focus is on real-world large-scale systems – millions of lines of code written by hundreds of programmers – because going from a small program to a large system introduces fundamental challenges that cannot be addressed with the techniques that work at small scale. George's academic work has been rewarded with the first Eurosys Jochen Liedtke Young Researcher Award (2014) and an ERC StG award (2011), as well as Best Paper Award at ASPLOS 2011. He received his PhD (2005) in computer science from Stanford and his BS (1997) and M.Eng. (1998) in electrical engineering and computer science from MIT.

Selected scientific publications:

- Jonas Wagner, Volodymyr Kuznetsov, George Candea, Johannes Kinder. "High System-Code Security with Low Overhead." IEEE Symposium on Security and Privacy (S&P), San Jose, CA, May 2015.
- Volodymyr Kuznetsov, Laszlo Szekeres, Mathias Payer, George Candea, R. Sekar, Dawn Song. "Code-Pointer Integrity." USENIX Symposium on Operating Systems Design and Implementation (OSDI), Broomfield, CO, October 2014.

George is also **Chairman of Cyberhaven, a cybersecurity company** he co-founded with his former students to defend sensitive data against advanced attacks, social engineering, and malicious insiders. George employs entrepreneurship as a way to channel research results from the lab into products that benefit society. In the past, George was CTO and later Chief Scientist of Aster Data Systems (now Teradata Aster), one of the first Silicon Valley "big data" companies he co-founded in 2005 with two Stanford colleagues. His entrepreneurial endeavors were rewarded with an M.I.T. TR35 Young Innovators award, and Aster Data Systems was named an Information Technology Pioneer by the World Economic Forum.

Notable engagements:

- Chairman of the Board at Cyberhaven, Inc.
- EPFL Innovation Council

Software:

- S^{2}E: A Platform for In-Vivo Multi-Path Software Analysis (http://s2e.epfl.ch/) – Silver Prize in 2011 Open Source Software World Challenge
- ASAP: Security that fits your budget (http://dslab.epfl.ch/proj/asap/)
- Cloud9: Automated software testing at scale (http://cloud9.epfl.ch/) – Gold Prize in 2013 Open Source Software World Challenge
- Gist: Failure sketching (http://dslab.epfl.ch/proj/gist/)
- Dimmunix: Immunity against concurrency bugs (http://dslab.epfl.ch/proj/dimmunix/)

Teaching related to digital trust:

- Principles of Computer Systems (MS/PhD)

Pierre Collin-Dufresne

Professor of Finance

Pierre Collin-Dufresne is a Professor at the Swiss Finance Institute of the École Polytechnique Fédérale de Lausanne. He has published extensively in leading international academic journals on fixed income and credit risk, asset allocation, and market microstructure. He is a current director of the American Finance Association and a research fellow of the Center for Economic Policy Research.

Selected Scientific Publications

- "Insider Trading, Stochastic Liquidity and Equilibrium Prices" *Econometrica*, 2016. (with Vyacheslav Fos).
- "Parameter Learning in General Equilibrium: Asset Pricing Implications'*American Economic Review*, 2016. (with Michael Johannes and Lars Lochstoer).
- 'Do Prices Reveal the Presence of Informed Trading: A Test of Standard Liquidity Measures' *Journal of Finance*2015. (with Vyacheslav Fos).
- 'On the Relative Pricing of Long Maturity Options and Collateralized Debt Obligations' *Journal of Finance* 2012. (with Robert Goldstein and Fan Yang).
- 'A General Formula for Pricing Defaultable Claims' Econometrica 2004. (with Robert Goldstein and Julien Hugonnier).
- 'The Determinants of Credit Spreads' *Journal of Finance* 2001. (with Robert Goldstein and Spencer Martin).

Notable Engagements

Professor Collin-Dufresne has worked several years in the Quantitative Strategies group of Goldman Sachs Asset Management and as a consultant for the Federal Reserve Bank of New York and the European Central Bank.

Other noteworthy digital trust initiatives:

Professor Collin-Dufresne's recent research focuses on decentralized trading platforms in fixed income markets and their impact on various measures of market quality, such as trading liquidity and price volatility. This has implications for the design of new bond and credit default swap trading platforms, where distributed ledger technologies could play an important role.

One of his PhD students has written a thesis on the microstructure and statistical properties of bitcoin prices based on a unique data set of bitcoin transactions from the (now defunct) Mt. Gox exchange.

Giovanni De Micheli

Professor of Integrated Systems

De Micheli’s research interests include several aspects of design technologies for integrated circuits and systems, such as synthesis for emerging technologies, networks on chips (NoCs) and quantum computing. He pioneered some new electronic devices (for computation and biosensing), he was a key inventor of the NoC technology and he has active interest in logic synthesis of quantum circuits. De Micheli cofounded INOCs, a NOC company whose technology was acquired by Arteris Inc., the major worldwide provider of Noc solutions.

Selected scientific publications:

- Majority Inverter Graph: A New Paradigm for Logic Optimization,” IEEE Transactions on CAD (with Amaru’ et al.), 2016 (Best paper award)
- Polarity Control in WSe2 Double Gate Transistors,’ Scientific reports (with Resta et al.), 2016
- “Nanowire Systems: Technology and Design,” in Philosophical Transactions of the Royal Society of London A, 372 (2012)
- (with Gaillardon et al.), 2014.
- ‘Networks on chips: A new SoC Paradigm’ IEEE Computers, vol. 35, No. 1 (with Benini), 2002.

Notable engagements:

- Director of the Institute of Electrical Engineering at EPFL
- Program Leader of the Nano-Tera.ch Swiss Federal Program

Touradj Ebrahimi

Professor of Media Security

Touradj Ebrahimi is an expert in multimedia signal processing (h-index: 62, citations: 19’875) with research activities evolving around image and video coding, quality of multimedia experience and media security. In **media security**, he has made key contributions to **content protection** (copyright via watermarking and robust content integrity verification), **access control** (region of interest scrambling), **trust modeling in social media and privacy protection** in video surveillance and social media, as well as design of visual privacy filters and media security standards.

Selected scientific publications:

- L. Yuan and Touradj Ebrahimi. “Image Privacy Protection with Secure JPEG Transmorphing.” *IET Signal Processing Journal*, August 2017.
- I. Ivanov, P. Vajda, P. Korshunov and T. Ebrahimi. “Comparative Study of Trust Modeling for Automatic Landmark Tagging.” *IEEE Transactions on Information Forensics and Security*, Vol. 8, Nr. 6, pp. 911–923, 2013.

Notable engagements:

- Convenor (Chairman) of JPEG standardization committee
- Editor of Secure JPEG 2000 Standard (JPSEC)

Software:

- ProShare: Privacy-preserving photo sharing for iOS on Apple Store https://itunes.apple.com/us/app/proshare/id1047578277?mt=8
- ProShare: Privacy-preserving photo sharing for Android on Google Play https://play.google.com/store/apps/details?id=ch.epfl.proshare&hl=en
- ProShare Web-based Portal: Privacy-preserving photo sharing web portal for use from generic browsers: http://grebproshare.epfl.ch/

Teaching related to digital trust:

- Teaching Media Security Course for EPFL Master students in EE, CS and SysCom (6 ECTS)

Current digital trust projects with non-academic partners:

- Standardization of JPEG Privacy and Security (ISO/IEC JTC1/SC29/WG1) https://jpeg.org/jpegsystems/privacy_security.html

Other noteworthy digital trust initiatives:

- Transmorphing granted patent for privacy protection in images,
  Priority Date: 31 July 2015, Grant Date: 18 July 2017
  https://patents.google.com/patent/US9712845B2/en?inventor=touradj+ebrahimi&assignee=epfl

Rüdiger Fahlenbrach

Professor of the Swiss Finance Institute

Fahlenbrach is an international leader in corporate finance research. He has particular research interests in corporate governance and entrepreneurship. One of his current projects examines the emerging initial coin offering phenomena and asks to what extent ICOs can replace more traditional fund-raising methods.

Selected scientific publications:

- Fahlenbrach, Rüdiger, Angie Low, and René M. Stulz. "Do independent director departures predict future bad events?" *Review of Financial Studies,* 30, pp. 2313–2358, 2017.
- Schmidt, Cornelius, and Rüdiger Fahlenbrach. "Do exogenous changes in passive institutional ownership affect corporate governance and firm value?" *Journal of Financial Economics*,124, pp. 285–306, 2017.
- Fahlenbrach, Rüdiger, and René M. Stulz. "Bank CEO Incentives and the Credit Crisis." *Journal of Financial Economics,* 99, pp. 11–26, 2011.

Notable engagements:

- Director of the European Finance Association
- Member, Innogrant Committee EPFL

Other noteworthy digital trust initiatives:

- Swiss Finance Institute at EPFL gathers expertise in financial institutions, market structures, and game theory applied to decentralized trading systems. SFI will collaborate with the Center for Digital Trust in the context of blockchains and distributed ledger technologies in finance and insurance.

Babak Falsafi

Professor of Computer and Communication Sciences

Falsafi is a professor and the founding director of the EcoCloud research center investigating future data-centric information technology at EPFL. Falsafi is interested in software and hardware technologies to allow bridging private and public clouds including technologies for confidential computing, secure server design for the post-Moore era, and accelerators for security, monitoring and policy enforcement in IT platforms. He is a recipient of an Alfred P. Sloan Research Fellowship, and a fellow of ACM and IEEE.

Falsafi has made numerous contributions to computer system design and evaluation including the first family of NUMA servers by Sun Microsystems (now Oracle), performance and power optimizing technologies in memory systems that are incorporated into IBM BlueGene and ARM Cortex A-72 cores, and computer system simulation sampling methodologies that have been in use by AMD and HP for research and product development. His open-source cloud benchmarking technologies have been adopted by Google PerfKit. His recent work on workload-optimized scale-out processor design for servers lays the foundation for Cavium ThunderX, an ARM-based manycore server processor.

Selected scientific publications:

- M Ferdman, A Adileh, O Kocberber, S Volos, M Alisafaee, D Jevdjic, et al. "Clearing the clouds: a study of emerging scale-out workloads on modern hardware." *ACM SIGPLAN Notices* 47 (4), 37–48.
- N Hardavellas, M Ferdman, B Falsafi, A Ailamaki. "Toward dark silicon in servers." *Micro*, IEEE 31 (4), 6–15.

Notable engagements:

- Founding director of EcoCloud, a consortium of EPFL research and industrial affiliates investigating data-centric technologies.
- Board member of ACM SIGARCH, ACM's special interest group on computer architecture.
- Scientific advisory board member of Eayun, Inc.

Software:

- CloudSuite: Open-source workloads to benchmark datacenter-scale services.
- QFlex: Full-system server emulation platform.

Boi Faltings

Professor of Computer and Communication Sciences

Professor Boi Faltings is the head of the EPFL Artificial Intelligence Laboratory. One of his research interests is in trust and privacy in distributed intelligent systems, using game-theoretic and cryptographic schemes.

Selected scientific publications:

- Boi Faltings and Goran Radanovic. "Game Theory for Data Science: Eliciting Truthful Information." Morgan & Claypool Publishers, 2017.
- Thomas Léauté and Boi Faltings. "Protecting Privacy through Distributed Computation in Multi-agent Decision Making." *Journal of Artificial Intelligence Research*, 47, pp. 649–695, 2013.
- Radu Jurca, Boi Faltings, and Walter Binder. "Reliable QoS monitoring based on client feedback." 16th WWW Conference, pp. 1003–1012, 2007.

Notable engagements

The EPFL spinoff NexThink is one of 6 startup companies co-founded by Professor Faltings, based on machine learning work in the Artificial Intelligence Laboratory.

Jacques Fellay

Professor of Life Sciences

Fellay is a biomedical researcher working in human genomics of infection and immunity, computational biology and personalized health. **Worldwide, he is among the genomic researchers with the strongest publication record on data protection**.

Selected scientific publications:

- McLaren PJ, Raisaro JL, Aouri M, et al. "Privacy-preserving genomic testing in the clinic – a model using HIV treatment." *Genetics in Medicine,* 18(8):814-22, 2016.
- Naveed M, Eyday E, Clayton EW, et al. "Privacy in the Genomic Era." *ACM Computing Surveys*, 48 (1), Article 6, 2015.

As the head of Precision Medicine at the Lausanne University Hospital (CHUV), Fellay is a key player in efforts to use genomic techniques in patient care in Switzerland.

Notable engagements:

- Co-director of the Health2030 Genome Center at Campus Biotech in Geneva.
- Member of the Organizing Committee of the Expert Workshop "Trust in Precision Medicine", 23–24 November 2017, Campus Biotech, Geneva

Health2030 is an initiative designed to promote research, training and services in the field of digital and personalized health in western Switzerland.

Damir Filipović

Professor of the Swiss Finance Institute

Filipović is an international leader in quantitative finance and risk management research.

Selected scientific publications:

- M. Cambou and D. Filipović. “Model Uncertainty and Scenario Aggregation.” *Mathematical Finance*, 27, 534–567, 2017
- D. Filipović and A. Trolle. “The Term Structure of Interbank Risk.” *Journal of Financial Economics*, 109, 707–733, 2013

Filipović has co-developed the Swiss Solvency Test at the Swiss Federal Office of Private Insurance. He currently acts as the president of the Bachelier Finance Society, an international organization in mathematical finance. His latest research interests include **crypto-currency modeling**.

Notable engagements:

- Member of the Board of Directors of Swiss Life Holding Ltd
- Scientific Advisor for EdgeLab (a Swiss Fintech company)

Other noteworthy digital trust initiatives:

- Swiss Finance Institute at EPFL gathers expertise in financial institutions, market structures, and **game theory applied to decentralized trading systems.** SFI will collaborate with the Center for Digital Trust in the context of **blockchains and distributed ledger technologies** in finance and insurance.

Bryan Ford

Professor of Computer and Communication Sciences

Ford is a globally influential researcher in the fields of **security, privacy, and decentralized systems**. He focuses broadly on building secure decentralized systems, touching on topics including private and anonymous communication, scalable decentralized systems, blockchain technology, Internet architecture, and operating systems. Ford earned his BS at the University of Utah and his PhD. at MIT, then joined the faculty of Yale University where his work received the Jay Lepreau Best Paper Award and grants from NSF, DARPA, and ONR, including the NSF CAREER award. His continuing work receives support from EPFL and the AXA Research Fund.

Selected scientific publications:

- Kirill Nikitin, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Nicolas Gailly, Linus Gasser, Ismail Khoffi, Justin Cappos, and Bryan Ford. "CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds." USENIX Security Symposium, August 2017.
- Ewa Syta, Philipp Jovanovic, Eleftherios Kokoris Kogias, Nicolas Gailly, Linus Gasser, Ismail Khoffi, Michael J. Fischer, and Bryan Ford. "Scalable Bias-Resistant Distributed Randomness." IEEE Security & Privacy, May 2017.

Ford is one of a handful of academics worldwide to have developed a **complete blockchain system**, which his lab has released publicly as open source software. Numerous industry partners are working with Ford's lab to adopt and use the lab's blockchain for a variety of applications in finance, commerce, communications, and digital data management.

Notable engagements:

- Information Science and Technology advisory board of the US Defense Advanced Research Projects Agency (DARPA);
- Advisory board of the Swiss Fintech Innovations association.

Software:

- Cothority: scalable collective authority framework
- Kyber: advanced cryptography library for decentralized systems

Current digital trust projects with non-academic partners:

- AXA Research Fund chair in information security and privacy (€1.5M)
- DFINITY foundation project to create a "blockchain computer"

Broader-audience education and advocacy activities on digital trust:

- Speech on technology and governance at ACM Turing 50 celebration
- Essay on Apple-vs-FBI controversy and software transparency on Freedom to Tinker
- Personal blogging on digital trust, blockchain systems, and their impact on society

Teaching related to digital trust:

- Decentralized Systems Engineering course (CS-438): teaches decentralized systems principles, guiding students through the development of their own decentralized system incorporating messaging, encryption, and blockchain concepts.

Matthias Grossglauser

Professor of Computer and Communication Sciences

Grossglauser is an expert on machine learning and large-scale analytics for network data, including social, mobile, and biological networks.

Selected publications:

- P. Pedarsani and M. Grossglauser. "On the Privacy of Anonymized Networks." *KDD 11*, San Diego, August 2011.
- E. Kazemi, H. Hassani, M. Grossglauser, and H. P. Modarres. "PROPER: Global Protein Interaction Network Alignment through Percolation Matching." *BMC Bioinformatics*, 17:527, December 2016.

Our group participates in data challenges and develops prototype online services to demonstrate the performance of our data analytics methods. For example, see http://sidekick.epfl.ch/ for a prediction engine for the success of Kickstarter projects, based on financial and social media real-time data.

Notable engagements:

- Director of the Internet Laboratory and member of the CEO Technology Council at Nokia (2007–2010)
- Steering board member, Future Internet Programme, Strategic Center of Excellence in Science, Technology and Innovation in ICT (Finland) (2007–2010)
- CISCO Forward-looking Architectures, Services and Technologies (FAST) Advisory Board (2015)

Software:

- Open-source library for large-scale inference with comparison and ranking data: https://github.com/lucasmaystre/choix

Rachid Guerraoui

Professor of Computer and Communication Sciences

Guerraoui is the author of hundreds of publications and several books on **secure and reliable distributed programming**. He is a senior ERC ACM fellow, and winner of a Google Focused Award. He worked with Swiss banks on how to make their IT reliable and secure, and with Google on how to ensure privacy and personalization.

Guerraoui recently established **the unfairness of blockchain**. Blockchain, at the heart of bitcoin, relies on a consensus protocol that seeks to preserve the consistency of a distributed ledger. This protocol in turns relies on a leader election based on mining. Part of the success of blockchain is based on the very idea that miners are awarded proportionally to their contribution. Rachid Guerraoui and his student Jingjing Wang have recently shown that this folklore belief is wrong. In fact, the topology of the network plays a crucial role and the distance between nodes can bias the reward in a significant manner. Blockchain is inherently unfair. Together with his postdoc Jad Hamza and colleagues from INRIA, they have also shown that blockchain ensures only a weak consistency criteria (called prefix consistency): it is also inherently inconsistent.

Guerraoui also worked on **enhancing privacy on the Internet**. There is a general belief that once users click on an Internet site, they reveal private information. Together with his student Tahsiki Mahsa and Anne-Marie Kermarrec, Rachid Guerraoui has shown that this is not always true. Some clicks can in fact hide the person behind the click. Based on this observation, they proposed the idea of a click advisor: an oracle that can be used to guide users in their Internet navigation. The idea has recently been patented by EPFL.

Selected Publications:

- C. Cachin, R. Guerraoui, L. Rodrigues. "Introduction to Reliable and Secure Distributed Programming." Springer, 2011.
- Alain Girault, Gregor Gössler, Rachid Guerraoui, Jad Hamza, and Dragos-Adrian Seredinschi. "Why You Can't Beat Blockchains: Consistency and High Availability in Distributed Systems." arXiv preprint arXiv:1710.09209 (2017).

Jean-Pierre Hubaux

Professor of Computer and Communication Sciences

Worldwide, Hubaux is among the top five most cited researchers in privacy protection (h-index: 78) and the most productive one on data protection for personalized health and genomics.

Selected scientific publications:

- Z. Huang, H. Lin, J. Fellay, Z. Kutalik and J.-P. Hubaux. "SQC: Secure Quality Control for Meta-Analysis of Genome-Wide Association Studies." *Bioinformatics*, 33(15):2273–2280, 2017.
- K. Olejnik, I. Dacosta, J. S. Machado, K. Huguenin, M. E. Khan, J.-P. Hubaux. "SmarPer: Context-Aware and Automatic Runtime-Permissions for Mobile Devices". *Proceedings of the 38th IEEE Symposium on Security and Privacy (S&P)*, 2017.

In the past, Hubaux has pioneered the topics of location privacy and secure vehicular communications. In the last six years, he has collaborated extensively **with hospitals and health practitioners**.

Notable engagements:

- Scientific Advisory Board of Sophia Genetics (MIT Technology Review top-30 "smartest" startups of 2017)
- One of the seven members of the Swiss Federal Communications Commission
- Member of the "Information Security Task Force", set up by the Swiss federal government

Software:

- PriFi (anonymous communication network): prifi.net
- UnLynx and MedCo: Decentralized System for Privacy-Conscious Data Sharing (source code will soon be available)

Current digital trust projects with non-academic partners:

- Since 2012, collaboration with CHUV on protection of genomic data; CHUV funding
- Since 2013, collaboration with Sophia Genetics on protection of genomic data; CTI funding

Other noteworthy digital trust initiatives:

- Co-founded in 2014 the International Workshop on Genomic Privacy; Chair of the Steering Committee
- Member of the leadership team of the Security Working Group of the International Alliance for Genomics and Health

Teaching related to digital trust:

- EPFL Doctoral Course CS-622 Advanced Topics in Privacy Protection

Julien Hugonnier

Professor of the Swiss Finance Institute – Financial Engineering

Hugonnier works at the interface of financial economics and mathematics. His research deals with theoretical issues in asset pricing, market microstructure, and decision-making under uncertainty. In particular, his recent work focuses on the impact of investor heterogeneity on the **equilibrium outcomes of decentralized markets**.

Selected scientific publications:

- J. Hugonnier and E. Morellec. "Bank capital, liquid reserves, and insolvency risk." *Journal of Financial Economics* 125(2): 266–285, 2017.
- J. Hugonnier and R. Prieto. "Asset pricing with arbitrage activity." *Journal of Financial Economics*, 115(2):411–428, 2015.

Julien Hugonnier has conducted research on the consequences of the implementation of the Basel III capital and liquidity requirements framework in banks, and served as a consultant for various financial institutions on topics that include portfolio management, capital requirements, and derivatives pricing/hedging.

Notable engagements:

- Head of EPFL's master in **Financial Engineering** at EPFL

Paolo Ienne

Professor of Computer and Communication Sciences

Ienne's research interests are at the intersection of computer and processor architecture with electronic design automation. Most of his work in recent years is centered on reconfigurable computing, spanning from the introduction of new architectures for FPGAs to tackling programmability issues.

Over the years, he has worked on several aspects of hardware security and in particular on preventing side-channel attacks. With his colleagues, he published the first method to automatically apply power-analysis countermeasures to arbitrary unprotected cryptographic software. He has also coauthored various hardware countermeasures against differential power analysis, ranging from transistor-level techniques up to architectural ideas.

Selected scientific publications:

- Andrew Becker, Wei Hu, Yu Tai, Philip Brisk, Ryan Kastner, and Paolo Ienne. "Arbitrary precision and complexity tradeoffs for gate-level information flow tracking." In *Proceedings of the 54th Design Automation Conference*, pages 5:1 – 5:6, Austin, Tex., June 2017.
- Ali Galip Bayrak, Francesco Regazzoni, David Novo Bruna, Philip Brisk, François-Xavier Standaert, and Paolo Ienne. "Automatic application of power analysis countermeasures." *IEEE Transactions on Computers*, C-64(2):329-41, February 2015.
- Ali Galip Bayrak, Francesco Regazzoni, David Novo Bruna, and Paolo Ienne. "Sleuth: Automated verification of software power analysis countermeasures. In Cryptographic Hardware and Embedded Systems (CHES 2013)", *Lecture Notes in Computer Science*. Springer, pages 293–310, Heidelberg, Germany, September 2013.
- Alessandro Cevrero, Francesco Regazzoni, Michael Schwander, Stéphane Badel, Paolo Ienne, and Yusuf Leblebici. "Power-gated MOS current mode logic (PG-MCML): A power aware DPA-resistant standard cell library." In *Proceedings of the 48th Design Automation Conference*, pages 1014-19, San Diego, Calif., June 2011.
- Francesco Regazzoni, Alessandro Cevrero, François-Xavier Standaert, Stephane Badel, Theo Kluter, Philip Brisk, Yusuf Leblebici, and Paolo Ienne. "A design flow and evaluation framework for DPA-resistant instruction set extensions." In Christophe Clavier and Kris Gaj, editors, *Cryptographic Hardware and Embedded Systems* (CHES 2009), volume 5747 of Lecture Notes in Computer Science, pages 205-19. Springer, Heidelberg, Germany, September 2009.

Martin Jaggi

Professor of Computer and Communication Sciences

Martin Jaggi is a Tenure Track Assistant Professor at EPFL, leading the Machine Learning and Optimization Laboratory. Before that, he was a postdoctoral researcher at ETH Zurich, at the Simons Institute in Berkeley, and at École Polytechnique in Paris. He has earned his PhD in Machine Learning and Optimization from ETH Zurich in 2011, and a MSc in Mathematics also from ETH Zurich. He is a co-founder of the text analytics startup SpinningBytes, and also the founder of the Zurich Machine Learning and Data Science Meetup.

Selected scientific publications:

- Sebastian Stich, Anant Raj, Martin Jaggi. "Safe Adaptive Importance Sampling." NIPS 2017: Advances in Neural Information Processing Systems, 2017
- Martin Jaggi, Virginia Smith, Martin Takáč, Jonathan Terhorst, Sanjay Krishnan, Thomas Hofmann, Michael I. Jordan. "Communication-Efficient Distributed Dual Coordinate Ascent."NIPS 2014: Advances in Neural Information Processing Systems, 2014
- Matteo Pagliardini, Prakhar Gupta, Martin Jaggi. "Unsupervised Learning of Sentence Embeddings using Compositional n-Gram Features." NAACL: North American Chapter of the Association for Computational Linguistics 2018

Notable engagements:

- Co-organizer of Applied Machine Learning Days, one of Europe's largest machine learning and artificial intelligence events
- Area Chair at AISTATS 2018 and ICML 2017 and 2018

Software:

- CoCoA algorithm for distributed and federated machine learning (e.g. part of TensorFlow)
- sent2vec: General purpose features for learning on text

Current digital trust projects with non-academic partners:

- Research collaboration on text understanding and Scientific Advisory Board of Iprova
- CTI project with PwC and ZHAW on "ADA – advanced algorithms for artificial data analyst," towards more reliable, automated and reproducible machine learning models.
- MLbench: Distributed Machine Learning Benchmark (open source project)

Dimitar Jetchev

Professor of Computer and Communication Sciences

Jetchev has been granted a Swiss National Science Foundation professorship for his research in **mathematical cryptography**. He is notably working on areas such as elliptic curve cryptography, leakage-resilient cryptography and secure multiparty computing.

Selected scientific publications:

- C. Boura, I. Chillotti, N. Gama, A. Petric, S. Peceny and D. Jetchev. "High-precision privacy-preserving real-valued function evaluation" submitted, 2017.
- A. Duc and D. Jetchev. "Hardness of computing individual bits for one-way functions on elliptic curves." *Advances in Cryptology*, CRYPTO, 2012.

Interested in the application of his research, Jetchev worked with Microsoft to develop cryptographic software licensing schemes and other applications. In addition, Jetchev has prior industry experience in applying algorithms for statistical learning in financial technology and more recently, on privacy-preserving machine learning applications in fintech and healthcare.

Notable engagements:

- Cofounder, CTO and board member of Inpher Inc/Sarl (a Swiss/US startup that develops privacy-preserving machine learning tools and other privacy software).

Software:

- https://www.inpher.io/mainproducts/#productdescription
  - *Inpher _Ultra* – a Java SDK for secure sharing and secure search on encrypted data for the cloud (licensable)
  - *Inpher XOR Secret Computing Engine* – a compiler allowing to build and evaluate machine learning algorithms on multiple sensitive data sources in a privacy-compliant manner (licensable).

Current digital trust projects with non-academic partners:

- Project with Swisscom on evaluating cryptographic protocols for eSIM

Other noteworthy digital trust initiatives:

- Collaboration with RISELab, UC Berkeley
- Collaboration with Microsoft Corp. (Azure trusted services) and Microsoft Research.
- Collaboration with Broad Institute on applications of SMPC in genomic research

Teaching related to digital trust:

- *Number theory in Cryptography* (algorithms and cryptanalysis in public-key cryptography; fast integer, modular and finite field arithmetic, integer factorization and RSA, computing discrete logarithms, lattices and elliptic curves) – EPFL Master Course/Math 489
- *Algebraic curves in Cryptography* (advanced theory and applications of curve-based cryptography; theory of algebraic curves, cryptographic pairings, short signatures, identity-based encryption, proxy-reencryption, pairing-based algorithms for secure search) – EPFL Master Course/Math 409

Viktor Kunčak.

Professor of Computer and Communication Sciences

Viktor Kunčak is an associate professor in the School of Computer and Communication sciences which he in 2007, after receiving a PhD degree from MIT. He leads the EPFL Laboratory for Automated Reasoning and Analysis that has developed several tools for **automated formal verification and synthesis of software** in programs written in the Scala programming language widely used in industry. He received a single-investigator European Research Council (ERC) grant of 1.5M EUR to advance the techniques of software synthesis. He was recently awarded a Swiss NSF grant to deeply integrate verification technology into mainstream Scala platform. A paper on automated test generation he coauthored received an ACM SIGSOFT distinguished paper award at ICSE, whereas a PLDI paper he coauthored got published in the Communications of the ACM as a Research Highlight. He is an associate editor of ACM Transactions on Programming Languages and Systems (TOPLAS) and served as a co-chair of conferences on Computer Aided Verification (CAV), Formal Methods in Computer Aided Design (FMCAD), and Verification, Model Checking, and Abstract Interpretation (VMCAI). Former members of his group have gone to become researchers or developers at institutions including MIT, Yale, Berkeley, TwoSigma, IBM Research, Google, Standard Chartered Bank, and Credit Suisse.

Viktor Kunčak plans to pursue **automated verification of 1) smart contracts and 2) digital trust software infrastructure**. The verification of smart contracts technology will leverage the rigor of mathematical proof and the power of automated theorem proving to ensure that smart contracts deliver on its transformative potential without incurring unacceptable risks that have been revealed through, for example, Distributed Autonomous Organization failure. **The verification of software infrastructure can dramatically reduce the possibilities for exploits in the underlying support software infrastructure** (operating systems, browsers, compilers) through combined used of safe programming languages such as Scala compiled to native code, and verification technology to ensure desired properties at a deeper level.

Selected scientific publications:

- Ravichandhran Madhavan, Sumith Kulal and Viktor Kuncak. "Contract-based resource verification for higher-order functions with memorization." ACM POPL 2017.
- Philippe Suter, Mirco Dotta, and Viktor Kuncak. "Decision Procedures for Algebraic Data Types with Abstractions." ACM POPL 2010

Notable engagements:

- Advisor for London-based startup Prodo.AI – applying AI to software development

Software:

- Stainless verification framework for Scala: https://github.com/epfl-lara/stainless

Teaching related to digital trust:

- Synthesis, Analysis, and Verification, MSc course, EPFL
- Computer Language Processing, 3rd year undergraduate course on compilers, EPFL
- Parallel Programming MOOC on Coursera, part of Functional Programming in Scala specialization

James Larus

Professor of Computer and Communication Sciences

Larus is Professor and **Dean of the School of Computer and Communication Sciences** (IC) at EPFL (École Polytechnique Fédérale de Lausanne). Prior to joining IC in October 2013, Larus was a researcher, manager, and director in Microsoft Research for over 16 years and an assistant and associate professor in the Computer Sciences Department at the University of Wisconsin, Madison. Larus has been an active contributor to numerous communities. He published over 100 papers (with 9 best and most influential paper awards), received over 30 US patents, and served on numerous program committees and NSF, NRC, and DARPA panels. His book, Transactional Memory (Morgan Claypool) appeared in 2007. Larus received a National Science Foundation Young Investigator award in 1993 and became an ACM Fellow in 2006.

Larus joined Microsoft Research in 1998 to start and lead the Software Productivity Tools (SPT) group, which developed and applied a variety of innovative program analysis techniques to build tools to find software defects. This group's **groundbreaking research in program analysis and software defect detection** is widely recognized by the research community, as well as being shipped in Microsoft products such as the Static Driver Verifier, FX/Cop, and other software development tools. Larus became an MSR Research Area Manager for programming languages and tools and started the Singularity research project, which demonstrated that modern programming languages and software engineering techniques can fundamentally improve software architectures. Subsequently, he helped start XCG, an effort in MSR to develop hardware and software support for cloud computing. In XCG, Larus started the development of the Orleans framework for cloud programming and the Catapult FPGA accelerator for the Bing search engine.

Selected scientific publications:

- Andrew Putnam, et al. "A Reconfigurable Fabric for Accelerating Large-Scale Datacenter Services." *Communications of the ACM (CACM)*, Vol. 59, No. 11, pp. 10–22, November 2016.
- James Larus, Galen Hunt. "The Singularity System." *Communications of the ACM (CACM)*, Vol. 53, No. 8, pp. 72–79, August 2010.

Notable engagements:

- Director, Microsoft Research
- Dean of IC at EPFL (2013 -)

Software:

- Singularity, a new operating system written in a high-level language (C#) with an architecture that facilitated **verification and program isolation**.

Jean-Yves Le Boudec

Professor of Computer and Communication Sciences

Le Boudec is professor at EPFL and active in the area of the theory of computer networking and performance evaluation. He has an h-index of 73 and is Fellow of the IEEE for his work on network calculus. His current work is on reliable digital control systems for electric grids.

Selected scientific publications:

- A Bernstein, L Reyes-Chamorro, JY Le Boudec and M. Paolone. "A composable method for real-time control of active distribution networks with explicit power setpoints. Part I: Framework." *Electric Power Systems Research*, 2015.
- Jayasinghe, U., Barreto, S., Popovic, M., Tesfay, T. T., & Le Boudec, J. Y. "Security Vulnerabilities of the Cisco IOS Implementation of the MPLS Transport Profile." *Proceedings of the 2nd Workshop on Smart Energy Grid Security,* ACM, November 2014, pp. 45–50.

As part of the Commelec project, funded by SNSF and CTI, we are developing a **reliable and secure platform for the real-time control of electrical grids**.

Software:

- IP Parallel Redundancy Protocol https://github.com/LCA2-EPFL/iprp
- API for the Commelec Smart Grid control platform https://github.com/LCA2-EPFL/commelec-api

Martin Odersky

Professor of Computer and Communication Sciences

Odersky is the creator of **Scala**, one of the dominant languages in FinTech (mission critical at Goldman Sachs, UBS, etc.) and other industries. It allows **securely embedded domain specific languages, a key enabling technology for digital contracts,** and is suitable for high-performance distributed computing.

Software:

- Scala compiler and a large code base of related tools

Mario Paolone

Professor of Electrical and Computer Engineering

Paolone's conducts research in power systems with particular reference to real-time monitoring and operation, power system protections, power system dynamics and power system transients. He is particularly interested in the development of smart grid concept solutions in order to efficiently deliver sustainable, economic and secure electricity supply. He is the author or coauthor of over 280 scientific papers published in reviewed journals and international conferences. Among other duties on editorial and conference boards, he is notably the editor in chief of the Elsevier journal on Sustainable Energy, Grids and Networks.

Selected scientific publications:

- S. Barreto Andrade, M. Pignati, G. Dán, J.-Y. Le Boudec and M. Paolone, "Undetectable Timing-Attack on Linear State-Estimation by Using Rank-1 Approximation", IEEE Trans. on Smart Grids, vol. 9, no.4, pp. 3530–3542, July, 2018.
- A Bernstein, L Reyes-Chamorro, J.-Y. Le Boudec and M. Paolone. "A composable method for real-time control of active distribution networks with explicit power setpoints. Part I: Framework." Electric Power Systems Research, 2015.
- W.K. Chai, N. Wang, K.V. Katsaros, G. Kamel, G. Pavlou, S. Melis, M. Hoefling, B. Vieira, P. Romano, S. Sarri, T.T. Tesfay, B. Yang, F. Heimgaertner, M. Pignati, M. Paolone, M. Menth, M. E. Poll, M. Mampaey, H.H.I. Bontius, C. Develder, "An Information-Centric Communication Infrastructure for Real-Time State Estimation of Active Distribution Networks," IEEE Trans. on Smart Grid, vol. 6, Issue 4, pp. 2134–2146, July 2015.

Paolone's work is highly applicable and aims to integrate intelligently the actions of all users connected to modern electrical networks whether they are generators or consumers. By relying on innovative products and services together with intelligent monitoring, control, communication and self-healing technologies, he aims to develop solutions to:

- facilitate the connection and operation of generators of all sizes and technologies;
- allow consumers to play a part in optimizing the operation of the system;
- provide consumers with greater information and choice of supply;
- significantly reduce the environmental impact of the whole electricity supply system;
- deliver enhanced levels of reliability and security of supply while accounting for the uncertainty of renewable energy sources, the increase of dispersed generation and storage facilities and the rules inherent to the liberalization of the electricity market.

Notable engagements:

- Head of FURIES (Future Swiss Electrical infrastructure)
- Chair of the EPFL Energy Center Directorate.
- Executive Board of the European Energy Research Alliance (EERA)
- Commission Fédérale pour la Recherche Energétique (CORE) of the Swiss Federal Office of Energy (SFOE).

Software:

- Composable method for real-time control of active distribution networks with explicit power setpoints (COMMELEC).
- Full replica of the dynamic model of the IEEE 39-bus power system, including dynamic models of conventional generation and dynamic load profiles

Teaching:

- Smart Grids Technologies, EPFL MSc 2nd semester

Mathias Payer

Assistant Professor Computer and Communication Sciences

Payer's research focuses on several aspects of software security and systems security. The HexHive group focuses on making programs resilient against attacks along two dimensions: software testing (finding and fixing bugs) and attack mitigation (protecting against unknown/unpatched bugs). For software testing, he combines the development of sanitizers that enforce security policies to detect violations with novel approaches to fuzzing, exposing deep hidden bugs. For software mitigation, he develops strong policies that fit into the tight runtime constraints to protect against control-flow hijacking and type-based attacks. Payer serves on the program committee of all four major security conferences as well as a number of specialized symposiums and workshops.

Selected scientific publications:

- Hui Peng, Yan Shoshitaishvili, and Mathias Payer, "T-Fuzz: fuzzing by program transformation" In *Oakland'18: IEEE International Symposium on Security and Privacy*, 2018
- Nathan Burow, Derrick McKee, Scott A. Carr, and Mathias Payer, "CFIXX: Object Type Integrity for C++ Virtual Dispatch", in *NDSS'18: Network and Distributed System Security Symposium*, 2018
- Yuseok Jeon, Priyam Biswas, Scott A. Carr, Byoungyoung Lee, and Mathias Payer, "HexType: Efficient Detection of Type Confusion Errors for C++", in *CCS'17: ACM Conf on Computer and Communication Security*, 2017
- Terry Ching-Hsiang Hsu, Kevin Hoffman, Patrick Eugster, and Mathias Payer, "Enforcing Least Privilege Memory Views for Multithreaded Applications," in CCS'16: *ACM Conf on Computer and Communication Security*, 2016
- Chao Zhang, Scott A. Carr, Tongxin Li, Yu Ding, Chengyu Song, Mathias Payer, and Dawn Song, "VTrust: Regaining Trust on Your Virtual Calls", in *NDSS'16: Network and Distributed System Security Symposium*, 2016

All implementation prototypes developed during research projects in the HexHive group are published as open-source to foster collaborations and open access to new security mechanisms. In addition to open-sourcing mechanisms, the prototypes are often upstreamed into the corresponding open-source projects, allowing wide dissemination and usage.

Software:

- All mechanisms are open-sourced at https://github.com/HexHive/

Teaching and advocacy:

- Topics in language-based software security in fall 2018
- Software security elements in other courses
- Advisor of the Capture-the-Flag security team

Other noteworthy digital trust initiatives:

- Collaboration with SANDIA National Labs on developing security mechanisms for embedded systems and low-end IoT systems

Marcel Salathé

Professor of Life Sciences & Computer and Communication Sciences

Salathé is an Associate Professor in both the School of Life Science and Computer and Communication Sciences. He has pioneered the field of **digital epidemiology**, working on **social media data for health purposes** since 2009.

Selected scientific publications:

- Salathé, M., Bengtsson, L., Bodnar, T.J., Brewer, D.D., Brownstein, J.S., Buckee, C., Campbell, E.M., Cattuto, C., Khandelwal, S., Mabry, P.L. and Vespignani, A. "Digital Epidemiology." *PLoS Computational Biology*, 8(7), p.e1002616, 2012.
- Salathé, M., Freifeld, C.C., Mekaru, S.R., Tomasulo, A.F. and Brownstein, J.S. "Influenza A (H7N9) and the Importance of Digital Epidemiology." *The New England Journal of Medicine*, 369(5), p. 401, 2013.

Salathé advised both the US and the Swiss government about to use of social media data for public health purposes. He is the founder of **open data platforms** such as crowdAI.org and openfood.ch.

Notable engagements:

- Founder and academic director of the EPFL Extension School, a new online school dedicated to continued education for digital skills (data science, web and mobile development, etc.): https://exts.epfl.ch

Software:

- All open source code is available at https://github.com/salathegroup

Other noteworthy digital trust initiatives:

- MyOpenFood: A citizen science project reaching 1000s of healthy people from the Swiss population to measure food intake, postprandial glucose levels, and their microbiome. We are working with the MIDATA initiative to explore the model of **data cooperatives for storing personal health data**.

Sabine Süsstrunk

Professor of Computer and Communication Sciences

Sabine is Full Professor for Images and Visual Representation in IC and Director of the Digital Humanities Institute in the College of Humanities at EPFL. Her specialty is computational imaging, color computer vision and image processing, and computational aesthetics. She is a Fellow of IEEE and IS&T, and received the 2013 IS&T/SPIE Electronic Imaging Scientist of the Year award.

Selected scientific publications:

- S. Arpa, S. Süsstrunk, and R.D. Hersch. "Revealing Information by Averaging." *Journal of the Optical Society of America A*, vol. 34, num. 5, pp. 743–751, 2017.
- R. Achanta, A. Shaji, K. Smith, A. Lucchi, P. Fua, S. Süsstrunk. "SLIC superpixels compared to state-of-the-art superpixel methods." *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vo. 34, num. 11, pp. 2274–2282, 2012.

We have conducted research on how to **hide information in video** that only becomes visible through long exposures with a camera.

Notable engagements:

- Member of the SNSF Foundation Board
- EPFL Innovation Council
- President, EPFL WISH Foundation

Software:

- SLIC Superpixels: http://ivrl.epfl.ch/research/superpixels
- FASA Saliency: http://ivrl.epfl.ch/research/saliency/fast_saliency
- FAN/EFAN: http://ivrl.epfl.ch/research/image_completion
- Deep Aesthetics: http://ivrlwww.epfl.ch/~bjin/project_aesthetics/Image_Aesthetics.html
- for more see http://ivrl.epfl.ch/research

Carmela Troncoso

Professor of Computer and Communication Sciences

Troncoso is a renowned researcher in the field of **Privacy Enhancing Technologies**. Her research has a strong focus on the **design of end-to end secure and privacy-preserving systems**, and the development of systematic means of quantifying privacy protection.

Selected scientific publications:

- Gürses, C Troncoso, C Diaz. "Engineering privacy by design." *Computers, Privacy & Data Protection,* 2011
- J Balasch, A Rial, C Troncoso, B Preneel, I Verbauwhede, C Geuens. "PrETP: Privacy-Preserving Electronic Toll Pricing. " *USENIX Security Symposium* 10, 63–78.

Troncoso has years of experience of working with industry at Gradiant, the Galician Research and Development Center in Advanced Telecommunications, an Innovation-oriented research center in Spain. She notably designed the **cloud-to-vehicle security architecture** for PSA Peugeot Citroën and an **eVoting system** for deployment in Latin America.

Notable engagements:

- Expert for the European Union Agency for Network and Information Security (ENISA) (2015-)

Software:

- ClaimChain decentralized: https://claimchain.github.io/

Current digital trust projects with non-academic partners:

- Collaboration with Merlinux, in the frame of a European H2020 project, to develop a privacy-preserving decentralized messaging system (http://nextleap.eu/).
- Collaboration with Scytl, funded by a Spanish government grant, on eVoting

Other noteworthy digital trust initiatives:

- Member, since 2012, of the PETS Board, the Steering Committee of the Privacy Enhancing Technologies Symposium.

Serge Vaudenay

Professor of Computer and Communication Sciences

Vaudenay is a leading expert and highly cited researchers (7000 citations) in the areas of **security assessment of cryptographic products, post-quantum cryptography, and security and trust models**. He is notably the author of the most prominent privacy model for RFID.

Selected scientific publications:

- B. Canvel; A. Hiltgen; S. Vaudenay; M. Vuagnoux. "Password interception in a SSL/TLS channel." *Lecture Notes in Computer Science*, volume 2729. Presented at: The 23rd Annual International Cryptology Conference, CRYPTO '03, Santa Barbara, CA, USA
- FB. Durak; S. Vaudenay. "Breaking The FF3 Format-Preserving Encryption Standard Over Small Domains." *Lecture Notes in Computer Science*, volume 10402. Presented at: The 37th Annual International Cryptology Conference, CRYPTO '17, Santa Barbara, CA, USA

Notable engagements:

- Board of directors member of the International Association for Cryptologic Research (2007–2012)
- Organizer of 15 conferences, program chair of 10 international research conferences, member of over 100 program committees

Robert West

Professor of Computer and Communication Sciences

West is an assistant professor in the School of Computer and Communication Sciences at EPFL, where he **leads the Data Science Lab**. His research aims to understand, predict, and enhance human behavior in social and information networks by developing techniques in data science, data mining, network analysis, machine learning, and natural language processing. Much of his research has to do with **data that carries personally identifiable information**, and **privacy considerations** have played an increasing role in his work. West holds a PhD in computer science from Stanford University, a Master's from McGill University, and a Diplom from Technische Universität München.

Selected scientific publications:

- V. Hartmann, J. Pujol, R. West. "SecVM: A Framework for Privacy-Preserving SVM Training on Distributed Data." In preparation for KDD, 2018.
- R. West, H. Paskov, J. Leskovec, C. Potts. "Exploiting Social Network Structure for Person-to-Person Sentiment Analysis." TACL, 2014.
- S. Kumar, R. West, J. Leskovec. "Disinformation on the Web: Impact, Characteristics, and Detection of Wikipedia Hoaxes." WWW, 2016.
- R. West, R.W. White, E. Horvitz. "From Cookies to Cooks: Insights on Dietary Patterns via Analysis of Web Usage Logs." WWW, 2013

Notable engagements:

- Co-organizer of **Applied Machine Learning Days**, one of Europe's largest machine learning and artificial intelligence events
- Founder and co-organizer of Wiki Workshop (held at ICWSM 2015, WWW 2016, ICWSM 2016, WWW 2017, WWW 2018), the primary workshop event for Wikipedia researchers.

Current digital trust projects with non-academic partners:

- Collaboration with CLIQZ, a privacy-aware Web browser: development and deployment of a decentralized machine learning framework for learning user models while learning nearly nothing about individual users.