Quattro S **Initiative**

Security, **S**afety, **S**overeignty, **S**ocial Product

Eradicate Faults and Backdoors in Information Technology and Facilitate Innovation

The ***Quattro S*** **Initiative** proposes to use the emerging approaches of openness and formal verification (mathematical proof techniques) *to develop a complete value chain for the key components of trustworthy IT systems.* This will allow eradicating accidental faults as well as backdoors, including those inserted by malicious state actors (Fig. 1, 2). We aim for a level of assurance that cannot be attained through traditional approaches based on testing, artefact inspection or post-hoc patching. The proposed research includes the topic of the control of the supply chain. It is suggested to set up internationally cooperating groups to share costs, but also to conduct risk analyses, to explore technical alternatives and to develop policy options.

Applying the paradigm of openness and formal verification to the complete IT value chain is important for protecting critical infrastructure, as well as the reputation of manufacturers of IT systems, and ready them for emerging regulation, e.g. of the Internet of Things (IoT). This will take time and require (but also stimulate) further innovation. The feasibility of this approach has been demonstrated by the formal verification of the seL4 operating system kernel (Klein et al. 2009). On-going research applies it to other software components, such as file systems (Chen et al. 2015, Amani et al. 2016) and processors (Wilding et al. 2010). Applying the approach eliminates several risks and will enable a more secure re-use of complex legacy software by sandboxing. It will raise the bar for attackers, who will then have to attack more difficult targets, e.g. by introducing Trojan horses at the hardware level, or by compromising the supply chain or the software tools used in chip design.

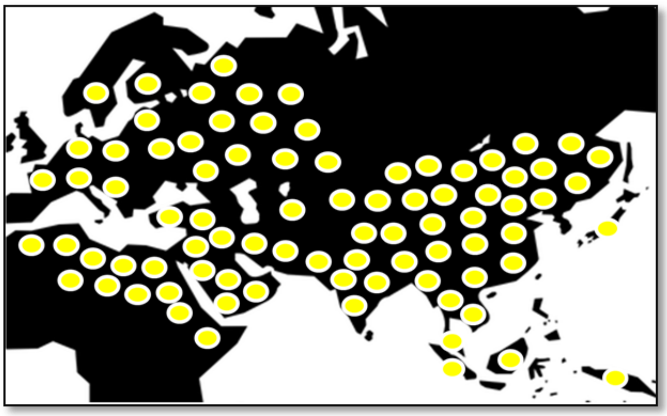	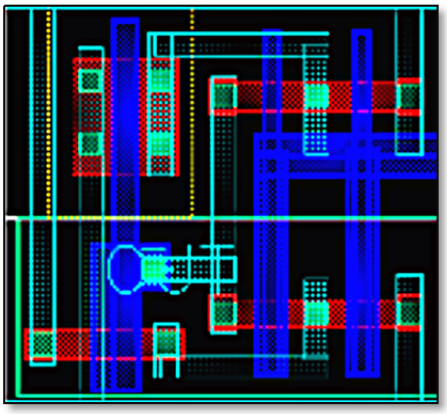
***Figure 1**:* Computers compromised by NSA. Each dot represents >500 compromised machines. Snowden revealed that, e.g., systems from HP, Dell and Cisco were compromised and Belgacom and Gemalto hacked. Illustration redesigned based on the Snowden slide "Worldwide SIGINT". Global supply chain risks have increased since.	***Figure 2:*** "The new concept of weapons… computer logic bombs." Colonels Liang and Xiangsui, PLA. Image shows hardware Trojan from research by Yang et al.

A core challenge is to secure manufacturing by untrusted semiconductor fabrication plants (fabs), which is essential for retaining the cost and energy efficiency advantages of state-of-the-art silicon processes which require investments in the billions that can only be amortized by huge production volumes.

Open design can be regarded as an important step for supporting innovation, reducing cost and enabling security analysis. It is well established for software, e.g. operating systems such as Linux and Android for servers and mobiles, and is emerging for hardware, with processor designs such as RISC-V, used, among others, by Microsemi and Secure-IC. Verification can certainly be improved, e.g. with machine-based analysis and evaluations conducted by different groups.

However, without formal proofs one can never be certain of having eliminated all vulnerabilities, so attackers might identify and hoard one for future use. The feasibility of verified real-world-capable components was established by the formal verification of the seL4 operating system kernel (Fig. 3), which triggered a wave of activities on verified software components. In hardware, formal verification of parts of designs has been in routine use for decades, triggered by the Intel floating-point bug, and there is significant activity on verifying complete open-source RISC-V processors. Much of the open work has originated in public-sector and university research labs but is now attracting private investment. The US Department of Defense is strongly supporting the new paradigm:

"*Current commodity computer hardware and software are proprietary. A thorough security review cannot be performed on systems with undisclosed components."*

DARPA, 2019

Figure 3: Unmanned Boeing helicopter under control of mathematically proved seL4.

Openness and formal verification of critical components can increase security and can facilitate the secure composition of (sub-) systems. Thus, evaluated ready-to-use components will become available and can be included in innovative products.

Open architecture and hardware implementations will allow sourcing from different fabs, and also remove licensing costs. A strengthened security story will produce a competitive advantage to those building on this technology and will lower the cost of complying with stricter regulations. Beyond the obvious target market of defense, where the new paradigm will provide sovereignty regarding the components of the entire supply chain, it will also help securing critical infrastructure, cars, medical devices, the IoT, etc.

Making this a reality requires funding for the following lines of action and research:

1. ***Creation of national and international cooperating planning groups***
   - For creating plans on developing more and more open secure IT-components and entire value chains, if possible in international cooperation, for reducing costs e.g. of proofs. Covering topics such as business cases, local competences (e.g. fabs), standardization (e.g. modification of Common Criteria to focus on open design) and legislation.
   - Conducting risk analyses.
   - Disseminating findings and plans.
2. ***Work on proofs***
   - Development of a complete, proven chain of openly available components of an IT system, which has not yet been done, is costly and should therefore likely be performed in some cost sharing.
   - Work on improving formal methods for making their use easier and cheaper, e.g. for producing updates by the open-source community, who so far in general did not use proofs.
   - Integration of formal methods, e.g. into open Electronic Design Automation tools used in hardware production, such that they are without fault and/or produce verified results, to protect against Trojans and to ease innovation.

Examples of application: Components for communications systems, a security module or an AI-edge TPU (cf. Fig. 4, 5).

3. Work on securing chips from remote fabs

Development of methods for securing key elements of the entire supply chain, from mask production to the Printed Circuit Board, such as:

- Work on technology that prevents untrusted fabs from inserting malicious functionality, e.g., through cryptographically secure obfuscation, probabilistically checkable proofs of correctness or split production (cf. Šišejković et al., Seifert/Bayer, Sengupta et al.).
- Tracing chips using physically unclonable functions (PUFs; cf. Bruneau et al. 2019).

This needs to be done in an open way and evaluated for security as well as for organizational and economic feasibility.

Getting this project started will require initial funding of about €10 million, which can be split between investors and public institutions. Taking it to full scale may require funding comparable to what DARPA is slated to spend on IT for defense ($1.5 billion for its Electronic Resurgence Initiative, aiming at trustworthy, local supply chains, cf. Salmon 2017) - consider that China aims at locally controlled production, too. The benefit will be the availability of an increasing range of secure products from an increasing number of vendors, with open source elements, built to open standards thus ensuring interchangeability, cost competitiveness and economic welfare.

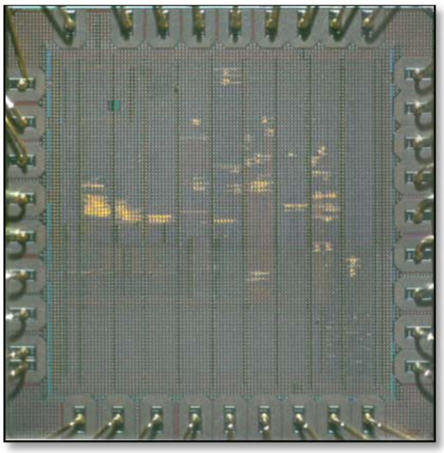	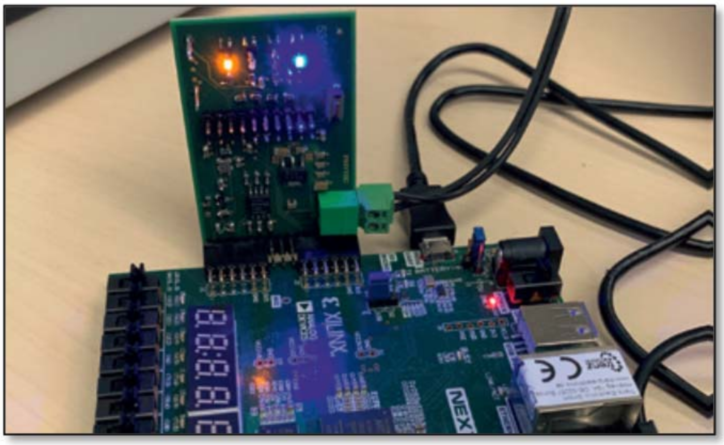
Figure 4: Secure element with open LEON SPARC v8 processor (Guilley).	***Figure 5:*** Proof-of-concept of an open source security module based on *VexRiscv*, with an integrated hardware accelerator for the *ChaCha* stream cipher, designed using open tools only, running on an FPGA (Schultz/Reith).

Further Information

White Paper: http://www.QuattroS-Initiative.org/

Weber, A.; Reith, S.; Kuhlmann, D.; Kasper, M.; Seifert, J.-P.; Krauß, C.: Open Source Value Chains for Addressing Security Issues Efficiently. IEEE CRE (CRS-C), Lisbon 2018. https://ieeexplore.ieee.org /document/8432033/

References

Amani, S. et al.: Cogent: verifying high-assurance file system implementations. ASPLOS '16. http://ssrg.nicta.com/publications/nicta_full_text/8956.pdf

Bruneau, N. et al.: Development of the Unified Security Requirements of PUFs During the Standardization Process. SecITC 2018. LNCS 11359. https://hal.archives-ouvertes.fr/hal-02265318/document

Chen, H. et al.: Using Crash Hoare Logic for Certifying the FSCQ File System. SOSP 2015. https://pdos.csail.mit.edu/papers/fscq:sosp15.pdf

Klein G. et al.: seL4: Formal Verification of an OS Kernel, ACM SIGOPS Symposium on Operating Systems Principles 2009. https://www.sigops.org/s/conferences/sosp/2009/papers/klein-sosp09.pdf

Salmon, L.: A Perspective on the Role of Open-Source IP In Government Electronic Systems. RISC-V Workshop 2017. https://content.riscv.org/wp-content/uploads/2017/12/Wed-1042-RISCV-Open-Source-LintonSalmon.pdf

Seifert, J.-P.; Bayer, C.: Trojan-Resilient Circuits. In: Pathan, A. (ed.): Securing Cyber-Physical Systems, Boca Raton 2015

Sengupta, A. et al.: A New Paradigm in Split Manufacturing: Lock the FEOL, Unlock at the BEOL. 2019. https://ieeexplore.ieee.org/document/8715281

Šišejković, D.; Merchant, F.; Leupers, R.; Ascheid, G.; Kegreiss, S.: Control-Lock: Securing Processor Cores Against Software-Controlled Hardware Trojans. ACM Great Lakes Symposium on VLSI 2019. https://dl.acm.org/citation.cfm?doid=3299874.3317983

Wilding, M. et al.: Formal Verification of Partition Management for the AAMP7G Microprocessor. Design and Verification of Microprocessor Systems for High-Assurance Applications 2010

About the Members of the Initiative

Prof. Anupam Chattopadhyay received his B.E. degree from Jadavpur University, India, MSc. from ALaRI, Switzerland and PhD from RWTH Aachen, Germany. During his doctoral studies, he worked on automatic RTL generation from the architecture description language LISA, which led to a spin-off which was acquired by Synopsys. In Aachen he led the multiprocessor system-on-chip architectures group as a Junior Professor. He developed several EDA techniques and hardware accelerators, which were successfully transferred to the semiconductor industry. In 2019 he became Professor at SCSE, Nanyang Technical University, Singapore. Anupam received the Borcher's plaque for his dissertation, nomination for the best IP award in the ACM/IEEE DATE Conference 2016 and nomination for the best paper award in the International Conference on VLSI Design 2018. He is an editor of the Springer book series on Computer Architecture and Design Methodologies.

Prof. Sylvain Guilley is CTO at Secure-IC, a French company offering security for embedded systems. Sylvain is also professor at Télécom-ParisTech, research associate at École Normale Supérieure (ENS), and adjunct professor at the Chinese Academy of Sciences (CAS). His research interests are trusted computing, cyber-physical security, secure prototyping in FPGA and ASIC, and formal/mathematical methods. Since 2012, he organizes the PROOFS workshop, which brings together researchers whose objective is to increase the trust in the security of embedded systems. Sylvain is also lead editor of international standards, such as ISO/IEC 20897 (Physically Unclonable Functions) and ISO/IEC 20085 (Calibration of non-invasive testing tools). Sylvain has co-authored 250+ research papers and filed 40+ patents. He is member of the IACR, the IEEE and senior member of the CryptArchi club. He is an alumnus of École Polytechnique and Télécom-ParisTech.

Prof. Gernot Heiser is Chief Research Scientist at CSIRO's Data61, the Australian government data research institution, and Scientia Professor at UNSW Sydney, where he holds the John Lions Chair of Operating Systems. He is the founder of Data61's Trustworthy Systems group which produced seL4, the world's first operating system with a mathematical correctness proof. His expertise is in operating systems, real-time systems, computer security and cyber-physical systems safety. He was the founder of Open Kernel Labs, whose L4 microkernel was deployed in billions of devices and now runs on the Secure Enclave of all iOS devices. He serves as Chief Scientist (Software) at German startup HENSOLDT Cyber. He is a Fellow of the Australian Academy of Technology and Engineering and a Fellow of the ACM and the IEEE. He has won multiple international prizes and awards, and authored many high-impact research publications.

Michael Kasper is heading the Cyber- and Information Security department at Fraunhofer Singapore and co-founder of opentrust.ai in Singapore. He is associated senior scientist with Fraunhofer Institute for Secure Information Technology, department of Cyber-Physical Systems in Darmstadt, Germany.

Prof. Christoph Krauß is head of the department Cyber-Physical Systems Security at Fraunhofer Institute for Secure Information Technology (SIT), Germany and professor for network security at University of Applied Sciences Darmstadt.

Philipp S. Krüger is Accenture Security's Managing Director for Germany, Switzerland, Austria and Russia. He was the founding Managing Director of the German National Digital Hub Cybersecurity, an initiative of the German Federal Ministry for Economic Affairs and Energy and Fraunhofer SIT. He has been Senior Strategic Advisor for the Commissioner for Strategic Armament for Cyberspace and Innovation at the German Federal Ministry of Defence and is a Non-resident Fellow and head of the Agile Cyber Deterrence Group at the Institute for Security Policy at Christian-Albrechts-University Kiel.

Dirk Kuhlmann is Senior Researcher at Fraunhofer Institute for Systems- and Innovation Research, Karlsruhe, Germany. From 1995 to 2017, he was a researcher at Hewlett Packard Laboratories Bristol, UK, focusing on the utilization of Open Source based components for improving platform and system security.

Prof. Steffen Reith is Professor of Theoretical Computer Science at the RheinMain University of Applied Sciences, Wiesbaden, Germany. He started his career at Elektrobit Automotive, a supplier of embedded software and services for the automotive industry where he was responsible for the development of products for BMW, Daimler and other automobile manufacturers and suppliers. Within the scope of this activity, digital signatures for secure firmware updates, mechanisms for activation codes and algorithms for cryptographically secured onboard networks were implemented. These products are still used in millions of vehicles today. Furthermore, he played a decisive role in the development of the predecessors of the AUTOSAR crypto-stack. Today, Steffen continues to work on cryptographic hardware and software for the automotive industry, including post-quantum cryptography.

Martin Schallbruch is the Deputy Director of the ESMT's Digital Society Institute (DSI) and Senior Researcher for Cyber Innovation and Cyber Regulation in Berlin, Germany. His research focuses on issues of cyber policies, cyber security and regulation in cyberspace. As a longtime Director General for Information Technology, Digital Society and Cyber Security in the German Federal Ministry of the Interior. Martin developed and implemented several government programs and legislative proposals such as the German National Cyber Security Strategy and the IT security act. He is a lecturer for IT security law at the Karlsruhe Institute of Technology (KIT) and co-author of the book "Cybersecurity in Germany" (Springer, 2018).

Prof. Jean-Pierre Seifert is the Einstein Foundation endowed Einstein Professor chairing the field "Security in Telecommunications" at TU Berlin and at Telekom Innovation Laboratories, Berlin (Germany). He has been working in research and development on hardware security at Infineon Technologies (Munich), Intel (Portland) and Samsung (San Jose) in the USA. Prof. Seifert has been honored by Infineon Technologies with the "Inventor of the Year" award and has received as well several "Intel Achievement Awards" for his new CPU security instructions for the Intel i7 Microprocessor series. He holds 40+ patents in the IT security field and was the key driver for several startups in the area of dependable and high assurance systems with successful exit strategies.

Dr. Arnd Weber is an economist, with a PhD in sociology. He has worked on digitally signed electronic money at Goethe University, Frankfurt and NTT, Yokosuka. He was Senior Researcher with the Institute for Technology Assessment and Systems Analysis of Karlsruhe Institute of Technology, Germany until retirement in 2018. Arnd has worked in various IT-related research projects, including several on behalf of the European Commission, the European Parliament and the German Federal Government. In 2004, he forecasted future economic problems of the European mobile industry due to insufficient support of cost-effective mobile Internet services.

Contacts

- Anupam Chattopadhyay: anupam@ntu.edu.sg
- Sylvain Guilley: sylvain.guilley@telecom-paristech.fr
- Gernot Heiser: gernot@unsw.edu.au
- Michael Kasper: michael.kasper@fraunhofer.sg
- Christoph Krauß: christoph.krauss@sit.fraunhofer.de
- Philipp S. Krüger: philipp.krueger@alumni.digitalhub-cybersecurity.com
- Dirk Kuhlmann: dirk.kuhlmann@alumni.tu-berlin.de
- Steffen Reith: Steffen.Reith@hs-rm.de
- Martin Schallbruch: martin.schallbruch@esmt.org
- Jean-Pierre Seifert: jpseifert@sect.tu-berlin.de
- Arnd Weber: arnd.weber@alumni.kit.edu

V. 1.7, 2019