Lucjan Hanzlik

+1 (650) 861-9289
hanzlik@cispa.saarland

Education

2011–2016 **PhD in Computer Science (mathematical sciences)**, *Institute of Computer Science Polish Academy of Sciences*, Warsaw, Poland.
Thesis with distinction: "Cryptographic Protocols for Modern Identification Documents", thesis advisors: prof. Mirosław Kutyłowski and dr Przemysław Kubiak.

2006–2011 **Master of Science in Computer Science**, *Wrocław University of Technology*, Wrocław, Poland.
Thesis: "Two Party Distributed RSA Key Generation - implementation on Java Cards", thesis advisor: dr Przemysław Kubiak.

Professional Experience

01.08.2020–currently **Faculty**, *CISPA-Helmholtz Center for Information Security*.
Responsibilities: research in the areas of cryptography and cybersecurity.

01.09.2018–31.07.2020 **Visiting Assistant Professor**, *Stanford University*.
Responsibilities: research in the areas of cryptography and cybersecurity.

01.07.2017–31.07.2020 **Research Group Leader**, *CISPA-Helmholtz Center for Information Security*.
Responsibilities: research in the areas of cryptography and cybersecurity.

01.10.2016–30.06.2017 **Research Assistant**, *Wrocław University of Technology*.
Responsibilities: teaching graduate and undergraduate students and conducting research.

01.10.2015–30.09.2016 **Principal investigator**, *Wrocław University of Technology*.
Project "Blind signatures and electronic identity documents". Responsibilities: project management, design of cryptographic algorithms, implementation on smart cards.

11.07.2016–31.08.2016 **External expert**, *Polish Ministry of Digital Affairs*.
Polish electronic identity document project (PL.ID). Responsibilities: consultation.

01.07.2015–30.09.2015 **PhD Fellow**, *Wrocław University of Technology*.
Internship in the Department of Computer Science, topic of internship "Anonymous online auctions using smart cards and auction theory". Responsibilities: design of cryptographic algorithms.

2015 **Investigator**, *Wrocław University of Technology*.
FNP IMPULS project "Biometric Keypress". Responsibilities: implementation of biometric techniques on a STM32F21X microcontroller.

01.09.2014–30.11.2014 **PhD Fellow**, *IBM Research*, Zurich, Switzerland.
Internship in the research group of dr Jan Camenisch, work on project FutureID EU FP7 318424. Responsibilities: designing a mechanism to backup device-bound anonymous credentials.

23.07.2014–31.08.2014 **Java Card Programmer**, *Research & Engineering Center (REC)*, Wrocław.
Short term contract. Responsibilities: programming of Java Cards.

01.07.2012–30.04.2014 **Principal investigator**, *Institute of Computer Science Polish Academy of Sciences.*
Project "Secure and authenticated communication between modern identity documents and a reader". Responsibilities: project management, design of cryptographic algorithms, implementation on smart cards.

01.03.2012–30.11.2013 **Independent analyst**, *Wrocław University of Technology*.
R&D project "Biometric techniques and PKI in modern identity documents and in the protection of information systems". Responsibilities: design of cryptographic algorithms, implementation on smart cards and implementation of a terminal on a raspberry Pi.

07.11.2011–31.12.2012 **Independent analyst**, *Wrocław University of Technology*.
R&D project "Detectors and sensors for measuring factors hazardous to environment - modeling and monitoring of threats". Responsibilities: design and implementation of a counting system based on GSM technology.

01.03.2011–30.06.2011 **Technician**, *Wrocław University of Technology*.
R&D project "Electronic signature for administration purposes". Responsibilities: design of cryptographic procedures.

Fellowships and Awards

2016 PhD thesis distinction "Cryptographic Protocols for Modern Identification Documents"

2015 PRELUDIUM program Laureate from National Science Center

2015 Award of the Dean of the Faculty of Fundamental Problem of Technology, Wrocław University of Technology

2014 IBM Great Minds Award

2014 Award of the Rector of Wrocław University of Technology

2014 Scholarship for best PhD students at Wrocław University of Technology

2013 Scholarship for best PhD students at Wrocław University of Technology

2012 VENTURES program Laureate from Foundation for Polish Science

2012 Scholarship given by the Foundation for Polish Science

Selected Publications

CCS'19 "Membership Privacy for Fully Dynamic Group Signatures"

USENIX Security'19 "simTPM: User-centric TPM for Mobile Devices"

Eurocrypt'19 "Ring Signatures: Logarithmic Size, No Setup – from Standard Assumptions"

PKC'19	"Efficient Non-Interactive Zero-Knowledge Proofs in Cross-Domains without Trusted Setup"
Asiacrypt'18	"Signatures with Flexible Public Key: Introducing Equivalence Classes for Public Keys."
APKC'17	"Two-Move and Setup-Free Blind Signatures with Perfect Blindness"
FC'16	"Blind Signatures from Knowledge Assumptions"

Academic Service

PC Member	SOFSEM 2021, IFIP SEC 2020, IFIP SEC 2018, SECPID 2017, Inscrypt 2017.
External Reviewing	Crypto 2019, CCS 2018, S&P 2017, Euro S&P 2017, ASIA CCS 2016, ESORICS 2014, ESORICS 2013.
Journals	Fundamenta Informaticae, International Journal of Information Security.

Languages

Polish	Native
English	Advanced
German	Advanced