Helger Lipmaa's Curriculum Vitae

Personal Particulars

1. Name: Helger Lipmaa
2. Date of birth: April 8th, 1972.
3. Citizenship: Estonian
4. Address:
   - Institute of Computer Science, Ülikooli 17, 51005 Tartu, Estonia
   - phone: +372 737 5429 (work)
   - email: `firstname.lastname[at]gmail.com`
   - WWW: `http://www.cs.ut.ee/~lipmaa`
5. Education: PhD, University of Tartu, 1999
6. Language skills: Estonian (native), English (fluent), Russian (passive)
7. Affiliation:
   (a) Lead research fellow(corresponds to research professor), University of Tartu, Estonia
   (b) Lead research fellow, Smartmatic-Cybernetica Centre of Excellence for Internet Voting (`http://www.ivotingcenter.ee`) (20%)

Work Experience

1989 Computer lab manager, Pärnu, Estonia.
1991–1991 Programmer, Pärnu Commerce Bank, Estonia.
1992–1992 Programmer, MesoCom Ltd (large scale databases), Estonia.
1994–1995 System-administrator and webmaster at the Department of Mathematics, University of Tartu, Estonia (Linux, WWW, ...).
1995–1995 Junior researcher at Institute of Computer Science, University of Tartu (complexity theory), Estonia.
01.11.1995–12.12.1995 Senior assistant at Institute of Computer Science, University of Tartu (complexity theory), Estonia.
12.11.1996–28.07.1997 Junior researcher at Institute of Cybernetics, Tallinn (cryptography), Estonia.
01.08.1997–31.03.2000 Senior research engineer at Küberneetika AS, a state-owned research and development company, a spin-off of Institute of Cybernetics (cryptography), Estonia.
01.02.2000–31.03.2001 Half-time lecturer (assistant professor) at Institute of Computer Science, University of Tartu, Estonia.
01.04.2000–31.07.2000 Researcher at Telecommunications Software and Multimedia Laboratory (TML), Helsinki University of Technology, Finland. (50%)
01.08.2000–31.07.2001 Senior researcher at the TML, Helsinki University of Technology, Finland.
01.08.2001–31.12.2004 Professor (pro tem) at the Laboratory for Theoretical Computer Science, Helsinki University of Technology, Finland.
01.01.2005–31.03.2005 Teaching researcher at the Laboratory for Theoretical Computer Science, Helsinki University of Technology, Finland.
01.04.2005–31.08.2006 Senior researcher, Cybernetica AS, Estonia.
01.04.2005–31.08.2006 Professor, University of Tartu, Estonia. (50%)
01.09.2006–31.07.2008 Senior lecturer, University College London, UK.
01.08.2008–31.07.2011 Senior researcher, Cybernetica AS, Estonia.
15.09.2008–31.08.2009 Docent (associate professor), University of Tartu, Estonia. (25%)
01.11.2009–2011 Professor, Tallinn University, Estonia. (30%)
01.08.2011–31.12.2013 Senior research fellow, University of Tartu, Estonia.
01.01.2014–... Lead research fellow (research professor), University of Tartu, Estonia.
01.09.2015–... Lead research fellow, Smartmatic-Cybernetica Centre of Excellence for Internet voting. (10%) (`http://www.ivotingcentre.ee/`)

Awards and main achievements (incomplete)

1987 Seventh place at the Estonian Chemistry Olympiad.
1988 Fourth place at the Estonian Mathematics Olympiad.
1990 Third place at the Estonian Mathematics Olympiad, fourth place at the Estonian Olympiad of Informatics. Member of the Estonian team at the Soviet Informatics Olympiad.
1992 Award from INTENTIA Dataarkitekten AB for successful studies.
1993 Finished undergraduate studies in 3 years instead of 4 (5/5 grades in all mathematical subjects).
1998 My first ever submitted paper was accepted to CRYPTO, the leading annual cryptographic conference (acceptance ratio 22.9%).
1998 Award from Estonian Science Foundation, Commission for Exact Sciences, for successful research.
1999 Publication "Time-stamping with Binary-linking schemes" was the only publication of high-importance from Institute of Computer Science, University of Tartu, mentioned in "Overview of Estonian Research and Development, 1996–1999".
1999 Award from Estonian Science Foundation, Commission for Exact Sciences, for successful research.
2000 Publication "Accountable Certificate Management using Undeniable Attestations" (ACM CCS 2000) invited to the Journal of Computer Security as one of the three best papers of ACM CCS 2000, a leading conference on general data security. (ACM CCS 2000 had acceptance ratio 21.4%)
2000 My student Oleg Mürk got an award from Estonian Academy of Sciences for successful research during undergraduate studies.
2001 Professor (pro tem) position at the Helsinki University of Technology at age 29, probably one of the youngest professors at this university.
2005 My student Johan Wallén got the Best Finnish Computer Science MSc Thesis Award by The Finnish Society for Computer Science.
2005 My work on cryptographic protocols was named as one of the two main achievements of the Institute of Computer Science, University of Tartu, 2005. (Another main achievement was Peeter Laud's work, with papers in ACM CCS 2005 etc.)
2006 My student Ago-Erik Riet won a prestigious stipend from Skype to continue graduate studies at the Cambridge University.
2006 Senior lecturer position at University College London, one of top 25 universities in the world.
2009 My student Ho Bae (UCL) has won the best paper award at a competition run by the National Intelligence Service of the Republic of Korea. The topic is related to Private Information Retrieval.
2010–2012 Member of the Board of Directors of International Association of Cryptologic Research.
2011 My student Bingsheng Zhang (Tartu) finished his PhD studies in two years (expected: four), having 8 papers.
2012 Our paper (coauthored with Bingsheng Zhang), published at SCN 2012, was one of the best papers that were further invited to the Journal of Computer Security
2014 Our paper (coauthored with Prastudy Fauzi and Bingsheng Zhang), published at FC 2014, was one of the best papers that were further invited to the journal "Information Security"
2016 My paper at AFRICACRYPT 2016 was invited to the journal "ÃŇnternational Journal of Applied Cryptography" as one of the best papers

Organisational activities and services to community

- A member of the IACR (International Association for Cryptologic Research). Member of the board of directors in 2010–2011.
- Doctoral school in computer science at University of Latvia, foreign representative for the governing board of the school.
- External reviewer for the next grant organisations: Hongkong's Research Grants Council (Competitive Earmarked Research Grant).
- Membership in steering committees: Nordic Workshop on Secure IT Systems (annual, Nordsec, 2002...), the Estonian Winter School in Computer Science (annual, 1998...), Estonian Theory Days (twice a year, 2002...).
- Member of editorial board: Baltic Journal of Modern Computing (`http://www.lu.lv/baltic-journal-of-modern-computing/editorial-board/`)
- General chair: *Eurocrypt 2011 (Tallinn, Estonia, 2011)*, Ecrypt II Hash function workshop (Tallinn,

Estonia, 2011 — with Andrea Röck), VOTEID 2011 (Tallinn, Estonia, 2011).

- Program Committee chair: Estonian Winter School in Computer Science 1998 (Palmse, Estonia), Seminar on Network Security 2002 (Sjökulla, Finland), NordSec 2005 (Tartu, Estonia — with Dieter Gollman), Inscrypt 2006 (Beijing, China — with Moti Yung), VoteID 2011 (Tallinn, Estonia — with Aggelos Kiayias), NordSec 2017 (Tartu, Estonia — with Katerina Mitrokotsa).
- Program Committee memberships (as a non-chair): SAC 2002 (St. John's, Newfoundland, Canada), FC 2003 (Guadeloupe), *FSE 2003 (Lund, Sweden)*, WISA 2003 (Jeju Island, Korea), ISC 2003 (Bristol, UK), NordSec 2003 (Gjøvik, Norway), IWAP 2003 (Kokura, Japan), INDOCRYPT 2003 (Delhi, India), FC 2004 (Key West, FL, USA), ACNS 2004 (Yellow Mountain, China), *ACM CCS 2004 (Washington, D.C., USA)*, Privacy and Security Aspects of Data Mining 2004 (Brighton, UK), NordSec 2004 (Helsinki, Finland), FC 2005 (Roseau, The Commonwealth Of Dominica), *CT-RSA 2005 (San Franscisco, CA, USA)*, ISC 2005 (Singapore), PSDM 2005 (New Orleans, LA, USA), ICISC 2005 (Seoul, Korea), FC 2006 (Anguilla BWI), *Eurocrypt 2006 (St Petersburg, Russia)*, WISA 2006 (Jeju Island, Korea), ISC 2006 (Samos Island, Greece), NordSec 2006 (Linköping, Sweden), ICISC 2006 (Busan, Korea), PADM 2006 (Hong Kong, China), *CT-RSA 2007 (Berkeley, Ca, USA)*, WCC 2007 (Circester, UK), PADM 2007 (Omaha, USA), ISC 2007 (Valparaiso, Chile), ProvSec 2008 (Shanghai, China), Indocrypt 2008 (Kharagpur, India), AFRICACRYPT 2009 (Gammarth, Tunisia), ProvSec 2009 (Guanzhou, China), CANS 2009 (Kanazawa, Japan), RLCPS 2010 (Tenerife, Spain), FC 2010 (Tenerife, Spain), *CT-RSA 2010 (Berkeley, USA)*, *Eurocrypt 2010 (Monaco)*, ESSCAS 2010 (Pedase, Estonia), NordSec 2010 (Helsinki, Finland), FC 2011 (St Lucia), RLCP 2011 (St Lucia), ESSCAS 2011 (Pedase, Estonia), ECML/PKDD 2011 (Athens, Greece), NordSec 2011 (Tallinn, Estonia), CANS 2011 (Sanya, China), FC 2012 (Bonaire, Netherlands Antilles), AFRICACRYPT 2012 (Ifrane, Morocco), Nordsec 2012 (Sweden), VOTEID 2013 (Surrey, UK), ISC 2013 (Dallas, USA), FC 2014 (Barbados), CANS 2014 (Heraklion, Greece), FC 2015 (San Juan, Puerto Rico), Cryptography and Coding 2015 (Oxford, UK), MFCS 2016 (Krakow, Poland), ISC 2016 (Honolulu, USA), VOTING 2017 workshop (Malta), IMA CC 2017 (Oxford).
- Session organizer: cryptography session at CIE 2017 (Turku, Finland).
- Session chair: Information Security Conference 2002 (São Paulo), *Fast Software Encryption 2003 (Lund, Sweden)*, NordSec 2003 (Gjøvik, Norway), Financial Cryptography 2004 (Key West, FL, USA), *Public Key Cryptography 2004 (Singapore)*, NordSec 2004 (Espoo, Finland), *ICALP 2005 (Lisboa, Portugal)*, ICICS 2005 (Beijing, China), CANS 2005 (Xiamen, China), *Eurocrypt 2006 (St Petersburg, Russia)*, Inscrypt 2006 (Beijing, China), CANS 2008 (Hong Kong, China), VOTEID 2009 (Luxembourg), NordSec 2009 (Oslo, Norway), *Eurocrypt 2010 (Monaco)*, *ESORICS 2010 (Athens, Greece)*, PQCrypto 2011 (Taipei, Taiwan), SCN 2012 (Amalfi, Italy), *ICALP 2013 (Riga, Latvia)*, *Asiacrypt 2013 (Bangalore, India)*, FC 2014 (Bridgetown, Barbados), AFRICACRYPT 2016 (Fez, Morocco). Estonian Winter School in Computer Science and Estonian Theory Days and Estonian Theory Days (many times).
- Rump session chair: Inscrypt 2006 (Beijing, China).
- The rest:
  - One of the organisers of the 1998 cryptography seminars in Tartu.
  - One of the organisers of the 1998-99 quantum computing seminars in Tartu.
  - One of the organisers of the 2000 seminar on the "Information Technology And Its Business Aspects" in Tartu.

Visibility

- As of 15.01.2017, according to Scholar.Google.Com, I have 3201 citations and H-index 27. (See `http://www.cs.ut.ee/~lipmaa/cites/` for more information.)

Grants

As a grant owner:
1994 Tempus S_JEP-06145-94 grant, 3 month study period in Aarhus University, Complexity Theory.
1996 Tempus Individual Mobility Grant, 4.5 month study period in Aarhus University.
1997 Estonian Science Foundation grant, "Research and Studies in the Field of Cryptology".

2000 Senior researcher grant from TEKES (Finnish National Technology Agency) for one year. Results: three papers.

2001 AWACS-HUT grant for two months (Nokia). Results: two papers and one patent application.

2001–2005 Scientific leader of the Krypto project at the HUT, funded by the Finnish Defence Forces. From 2002 to 2004 employed Markku-Juhani O. Saarinen and Johan Wallén, in 2005 employed Johan Wallén and Emilia Käsper. (From April 1, 2005, project was led by prof. Kaisa Nyberg.)

2004–2007 Cryptology and Data-mining (CRYDAMI) project, HUT, funded by the Finnish Academy of Sciences. Employed one PhD student (Sven Laur). (From April 1, 2005, project was led by prof. Kaisa Nyberg.)

2005–2007 Base funding grant from the University of Tartu to start up a new research project. Subject: "Cryptographic protocols".

2006–2008 ETF (Estonian Science Foundation) grant 6848, "Privacy-Preserving Data Mining: Cryptographic Methods."

2009–2011 ETF (Estonian Science Foundation) grant 8058, "Efficient Cryptocomputing."

2012–2014 ETF (Estonian Science Foundation) grant 9303, "Efficient and Secure Cryptographic Protocols."

As one of the main researchers (but not grant owner, very incomplete):

1994–95 Estonian Science Foundation grant. no. 1203, "Counting hierarchy and complexity of Boolean formulae with quantifiers". (Grant owner: Mati Tombak)

1998 Estonian Science Foundation grant 3742, "Digital Time-Stamping".

1999 Phare HESR grant "Time-Stamping Server". Results (combined with the previous grant): 3 papers, PhD thesis and one patent application.

2004–2005 Participant of the GO-SEC project (HUT, funded by the Tekes), 8 months. Employed one MSc student (Emilia Käsper).

2006–2010 Target funding "Theoretical and Practical Security of Heterogeneous Information Systems" (grant owner Ahto Buldas)

2013–2018 Institutional Research Funding IUT2-1 "Provably Secure and Verifiable Systems" (grant owner Dominique Unruh)

2013–2015 ICT Programme grant, "Quantum cryptography beyond key distribution" (grant owner Dominique Unruh)

2013– Estonian representative of the COST action "Computational Social Choice"

2013– Estonian representative of the COST action "Cryptography for Secure Digital Interaction"

2015– Site coordinator of the H2020 Project "Panoramix"

Teaching qualifications

1. As the principal investigator from University of Tartu, participated in creating a joint Nordic Master Programme in data security and mobile computing, NordSecMob, `http://nordsecmob.tkk.fi/`
2. Pedagogical training: attended a course on Didactics of Informatics (1992)
3. Practical experience of teaching:
   - Lead several exercise sessions in 1994. . . 1996
   - Taught lecture courses:
     - "Introduction to Cryptology", Tallinn Technical University, Spring 1997. (2 hours a week)
     - "Cryptology", University of Tartu, Autumn 1997. (2 hours a week)
     - "Cryptology", University of Tartu, Spring 2000. (2 hours a week). Course notes in Estonian.
     - "Seminar on Network Security", Helsinki University of Technology (HUT), Autumn 2000.
     - "Methods of Cryptology", HUT, Spring 2001. (2 hours a week)
     - "Special Course on Cryptology", HUT, Autumn 2001–2003. (2 hours a week)
     - "Seminar on Cryptology and Security Protocols", HUT, Autumn 2001.
     - "Cryptography and Data Security", HUT, Spring 2002–2004. (3 hours a week) Slides in English
     - "Cryptology: Special Topics", HUT, Spring 2002–2005. (2 hours a week)
     - "Postgraduate Course in Theoretical Computer Science", HUT, Autumn 2004. (2 hours a week)

  - "Research Seminar in Cryptography", University of Tartu, Autumn 2005. (2 hours a week) — student evaluation 4.67/5 (average in Institute: 3.64/5)
  - "Cryptographic Protocols", University of Tartu, Spring 2006. (2 hours a week)
  - "Graduate Seminar in Cryptography", University of Tartu, Spring 2006. (2 hours a week)
  - "Crypto II", University College London, Spring 2008. (total 30 hours)
  - "Graduate Seminar in Cryptography", University of Tartu, Autumn 2008. (2 hours a week)
  - "Research Seminar in Cryptography", University of Tartu, Spring 2009. (2 hours a week)
  - "Cryptographic Protocols", University of Tartu, Fall 2011, 2012, 2013, 2014, 2015. (2 hours a week)
  - "Complexity Theory", University of Tartu, Fall 2012 and 2013. (2 hours a week)
- Lecture courses in summer/winter schools:
  - "Zero-knowledge: theory and applications" in Nordic Research Training course "Cryptology and Its Applications", Bergen, June 10-18, 2004
  - Lecture course on cast-as-intended e-voting in the Second International Summer School on Secure Voting, SecVote 2012, Dagstuhl, July 16–20, 2012
- PhD theses supervised: Sven Laur (2008, Helsinki University of Technology), Bingsheng Zhang (2011, University of Tartu), Prastudy Fauzi (2017, University of Tartu), Rafik Chaabouni (2017, EPFL).
- BSc/MSc theses supervised:
  - From the University of Tartu: Piret Ulp (BSc in 1998, cum laude), Meelis Roos (MSc in 1999, cum laude), Priit Karu (semester work 1999, BSc 2000, cum laude), Rasmus Alop (semester work 1999), Oleg Mürk (semester work, 2000, for this Oleg won an award from Estonian Academy of Sciences; BSc thesis, 2001, cum laude), Sven Laur (MSc thesis 2002, cum laude), Emilia Käsper (MSc 2006, Prastudy Fauzi (MSc, 2012, Complexity Analysis of Hardware-Assisted Attacks on A5/1), Kairi Kangro (BSc 2013), Hendri (MSc 2013), Janno Siim (MSc 2016).
  - From the Helsinki University of Technology: Lauri Tarkkala (MSc in 2001), Johan Wallén (MSc in 2003, the Best Finnish Computer Science MSc Thesis Award by The Finnish Society for Computer Science, 2005)
  - From the University College London: Ho Bae and Bingsheng Zhang (co-supervisor with Jens Groth, MSc 2008).
- Current students: Janno Siim (PhD student, University of Tartu, started in September 2016), Behzad Abdolmaleki (PhD student, Tartu, started in April 2016), Karim Baghery (PhD student, Tartu, started in September 2016), Annabell Kuldmaa (MSc student, Tartu, started in September 2015).
- Joint papers with students (while they were students): 6 with Sven Laur, 2 with Johan Wallén, 2 with Bingsheng Zhang, 2 with Rafik Chaabouni, 4 with Prastudy Fauzi.
- Opponent/reviewer of the following theses:
  - Jan Willemson (PhD thesis "Size-efficient Interval Time Stamps", University of Tartu, 2002).
  - Lan Duy Nguyen (PhD thesis "Cryptographic-based Privacy Enhanching Technology", University of Wollongong, Australia, 2005).
  - Mårten Trolin (PhD thesis "Electronic Cash and Hierarchical Group Signatures", KTH, Sweden, 2006).
  - Margus Niitsoo (PhD thesis "Black-box Oracle Separation Techniques with Applications in Time-stamping", University of Tartu, Estonia, 2011).
  - Björn Terelius (PhD thesis "Some Aspects of Cryptographic Protocols with Applications in Electronic Voting and Digital Watermarking", KTH, Sweden, 2015).
  - Bernardo David (PhD thesis "A Framework For Efficient Homomorphic Universally Composable Commitments", University of Aarhus, Denmark, 2017).
- Participant in PhD committees (*not* including Estonia):
  - Salerno, Italy, 15.04.2012. (5 defenses, including two in cryptography: Angelo De Caro, Alessandra Scafuro)

4. Produced teaching materials: two books in Estonian, slides for various courses. One book chapter

on e-voting in "The Handbook of Information Security" (Wiley, 2005).

5. Member of the Steering and Program Committee of the Estonian Winter School of Computer Science (1998–2010), organiser of the Estonian Theory Days (since 2002), and various extra-curriculum seminars in Estonia in 1998. . . 2000.
6. Organised the next mini-courses at the Helsinki University of Technology: "Provable Security" (Phil Rogaway, 2002), "Quantum Computation" (Andris Ambainis, 2002), "Design of AES" (Vincent Rijmen, 2003), at the University of Tartu: "Selected Topics in Algorithmic Game Theory" (Edith Elkind, 2005), "Software Obfuscation" (Yury Lifshits, 2006), and at the Tallinn University: "Algorithmic Game Theory" (Edith Elkind, 2010).

Impact in practice

- Governmental projects
  - Participant in time-stamping project (1997–2000; other members: Ahto Buldas, Jan Willemson, Peeter Laud, Meelis Roos, Arne Ansper, . . .) that was initiated to create the necessary technical background to the Estonian Law of Digital Signatures. The law is in force since December 2000.
  - Contractor for Estonian government, electronic voting project, 2001. Member of the e-voting project, 2003. Contractor in new e-voting project, 2012.
  - Participated in the preparation of the Norwegian Internet voting project, 2009. We proposed the setting (specified in our Esorics 2010 publication) that was/is in Norway.
- Patent applications (both cancelled for various reasons):
  - U.S. patent application. Application No. 09,375,935 for: Time-stamping with Binary Linking Schemes. File No.: A-66712. (Inventors Ahto Buldas, Peeter Laud, Helger Lipmaa and Jan Villemson).
  - 1 more patent application (Nokia) was withdrawn.
- Member of the Technical Advisory Board, GuardTime
- Standardisation activities: my work, co-authored with Buldas et alt., on time-stamping has been under standardisation in the ISO SC27 work group. I was an active participant of the AES (Advanced Encryption Standard) process (publications [13,76,92]).

Additional studies and research visits

1987–1990 The school of exact sciences (mathematics exercises of olympiad level, graded by university teachers).
1987–1990 Member of the Research Union of School Students (mathematics).
1989–1990 Chemistry club at the high school.
1989–1990 Training sessions for mathematics olympiads. (Lectures and laboratories by university professors etc.)
1994 DAIMI, Aarhus University, Denmark (3 months, complexity theory)
1996 DAIMI, Aarhus University, Denmark (4.5 months, complexity theory and cryptography)
1997 New Trends in Computer Science and Information Technology, Palmse (1 week)
1997 School on Natural Computation, Turku (1 week)
1998 Parallel and Quantum Computation, Palmse, Estonia (1 week)
1998 Summer School in Cryptography and Data Security, Aarhus, Denmark (1 week)
1999-2005 Estonian Winter School in Computer Science (Palmse, Estonia, à 1 week)
2000 Nevanlinna Prize Special Event, Helsinki, Finland (1 day)
2000 Tutorial "Network Security and IPsec" (J. Ioannides (AT&T) and A. Keromytis (Univ. of Pennsylvania)), Athens, Greece
2000 Tutorial "Electronic Payment Technologies" (Y. Frankel, eCash Technologies), Athens, Greece
2002 Tutorial "Constructive Applications of the Weil and Tate Pairings" (Alfred Menezes, University of Waterloo), Hyderabad, India
2004 "The State of Art in Stream Ciphers", (Brugge, Belgium, 3 days)
2005 Two-week research visit to I2R, Singapore.
2007 Two-week research visit to CUHK, Hong Kong.

2008 Three-week research visit to Tsinghua University, China.
2009 Short research visit to Macquarie University, Australia.
2011 Short research visit to NTU, Singapore.
2013 Short research visit to University of Latvia.
2014 Research visit (3 weeks) to University of Athens, Greece.
2014 Short research visit to Aalto University, Finland.
2016 Short research visit to University of Warsaw, Poland.
2017 Two-week research visit to University of Athens, Greece.

Other information

- Computer experience: started active programming during the high school (assembly coding for 6502 and Z80, finished a few games and partial game development environments for two different home computers). Programmed in many programming languages (including some constructed by myself) and operating systems (including Apple DOS, CP/M, MSX DOS, MS DOS and derivatives, VMS, different Unix platforms). Most of the research is backed by actual computer implementations. Author of the world's fastest implementations of several block ciphers, most importantly AES, for the early Pentium family (Pentium Pro, Pentium MMX, Pentium II) of microprocessors.

Publications

Books

1. Vello Hanson, Ahto Buldas, Tarvi Martens, Helger Lipmaa, Arne Ansper, Viljar Tulit, "Infosüsteemide turve I. Turvarisk" Küberneetika AS, 1997, 125 pages ["Security of Information Systems I.", book, in Estonian. This and the next book can be bought online at `http://www.raamatukoi.ee/cgi-bin/kirjastus?300`]
2. Vello Hanson, Ahto Buldas, Tarvi Martens, Helger Lipmaa, Arne Ansper, Viljar Tulit, "Infosüsteemide turve II. Turbetehnoloogia" Küberneetika AS, 1998, 372 pages ["Security of Information Systems II", book, in Estonian]

Chapters in Books

3. Helger Lipmaa, "Kvantarvutid", Eesti Füüsika Seltsi 9. aastaraamat, 1999, pp. 102–125 ["Quantum Computing", Ninth Annual of the Estonian Physics Society. In Estonian. Invited paper.]
4. Helger Lipmaa. Secure Electronic Voting Protocols. A chapter from The Handbook of Information Security, volume 2, pages 647–657, Hossein Bidgoli, Editor-in-Chief. John Wiley & Sons, Inc., 2005.

Edited Books and Proceedings

5. Helger Lipmaa, Heidi Pehu-Lehtonen, 'Mobile security : proceedings of the Helsinki University of Technology Seminar on Network Security", Fall 2000. Espoo, Helsinki University of Technology, 2000.
6. Helger Lipmaa, Moti Yung, editors, "Inscrypt 2006", volume 4318 of *LNCS*, Springer, December 2006.
7. Aggelos Kiayias, Helger Lipmaa, editors, "VoteID 2011", volume 7397 of *LNCS*, Springer.

Thesis

8. Master thesis "Survey on the communication complexity", University of Tartu, 1995 (in Estonian)
9. PhD thesis "Secure and Efficient Time-Stamping Systems", University of Tartu, 1999.

Refereed proceedings and journals

10. Helger Lipmaa. IDEA: A cipher for multimedia architectures? In Stafford Tavares and Henk Meijer, editors, *Selected Areas in Cryptography '98*, volume 1556 of *LNCS*, pages 248–263, Kingston, Canada, 17–18 August 1998. Springer, Heidelberg.

11. Ahto Buldas, Peeter Laud, Helger Lipmaa, and Jan Villemson. Time-Stamping with Binary Linking Schemes. In Hugo Krawczyk, editor, *Advances in Cryptology — CRYPTO '98*, volume 1462 of *LNCS*, pages 486-501. Springer, Heidelberg, 1998.
12. Ahto Buldas, Helger Lipmaa, and Berry Schoenmakers. Optimally Efficient Accountable Time-Stamping. In Hideki Imai and Yulieng Zheng, editors, *Public Key Cryptography '2000*, volume 1751 of Lecture Notes in Computer Science, pages 293–305, Melbourne, Australia, 18–20 January 2000. Springer Verlag.
13. Kazumaro Aoki and Helger Lipmaa. Fast Implementations of AES Candidates. In *Third AES Candidate Conference*, New York City, USA, 13–14 April 2000.
14. Ahto Buldas, Peeter Laud, and Helger Lipmaa. Accountable Certificate Management using Undeniable Attestations. In Sushil Jajodia and Pierangela Samarati, editors, *7th ACM Conference on Computer and Communications Security*, pages 9–18, Athens, Greece, 1–4 November 2000. ACM Press.
15. Helger Lipmaa and Shiho Moriai. Efficient Algorithms for Computing Differential Properties of Addition. In Mitsuru Matsui, editor, *Fast Software Encryption '2001*, volume 2355 of *LNCS*, pages 336–350, Yokohama, Japan, 2–4 April 2001. Springer, Heidelberg, 2002.
16. Helger Lipmaa, N. Asokan, Valtteri Niemi, Secure Vickrey Auctions without Threshold Trust. In Matt Blaze, editor, *Financial Cryptography 2002*, volume 2357 of *LNCS*, Southampton Beach, Bermuda, 11–14 March 2002. Springer, Heidelberg.
17. Ahto Buldas, Peeter Laud, and Helger Lipmaa. Eliminating Counterevidence with Applications to Accountable Certificate Management. *Journal of Computer Security*, 10(3):273–296, 2002. Special issue for the best papers of ACM CCS 2000. One of the three invited papers.
18. Helger Lipmaa. Fast Software Implementations of SC2000. In Agnes Chan and Virgil Gligor, editors, *Information Security Conference 2002*, volume 2433 of Lecture Notes in Computer Science, pages 63–74, São Paulo, Brazil, 30 September — 2 October 2002. Springer, Heidelberg.
19. Helger Lipmaa. On Optimal Hash Tree Traversal for Interval Time-Stamping. In Agnes Chan and Virgil Gligor, editors, *Information Security Conference 2002*, volume 2433 of *LNCS*, pages 357–371, São Paulo, Brazil, 30 September — 2 October 2002. Springer, Heidelberg.
20. Helger Lipmaa. On Differential Properties of Pseudo-Hadamard Transform and Related Mappings. In Alfred Menezes and Palash Sarkar, editors, *INDOCRYPT 2002*, volume 2551 of *LNCS*, pages 48–61, Hyderabad, India, 15–18 December 2002. Springer, Heidelberg.
21. Helger Lipmaa. On Diophantine Complexity and Statistical Zero-Knowledge Arguments. In Chi Sung Laih, editor, *Advances on Cryptology — ASIACRYPT 2003*, volume 2894 of *LNCS*, pages 398–415, Taipei, Taiwan, November 30–December 4 2003. Springer, Heidelberg.
22. Helger Lipmaa. Verifiable Homomorphic Oblivious Transfer and Private Equality Test. In Chi Sung Laih, editor, *Advances on Cryptology — ASIACRYPT 2003*, volume 2894 of *LNCS*, pages 416–433, Taipei, Taiwan, November 30–December 4 2003. Springer, Heidelberg.
23. Edith Elkind and Helger Lipmaa. Interleaving Cryptography and Mechanism Design: The Case of Online Auctions. In Ari Juels, editor, *Financial Cryptography — Eighth International Conference*, volume 3110 of *Lecture Notes in Computer Science*, pages 117–131, Key West, FL, USA, February 9–12 2004. Springer, Heidelberg.
24. Andris Ambainis, Markus Jakobsson and Helger Lipmaa. Cryptographic Randomized Response Techniques. In Feng Bao, Robert H. Deng and Jianying Zhou, editors, *Public Key Cryptography 2004*, volume 2947 of *Lecture Notes in Computer Science*, pages 425–438, Singapore, March 1–4 2004. Springer, Heidelberg.
25. Helger Lipmaa, Johan Wallén and Philippe Dumas. On the Additive Differential Probability of Exclusive-Or. In Bimal Roy and Willi Meier, editor, *Fast Software Encryption 2004*, volume 3017 of *LNCS*, pages 317–331, Delhi, India, February 5–7 2004. Springer, Heidelberg.
26. Sven Laur and Helger Lipmaa. On Private Similarity Search Protocols. In Sanna Liimatainen and Teemupekka Virtanen, editors, *Proceedings of the Ninth Nordic Workshop on Secure IT Systems (NordSec 2004)*, pages 73–77, Espoo, Finland, November 4–5, 2004.
27. Bart Goethals, Sven Laur, Helger Lipmaa and Taneli Mielikäinen. On Private Scalar Product Computation for Privacy-Preserving Data Mining. In Choonsik Park and Seongtaek Chee, editors, *The 7th Annual International Conference in Information Security and Cryptology (ICISC 2004)*, volume 3506 of Lecture Notes in Computer Science, pages 104–120, Seoul, Korea, December 2–3,

2004. Springer, Heidelberg.
28. Edith Elkind and Helger Lipmaa. Small Coalitions Cannot Manipulate Voting. In Andrew Patrick and Moti Yung, editors, *Financial Cryptography and Data Security — Ninth International Conference*, volume 3570 of Lecture Notes in Computer Science, pages 285–297, Roseau, The Commonwealth Of Dominica, February 28–March 3, 2005. Springer, Heidelberg.
29. Helger Lipmaa, Guilin Wang and Feng Bao. Designated Verifier Signature Schemes: Attacks, New Security Notions and A New Construction. In Luis Caires, Guiseppe F. Italiano, Luis Monteiro, Catuscia Palamidessi, and Moti Yung, editors, *The 32nd International Colloquium on Automata, Languages and Programming, ICALP 2005*, volume 3580 of *LNCS*, pages 459–471, Lisboa, Portugal, July 11–15, 2005. Springer, Heidelberg.
30. Helger Lipmaa. An Oblivious Transfer Protocol with Log-Squared Communication. In Jianying Zhou and Javier Lopez, editors, *The 8th Information Security Conference (ISC'05)*, volume 3650 of Lecture Notes in Computer Science, pages 314–328, Singapore, September 20–23, 2005. Springer, Heidelberg.
31. Sven Laur, Helger Lipmaa and Taneli Mielikäinen. Private Itemset Support Counting. In Sihan Qing, Wenbo Mao and Javier Lopez, editors, *Seventh International Conference on Information and Communications Security, ICICS '05*, volume 3783 of Lecture Notes in Computer Science, pages 97–111, Beijing, China, December 10–13, 2005. Springer, Heidelberg.
32. Yong Li, Helger Lipmaa and Dingyi Pei. On Delegatability of Four Designated Verifier Signatures. In Sihan Qing, Wenbo Mao and Javier Lopez, editors, *Seventh International Conference on Information and Communications Security, ICICS '05*, volume 3783 of *LNCS*, pages 61–71, Beijing, China, December 10–13, 2005. Springer, Heidelberg.
33. Edith Elkind and Helger Lipmaa. Hybrid Voting Protocols and Hardness of Manipulation. In Xiaotie Deng and Dingzhu Du, editors, *The 16th Annual International Symposium on Algorithms and Computation, ISAAC 2005*, volume 3827 of *LNCS*, pages 206–215, Sanya, Hainan, China, December 19–21, 2005. Springer, Heidelberg.
34. Ammar Alkassar, Elena Andreeva and Helger Lipmaa. SLC: Efficient Authenticated Encryption for Short Packets. In Erik Zenner and Stefan Lucks, editors, *Workshop "Kryptographie in Theorie und Praxis", part of the conference Sicherheit 2006*, volume ? of ?, pages 270–278, Magdeburg, Germany, February 20–22, 2006.
35. Sven Laur, Helger Lipmaa and Taneli Mielikäinen. Cryptographically Private Support Vector Machines. In Lyle Ungar, Mark Craven, Dimitrios Gunopulos and Tina Eliassi-Rad, editors, *The Twelfth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD 2006*, pages 618–624, Philadelphia, USA, August 20–23, 2006. ACM.
36. Sven Laur and Helger Lipmaa. A New Protocol for Conditional Disclosure of Secrets And Its Applications. In Jonathan Katz and Moti Yung, editors, *ACNS 2007*, volume 4521 of *LNCS*, pages 207–225, Zhuhai, China, June 5–8, 2007. Springer, Heidelberg.
37. Philippe Dumas, Helger Lipmaa and Johan Wallén. Asymptotic Behaviour of A Non-Commutative Rational Series with A Nonnegative Linear Representation. *Discrete Mathematics and Theoretical Computer Science*, 9(1):247–274, October 2007.
38. Giovanni Di Crescenzo and Helger Lipmaa. Succinct NP Proofs from An Extractability Assumption. In Arnold Beckmann, Costas Dimitracopoulos and Benedikt Löwe, editors, *Computability in Europe*, volume 5028 of *LNCS*, pages 175–185, Athens, Greece, June 15–20, 2008. Springer, Heidelberg.
39. Helger Lipmaa. New Communication-Efficient Oblivious Transfer Protocols Based on Pairings. In Tzong-Chen Wu and Chin-Laung Lei, editors, *11th Information Security Conference, ISC 2008*, volume 5222 of *LNCS*, pages 441–454, Taipei, Taiwan, September 15–18, 2008. Springer, Heidelberg.
40. Yvo Desmedt, Helger Lipmaa and Duong Hieu Phan. Hybrid Damgård Is CCA1-Secure under The DDH Assumption. In Matthew K. Franklin, Lucas Chi Kwong Hui and Duncan S. Wong, editors, *The 7th International Conference on Cryptology And Network Security (CANS 2008)*, volume 5339 of *LNCS*, pages 18–30, Hong Kong, China, December 2–4, 2008. Springer, Heidelberg.
41. Jin Tamura, Kazukuni Kobara, Ryo Nojima, Hideki Imai and Helger Lipmaa. A note on the error of Optimized LFC Private Information Retrieval Scheme. In Hirosuke Yamamoto (?), editor, *2008 International Symposium on Information Theory and its Applications, ISITA 2008*, volume ? of ?,

pages ?–?, Auckland, New Zealand, December 7–10, 2008. IEEE.
42. Giovanni Di Crescenzo and Helger Lipmaa. 3-Message NP Arguments in The BPK Model with Optimal Soundness And Zero-Knowledge. In Seok-Hee Hong, Hiroshi Nagamochi and Takuro Fukunaga, editors, *The 19th International Symposium on Algorithm and Computation, ISAAC 2008*, volume 5369 of *LNCS*, pages 616–628, Gold Coast, Australia, December 15–17, 2008. Springer, Heidelberg.
43. Arne Ansper, Sven Heiberg, Helger Lipmaa, Tom André Øverland and Filip van Laenen. Security and Trust for the Norwegian E-voting Pilot Project *E-valg 2011*. In Audun Jøsang, Torleiv Maseng, and Svein J. Knapskog, editors, *NordSec 2009*, 2009, volume 5838 of *LNCS*, pages 207–222, Oslo, Norway, October 14–16, 2009. Springer, Heidelberg.
44. Helger Lipmaa. First CPIR Protocol with Data-Dependent Computation. In Donghoon Lee and Seokhie Hong, editors, *ICISC 2009*, volume 5984 of *Lecture Notes in Computer Science*, pages 193–210, Seoul, Korea, December 2–4, 2009. Springer, Heidelberg.
45. Helger Lipmaa and Bingsheng Zhang. Efficient Generalized Selective Private Function Evaluation with Applications in Biometric Authentication. In Feng Bao, Moti Yung, Dongdai Lin and Jiwu Jing, editors, *Inscrypt 2009*, volume 6151 of *LNCS*, pages 154–163, Beijing, China, December 11–15, 2009. Springer, Heidelberg.
46. Sven Laur and Helger Lipmaa. On the Feasibility of Consistent Computations. In Phong Q. Nguyen and David Pointcheval, editors, *PKC 2010*, volume 6056 of *LNCS*, pages 88–106, Paris, France, May 26–28, 2010. Springer, Heidelberg.
47. Jens Groth, Aggelos Kiayias and Helger Lipmaa. Multi-Query Computationally-Private Information Retrieval with Constant Communication Rate. In Phong Q. Nguyen and David Pointcheval, editors, *PKC 2010*, volume 6056 of *LNCS*, pages 107–123, Paris, France, May 26–28, 2010. Springer, Heidelberg.
48. Helger Lipmaa and Bingsheng Zhang. Two New Efficient PIR-Writing Protocols. In Jianying Zhou and Moti Yung, editors, *ACNS 2010*, volume 6123 of *LNCS*, pages 438–455, Beijing, China, June 22–25, 2010. Springer, Heidelberg.
49. Rafik Chaabouni, Helger Lipmaa and Abhi Shelat. Additive Combinatorics and Discrete Logarithm Based Range Protocols. In Ron Steinfeld and Philip Hawkes, editors, *ACISP 2010*, volume 6168 of Lecture Notes in Computer Science, pages 336–351, Sydney, Australia, July 5–7, 2010. Springer, Heidelberg.
50. Sven Heiberg, Helger Lipmaa, and Filip van Laenen. On E-Vote Integrity in the Case of Malicious Voter Computers. In Dimitris Gritzalis, Bart Preneel and Marianthi Theoharidou, editors, *Esorics 2010*, volume 6345 of LNCS, pages 373–388, Athens, Greece, September 20–22, 2010. Springer, Heidelberg.
51. Helger Lipmaa. On the CCA1-Security of Elgamal and Damgård's Elgamal. In Xuejia Lai and Moti Yung, editors, *Inscrypt 2010*, volume 6584 of Lecture Notes in Computer Science, pages 18–35, Shanghai, China, October 20–23, 2010. Springer, Heidelberg.
52. Rafik Chaabouni, Helger Lipmaa, and Bingsheng Zhang. A Non-Interactive Range Proof with Constant Communication. In Angelos Keromytis, editor, *FC 2012*, volume 7397 of Lecture Notes in Computer Science, pages 179–199, Bonaire, The Netherlands, February 27–March 2, 2012. Springer, Heidelberg.
53. Helger Lipmaa. Progression-Free Sets and Sublinear Pairing-Based Non-Interactive Zero-Knowledge Arguments. In Ronald Cramer, editor, *TCC 2012*, volume 7194 of Lecture Notes in Computer Science, pages 169–189, Taormina, Italy, March 18–21, 2012. Springer, Heidelberg.
54. Helger Lipmaa. Secure Accumulators from Euclidean Rings without Trusted Setup. In Feng Bao, Pierangela Samarati and Jianying Zhou, editors, *ACNS 2012*, volume 7341 of Lecture Notes in Computer Science, pages 224–240, Singapore, June 26–29, 2012. Springer, Heidelberg.
55. Helger Lipmaa and Bingsheng Zhang. A More Efficient Computationally Sound Non-Interactive Zero-Knowledge Shuffle Argument. In Ivan Visconti and Roberto De Prisco, editors, *SCN 2012*, volume 7485 of Lecture Notes in Computer Science, pages 477–502, Amalfi, Italy, September 5–7, 2012. Springer, Heidelberg.
56. Bingsheng Zhang, Helger Lipmaa, Cong Wang and Kui Ren. Practical Fully Simulatable Oblivious Transfer with Sublinear Communication. In Ahmad-Reza Sadeghi, editor, *FC 2013*, volume 7859 of Lecture Notes in Computer Science, pages 78–95, Okinawa, Japan, April 1–5, 2013. Springer,

Heidelberg.
57. Helger Lipmaa and Tomas Toft. Secure Equality and Greater-Than Tests with Sublinear Online Complexity. In Fedor V. Fomin, Marta Kwiatkowska and David Peleg, editors, *ICALP 2013*, volume 7966 of Lecture Notes in Computer Science, pages 645–656, Riga, Latvia, July 8–12, 2013. Springer, Heidelberg.
58. Prastudy Fauzi, Helger Lipmaa and Bingsheng Zhang. Efficient Modular NIZK Arguments from Shift and Product. In Michel Abdalla, Cristina Nita-Rotaru and Ricardo Dahab, editors, *CANS 2013*, volume 8257 of Lecture Notes in Computer Science, pages 92–121, Paraty, Brazil, November 20–22, 2013. Springer, Heidelberg.
59. Helger Lipmaa. Succinct Non-Interactive Zero Knowledge Arguments from Span Programs and Linear Error-Correcting Codes. In Kazue Sako and Palash Sarkar, editors, *ASIACRYPT 2013*, volume 8269 of Lecture Notes in Computer Science, pages 41–60, Bangalore, India, December 1–5, 2013. Springer, Heidelberg.
60. Helger Lipmaa and Bingsheng Zhang. A More Efficient Computationally Sound Non-Interactive Zero-Knowledge Shuffle Argument. Journal of Computer Security, 21 (5):685–719, November 2013. IOS Press.
61. Prastudy Fauzi, Helger Lipmaa and Bingsheng Zhang. Efficient Non-Interactive Zero Knowledge Arguments for Set Operations. In Nicolas Christin and Rei Safavi-Naini, editors, *FC 2014*, volume ? of Lecture Notes in Computer Science, pages ?–?, Barbados, March 3–7, 2014. Springer, Heidelberg.
62. Helger Lipmaa. Efficient NIZK Arguments via Parallel Verification of Benes Networks. In Michel Abdalla and Roberto de Prisco, editor, SCN 2014, volume 8642 of Lecture Notes in Computer Science, pages 416–434, Amalfi, Italy, September 3–5, 2014. Springer, Heidelberg.
63. Helger Lipmaa and Vitaly Skachek. Linear Batch Codes. In Raquel Pinto and Paula Rocha, editors, ICMCTA 2014, volume ? of LNCS, pages ?–?, Palmela, Portugal, September 15–18, 2014. Springer, Heildeberg.
64. Aggelos Kiayias, Nikos Leonardos, Helger Lipmaa, Kateryna Pavlyk and Qiang Tang. Communication Optimal Tardos-based Asymmetric Fingerprinting. In Kaisa Nyberg, editor, *CT-RSA 2015,* volume 9048 of LNCS, pages 469–486, San Franscisoo, CA, USA, April 20–24, 2015. Springer, Heildeberg.
65. Aggelos Kiayias, Nikos Leonardos, Helger Lipmaa, Kateryna Pavlyk and Qiang Tang. Optimal Rate Private Information Retrieval from Homomorphic Encryption. Proceedings on Privacy Enhancing Technologies (2):222-243, 2015. De Gruyter Open.
66. Helger Lipmaa and Kateryna Pavlyk. Analysis and Implementation of An Efficient Ring-LPN Based Commitment Scheme. In David Naccache and Mike Reiter, editors, *CANS 2015*, volume ? of Lecture Notes in Computer Science, pages ?–?, Marrakesh, Morocco, December 8–12, 2015. Springer, Heidelberg.
67. Prastudy Fauzi and Helger Lipmaa. Efficient Culpably Sound NIZK Shuffle Argument without Random Oracles. In Kazue Sako, editor, *CT-RSA 2016*, volume 9610 of Lecture Notes in Computer Science, pages 200–216, San Franscisco, CA, USA, February 29–March 4, 2016. Springer, Heidelberg.
68. Helger Lipmaa. Prover-Efficient Commit-And-Prove Zero-Knowledge SNARKs. In David Pointcheval, editor, *AFRICACRYPT 2016*, volume 9646 of Lecture Notes in Computer Science, pages 185–206, Fes, Morocco, April 13–15, 2016. Springer, Heidelberg.
69. Prastudy Fauzi, Helger Lipmaa and Michał Zając. A Shuffle Argument Secure in the Generic Model. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016*, volume 10032 of Lecture Notes in Computer Science, pages 841–872, Hanoi, Vietnam, December 4–8, 2016. Springer, Heidelberg.
70. Florian Bourse, Fabrice Benhamouda and Helger Lipmaa. CCA-Secure Inner-Product Functional Encryption from Projective Hash Functions. In Serge Fehr, editor, *PKC 2017*, volume 10175 of Lecture Notes in Computer Science, pages 36–66, Amsterdam, Netherlands, March 28–31, 2017. Springer, Heidelberg.
71. Helger Lipmaa. Optimally Sound Sigma Protocols Under DCRA. In Aggelos Kiayias, editor, *FC 2017*, volume ? of Lecture Notes in Computer Science, pages ?–?, Malta, April 3–7, 2017. Springer, Heidelberg. Accepted.
72. Helger Lipmaa and Kateryna Pavlyk. A Simpler Rate-Optimal CPIR Protocol. In Aggelos Kiayias,

editor, *FC 2017*, volume ? of Lecture Notes in Computer Science, pages ?–?, Malta, April 3–7, 2017. Springer, Heidelberg. Accepted.

73. Helger Lipmaa. Prover-Efficient Commit-And-Prove Zero-Knowledge SNARKs. *International Journal of Applied Cryptography*, ? (?):?–?, ?. Accepted. (Invited as one of the best papers of AFRICACRYPT 2016.)
74. Prastudy Fauzi, Helger Lipmaa, Janno Siim and Michał Zając. An Efficient Pairing-Based Shuffle Argument. In Thomas Peyrin and Tsuyoshi Takagi, editors, *ASIACRYPT 2017*, volume ? of Lecture Notes in Computer Science, pages ?–?, Hong Kong, China, December 3–7, 2017. Springer, Heidelberg. Accepted.
75. Behzad Abdolmaleki, Karim Baghery, Helger Lipmaa and Michał Zając. A Subversion-Resistant SNARK. In Thomas Peyrin and Tsuyoshi Takagi, editors, *ASIACRYPT 2017*, volume ? of Lecture Notes in Computer Science, pages ?–?, Hong Kong, China, December 3–7, 2017. Springer, Heidelberg. Accepted.

Non-refereed workshops and invited papers (with publications)

76. Helger Lipmaa, Phillip Rogaway, and David Wagner. Comments to NIST Concerning AES-modes of Operations: CTR-mode Encryption. In *Symmetric Key Block Cipher Modes of Operation Workshop*, Baltimore, Maryland, US, 20 October 2000. Electronic proceedings available from `http://www.nist.gov/modes`.
77. Masahiko Takenaka, Helger Lipmaa, Naoya Torii.The Implementation of The Block Cipher SC2000 (III). In *ISEC Technical group meeting*, Tohoku University, Sendai, Japan, 18–19 July 2002. In Japanese.
78. Helger Lipmaa. Statistical Zero-Knowledge Arguments: Theory and Practice. In *4th European Congress on Computational Methods in Applied Sciences and Engineering (ECCOMAS 2004)*, Jyväskylä, Finland, 24-28 July 2004. Invited paper

Workshops without Publication

79. Andris Ambainis, Markus Jakobsson, Helger Lipmaa. Cryptographic Randomized Response Techniques. In *DIMACS/PORTIA Workshop on Privacy-Preserving Data Mining*. Rutgers University, Piscataway, NJ, USA, 15–16 March 2004. Program available at `http://dimacs.rutgers.edu/Workshops/Privacy/`
80. Edith Elkind and Helger Lipmaa. How Hard is it to Manipulate Voting?. In *DIMACS Workshop on Electronic Voting*, Rutgers U, NJ, USA, 26–27 May 2004. Program available at `http://dimacs.rutgers.edu/Workshops/Voting/`
81. Edith Elkind and Helger Lipmaa. Hybrid Voting Protocols and Hardness of Manipulation. In *First Spain Italy Netherlands Meeting on Game Theory*, Maastricht, The Netherlands, 24–26 June 2004. Webpage at `http://www.fdewb.unimaas.nl/sing/`
82. Helger Lipmaa. An Oblivious Transfer Protocol with Log-Squared Communication. In *The Past, Present and Future of Oblivious Transfer, Satellite workshop of the Fifth Haifa Workshop on Interdisciplinary Applications of Graph theory, Combinatorics, and Algorithms*, Haifa, Israel, May 17, 2005. Webpage at `http://cri.haifa.ac.il/events/2005/graph/oblivious.htm`.
83. Edith Elkind and Helger Lipmaa. Hybrid Voting Protocols and Hardness of Manipulation. In *1st International Workshop on Computational Social Choice*, Amsterdam, 6-8 December 2006. Webpage at `http://staff.science.uva.nl/~ulle/COMSOC-2006`.
84. Helger Lipmaa and Bingsheng Zhang. A More Efficient Computationally Sound Non-Interactive Zero-Knowledge Shuffle Argument. In *Verifiable Voting Schemes Workshop, from Theory to Practice*, Luxembourg, March 21–22, 2013. Webpage at`http://wwwen.uni.lu/snt/research/apsia/events`

Posters

85. Andris Ambainis, Markus Jakobsson, Helger Lipmaa, "Cryptographic Randomized Response Techniques", Estonian Winter School in Computer Science, Palmse, Estonia, March 3–7 2003.

Introductory Articles in Mass Media

86. Helger Lipmaa, "Turvalised virtuaalsed privaatvõrgud," Arvutimaailm 2/97, pp 6-7 ["Virtual Private Networks", a survey in Estonian.], 1997
87. Ahto Buldas, Helger Lipmaa, "Ajatemplid digitaaldokumentidel", Arvutimaailm 2/98, pp 45-47 ["Time-stamps on the digital documents", a technical survey in Estonian.]

Public Surveys, Preprints and Technical Reports (not complete)

88. Ahto Buldas, Peeter Laud, Helger Lipmaa, Jan Villemson, "Ajatempli protokollid, turvavajadused ja tehnilised nõuded", Technical Report DO-LU-X-22-1297, Küberneetika AS, 1997, 46 pages ["Timestamp protocols, security needs and technical requirements". Written by the order of Estonian Informatics Center for the work of committee preparing the legal use of electronic documents. In Estonian.]
89. Ahto Buldas, Helger Lipmaa, "Digital Signatures, Timestamps and the corresponding Infrastructure", Küberneetika AS, Technical Report 1998-21, Jan 1998, 7 pages
90. Ahto Buldas, Peeter Laud, Helger Lipmaa, Jan Villemson. Ajatemplisüsteemide teoreetilised alused. Küberneetika AS, Infotehnoloogia osakond, DO-AR-X-14-0698, 1998
91. Ahto Buldas, Peeter Laud, Alar Leibak, Helger Lipmaa, Jan Villemson, Krüptograafiliste protokollide formaalne turvaanalüüs. Küberneetika AS, Infotehnoloogia osakond, DO-AR-T-28-1298, 1998
92. Helger Lipmaa, "AES Candidates: A Survey of Implementations", Technical Report. Available from the list of submissions to the AES2 conference NIST Webpage, 8 pages, 1999.
93. Helger Lipmaa, "Security in On-Line Governance". Survey prepared under UNESCO project "Developing Telematics and Information Networks for On-Line Governance", June 1999. Available from `http://www.cc.ioc.ee/training/unesco/onlinegov/security/`
94. Ahto Buldas, Helger Lipmaa, Meelis Roos, Jan Villemson. Turvalised ja efektiivsed ajatemplisüsteemid. Küberneetika AS, Infotehnoloogia osakond, DO-LU-T-30-1299, 1999
95. Helger Lipmaa, "Digital Signatures and Authentication", June 1999. Updated version of a module in "Security in On-Line Governance". Available from `http://www.cyber.ee/research/publications/auth/`
96. Ahto Buldas, Helger Lipmaa, Jan Villemson. Avaliku võtme sertifikaatide haldus, kasutades vaidlustamatuid kehtivustõendeid. Küberneetika AS, Infotehnoloogia osakond, DO-AR-S-04-0500, 2000.
97. Ahto Buldas, Peeter Laud and Helger Lipmaa, "Accountable Certificate Management using Undeniable Attestations", Cryptology ePrint Archive, Report 2000/027, 2000. (Published in ACM CCS 2000.)
98. Helger Lipmaa, Shiho Moriai, "Efficient Algorithms for Computing Differential Properties of Addition", Cryptology ePrint Archive, Report 2001/001, 2001. (Published in FSE 2001.)
99. Helger Lipmaa, Oleg Mürk, 'E-valimiste realiseerimisvõimaluste analüüs", 33 pp, April 2001. In Estonian. ['An analysis of the possibility to organise e-voting". Analysis ordered by Estonian Department of Justice. Available from the governmental webpage of E-Voting, `http://www.riik.ee/evalimised/`]
100. Helger Lipmaa, "New Auction Mechanism with Bid Privacy and Minimal Cognitive Cost", 17 pp, 16 August 2001. (Nokia internal report.)
101. Helger Lipmaa, "Statistical Zero-Knowledge from Diophantine Equations", Cryptology ePrint Archive, Report 2001/086, 2001. (Superseded by 2003/105.)
102. Helger Lipmaa and N. Asokan and Valtteri Niemi, "Secure Vickrey Auctions without Threshold Trust", Cryptology ePrint Archive, Report 2001/095, 2001. (Published in FC 2002.)
103. Helger Lipmaa, "On Optimal Hash Tree Traversal for Interval Time-Stamping", Cryptology ePrint Archive, Report 2002/124, 2002. (Published in ISC 2002.)
104. Edith Elkind and Helger Lipmaa, "Interleaving Cryptography and Mechanism Design: The Case of Online Auctions", Cryptology ePrint Archive, Report 2003/021, 2003. (Published in FC 2004.)
105. Andris Ambainis, Markus Jakobsson, Helger Lipmaa, "Cryptographic Randomized Response Techniques", Cryptology ePrint Archive, Report 2003/027, 2003. (Published in PKC 2004.)
106. Helger Lipmaa, "On Diophantine Complexity and Statistical Zero-Knowledge Arguments", Cryp-

tology ePrint Archive, Report 2003/105, 2003. (Published in ASIACRYPT 2003.)
107. Helger Lipmaa, "An Oblivious-Transfer Protocol with Log-Squared Communication", Cryptology ePrint Archive, Report 2004/063, 2004.
108. Sven Laur and Helger Lipmaa, "Additive Conditional Disclosure of Secrets And Applications", Cryptology ePrint Archive, Report 2005/378, 2005.
109. Sven Laur and Helger Lipmaa, "Consistent Adaptive Two-Party Computations", Cryptology ePrint Archive, Report 2006/088, 2006.
110. Sven Laur, Helger Lipmaa and Taneli Mielikäinen. "Cryptographically Private Support Vector Machines", Cryptology ePrint Archive, Report 2006/198, 2006.
111. Emilia Käsper, Sven Laur and Helger Lipmaa. "Black-Box Knowledge Extraction Revisited: Universal Approach with Precise Bounds", Cryptology ePrint Archive, Report 2006/356, 2006.
112. Helger Lipmaa. "New Communication-Efficient Oblivious Transfer Protocols Based on Pairings", Cryptology ePrint Archive, Report 2007/133, 2007.
113. Helger Lipmaa. "Private Branching Programs: On Communication-Efficient Cryptocomputing", Cryptology ePrint Archive, Report 2008/107, 2008.
114. Helger Lipmaa. "How to Disassemble CPIR: First CPIR with Database-Dependent Computation", Cryptology ePrint Archive, Report 2009/395, 2009.
115. Rafik Chaabouni, Helger Lipmaa, and Abhi Shelat. "Additive Combinatorics and Discrete Logarithm Based Range Protocols", Cryptology ePrint Archive, Report 2009/469, 2009.
116. Sven Heiberg, Helger Lipmaa, and Filip Van Laenen. "On E-Vote Integrity in the Case of Malicious Voter Computers", Cryptology ePrint Archive, Report 2010/195, 2010.
117. Helger Lipmaa. "Progression-Free Sets and Sublinear Pairing-Based Non-Interactive Zero-Knowledge Arguments". Cryptology ePrint Archive, Report 2011/009, 2011.
118. Helger Lipmaa. "Two Simple Code-Verification Voting Protocols". Cryptology ePrint Archive, Report 2011/317, 2011.
119. Helger Lipmaa and Bingsheng Zhang. "A More Efficient Computationally Sound Non-Interactive Zero-Knowledge Shuffle Argument". Cryptology ePrint Archive, Report 2011/394, 2011.
120. Prastudy Fauzi, Helger Lipmaa and Bingsheng Zhang. "Efficient Modular NIZK Arguments from Shift and Product", Cryptology ePrint Archive, Report 2012/548, 2012.
121. Helger Lipmaa. "Succinct Non-Interactive Zero Knowledge Arguments from Span Programs and Linear Error-Correcting Codes". Cryptology ePrint Archive, Report 2013/121, 2013.
122. Prastudy Fauzi and Helger Lipmaa and Bingsheng Zhang. "Efficient Non-Interactive Zero Knowledge Arguments for Set Operations". Cryptology ePrint Archive, Report 2014/006, 2014.
123. Helger Lipmaa. A Simple Cast-as-Intended E-Voting Protocol by Using Secure Smart Cards. Cryptology ePrint Archive, Report 2014/348, 2014.
124. Helger Lipmaa. Almost Optimal Short Adaptive Non-Interactive Zero Knowledge. Cryptology ePrint Archive, Report 2014/396, 2014.

Presentations

Invited Talks at Conferences/Workshops

1. How hard is it to manipulate voting? Invited talk at the VOTEID 2009 workshop, 08.09.2009, Luxembourg.
2. Critical look at Estonian E-voting protocol. Invited talk at the Swiss E-Voting Workshop 2010, 06.09.2010, Fribourg, Switzerland.
3. Almost Optimal Short Adaptive Non-Interactive Zero Knowledge. Invited talk at CECC 2014, Budapest, Hungary.
4. A Shuffle Argument Secure in the Generic Model. Invited talk at CIE 2017, Turku, Finland.

Tutorials at conferences

1. Cryptographic techniques in privacy-preserving data-mining. In ECML/PKDD 2006, 18-22.09.2006, Berlin, Germany.
2. Cryptographic techniques in privacy-preserving data-mining. In Inscrypt 2006, 29.11-01.12.2006, Beijing, China.

Paper Presentations at Conferences

1. SAC 1998 (Kingston, Canada, 1998)
2. PKC 2000 (Melbourne, Australia, 2000)
3. ACM CCS 2000 (Athens, Greece, 2000)
4. FSE 2001 (Yokohama, Japan, 2001)
5. FC 2002 (Bermuda, 2002)
6. ISC 2002 (São Paulo, 2002, presented two papers)
7. INDOCRYPT 2002 (Hyderabad, 2002)
8. ASIACRYPT 2003 (Taipei, Taiwan, 2003, presented two papers)
9. FC 2004 (Key West, FL, USA, 2004)
10. PKC 2004 (Singapore, 2004)
11. ICALP 2005 (Lisbao, Portugal, 2005)
12. ISC 2005 (Singapore, 2005)
13. ACNS 2007 (Zhuhai, China, 2007)
14. ISC 2008 (Taipei, Taiwan, 2008)
15. CANS 2008 (Hong Kong, China, 2008)
16. ISAAC 2008 (Gold Coast, Australia, 2008)
17. Esorics 2010 (Athens, Greece, 2010)
18. Inscrypt 2010 (Shanghai, China, 2010)
19. FC 2012 (Bonaire, 2012)
20. TCC 2012 (Taormina, Italy, 2012)
21. ACNS 2012 (Singapore, 2012)
22. SCN 2012 (Amalfi, Italy, 2012)
23. FC 2013 (Okinawa, Japan, 2013)
24. ASIACRYPT 2013 (Bangalore, India, 2013)
25. FC 2014 (Barbados, 2014)
26. SCN 2014 (Amalfi, Italy, 2014)
27. CANS 2015 (Marrakech, Morocco, 2015)
28. AFRICACRYPT 2016 (Fez, Morocco, 2016)

Other Invited Presentations

1. "Virtual Private Networks", The Second Annual Information Security Training Seminar of the Institute of Cybernetics, Tallinn, 1996.
2. "IP-level encryption," The Third Annual Information Security Training Seminar, Tallinn, 1997, Küberneetika AS Technical Report DO-ÜV-T-20-1297, 16 pages
3. "Quantum algorithms," Estonian Autumn School of Young Physicists, 04.10.98-06.10.98.
4. "Fast cryptographic algorithms on multimedia processors", The Autumn Seminar of the Institute of Cybernetics, 1998.
5. "Formal security analysis of cryptographic protocols", The Autumn Seminar of the Institute of Cybernetics, 1998.
6. "Quantum algorithms," Seminars on quantum mechanics 1998.
7. "Three-Move Identification Schemes", Cybernetica Seminars, May 23 1999, slides 36 pages
8. "Optimally Efficient Accountable Time-Stamping", The Autumn Seminar of the Institute of Cybernetics, 1999.
9. Ahto Buldas, Helger Lipmaa, "Cryptographic methods and the security of e-commerce", E-commerce seminar of Estonian Chamber of Commerce and Industry, 27.10.1999.
10. "Fast Implementations of AES Candidates", Queensland University of Technology, Brisbane, Australia, 24.01.2000.
11. "Secure and Efficient Time-Stamping Systems", University of Wollongong, Wollongong, Australia, 25.01.2000.
12. "Secure and Efficient Time-Stamping Systems", Helsinki University of Technology, Helsinki, Finland, 07.03.2000.
13. "Secure and Efficient Time-Stamping Systems", University of Latvia, Riga, Latvia, 17.03.2000.
14. "Cryptography: from theory to practice", assembly of Estonian Mathematical Society, 25.03.2000.

15. "Accountable Certificate Management", Helsinki University, Helsinki, Finland, 26.09.2000.
16. "Efficient Algorithms for Differential Probability of Addition modulo 2^n and Related Problems", Helsinki University of Technology, Laboratory of Theoretical Computer Science, 14.12.2000.
17. "On Accountable Time-Stamping and Certificate Management", NTT Laboratories, Japan, 05.04.2001.
18. "Secure Vickrey Auctions without Threshold Trust", Estonian Theory Day, Roosta, Estonia, 16-17.10.2002.
19. "On Diophantine Complexity and Statistical Zero-Knowledge Arguments", Estonian Theory Day, Pedase, Estonia, 03-05.10.2003.
20. "Interleaving Cryptography and Mechanism Design: The Case of Online Auctions", Estonian Theory Day, Koke, Estonia, 30.01-01.02.2004.
21. "An Oblivious Transfer Protocol with Log-Squared Communication", Estonian Theory Day, Veskisilla, Estonia, 1-3.10.2004.
22. Invited for a research visit to Singapore, 16-31 Jan 2005. One talk: "An Oblivious Transfer Protocol with Log-Squared Communication", 25.01.2005.
23. "Designated Verifier Signatures: Attacks, New Security Notions And A Construction", Estonian Theory Day, Koke, Estonia, 04-06.02.2005.
24. "An Oblivious Transfer Protocol with Log-Squared Communication", University of Indiana at Bloomington, 14.02.2005.
25. "Designated Verifier Signatures: Attacks, New Security Notions And A Construction", National University of Singapore, Singapore, 26.09.2005.
26. "On delegatability of four designated verifier signatures", Estonian Theory Day, Viinistu, Estonia, 28.10.2005.
27. "An Oblivious Transfer Protocol with Log-Squared Communication", Xiamen University, China, 17.12.2005.
28. "Designated Verifier Signatures: Attacks, New Security Notions And A Construction", University College London, UK, 23.02.2006.
29. "Succinct NP Proofs from An Extractable-Algorithm Assumption", Estonian Theory Days, Voore, Estonia, 01.10.2006.
30. Cryptographic techniques in privacy-preserving data-mining (tutorial). In University of Bristol, UK, 22.01.2007.
31. Cryptographic techniques in privacy-preserving data-mining (tutorial). In Estonian Theory Days, UK, 28.01.2007.
32. Research visit, Chinese University of Hong Kong, March 2007 (2 weeks). Talks:
    - Cryptographic techniques in privacy-preserving data-mining (tutorial).
33. "Hybrid Damgård is CCA1-Secure", Estonian Theory Days, Estonia, 30.9.2007.
34. On Some Open Problems in Communication-Efficient Cryptocomputing, Royal Holloway, University of London, UK, 20.03.2008.
35. Research visit, Tsinghua University, China, May 12–31, 2008. Talks:
    - Private Branching Programs: On Communication-Efficient Cryptocomputing. Tsinghua, Beijing, China, 21.05.2008.
36. "Private branching programs: on communication-efficient cryptocomputing", Estonian Theory Days, Jõulumäe, Estonia, 03.10.2008.
37. Research visit, Macquarie University, Australia, Dec 18–22, 2008. Talks:
    - Private Branching Programs: On Communication-Efficient Cryptocomputing. Macquarie University, Sydney, Australia, 19.12.2008.
38. Research visit, National Technical University, Singapore, Jan 11–30, 2009. Talks:
    - Private Branching Programs: On Communication-Efficient Cryptocomputing. NTU, Singapore, 16.01.2009.
39. Additive combinatorics and discrete logarithm based range protocols. Estonian Theory Days, Mäetaguse, Estonia, 04.10.2008.
40. Multi-Query Computationally-Private Information Retrieval with Constant Communication Rate. Estonian Theory Days, Elva, Estonia, 13.06.2010.
41. On Norwegian Internet Voting Protocols. Joint Estonian-Latvian Theory Days, Rakari, Latvia, ??.10.2010.

42. Progression-Free Sets and Sublinear Pairing-Based Non-Interactive Zero-Knowledge Arguments. Estonian Theory Days, Nelijärve, Estonia 04.02.2011.
43. On Norwegian Internet Voting. Crypto/Security Reading Group, Tartu, Estonia. 20.04.2011.
44. Two presentations (on Estonian E-voting and Norwegian E-Voting), Dagstuhl seminar 11281 (Verifiable Elections and the Public), 10-15.07.2011.
45. A more efficient computationally sound non-interactive zero-knowledge shuffle argument. Estonian Theory Days, Tõrve, Estonia, 07.10.2011.
46. Progression-Free Sets and Sublinear Pairing-Based Non-Interactive Zero-Knowledge Arguments. Estonian Theory Days, Kubija, Estonia, 28.01.2012.
47. Progression-Free Sets and Sublinear Pairing-Based Non-Interactive Zero-Knowledge Arguments. Crypto reading group, University of Tartu, Estonia, 17.05.2012.
48. On Lattice-Based Cryptography. Crypto Day, University of Latvia, Riga, Latvia, 30.05.2012.
49. New Non-Interactive Zero-Knowledge Subset Sum, Decision Knapsack And Range Arguments. Joint Estonian-Latvian Theory Days, Medzabaki, Latvia, 29.09.2012.
50. Succinct Non-Interactive Zero Knowledge Arguments from Span Programs and Linear Error-Correcting Codes. In TCS seminar, University of Tartu, 14.03.2013.
51. A more efficient computationally sound non-interactive zero-knowledge shuffle argument. In "Verifiable and Secure Voting Workshop", Luxembourg, March 2013.
52. Succinct Non-Interactive Zero Knowledge Arguments from Span Programs and Linear Error-Correcting Codes. In "Quantum and Crypto Day", University of Latvia, 25.04.2013.
53. Succinct Non-Interactive Zero Knowledge Arguments from Span Programs and Linear Error-Correcting Codes. In workshop "Algebra and Its Applications", Piusa, Estonia, 26.04.2013.
54. Succinct Non-Interactive Zero Knowledge Arguments from Span Programs and Linear Error-Correcting Codes. In Finnish-Estonian Mathematics Days 2014 (Helsinki, Finland, 9-10.01.2014)
55. Almost Optimal Short Adaptive Non-Interactive Zero-Knowledge. CECC 2014 (Budapest, Hungary, May, 2014)
56. Efficient NIZK Argument for NP. In Joint Estonian-Joint Estonian-Latvian Theory Days, Ratnieki, Latvia, 04.10.2012
57. On More Efficient Computationally Sound Non-Interactive Zero-Knowledge Shuffle Arguments. Aalto University, Helsinki, Finland, 10.10.2014
58. Prover-Efficient Adaptive Zero-Knowledge SNARKs. University of Turku, Finland, 01.04.2015
59. Optimal Rate Private Information Retrieval from Homomorphic Encryption. Estonian Theory Days, Jõeküla, Estonia, 02.10.2015.
60. Optimal Rate Private Information Retrieval from Homomorphic Encryption. Invited talk at FIT 2016 (Yearly Polish meeting of Theoretical Computer Science), Warsaw, Poland.
61. Cryptographically Secure Mix-Nets. Summer School "Summer Research Institute 2016", EPFL, Lausanne, Switzerland, 21.06.2016.
62. Non-interactive Zero-Knowledge Proofs and Applications. 6th Crypto.Sec Day, Athens, Greece, 18.07.2016.
63. A Shuffle Argument Secure in the Generic Model. Estonian-Latvian Theory Days, Lilaste, Latvia, 14.10.2016.

Rump Session Presentations

1. "Efficient Algorithms for Differential Probability modulo 2^n and Related Problems" (Eurocrypt 2000, joint work with Shiho Moriai)
2. "On Optimal Hash Tree Traversal" (EWSCS 2001)
3. "On Additive Differential Probability of Exclusive Or" (Eurocrypt 2003, joint work with Johan Wallén, presented by Johan)
4. "How Hard is it to Manipulate Voting?" (FC 2004, joint work with Edith Elkind, presented by Edith)

Other Presentations

1. Several presentations at the Estonian Winter School in Computer Science, 1998–1999.

Panelist

1. "E-Voting: Challenge to the Society", Tallinn, Estonia, 19.06.2003.
2. Seminar on e-voting, Tartu, Estonia, 17.05.2004. Panel leader.
3. Swiss Workshop on e-voting, Fribourg, Switzerland, 06.09.2010

Last updated: August 14, 2017