CHES2014: Accepted Papers (in submission order)

1. **“Ooh Aah... Just a Little Bit”': A small amount of side channel can go a long way**
   Naomi Benger, Joop van de Pol, Nigel P. Smart, and Yuval Yarom
   University of Adelaide; University of Bristol; University of Bristol; University of Adelaide

2. **Embedded Evaluation of Randomness in Oscillator Based Elementary TRNG**
   Viktor Fischer and David Lubicz
   Hubert Curien Laboratory, University of Lyon; DGA-Maîtrise de l'information, Université de Rennes 1

3. **Cofactorization on Graphics Processing Units**
   Andrea Miele, Joppe W. Bos, Thorsten Kleinjung and Arjen K. Lenstra
   EPFL Lausanne; NXP Leuven; EPFL Lausanne; EPFL Lausanne

4. **EM Attack Is Non-Invasive? - Design Methodology and Validity Verification of EM Attack Sensor**
   Naofumi Homma, Yu-ichi Hayashi, Noriyuki Miura, Daisuke Fujimoto, Daichi Tanaka, Makoto Nagata, and Takafumi Aoki
   Tohoku University; Tohoku University; Kobe University; Kobe University; Kobe University; Kobe University; Tohoku University;

5. **Side-Channel Leakage through Static Power – Should We Care about in Practice?**
   Amir Moradi
   HGI, Ruhr University Bochum

6. **FOAM: Searching for Hardware-Optimal SPN Structures and Components with a Fair Comparison**
   Khoongming Khoo, Thomas Peyrin, Axel Poschmann, and Huihui Yap
   DSO National Laboratories; SPMS, Nanyang Technological University; NXP Semiconductors; DSO National Laboratories

7. **Entropy Evaluation for Oscillator-Based True Random Number Generators**
   Yuan Ma, Jingqiang Lin, Tianyu Chen, Changwei Xu, Zongbin Liu, and Jiwu Jing
   Institute of Information Engineering, Chinese Academy of Sciences

8. **A Statistical Model for Higher Order DPA on Masked Devices**
   Adam Ding, Liwei Zhang, Yunsi Fei, and Pei Luo
   Northeastern University

9. **FPGA implementations of SPRING (And their Countermeasures against Side-Channel Attacks)**
   Hai Brenner, Lubos Gaspar, Gaëtan Leurent, Alon Rosen, and François-Xavier Standaert.
   IDC Herzliya; UCL Crypto Group; INRIA Team SECRET; IDC Herzliya; UCL Crypto Group

10. **Destroying Fault Invariant with Randomization - A Countermeasure for AES against Differential Fault Attacks**
    Harshal Tupsamudre, Shikha Bisht, and Debdeep Mukhopadhyay
    IIT Kharagpur

11. **Fast Evaluation of Polynomials over Binary Finite Fields and Application to Side-channel Countermeasures**
    Jean-Sébastien Coron, Arnab Roy, and Srinivas Vivek
    University of Luxembourg, Luxembourg; University of Luxembourg, Luxembourg and Technical University of Denmark; University of Luxembourg, Luxembourg

12. **Reversing Stealthy Dopant-Level Circuits**
    Takeshi Sugawara, Daisuke Suzuki, Ryoichi Fujii, Shigeaki Tawa, Ryohei Hori, Mitsuru Shiozaki, and Takeshi Fujino
    Mitsubishi Electric Corp.; Mitsubishi Electric Corp.; Mitsubishi Electric Corp.; Mitsubishi Electric Corp.; Ritsumeikan Univ.; Ritsumeikan Univ.; Ritsumeikan Univ.

CHES2014: Accepted Papers (in submission order)

13. **Side-Channel Attack Against RSA Key Generation Algorithms**
    Aurélie Bauer, Eliane Jaulmes, Victor Lomné, Emmanuel Prouff, and Thomas Roche
    ANSSI

14. **Secure Lightweight Entity Authentication with Strong PUFs: Mission Impossible?**
    Jeroen Delvaux, Dawu Gu, Dries Schellekens, and Ingrid Verbauwhede
    Katholieke Universiteit Leuven and Shanghai Jiao Tong University; Shanghai Jiao Tong University; Katholieke Universiteit Leuven; Katholieke Universiteit Leuven

15. **Secure Conversion between Boolean and Arithmetic Masking of any order**
    Jean-Sébastien Coron, Johann Großschädl, and Praveen Kumar Vadnala
    University of Luxembourg

16. **Efficient Pairings and ECC for Embedded Systems**
    Thomas Unterluggauer and Erich Wenger
    IAIK, Graz University of Technology

17. **A New Framework for Constraint-Based Probabilistic Template Side Channel Attacks**
    Yossef Oren, Ofir Weisse, and Avishai Wool
    Columbia University; Tel Aviv University; Tel Aviv University

18. **Making RSA-PSS Provably Secure Against Non-Random Faults**
    Gilles Barthe, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, Mehdi Tibouchi, and Jean-Christophe Zapalowicz
    IMDEA Software Institute; IMDEA Software Institute; Université de Rennes 1, Institut Universitaire de France; INRIA; NTT Secure Platform Laboratories; INRIA

19. **Enhanced Lattice-Based Signatures on Reconfigurable Hardware**
    Thomas Pöppelmann, Léo Ducas, and Tim Güneysu
    Ruhr University Bochum; University of California, San-Diego; Ruhr University Bochum

20. **Early Propagation and Imbalanced Routing, How to Diminish in FPGAs**
    Amir Moradi and Vincent Immler
    HGI, Ruhr University Bochum; Fraunhofer Institute AISEC, Munich

21. **ICEPOLE: High-speed, Hardware-oriented Authenticated Encryption**
    Pawel Morawiecki, Kris Gaj, Ekawat Homsirikamol, Krystian Matusiewicz, Josef Pieprzyk, Marcin Rogawski, Marian Srebrny, and Marcin Wójcik
    Institute of Computer Science, Polish Academy of Sciences, Poland and University of Commerce, Kielce, Poland; George Mason University, USA; George Mason University, USA; Intel, Gdansk, Poland; Queensland University of Technology, Brisbane, Australia and Macquarie University, Australia; Cadence Design Systems, San Jose, USA; Institute of Computer Science, Polish Academy of Sciences, Poland and University of Commerce, Kielce, Poland; Cryptography and Information Security Group, University of Bristol, United Kingdom

22. **Compact Ring-LWE based Cryptoprocessor**
    Sujoy Sinha Roy, Frederik Vercauteren, Nele Mentens, Donald Donglong Chen, and Ingrid Verbauwhede
    COSIC, KU Leuven; COSIC, KU Leuven; COSIC, KU Leuven; City University of Hong Kong; COSIC, KU Leuven

23. **Efficient Power and Timing Side Channels for Physical Unclonable Functions**
    Ulrich Rührmair, Xiaolin Xu, Jan Sölter, Ahmed Mahmoud, Mehrdad Majzoobi, Farinaz Koushanfar, and Wayne Burleson
    TU München; UMass Amherst; FU Berlin; TU München; Rice University; Rice University; UMass Amherst

24. **How to Estimate the Success Rate of Higher-Order Side-Channel Attacks**

CHES2014: Accepted Papers (in submission order)

Victor Lomné, Emmanuel Prouff, Matthieu Rivain, Thomas Roche, and Adrian Thillard
ANSSI; ANSSI; CryptoExperts; ANSSI; ANSSI

25. **Gate-Level Masking Under a Path-Based Leakage Metric**
Andrew J. Leiserson, Mark E. Marson, and Megan A. Wachs
Cryptography Research, Inc.

26. **Physical Characterization of Arbiter PUFs**
Shahin Tajik, Enrico Dietz, Sven Frohmann, Dmitry Nedospasov, Jean-Pierre Seifert, Clemens Helfmeier, Christian Boit, and Helmar Dittrich
Technische Universität Berlin

27. **Get Your Hands Off My Laptop: Physical Side-Channel Key-Extraction Attacks on PCs**
Daniel Genkin, Itamar Pipman, and Eran Tromer
Technion and Tel Aviv University; Tel Aviv University; Tel Aviv University

28. **Good is Not Good Enough: Deriving Optimal Distinguishers from Communication Theory**
Annelie Heuser, Olivier Rioul, and *Sylvain Guilley*
Télécom ParisTech

29. **RSA meets DPA: Recovering RSA Secret Keys from Noisy Analog Data**
Noboru Kunihiro and Junya Honda
The University of Tokyo

30. **Simple Power Analysis on AES Key Expansion Revisited**
Christophe Clavier, Damien Marion, and Antoine Wurcker
University of Limoges, France

31. **Bitline PUF: Building Native Challenge-Response PUF Capability into Any SRAM**
Daniel E. Holcomb and Kevin Fu
University of Michigan

32. **Constructing S-boxes for Lightweight Cryptography with Feistel Structure**
Yongqiang Li and Mingsheng Wang
The State Key Laboratory of Information Security, Institute of Information Engineering,
Chinese Academy of Sciences

33. **Curve41417: Karatsuba revisited**
Daniel J. Bernstein, Chitchanok Chuengsatiansup, and Tanja Lange
University of Illinois at Chicago and Technische Universiteit Eindhoven; Technische Universiteit Eindhoven;
Technische Universiteit Eindhoven