LATINCRYPT | BOGOTÁ 2021

7th International Conference on Cryptology and Information Security in Latin America

1.**Tight Bounds for Simon's Algorithm**
Xavier Bonnetain
University of Waterloo, Canada

2. **Constructions for Quantum Indistinguishability Obfuscation**
Anne Broadbent, Raza Ali Kazmi
University of Ottawa and Bank of Canada, Canada

3. **On Forging SPHINCS + -Haraka Signatures on a Fault-tolerant Quantum Computer**
Robin M. Berger, Marcel Tiepelt
Karlsruhe Institute of Technology, Germany

4. **Post-Quantum Key-Blinding for Authentication in Anonymity Networks**
Edward Eaton, Douglas Stebila, Roy Stracovsky
University of Waterloo, Canada

5. **Implementing and measuring KEMTLS**
Sofía Celi, Armando Faz-Hernández, Nick Sullivan, Goutam Tamvada, Luke Valenta, Thom Wiggers, Bas Westerbaan, Christopher Wood.
Cloudflare Inc., USA, and University of Waterloo, Canada, and Radboud University, The Netherlands, and PQShield Ltd., United Kingdom

6. **A Monolithic Hardware Implementation of Kyber: Comparing Apples to Apples in PQC Candidates**
Mojtaba Bisheh-Niasar, Reza Azarderakhsh, Mehran Mozaffari-Kermani
Florida Atlantic University and University of South Florida, USA

7. **Attribute-Based Access Control for Inner Product Functional Encryption from LWE**
Tapas Pal, Ratna Dutta
Indian Institute of Technology Kharagpur, India

8. **Classical Attacks on a Variant of the RSA Cryptosystem**
Abderrahmane Nitaj, Muhammad Rezal Kamel Ariffin, Nurul Nur Hanisah Adenan, Nur Azman Abu
University of Caen Normandy, France, and Universiti Putra Malaysia and Universiti Teknikal Malaysia Melaka, Malaysia

9. **Improved attacks against key reuse in learning with errors key exchange**
Nina Bindel, Douglas Stebila, Shannon Veitch
University of Waterloo, Canada

10. **Differential-ML Distinguisher: Machine Learning based Generic Extension for Differential Cryptanalysis**
Tarun Yadav, Manoj Kumar
Defence Research and Development Organization, India

11. **Train or Adapt a Deeply Learned Profile**
Christophe Genevey-Metat, Univ Rennes, Inria, CNRS, IRISA, Rennes, France Annelie Heuser, Benoit Gérard
Université de Rennes, Inria, CNRS, IRISA and DGA.MI, France

12. **Autocorrelations of vectorial Boolean functions**
Anne Canteaut, Lukas Kölsch, Chao Li, Chunlei Li, Kangquan Li, Longjiang Qu, Friedrich Wiemer
Inria, France, and University of Rostock, Germany, and National University of Defense Technology, China, and Human Engineering Research Center of Commercial Cryptography Theory and Technology Innovation, China, and University of Bergen, Norway, and Ruhr University Bochum, Germany, and Cryptosolutions, Germany

13. **Automatic Search for Bit-based Division Property**
Shibam Ghosh, Orr Dunkelman
University Of Haifa, Israel

14. **TEDT2 - Highly Secure Leakage-resilient TBC-based Authenticated Encryption**
Eik List
Bauhaus-Universität Weimar, Germany

15. **Stronger Notions and a More Efficient Construction of Threshold Ring Signatures**
Alexander Munch-Hansen, Claudio Orlandi, Sophia Yakoubov
Aarhus University, Denmark

16. **Improved Threshold Signatures, Proactive Secret Sharing and Input Certification from LSS Isomorphisms**
Diego Aranha, Anders Dalskov, Daniel Escudero, Claudio Orlandi
Aarhus University, Denmark

17. **Implementing Secure Reporting of Sexual Misconduct - Revisiting WhoToo**
Alejandro Hevia, Ilana Mergudich-Thal
University of Chile, Chile

18. **Weight-Based Nakamoto-Style Blockchains**
Simon Holmgaard Kamp, Bernardo Magri, Christian Matt, Jesper Buus Nielsen, Søren Eller Thomsen, Daniel Tschudi
Concordium Blockchain Research Center and Aarhus University, Denmark

19. **LOVE a Pairing**
Diego F. Aranha, Elena Pagnin, Francisco Rodríguez-Henríquez
Aarhus University, Denmark, and Lund University, Sweden, and CINVESTAV-IPN, Mexico, and CRC-TII, United Arab Emirates

20. **Full-Threshold Actively-Secure Multiparty Arithmetic Circuit Garbling**
Eleftheria Makri, Tim Wood
KU Leuven, Belgium, and Saxion University of Applied Sciences, The Netherlands, and University of Bristol, United Kingdom

21. **The Cost of IEEE Arithmetic in Secure Computation**
David W. Archer, Shahla Atapoor, Nigel P. Smart
Galois Inc., USA, and KU Leuven, Belgium

22. **Honest Majority MPC with Abort with Minimal Online Communication**
Anders Dalskov, Daniel Escudero
Aarhus University, Denmark

LATINCRYPT | BOGOTÁ 2021

Organized by:

Universidad del Rosario | School of Engineering, Science and Technology

MACC
Applied Mathematics and Computer Science

In cooperation with:

Sponsor: