NIST Lightweight Cryptography Workshop 2016

LIST OF ACCEPTED PAPERS

1. *The Littlun S-box and the Fly block cipher, P. Karpman, and B. Grégoire*

2. *Considerations for a lightweight, usable, and quantum-secure IoT, O. Garcia-Morchon, R. Rietman, L. Tolhuizen*

3. *Update on SIMON and SPECK, R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks and L. Wingers*

4. *Walnut Digital Signature Algorithm: A lightweight, quantum-resistant signature scheme for use in passive, low-power, and IoT devices, D. Atkins*

5. *RAIN RFID and the Internet of Things: Industry Snapshot and Security Needs, M.J.B. Robshaw*

6. *SPARX: A Family of ARX-based Lightweight Block Ciphers Provably Secure Against Linear and Differential Attacks, D. Dinu, L. Perrin, A. Udovenko, V. Velichkov, J. Großschädl, A. Biryukov*

7. *Sequential Hashing with Minimum Padding, S. Hirose*

8. *EM-Side-Channel Resistant Symmetric-Key Authentication Mechanism for Small Devices, C. S. Jutla, R. Boivie, D. Friedman and G. Shahidi*

9. *On the importance of considering physical attacks when implementing lightweight cryptography, A. Adomnicai, B. Lac, A. Canteaut, J. J.A. Fournier, L. Masson, R. Sirdey, and A. Tria*

10. *A Pseudorandom-Function Mode Based on Lesamnta-LW and the MDP Domain Extension and Its Applications, S. Hirose, H. Kuwakado, and H. Yoshida*

11. *The SKINNY Family of Block Ciphers, C. Beierle, J. Jean, S. Kölbl, G. Leander, A. Moradi, T. Peyrin, Y. Sasaki, P. Sasdrich, and S. M. Sim*

12. *The Role of Energy in the Lightweight Cryptographic Profile, C. Patrick and P. Schaumont*

13. *Side-channel Analysis of Lightweight Ciphers: Current Status and Future Directions, A. Heuser, S. Picek, S. Guilley and N. Mentens*

14. *Lightweight Cryptography on ARM, R. J. Cruz, T. B. Reis, D. F. Aranha, J. López, H. K. Patil*

15. *Threshold Implementations of PRINCE – What is the Cost of Physical Security?, D. Božilov, M Knežević, and V. Nikov*

16. *SOK it to the IoT, M. Scott and K. McCusker*

17. *Galois Ultra Low Power High Assurance Asynchronous Crypto P. Beerel, J. Bielman, T. DuBuisson, T. Eliott, D. Hand, B. Huffman, J. Kiniry, W. Koven, D. Wager, D. Zimmerman*