*NIST Lightweight Cryptography Workshop 2015*

***List of Accepted Papers***

1. *Triathlon of Lightweight Block Ciphers for the Internet of Things*, Daniel Dinu, Yann Le Corre, Dmitry Khovratovich, Léo Perrin, Johann Großschädl, Alex Biryukov

2. *RECTANGLE: A Bit-slice Ultra-Lightweight Block Cipher Suitable for Multiple Platforms,* Wentao Zhang, Zhenzhen Bao, Dongdai Lin, Vincent Rijmen, Bohan Yang, Ingrid Verbauwhede

3. *A comprehensive and lightweight security architecture to secure the IoT throughout the lifecycle of a device based on HIMMO,* Oscar Garcia-Morchon, Ronald Rietman, Sahil Sharma, Ludo Tolhuizen, Jose Luis Torre-Arce

4. *Some observations on ACORN v1 and Trivia-SC,* Rebhu Johymalyo Josh, Santanu Sarkar

5. *RAIN RFID and the Internet of Things: Industry Snapshot and Security Needs*, Matthew Robshaw, Tyler Williamson

6. *Single-Cycle Implementations of Block Ciphers*, Pieter Maene, Ingrid Verbauwhede

7. *The Design Space of Lightweight Cryptography,* Nicky Mouha

8. *Chaskey: a Lightweight MAC Algorithm for Microcontrollers*, Nicky Mouha, Bart Mennink, Anthony Van Herrewege, Dai Watanabe, Bart Preneel, Ingrid Verbauwhede

9. *Algebraic Eraser: A lightweight, efficient asymmetric key agreement protocol for use in no-power, low-power, and IoT devices*, Derek Atkins

10. *Elliptic Curve Cryptography (ECC) for LWM2M (Light Weight Machine to Machine) Protocols,* Rakesh Kushwaha

11. *Low power wireless scenarios and techniques for saving bandwidth without sacrificing security*, David McGrew

12. *Simon and Speck: Block Ciphers for the Internet of Things,* Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, Louis Wingers

13. *FELICS - Fair Evaluation of Lightweight Cryptographic Systems,* Daniel Dinu, Alex Biryukov, Johann Großschädl, Dmitry Khovratovich, Yann Le Corre, Léo Perrin

14. *Performance of State-of-the-Art Cryptography on ARM-based Microprocessors*, Hannes Tschofenig, Manuel Pegourie-Gonnard

15. *Efficient Hardware Implementations of the Warbler Pseudorandom Number Generator*, Gangqiang Yang, Mark D. Aagaard, Guang Gong

16. *RPM: Lightweight Communication Security from Additive Stream Ciphers*, Giovanni Di Crescenzo, Glenn O. Veach

17. *Differential Cryptanalysis of the BSPN Block Cipher Structure*, Liam Keliher

18. *Japan CRYPTREC Activity on Lightweight Cryptography*, Shiho Moriai

19. *JAMBU Lightweight Authenticated Encryption Mode and AES-JAMBU*, Hongjun Wu, Tao Huang

20. *A New Distinguisher on Grain v1 for 106 Rounds*, Santanu Sarkar

21. *Thanks, but No Thanks: Current Cryptographic Standards are Sufficient for Software*, Dan Shumow

22. *Lightweight version of π-cipher*, Hristina Mihajloska, Mohamed El Hadedy, Danilo Gligoroski, Kevin Skadron

23. *PFLASH – Secure Asymmetric Signatures on Smart Cards*, Daniel Smith-Tone, Ming-Shing Chen and Bo-Yin Yang