Lightweight Cryptography Workshop

October 17-18, 2016

NIST – Gaithersburg, Maryland

Monday, October 17, 2016	
9:00 – 9:10	**Opening Remarks** Matt Scholl, Chief, Computer Security Division, NIST
9:10 – 10:30	**Session I: Lightweight Crypto Standardization** Session Chair: Larry Bassham 1. **NIST's Lightweight Crypto Project** – Meltem Sönmez Turan (30 mins) 2. **Portfolio Development** – Kerry McKay (25 mins) 3. **Lightweight Cryptography Standards Developed in ISO/IEC SC27** - Lily Chen (25 mins)
10:30 – 11:00	**Break**
11:00 – 11:50	**Session II: Implementation** Session Chair: Kerry McKay 1. ***The role of energy in the Lightweight Cryptographic Profile**, C. Patrick and P. Schaumont **(paper)*** 2. ***Lightweight Cryptography on ARM**, R. J. Cruz, T. B. Reis, D. F. Aranha, J. Lopez, H. K. Patil **(paper)***
11:50 – 12:25	**Session III: Invited talk** ***RAIN RFID and Internet of Things: Industry Snapshot and Security Needs*** – Matthew Robshaw **(*paper*)**
12:25 – 2:00	**Lunch**
2:00 – 3:40	**Session IV: Side Channel Attacks** Session Chair: Nicky Mouha 1. ***Side-channel Analysis of Lightweight Ciphers: Current Status and Future Directions**, A. Heuser, S. Picek, S. Guilley and N. Mentens **(paper)*** 2. ***Threshold Implementations of Prince**, D. Božilov, M Knežević, and V. Nikov **(paper)*** 3. ***EM-Side-Channel Resistant Symmetric-Key Authentication Mechanism for Small Devices.** C. S. Jutla, R. Boivie, D. Friedman and G. Shahidi **(paper)*** 4. ***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 **(paper)***
3:40 – 4:00	**Break**
4:00 – 5:00	**Session V: Open Discussion**

Workshop Event Page: http://go.usa.gov/xTYuQ/

Tuesday, October 18, 2016	
9:00 - 10:40	**Session VI: Block Cipher Designs** Session Chair: Meltem Sönmez Turan 1. ***The Littlun S-box and the Fly block cipher**, P. Karpman, and B. Gregoire **(paper)*** ***2.** **Update on SIMON and SPECK**, R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks and L. Wingers **(no paper)*** *3.* ***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 **(paper)*** 4. ***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 **(paper)***
10:40 – 11:00	**Break**
11:00 – 12:40	**Session VII: Verification and Protocols** Session Chair: Çagdas Çalık ***5.** **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 **(no paper)*** *1.* ***SOK it to the IoT**, M. Scott and K. McCusker **(paper)*** *2.* ***Considerations for a lightweight, usable, and quantum-secure IoT**, O. Garcia-Morchon, R. Rietman, L. Tolhuizen, S. Bhattcharya, J. Torre-Acre (**paper**)* *3.* ***Walnut Digital Signature Algorithm: A lightweight, quantum-resistant signature scheme for use in passive, low-power, and IoT devices**, D. Atkins **(paper)***
12:40 – 2:00	**Lunch**
2:00 – 2:50	**Session VIII: Hashing** Session Chair: John Kelsey ***1.** **Sequential Hashing with Minimum Padding**, S. Hirose **(paper)*** *2.* ***A Pseudorandom-Function Mode Based on Lesamnta-LW and the MDP Domain Extension and Its Application**, S. Hirose, H. Kuwakado, and H. Yoshida **(paper)***
2:50 – 4:15	**Session IX: Open Discussion and Closing Remarks**

Workshop Event Page: http://go.usa.gov/xTYuQ/