

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 <ol style="list-style-type: none">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 <ol style="list-style-type: none">1. The role of energy in the Lightweight Cryptographic Profile, C. Patrick and P. Schaumont (25 mins)2. Lightweight Cryptography on ARM, R. J. Cruz, T. B. Reis, D. F. Aranha, J. Lopez, H. K. Patil (25 mins)
11:50 – 12:35	Session III: Invited talk RAIN RFID and Internet of Things: Industry Snapshot and Security Needs – Matthew Robshaw (45 mins)
12:25 – 2:00	Lunch
2:00 – 3:40	Session IV: Side Channel Attacks Session Chair: Nicky Mouha <ol style="list-style-type: none">1. Side-channel Analysis of Lightweight Ciphers: Current Status and Future Directions, A. Heuser, S. Picek, S. Guilley and N. Mentens (25 mins)2. Threshold Implementations of Prince, D. Božilov, M Knežević, and V. Nikov (25 mins)3. EM-Side-Channel Resistant Symmetric-Key Authentication Mechanism for Small Devices, C. S. Jutla, R. Boivie, D. Friedman and G. Shahidi (25 mins)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 (25 mins)
3:40 – 4:00	Break
4:00 – 5:00	Session V: Open Discussion

Tuesday, October 18, 2016	
9:00 - 10:40	<p>Session VI: Block Cipher Designs Session Chair: Meltem Sönmez Turan</p> <ol style="list-style-type: none"> 1. <i>The Littlun S-box and the Fly block cipher</i>, P. Karpman, and B. Gregoire (25 mins) 2. <i>Update on SIMON and SPECK</i>, R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks and L. Wingers (25 mins) 3. <i>SPARX: A Family of ARX-based Lightweight Block Ciphers Provably Secure Against Linear and Differential Attacks</i>, D. Dinu, L. Perrin, A. Udovenko, V. Velichkov, J. Großschädl, A. Biryukov (25 mins) 4. <i>The SKINNY Family of Block Ciphers</i>, C. Beierle, J. Jean, S. Kölbl, G. Leander, A. Moradi, T. Peyrin, Y. Sasaki, P. Sasdrich, and S. M. Sim (25 mins)
10:40 – 11:00	Break
11:00 – 12:40	<p>Session VII: Verification and Protocols Session Chair: Çağdas Çalık</p> <ol style="list-style-type: none"> 1. <i>Galois Ultra Low Power High Assurance Asynchronous Crypto</i>, P. Beerel, J. Bielman, T. DuBuisson, T. Elliott, D. Hand, B. Huffman, J. Kiniry, W. Koven, D. Wager, D. Zimmerman (25 mins) 2. <i>SOK it to the IoT</i>, M. Scott and K. McCusker (25 mins) 3. <i>Considerations for a lightweight, usable, and quantum-secure IoT</i>, O. Garcia-Morchon, R. Rietman, L. Tolhuizen (25 mins) 4. <i>Walnut Digital Signature Algorithm: A lightweight, quantum-resistant signature scheme for use in passive, low-power, and IoT devices</i>, D. Atkins (25 mins)
12:40 – 2:00	Lunch
2:00 – 2:50	<p>Session VIII: Hashing Session Chair: John Kelsey</p> <ol style="list-style-type: none"> 1. <i>Sequential Hashing with Minimum Padding</i>, S. Hirose (25 mins) 2. <i>A Pseudorandom-Function Mode Based on Lesamnta-LW and the MDP Domain Extension and Its Application</i>, S. Hirose, H. Kuwakado, and H. Yoshida (25 mins)
2:50 – 4:15	Session IX: Open Discussion and Closing Remarks