Fast Software Encryption 2010
Rump Session

16:00 – 16:03  **Opening**  
Orr Dunkelman

**Announcements**

16:03 – 16:10  The International Association for Cryptologic Research  
Bart Preneel

16:10 – 16:12  CFP of IWSEC 2010  
Shoichi Hirose

16:12 – 16:13  CFP of Pairing 2010  
Shoichi Hirose

16:13 – 16:15  Africacrypt 2010  
Riaal Domingues

**Technical Results**

16:15 – 16:21  Related-Key Boomerang Attack on Block Cipher SQUARE  
Bonwook Koo, Yongjin Yeom, and Junghwan Song

16:21 – 16:26  Improved Cryptanalysis of ECHO and Grøstl  
Thomas Peyrin

16:26 – 16:32  Pseudo-preimage attack against SHAvite-3 compression function  
Praveen Gauravaram, Gaëtan Leurent, Florian Mendel, María Naya-Plasencia, Thomas Peyrin, Christian Rechberger, and Martin Schläffer

16:32 – 16:34  Solving Multivariate Polynomial Systems  
Tony Chou, Kevin Chen, Charles Bouilaguet, Bo-Yin Yang, Chen-Mou Cheng, and Ruben Niederhagen

16:34 – 16:41  What price a provably secure stream cipher?  
Ming-Shing Chen, Tien-Ren Chen, Chen-Mou Cheng, Ruben Niederhagen, Chun-Hang Hsiao, and Bo-Yin Yang

16:41 – 16:47  Low Data Complexity Attacks on AES  
Orr Dunkelman and Nathan Keller