Post-Quantum Cryptography 2013

List of Accepted Papers

1. **The Hardness of Code Equivalence over $\mathbb{F}_q$ and its Application to Code-based Cryptography**
   Nicolas Sendrier and Dimitris E. Simos

2. **Timing Attacks against the Syndrome Inversion in Code-based Cryptosystems**
   Falko Strenzke

3. **Quantum Key Distribution in the Classical Authenticated Key Exchange Framework**
   Michele Mosca and Douglas Stebila and Berkant Ustaoglu

4. **Solving the Shortest Vector Problem in Lattices Faster Using Quantum Search**
   Thijs Laarhoven and Michele Mosca and Joop van de Pol

5. **An efficient attack of a McEliece cryptosystem variant based on convolutional codes**
   Grégory Landais and Jean-Pierre Tillich

6. **Multivariate signature scheme using quadratic forms**
   Takanori Yasuda and Tsuyoshi Takagi and Kouichi Sakura

7. **Secure and Anonymous Hybrid Encryption from Coding Theory**
   Edoardo Persichetti

8. **Extended Algorithm for Solving Underdefined Multivariate Quadratic Equations**
   Hiroyuki Miura and Yasufumi Hashimoto and Tsuyoshi Takagi

9. **Fast Verification for Improved Versions of the UOV and Rainbow Signature Schemes**
   Albrecht Petzoldt and Stanislav Bulygin and Johannes Buchmann

10. **Degree of Regularity for HFEv and HFEv-**
Jintai Ding and Bo-Yin Yang

11. **Using LDGM Codes and Sparse Syndromes to Achieve Digital Signatures**
Marco Baldi and Marco Bianchi and Franco Chiaraluce and Joachim Rosenthal and Davide Schipani

12. **Software Speed Records for Lattice-Based Signatures**
Tim Güneysu and Tobias Oder and Thomas Pöppelmann and Peter Schwabe

13. **Cryptanalysis of Hash-based Tamed Transformation and Minus Signature Scheme**
Xuyun Nie and Zhaohu Xu and Johannes Buchmann

14. **Simple Matrix Scheme for Encryption**
Chengdong Tao and Adama Diene and Jintai Ding

15. **Improved Lattice-Based Threshold Ring Signature Scheme**
Schrek Julien and Bettaieb Slim

16. **A Classification of Differential Invariants for Multivariate Post-Quantum Cryptosystems**
Daniel Smith-Tone and Ray Perlne

17. **Quantum algorithms for the subset-sum problem**
Daniel J. Bernstein and Stacey Jeffery and Tanja Lange and Alexander Meurer