Accepted Papers Arctic Crypt 2016

1. Sonia Bogos, John Gaspoz and Serge Vaudenay,
   Analysis of a Homomorphic Encryption Scheme

2. Gizem Cetin, Yarkın Doröz, Berk Sunar and William Martin,
   Arithmetic Using Word-wise Homomorphic Encryption

3. Eloi de Cherisey, Sylvain Guilley, Annelie Heuser and Olivier Rioul,
   On the Optimality and Practicability of Mutual Information Analysis in Some Scenarios

4. Eric Chitambar, Ben Fortescue and Min-Hsiu Hsieh,
   Quantum Versus Classical Advantages in Secret Key Distillation (and Their Links to Quantum Entanglement)

5. Tingting Cui, Huaifeng Chen, Long Wen and Meiqin Wang,
   Statistic Integral Attack on CAST-256 and IDEA

6. Tomas Fabsic, Otokar Grosek, Karol Nemoga and Pavol Zajac,
   On generating invertible circulant binary matrices with a prescribed number of ones

7. Arman Fazeli, Alexander Vardy and Eitan Yaakobi,
   Private Information Retrieval without Storage Overhead: Coding Instead of Replication

8. Houda Ferradi, Rémi Géraud, Diana Maimut, Naccache David and Hang Zhou,
   Backtracking-Assisted Multiplication

9. Christian Forler, Eik List, Stefan Lucks and Jakob Wenzel,
   POEx: A Beyond-Birthday-Bound-Secure On-Line Cipher

10. Brett Hemenway and Rafail Ostrovsky,
    Efficient Robust Secret Sharing from Expander Graphs

11. Sam Kim, Kevin Lewi, Avradip Mandal, Hart Montgomery, Arnab Roy and David Wu,
    Function-Hiding Inner Product Encryption is Practical

12. Kamil Kluczniak, Lucjan Hanzlik and Mirosław Kutyłowski,
    Ad-Hoc-Domain Signatures for Personal eID Documents

13. Marie-Sarah Lacharité,
    Security of BLS and BGLS signatures in a multi-user setting

14. Valerie Nachef, Jacques Patarin and Emmanuel Volte,
    Generic Attacks with Standard Deviation Analysis on A-Feistel Schemes

15. Cecile Pierrot and Benjamin Wesolowski,
    Malleability of the blockchain's entropy

16. Geong Sen Poh, Moesfa Soeheila Mohamad and Ji-Jian Chin,
    Searchable Symmetric Encryption Over Multiple Servers

17. Shahram Rasoolzadeh and Håvard Raddum,
    Cryptanalysis of 6-round PRINCE using 2 Known Plaintexts

18. Greg Rose,
    KISS: A Bit Too Simple

19. Michael Scott,
    Missing a trick: Karatsuba revisited

20. Yuval Yarom, Daniel Genkin and Nadia Heninger,
    CacheBleed: A Timing Attack on OpenSSL Constant Time RSA