Christiane Peters

Publications

Technical Report

1. Klaus Kursawe, Christiane Peters.
   Structural weaknesses in the Open Smart Grid Protocol.
   Cryptology ePrint Archive, Report 2015/088, 2015.

Journal articles

2. Daniel J. Bernstein, Peter Birkner, Tanja Lange, Christiane Peters.
   ECM using Edwards curves.
   In Mathematics of Computation, Vol. 82, pp. 1139–1179, AMS, 2013.

Book chapters

3. Christiane Peters.
   Decoding algorithms.
   In Henk C. A. van Tilborg and Sushil Jajodia, editors, Encyclopedia of Cryptography and Security (2nd Ed.), pages 319–322. Springer-Verlag Berlin Heidelberg, second edition, 2011.

Publications in international refereed journals and conference proceedings (Peer-reviewed publications)

4. Daniel J. Bernstein, Tanja Lange, Christiane Peters.
   Wild McEliece Incognito.
   In Bo-Yin Yang, editor, PQCrypto, volume 7071 of Lecture Notes in Computer Science, pages 244–254. Springer, 2011.

5. Daniel J. Bernstein, Tanja Lange, Christiane Peters.
   Smaller Decoding Exponents: Ball-collision Decoding.
   In Phillip Rogaway, editor, CRYPTO, volume 6841 of Lecture Notes in Computer Science, pages 743–760. Springer-Verlag Berlin Heidelberg, 2011.

6. Daniel J. Bernstein, Tanja Lange, Christiane Peters, Peter Schwabe.
   Really Fast Syndrome-based Hashing.
   In Abderrahmane Nitaj and David Pointcheval, editors, AFRICACRYPT 2011, volume 6737 of Lecture Notes in Computer Science, pages 134–151. Springer-Verlag Berlin Heidelberg, 2011.

7. Daniel J. Bernstein, Tanja Lange, Christiane Peters, Peter Schwabe.
   Faster 2-regular Information-set Decoding.
   In Yeow Meng Chee, Zhenbo Guo, San Ling, Fengjing Shao, Yuansheng Tang Huaxiong Wang Chaoping Xing, editors, IWCC 2011, volume 6639 of Lecture Notes in Computer Science, pages 81–98. Springer-Verlag Berlin Heidelberg, 2011.

8. Daniel J. Bernstein, Tanja Lange, Christiane Peters.
   Wild McEliece.
   In Alex Biryukov, Guang Gong, Douglas Stinson, editors, Selected Areas in Cryptography, volume 6544 of Lecture Notes in Computer Science, pages 143–158. Springer-Verlag Berlin Heidelberg, 2011.

9. Christiane Peters.
   Information-set Decoding for Linear Codes over $\mathbf{F}_q$.
   In Nicolas Sendrier, editor, PQCrypto 2010, volume 6061 of Lecture Notes in Computer Science, pages 81–94. Springer-Verlag Berlin Heidelberg, 2010.

10. Daniel J. Bernstein, Tanja Lange, Ruben Niederhagen, Christiane Peters, Peter Schwabe.
    FSBday: Implementing Wagner's generalized birthday attack against the SHA-3 round-1 candidate FSB.
    In Bimal K. Roy and Nicolas Sendrier, editors, INDOCRYPT 2009, volume 5922 of Lecture Notes in Computer Science, pages 18–38. Springer-Verlag Berlin Heidelberg, 2009.

11. Daniel J. Bernstein, Tanja Lange, Christiane Peters, Henk C. A. van Tilborg.
    Explicit bounds for generic decoding algorithms for code-based cryptography.
    In Alexander Kholosha, Eirik Rosnes, Matthew Parker, editors, Pre-proceedings of WCC 2009, pages 168–180, Bergen, 2009.

12. Daniel J. Bernstein, Tanja Lange, Christiane Peters.
    Attacking and defending the McEliece cryptosystem.
    In Johannes Buchmann and Jintai Ding, editors, PQCrypto 2008, volume 5299 of Lecture Notes in Computer Science, pages 31–46. Springer-Verlag Berlin Heidelberg, 2008.

13. Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, Christiane Peters.
    Twisted Edwards curves.
    In Serge Vaudenay, editor, AFRICACRYPT 2008, volume 5023 of Lecture Notes in Computer Science, pages 389–405. Springer-Verlag Berlin Heidelberg, 2008.

14. Daniel J. Bernstein, Peter Birkner, Tanja Lange, Christiane Peters.
    Optimizing double-base elliptic-curve single-scalar multiplication.
    In Kannan Srinathan, Chandrasekaran Pandu Rangan, Moti Yung, editors, INDOCRYPT 2007, volume 4859 of Lecture Notes in Computer Science, pages 167–182. Springer-Verlag Berlin Heidelberg, 2007.