Stellingen

behorend bij het proefschrift

Curves, Codes, and Cryptography

van

Christiane Peters

1. Potential polynomial-searching attacks for the wild McEliece cryptosystem can be avoided by hiding the wild codes: consider codes built on polynomials $f \cdot g^{q-1}$ as suggested in [2].

2. Augot-Finiasz-Sendrier's 2-regular decoding algorithm [1] is an equivalent of Prange's plain information-set decoding algorithm [6]. Using collision-decoding techniques for 2-regular decoding yields an exponential speedup [3] over [1].

3. Recent improvements make 2-regular decoding a competitor of Wagner's generalized birthday attack for finding collisions in fast syndrome-based hash functions [4].

4. Post-quantum cryptography is the most promising way to protect sensitive data in the long term.

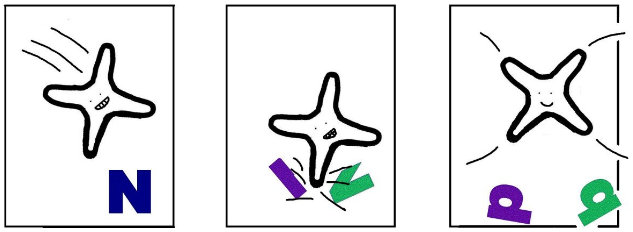
5. The designers of post-quantum encryption schemes should follow the NIST recommendation [5] of abandoning 80-bit security and aim at higher security levels.

6. Extension of the statement in Chapter 8 of this thesis "1000-bit security is far away from having any real-world relevance." Even going beyond our world doesn't help. There are fewer atoms in the observable universe; a rough estimate is 2^{265}.

7. Genus-1 algebraic-geometry codes are widely thought to be useless for code-based cryptography. This belief ignores the benefits of subfield subcodes.

8. Edwards curves can speed up elliptic-curve primality proving.

9. EECM should be used as part of the Number Field Sieve.



10. Addition of 0 is negligible.

11. Plagiarism is not a boyish prank.

12. No starfish were harmed in the writing of this thesis.

References

[1] Daniel Augot, Matthieu Finiasz, and Nicolas Sendrier. A fast provably secure cryptographic hash function, 2003. `http://eprint.iacr.org/2003/230`.

[2] Daniel J. Bernstein, Tanja Lange, and Christiane Peters. Wild McEliece Incognito. In preparation.

[3] Daniel J. Bernstein, Tanja Lange, Christiane Peters, and Peter Schwabe. Faster 2-regular information-set decoding. In *IWCC 2011*, volume 6639 of *Lecture Notes in Computer Science*. Springer-Verlag Berlin Heidelberg, 2011. To appear. `http://eprint.iacr.org/2011/120`.

[4] Daniel J. Bernstein, Tanja Lange, Christiane Peters, and Peter Schwabe. Really fast syndrome-based hashing. Cryptology ePrint Archive: Report 2011/074, 2011. `http://eprint.iacr.org/2011/074`.

[5] NIST – National Institute of Standards and Technology. Recommendation for Key Management, 2007. Special Publication 800-57 Part 1, NIST, 03/2007.

[6] Eugene Prange. The use of information sets in decoding cyclic codes. *IRE Transactions on Information Theory*, 8(5):5–9, September 1962.