Theses

accompanying the dissertation

High-Speed Cryptography and Cryptanalysis

by

Peter Schwabe

1. The best known algorithm to solve the discrete-logarithm problem in most prime-order elliptic-curve groups is Pollard's rho method. The iteration function in this algorithm can be defined to work on equivalence classes modulo the negation map; this saves an expected factor of $\sqrt{2}$ of the number of iterations required to solve the problem.

   When using adding walks the iteration function then needs to deal with fruitless cycles, but well-optimized implementations can still gain a speedup of the whole computation that is very close to a factor of $\sqrt{2}$ [1].

   [1] Daniel J. Bernstein, Tanja Lange, and Peter Schwabe. On the correct use of the negation map in the Pollard rho method. To appear in *Public Key Cryptography – PKC 2011*.

2. The main reason that the FSB hash function did not enter the second round of the SHA-3 competition is probably software speed. However, it is possible to design a hash function based on the FSB ideas that achieves 128-bit security and runs faster than SHA-256 on Intel Core 2 and Core i7 processors [2].

   [2] Daniel J. Bernstein, Tanja Lange, Christiane Peters, and Peter Schwabe. Really fast syndrome-based hashing. 2010.

3. SHA-2 will soon retire [3].

   [3] Michael Naehrig, Christiane Peters, Peter Schwabe. SHA-2 will soon retire, *Journal of Craptology*, 7, 2009.

4. **Definition 2.4.1** Let u be an integer such that

   $$\begin{aligned} p &= p(u) = 36u^4 + 36u^3 + 24u^2 + 6u + 1 \text{ and} \\ n &= n(u) = 36u^4 + 36u^3 + 18u^2 + 6u + 1 \end{aligned}$$

   are both prime. An elliptic curve E over $\mathbb{F}_p$ with $|E(\mathbb{F}_p)| = n$ is called a *Barreto-Naehrig curve*.

5. The SSE instruction set includes three different, logically equivalent, instructions to compute the xor of two 128-bit registers: `xorps`, `xorpd` and `pxor`; similar equivalences hold for other bit-logical instructions: `andps/andpd/pand` and `orps/orpd/por`. While `xorps` and `xorpd` consider their inputs as floating-point values, `pxor` works on integer inputs.

While it does not matter for the result of computations which of these equivalent instructions is used, it can have a huge impact on performance. For example, the Intel Core i7 can dispatch up to three instructions of `pxor`, `pand`, and `por` per cycle, but only one of the floating-point equivalents.

6. Compilers are optimized to produce binaries running at reasonable speed from bad source code in a short time. What we need for high-speed cryptography are compilers that produce binaries running at optimal (or close-to-optimal) speed from good source code in a potentially long time.

7. A great deal of time in research is spent on doing the same things over and over again by different groups and people. In part this redundant work is necessary to understand and verify previous results and techniques, but still a significant amount of time is wasted simply because results are not publicly available or not usable because of copyright restrictions. This wasted time could be saved if all results (including software) of all publicly funded research automatically entered the public domain.

8. It can be quite expensive to multiply by 1.

9. If you want to travel around the world and be invited to speak at a lot of different places, you do not necessarily have to write a Unix operating system.

   ("If you want to travel around the world and be invited to speak at a lot of different places, just write a Unix operating system." – Linus Torvalds)

10. Treffen sich zwei Flugzeuge, in beiden sitzt Tanja.

11. The list of countries where delicious food can be found in thesis 8 of the theses accompanying [4] is correct, but incomplete.

    [4] Peter Birkner. *Efficient Arithmetic on Low-Genus Curves.* Ph.D. thesis, Technische Universiteit Eindhoven, 2009.