Theses

accompanying the dissertation

Parallel Cryptanalysis

by

Ruben Niederhagen

1. Neither multiplication by 1 nor addition of 0 benefit from parallelization. (See [Sch11, Statement 8] and [Pet11, Statement 10].)

2. Some eight computers connected by a network do not make a proper cluster.

3. Non-disclosure of architectural details is just evil. The answer is: don't.
("Moving data is just evil. The answer is: don't."
— Jen-Hsun Huang, CEO of NVIDIA)

4. Coprocessors for direct memory access (DMA) operations might increase the performance of parallel programs on NUMA architectures. First experiments using an Infiniband card for copying data between the memory domains of a single NUMA machine give promising performance results.

5. Unified Parallel C [LBL] is a programming language for parallel architectures such as shared-memory architectures or distributed-memory architectures. It offers a common global address space for all computing units as an abstraction layer. The Cell processor has several Synergistic Processing Units that access a common main memory via explicit DMA instructions. Our paper "Evaluating the portability of UPC to the Cell Broadband Engine" [NL] evaluates the opportunities and pitfalls of implementing a UPC runtime system for the Cell processor and thus bringing UPC to the Cell processor.

6. Our paper "Fast exhaustive search for polynomial systems in $\mathbb{F}_2$" [BCC$^+$10] shows that quadratic systems of multivariate equations over $\mathbb{F}_2$ can be solved most efficiently by exhaustive search (brute force) on highly parallel architectures such as GPUs.

7. The root of the plagiarism case "Guttenberg" in Germany is the blind admiration of academic titles in the German society.

8. Personal experience shows that it is more easy to get adapted to the benefits of Taiwanese culture than to fall back to Western habits.

References:

[BCC+10] Charles Bouillaguet, Hsieh-Chung Chen, Chen-Mou Cheng, Tung Chou, Ruben Niederhagen, Adi Shamir, and Bo-Yin Yang. "Fast exhaustive search for polynomial systems in $\mathbb{F}_2$". In: *Cryptographic Hardware and Embedded Systems – CHES 2010*. Ed. by Stefan Mangard and François-Xavier Standaert. Vol. 6225. Lecture Notes in Computer Science. Springer-Verlag Berlin Heidelberg, 2010, pp. 203–218. DOI: 10.1007/978-3-642-15031-9_14. IACR ePrint archive: 2010/313.

[LBL] "Berkeley UPC—Unified Parallel C". Lawrence Berkeley National Laboratory and University of California, Berkeley. URL: http://upc.lbl.gov/.

[NL] Ruben Niederhagen and Stefan Lankes. "Evaluation of the portability of UPC to the Cell Broadband Engine". In: *State of the Art in Scientific and Parallel Computing – PARA 2008*. Ed. by Anne C. Elster. Vol. 6126,6127. Lecture Notes in Computer Science. To appear. Springer-Verlag Berlin Heidelberg.

[Pet11] Christiane Peters. "Stellingen behorend bij het proefschrift *Curves, Codes, and Cryptography*". 2011. URL: http://www2.mat.dtu.dk/people/C.Peters/thesis/stellingen.pdf.

[Sch11] Peter Schwabe. "Theses accompanying the dissertation *High-Speed Cryptography and Cryptanalysis*". 2011. URL: http://cryptojedi.org/users/peter/thesis/data/phdthesis-schwabe-statements.pdf.