Position Statement for the STORK (Strategic Roadmap for Cryptography) Workshop, November 26–27, 2002, Brussels

The Future of the Art of Cryptographic Implementations

Christof Paar
Chair for Communication Security
Electrical Engineering and Information Sciences Dept.
Ruhr-Universität Bochum, Germany
www.crypto.ruhr-uni-bochum.de

Background

It has become widely accepted that (1) information security is an important factor for most current and future IT applications, and (2) that cryptographic mechanisms are needed for providing security. A trivial conclusion from these observations is that cryptographic mechanisms have to be implemented if they are actually to be used in applications. Until relatively recently, roughly until the mid to late 1990s, the field of cryptographic implementations was only a niche discipline with relatively few people working in it. Publications were scattered over the cryptographic and engineering literature. It was often not very clear where the research problems were. In the late 1990s the situation began to change: On one hand, more and more researchers discovered cryptographic implementations as a research field, and on the other hand there has been a fast growing demand from industry for optimized solutions. Conferences such as the CHES (Cryptographic Hardware and Embedded Systems) Workshop series have helped to organize the field and to focus the research findings.

It turns out that the field of cryptographic implementation is intrinsically interdisciplinary. It draws from the disciplines of cryptography, efficient algorithms, hardware design and software. It is not always easy to find researchers with expertise in two or more of these areas.

Future Research Guidelines

1. Many early solutions focused on high performance implementation methods, e.g., fast RSA modular multiplication architectures or fast block cipher implementations. However, with the ever increasing speed of VLSI chips and processor clock rates, achieving speed will often not be main problem in the future. Instead, we should focus on developing implementation methods which optimize the performance-cost product, for instance achieving speed goal XY at the lowest possible cost.

2. Side channel attacks is a field which is still evolving and which poses a serious threat to cryptography in practice. Much more work has to be done in order to fully understand *all types* of side channel attacks, i.e., also non-power analysis attacks. At the same

time, we have to revisit established hardware and software implementation platforms and algorithms, and assess and modify them in light of side channel attacks.

3. The predicted advent of pervasive computing applications will require symmetric and asymmetric algorithms for extremely cost and power constraint environments. A lot of work has to be done in order to develop such algorithms, especially in the asymmetric case. Similarly, many existing security and distributed computation protocols are too costly in networks with constraint devices.

4. The efficiency of an implementation algorithm often depends heavily on the details of the target platform, e.g., on the instruction set or the pipeline structure of a processor. Hence, theoretical complexity measures, such as the bit complexity, can be misleading in practice. In the future, one should also focus on developing algorithms for software and hardware which take the nature of the target platform into account. References [1, 2] are examples for platform-targeted implementation methods.

5. We should try to work more interdisciplinarily. This could either mean to educate ourselves about other fields (e.g., novel VLSI technologies), but also to entice people from other disciplines to work on problems in applied cryptography (e.g., people who work on novel VLSI technologies). Many important implementation issues in cryptography, such as hardware-software co-design or true random number generators, are not very well understood in a cryptographic context and could greatly benefit from input by knowledgeable outsiders. Educating graduate students interdisciplinarily will be beneficial for the field in the medium and long term future.

6. Our brilliant, new and optimized implementation methods will only be used in practiced if they are accessible to engineers in industry. We have to make sure that our findings can be used and interpreted by practioners which often lack the background in abstract mathematics.

7. Many publications about implementations are ad-hoc and not very well researched. At the same time, the wheel is often re-invent in industry. Both of these effects can be reduced by providing good methods for disseminating results about implementation techniques in a systematic an accessible form (conferences, journals, books, courses).

References

[1] A. Klimov and A. Shamir, "A new class of invertible mappings," in *Workshop on Cryptographic Hardware and Embedded Systems - CHES 2002* (B. Kaliski, Ç. Koç, and C. Paar, eds.), vol. LNCS, (Redwood City, CA, USA), Springer-Verlag, August 2002.

[2] D. V. Bailey and C. Paar, "Efficient arithmetic in finite field extensions with application in elliptic curve cryptography," *Journal of Cryptology*, vol. 14, no. 3, pp. 153–176, 2001.