Leakage-resilient Stream Ciphers: an Overview

Olivier Pereira*
ICTEAM – Crypto Group
Université catholique de Louvain
B-1348 Louvain-la-Neuve – Belgium

March 10, 2011

Side-channel attacks are one of the most dangerous threats against secure devices. By exploiting physical properties of the circuits running cryptographic protocols, that is, by analyzing the power consumption, running time, or electomagnetic radiations of circuits computing on secret data, side-channel attacks circumvent traditional security proofs and show to be extremely effective in breaking the security properties expected from a wide range of devices.

Since the first demonstration of the power of side-channel attacks by Kocher, in 1996, a huge body of work has been developing for securing protocol implementations against these attacks, using circuit-level techniques such as gate masking, differential logic styles, or circuit shielding for instance.

More recently researchers started addressing the issue of side-channel attacks at the cryptographic protocol level, trying to design protocols in a way that would substantially reduce the security needs at the implementation level, by making protocols leakage resilient.

In this talk, we investigate the problem of building leakage resilient stream-ciphers. Stream ciphers or, at their core, pseudorandom stream generators, probably are the most important object one may want to implement securely, as they are part of essentially any cryptographic construction: we need pseudorandomness to run the common challenge-response authentication protocols that are implemented on most low-power secure devices, but also to build any semantically secure encryption scheme for instance.

Building efficient and provably secure leakage resilient stream ciphers shows to be a remarkably challenging task. The first challenge consists in defining a security model that captures side-channel attacks in a realistic way. The most common approach consists in allowing the adversary to receive an auxiliary input about the information stored in the device, under

*Olivier Pereira is a Research Associate of the Belgian Funds for Scientic Research F.R.S.-FNRS

the form of a leakage function. The class of leakage functions however has to be somehow restricted, else it could just leak the entire state of the device, making any security application essentially impossible.

Many restrictions on leakage functions have been proposed during the last few years: space-bounded leakages, HILL-pseudoentropy preserving leakages, low complexity leakages, non-invertible leakages, leakages without access to a random oracle, or simulatable leakages to cite a few. The motivations for all these proposals are similar. One the one hand, one would like to define a class of leakage functions that is sufficiently large to capture essentially everything that an adversary could derive from side-channel measurments. This can either be argued by demonstrating that any weaker model would imply the impossibility of designing a secure system, or by making the model empirically verifiable by implementers. On the other hand, in order to be of practical interest, the chosen security model should keep it possible to prove the security of efficient constructions: the most important targets for side-channel attacks are constrained devices.

We will describe various proposed solutions to these problems, underlining their respective strengths and weaknesses. None of these solutions is completely satisfactory however: either the security models appear to be overly restrictive, or the proposed constructions present some peculiarities that reduce their efficiency and appear to only reflect an overly strong security model. Meanwhile, our understanding of these issues keep improving, and one may hope to see fully convincing solutions appearing in a near future.

Acknowledgements We thank Sebastian Faust, Tal Malkin, Elisabeth Oswald, François-Xavier Standaert, Yu Yu, Moti Yung, and many others for enjoyable and interesting discussions.

References

[1] Francois-Xavier Standaert, Olivier Pereira, Yu Yu, Jean-Jacques Quisquater, Moti Yung, and Elisabeth Oswald. Leakage resilient cryptography in practice. Cryptology ePrint Archive, Report 2009/341, 2009. `http://eprint.iacr.org/`.

[2] Yu Yu, François-Xavier Standaert, Olivier Pereira, and Moti Yung. Practical leakage-resilient pseudorandom generators. In *Proceedings of the 17th ACM conference on Computer and communications security - CCS'2010*, pages 141–151. ACM, October 2010.