Leakage-resilient authentication and encryption from symmetric cryptographic primitives

Keywords : Encryption; Authentication; Side-channel attacks; Leakage resilience.

Olivier Pereira, François-Xavier Standaert, Srinivas Vivek

***Abstract* – The need for secure communication keeps increasing in a world in which small connected "things" will outnumber the world population within 2 years (Gartner, Nov. 2015). The challenges raised by this need are particularly acute when objects are readily accessible to an adversary: in this context, security is not only an algorithmic problem, but also a physical problem as devices may leak sensitive information through their power consumption or electromagnetic radiations.**

In this research, we investigate the design of authentication and encryption schemes that are both efficient and leakage-resilient, in the sense that security can be maintained even if a device continuously leaks information about its internal state. We develop new security models that account for information leakages, and propose new block-cipher based constructions that cause a marginal cost compared to non-leakage-resilient constructions. Finally, we prove the security of our constructions based on traditional assumptions on block-ciphers and on the possibility to* simulate *leakages, an empirically verifiable property of a device.

Leakage-resilient cryptosystems aim to maintain security in situations where their implementation leaks physical information about their internal secrets. Because of their efficiency and usability on a wide range of platforms, solutions based on symmetric primitives (such as block ciphers) are particularly attractive in this context.

So far, the literature has mostly focused on the design of leakage-resilient pseudorandom objects (e.g. PRGs, PRFs, PRPs). We now consider the complementary and practically important problem of designing secure authentication and encryption schemes. For this purpose, we follow a pragmatic approach based on the advantages and limitations of existing leakage-resilient pseudorandom objects, and rely on the (arguably necessary, yet minimal) use of a leak-free component. The latter can typically be instantiated with a block cipher implementation protected by traditional countermeasures, and we investigate how to combine it with the more intensive use of a much more efficient (less protected) block cipher implementation.

Based on these premises, we propose and analyse new constructions of leakage-resilient MAC and encryption schemes, which allow fixing security and efficiency drawbacks of previous proposals in this direction. One of our constructions, illustrated in Figure 1, is reminiscent of the widely used CBC-MAC mode. However, it uses a leak-free initialization step in order to derive a one-time key from a unique initialization vector (IV), and then keeps updating this one-time key with each message block, instead of reusing the same key in each round, hence reducing the amount of information that can be collected about the secret state.

For encryption, we additionally provide a detailed discussion of why previously proposed (indistinguishability based) security definitions cannot capture actual side-channel attacks, and suggest a relaxed and more realistic way to quantify leakage-resilience in this case, by reducing the security of many iterations of the primitive to the security of a single iteration, independent of the security notion guaranteed by this single iteration (that remains hard to define). Our encryption scheme, illustrated in Figure 1, is also based on a leak-free initialization step that produces a one-time key, which is then expanded using a leakage-resilient stream-cipher whose output is xored with the message blocks.

A natural direction for future works consists in addressing the challenge of building authenticated encryption schemes with associated data (AEAD) that would be both misuse-resistant and leakage-resilient.

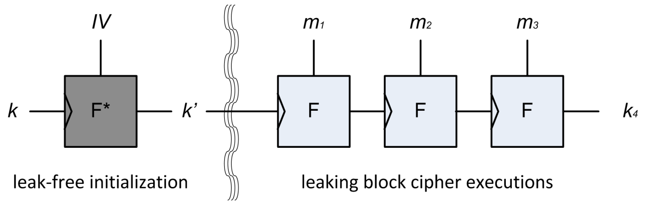

Figure 1: Leakage-resilient MAC.

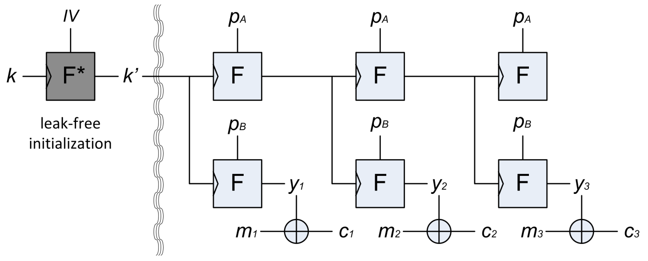

Figure 2: Leakage-resilient encryption scheme.

References

[1] Olivier Pereira, François-Xavier Standaert, and Srinivas Vivek. Leakage-Resilient Authentication and Encryption from Symmetric Primitives. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, pages 96–108. ACM, 10 2015.

[2] François-Xavier Standaert, Olivier Pereira, and Yu Yu. Leakage-Resilient Symmetric Cryptography under Empirically Verifiable Assumptions. In *Advances in Cryptology – CRYPTO 2013*, Lecture Notes in Computer Science, pages 335–352, 8 2013. Full version on http://eprint.iacr.org/2013/370.