Wiretap Coding in the Context of PUFs

Christoph Frisch

Technical University of Munich
Munich
Germany

The increasing amount of connected devices in today's world produces more and more sensible data that is transmitted. Encryption ensures the security of these data, but a secret key is needed. The general approach is to store the secret key in a Non-Volatile Memory (NVM). However, this memory is expensive and might be susceptible to attacks even if the chip is powered off. Securing the NVM results in additional costs and is even more difficult to realize under additional constraints in a lightweight application.
Silicon Physical Unclonable Functions (PUFs) [Gas03] can be used to store keys without NVM: Uncontrollable variations in the manufactoring process lead to intrinsic physical characteristics of a device which can be exploited by PUFs. In a sense these individual properties can be compared to human biometrics (e.g. fingerprint), but embedded in silicon. The underlying assumption is that an attacker cannot predict the PUF from the outside. Hence, the "device fingerprint" can be used to derive a secret.
The information theoretic wiretap coding [Wyn75] is based on a similar assumption: Secrecy is achieved as long as a channel to a legitimate user is better (i.e. less noisy) than the degraded wiretap channel to an attacker. Consequently, this talk discusses the applicability and the benefit of wiretap coding in the PUF context.

References

[Gas03] Blaise Gassend. *Physical Random Functions*. Master's thesis, 2003.

[Wyn75] Aaron D. Wyner. The wire-tap channel. *Bell Labs Technical Journal* 54(8):1355–1387, October 1975.

crypto day matters 28 (2018)
Beiträge vom 28. Kryptotag, 07.-08.06.2018, Kirchheim.
doi:10.18420/cdm-2018-28-24