E-USER

CRYPTO-ENABLED RFID TAGS

RÉGION WALLONNE

UCL Université catholique de Louvain

Radio-frequency identification (RFID) tags are small devices able to communicate via radio waves to exchange data with a reader. Their low price and ease of deployment make them very useful tools for identification and tracking purposes. They are more and more widespread everyday.

Typical RFID-based applications include:

- goods tracking (stock management, supermarket checkout, electronic article surveillance...)
- security (passports...)
- pet identification
- micropayment, e.g. in combination with mobile phones
- ticketing (road tolls, ski pass, public transportation...)

E-USER enables strong cryptographic applications on the next generation RFID tag

Security and privacy...

Many RFID-based applications require advanced **security** features: if a freely reloadable micropayment tag can be produced, or if an electronic ticket can be cloned, the potential loss for the infrastructure owner can quickly become unbearable.

Privacy-related issues are another important factor, as it is desirable, and often mandated by law, to protect the privacy of an individual, even if he keeps using the same RFID tag for several years.

Even contexts that do not involve personal data might require privacy-enabling technologies: goods revealing their nature and serial number to anyone equipped with an RFID reader might provide critical information on a production chain, or help thiefs locate lucrative targets.

but for a reasonable cost

Even when the need for security is real, the cost vs. benefit is a key factor for solution acceptance. We need a strong RFID tag, capable of performing secure operations in a short delay, but the price of this tag must remain low enough to make it a realistic option for commercial use.

Enabling cryptography on RFID tags

As a basic building block for secure applications, the RFID tag must support strong cryptographic primitives.

Our target was thus to implement a cryptographic co-processor for RFIDs providing a strong encryption primitive. This primitive can then be used as a basis for cryptographic protocols compliant with the current state of the art in security.

A standard-based approach

The cryptographic primitive we implemented is the widely accepted Advanced Encryption Standard (AES).

Using a standard brings two major advantages:

- We benefit from the wide attention AES has been receiving from the cryptographic community for the last ten years.
- It greatly simplifies interoperability issues. Applications interacting with an E-USER tag are easy to build based on one of the widely available AES implementations for various platforms.

.....Performance overview.....

Small size: 3500 GE
0.018 mm² in 65 nm

Speed: 36 kbps encryption

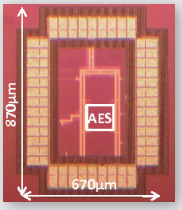
Low power: 0.25 µW @ 36 kbps

Low energy: 0.74 nJ per 128-bit

Low supply voltage: down to 0.32 V

Cycle count: 1142
Latency: ~4 ms

Architecture:
8-bit datapath,
32B RAM,
composite field
S-BOX.



Side-channel attacks

In parallel to the circuit design, we also conducted an analysis of the impact of nanoscale technologies on side-channel attacks. Our conclusion is that, besides cost and performances, an additional advantage of advanced technologies is that they provide enhanced resistance against such attacks. More precisely, we showed in[2] that device variability in our 65nm AES chips affect the usual leakage models used in Differential Power Analysis (DPA). Combined with usual countermeasures to protect implementations (e.g. masking, hiding), this observation is expected to lead to improved security levels.

What we developed

Thanks to Walloon region funding, we produced a prototype cryptographic co-processor optimized for RFID[2]. This co-processor fully exploits the advanced 65nm LP technology to offer AES encryption and decryption at 36 kbps (compliant with passive RFID applications) with a record power consumption of 0.25 µW. This extremely low power consumption is obtained thanks to the ultra low operating voltage (down to 0.32 V) enabled by adequate design choices (careful logic gate selection, upsized gate length MOSFET, adequate implementation flow with recharacterization of logic library).

In order to demonstrate the possibilities offered by our co-processor, we designed a privacy-preserving authentication protocol based on our co-processor[3]. In addition, this protocol verifies that the tag is indeed close to the reader to thwart relay attacks.

References

[1] M. Renauld, F.-X. Standaert, N. Veyrat-Charvillon, D. Kamel, D. Flandre, A Formal Study of Power Variability Issues and Side-Channel Attacks for Nanoscale Devices, in the proceedings of Eurocrypt 2011, Lecture Notes in Computer Science, vol 6632, pp 109-128.

[2] C. Hocquet, D. Kamel, F. Regazzoni, J.-D. Legat, D. Flandre, D. Bol, F.-X. Standaert, Harvesting the potential of nano-CMOS for lightweight cryptography: An ultra-low-voltage 65 nm AES coprocessor for passive RFID tags, in the Journal of Cryptographic Engineering, vol 1, num 1, pp 79-86, April 2011, Springer.

[3] C.H. Kim, G. Avoine, F. Koeune, F.-X. Standaert, O. Pereira, The Swiss-Knife RFID Distance Bounding Protocol, in the proceedings of ICISC 2008, Lecture Notes in Computer Science, vol 5461, pp 98-115, Seoul, Korea, December 2008, Springer.

Partnership We are looking for partners to undertake the production and exploitation of this new technology.

UCL Crypto Group
Place du Levant, 3 - 1348 Louvain-la-neuve
(+32) 10 47 81 41 - uclcryptogroup@listes.uclouvain.be