The Feasibility of On-the-Tag Public Key Cryptography

Marc Girault, Loïc Juniot and Matthew Robshaw
France Telecom Group - Orange Labs

RFID SECURITY 07, 11-13 July 2007

Prelude

- This talk comes as an illustration of sentences pronounced yesterday or today :
  - "Industry + academic CAN collaborate" (Melanie R. Rieback)
  - "An RFID security industry could help provide cheap RFID tags w/ lightweight crypto" (Melanie again)
  - "Public key cryptography requires too many gates in RFID" (Adi Shamir)
  - "GPS protocol has been proposed for RFID" (Serge Vaudenay)
  - And many others from Martin Feldhofer's talk…

RFID authentication – Why ?

- Many applications (should) require tag authentication,e.g.
  - e-passport and visas
  - ticketing (entertainment, sport)
  - public transport
  - access control
  - airline baggage handling
  - anti-counterfeiting (luxury, pharmaceutical products)
  - engine components (automotive or aeronautic industries)

- *Public key* authentication would be appreciated in open systems
  - the reader need not share a secret with the tag
  - the reader may be multi-application

RFID authentication – How ?

(GE = Gate Equivalent)

- Standard
  - AES (3400 GEs, *Feldhofer et al.'04*)
  - ECC (more than 20 000 GEs, *Batina et al.'06*, *Kumar-Paar'06*)
- Exotic
  - Many proposals (*HB+*, *LMAP*, *Chien et al.*..), often broken (except *Gilbert '00*)
  - NTRU (2850 GEs, *Gaubatz et al.'04)*
- Dedicated
  - DESXL (2300 GEs, *Poschmann et al.'07)* ; Present *(*1570 GEs, *Bogdanov et al.'07) ;* see also e-Stream project (Trivium, Grain,…) and A. Shamir's talk
  - **This talk**

Motivation and goal

- Motivations
  - It is not very clear if any of the previous proposals can satisfy **all the requirements** in terms of GEs, power consumption, time execution and security (AES ?)
  - It is very far from clear if public key can be implemented on low cost tags at all

- Goal
  - demonstrate the **concrete** feasibility of on-the-tag **well established** public key cryptography
  - price to pay : use the mode with coupons (not a drawback in many applications)

Main result

- A fully functioning FPGA prototype, which implements GPS scheme in coupon mode with only 2600 GEs

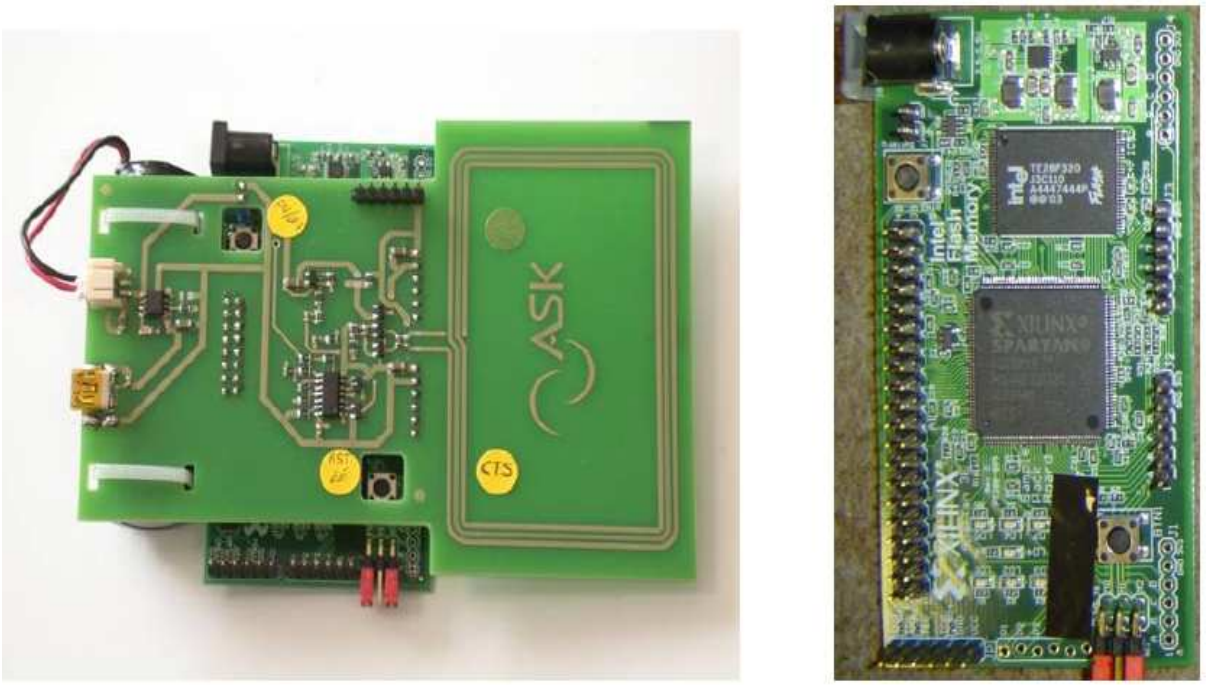


Fig. 2. The ECGPS prototype that simulates a tag.

GPS protocol

- "On the Fly Authentication and Signature Schemes Based on Groups of Unknown Order" (*M. Girault, G. Poupard and J. Stern*, JoC, Vol.19, N°4, Autumn 2006)
- Zero-knowledge (variant of Schnorr's protocol)
- Proven secure if discrete logarithm is hard
- ISO/IEC 9798-5
  - "Entity Authentication – Mechanisms using Zero-knowledge Techniques"

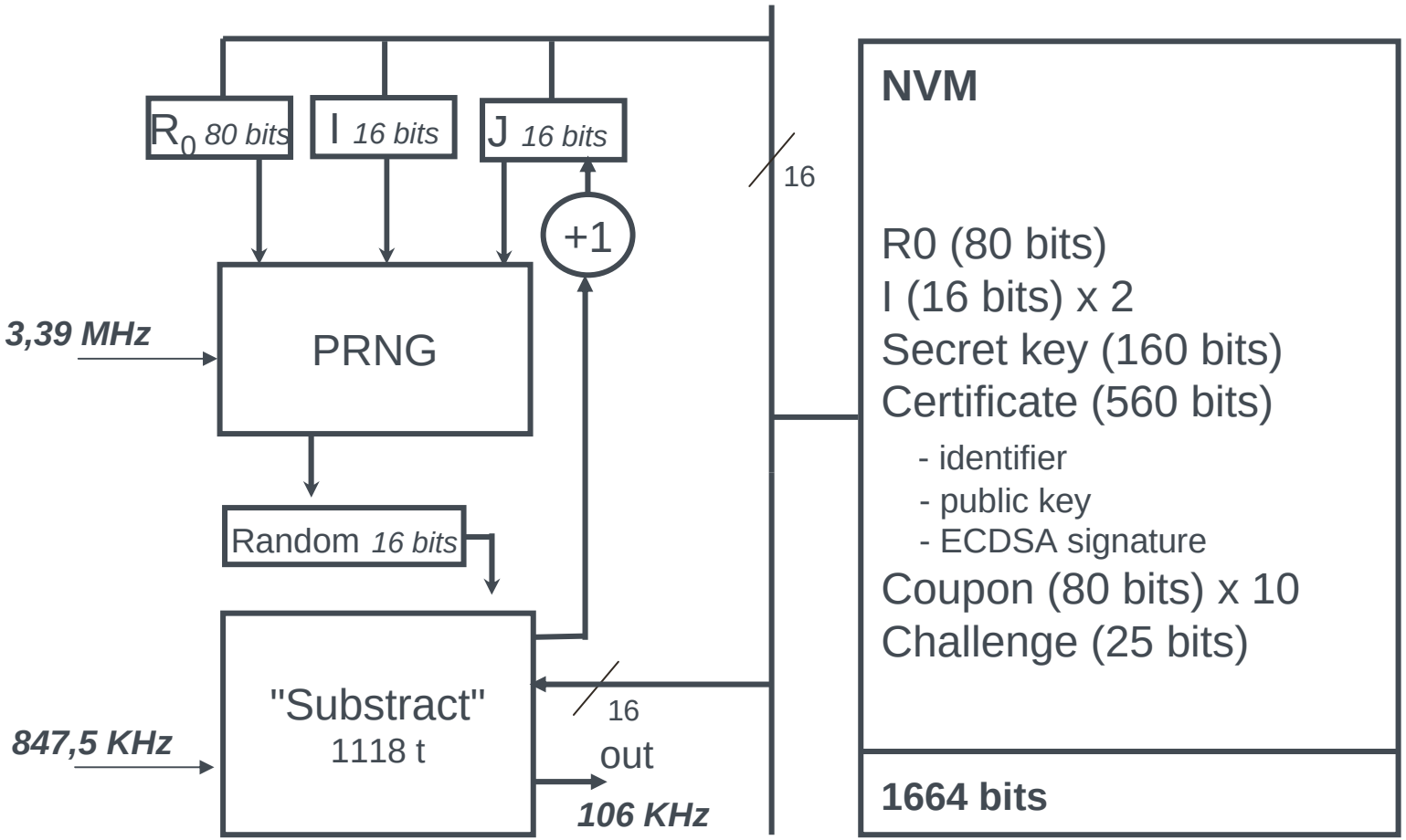
EC-GPS (overview)

Tag		Reader
PARAMETERS		
Curve $\mathcal{C}$, point P		Curve $\mathcal{C}$, point P
KEYS		
Secret $s \in_R \{0,1\}^\sigma$		
Public $V = sP$		Public $V = sP$
COUPON PRE-COMPUTATION WITH PRNG		
For $0 \leq i \leq t-1$		
Let $r_i = \text{PRNG}_k(i)$ where $\lvert r_i \rvert = \rho$		
Set $x_i = \texttt{hash}(r_i P)$		
Store coupon x_i		
PROTOCOL USING ON-TAG PRNG		
At time i fetch x_i	$\xrightarrow{x_i}$	
	$\xleftarrow{c}$	Pick $c \in_R \{0,1\}^\delta$
Generate $r_i = \text{PRNG}_k(i)$		
$y = r_i - (s \times c)$	$\xrightarrow{y}$	$\texttt{hash}(yP + cV) \stackrel{?}{=} x_i$

Further optimization

- "Public key Authentication With One (On-Line) Single Addition" (*M. Girault and D. Lefranc,* CHES 2004)
- Trick : challenge of a special form (very large, with a few ones judiciously spaced, transmitted and stored in a compressed form)
- Result : multiplication turned into a modest number of additions of the secret key *s*

Cryptographic module



Performances in a nutshell

- Space
  - **6000** GEs
  - **2600** GEs for cryptography only
  - **0,05 mm²** with 0,180 µm technology
- Time
  - total authentication time :**188 ms**
  - tag computation time : **14,2 ms**
  - RF communication time : **14,6 ms**

Space (in more details)

Table 1. Space requirements for the different components in the FPGA prototype.

component	$\approx$ *GEs*	$\approx$ *fraction of total*
GPS computation	600	10%
PRNG	1000	17%
Logic + memory	1000	17%
Supporting module	3400	56%
Total	6000	

Performance trade-offs

Some performance trade-offs for GPS in $0.180\mu m$ technology [19].

area (GE)	*current (μA)*	*time (cycles)*	*frequency (kHz)*
317	0.61	1088	100
431	0.67	136	100
900	1.43	68	100
431	2.26	136	500
900	4.91	68	500

Conclusion

- Secure public key authentication in RFID is desirable (# desired…) and possible
- A FPGA prototype exists, which can be moved to a RFID tag as soon as tomorrow (just ask ASK)
- Still to improve :
  - use a public PRNG validated by the cryptographic community (ideally standardized)
  - implement procedures for refreshing coupons when needed