Chip card sidelight on lightweight crypto

Marc Girault  
*Orange Labs Caen*  
CARDIS 2014  
5-7 November 2014
Contents

1. Back to 1985
   • Why 1985?
   • Public phones
   • Cryptology

2. Prepaid phone cards
   • Background
   • T1G
   • T2G
   • FAC
   • Looking back 25 years later

3. Conclusion
Warning

• Sorry but this talk mainly tells facts that occurred in France...

• A similar story, with actors in Germany, could (should) also be told
1. Back to 1985
Why 1985? (1)

- Because 1985 is a key year for massive deployment of chip cards in France
- In two sectors (mainly): public telephony and banking
- In two forms: memory card (without microprocessor) and smart card (with microprocessor)
- More precisely...
Why 1985? (2)

• This is the year when prepaid phone memory cards were massively deployed in France by (famous) pyjama-style
Why 1985 ? (3)

• This is also the year when French banks *decided* to move to smart cards

*Massively deployed some years later*
Why 1985 ? (4)

• This talk is only about phone cards (memory cards)
• Thanks to their microprocessor, bank cards did not need lightweight crypto
  – DES was on the point to be implemented in smart cards
  – In the mean-time, “medium-weight” proprietary algorithms were used (Telepass 1, Telepass2)
Public phones (1)

- In 1985, telephone is (prominently) fixed and analogic.
- Mobile telephones exist but are not portable, are expensive and don’t work everywhere.
- In France, Radiocom 2000 program (first cellular network) will start in 1986 and the handsets are priced at more than 4 000 €.
Public phones (2)

- To call outdoor requires phones in streets (booths) and public places (airports, stations...)

Chip card sidelight on lightweight crypto  Marc Girault (Orange Labs)
CARDIS 2014  Paris - 5-7 November 2014
Public phones (3)

- In France public phones long worked with coins...
- then specific tokens...
- ... then coins again!
- Not practical (collecting money) and dangerous (vandalism, theft)
- The idea of using cards instead of coins emerges in the late 70’s
Public phones (4)

• Several card technologies are tested: magnetic, holographic, thermo-magnetic...

• Finally PTT selects the “invented here” chip card
Public phones (5)

• 1993 (France)
  – 173 000 public phones in the streets : 123 000 with “télécartes”
  – 100 millions “télécartes” sold this year

• 1997 (France)
  – 1 billion of “télécartes” sold from the beginning but...
  – … first year the sales decrease

• 2002 (world)
  – 1.3 billion of prepaid cards sold this year but...
  – … first year the sales decrease
In 1985, DES and RSA undisputed crypto-stars
- DES: the glory (widely deployed)
- RSA: towards the glory (implemented in French bank cards as a static signature for card authentication)
Cryptology (2)

• Suitability for smart cards
  – DES: soon (1986)
  – RSA: later

• Suitability for memory cards
  – DES: never
  – RSA: never never never
Cryptology (3)

• Still (officially) unknown or uninvented
  – Differential cryptanalysis
  – Linear cryptanalysis
  – Attacks against modes of operation
  – Side-channel attacks
  – Alternatives to DES: FEAL, IDEA, RCx.... AES

• Lightweight crypto starts (nearly) from scratch
2. Prepaid phone cards
Goal: replace true money by virtual call units
   – A unit allows a local call during a little less than 1 minute

Dilemma: where is the balance? Who updates it?

Two main approaches
   – on-line approach
   – off-line approach
Background (2)

• **On-line approach**: virtual units are at operator’s side

• User buys a “number”
  – written on a plastic card or stored in a memory card
  – equivalent to $n$ units
  – built with (cryptographic) redundancy

• User provides this number to the phone and makes a call

• Operator progressively updates the balance
Background (3)

• **Off-line approach**: virtual units are at card’s side

• User buys a card
  – “containing” $n$ units
  – storing a (cryptographic) certificate

• User inserts the card in the phone and makes a call

• Public phone progressively updates the balance *inside the card*
On-line vs off-line approach

On-line
– pro: fake units cannot be forged
– con: many simultaneous connections

Off-line
– pro: a few simultaneous connections
– con: fake units could be forged

In the mid-80’s, off-line solution is preferred

Nowadays, on-line solution is preferred
Background (5)

• **Forging vs cloning**

• **Forging**
  – the enemy can forge a fake cards from scratch
  – he can choose any serial number → **untraceable**

• **Cloning**
  – the enemy can only clone (= duplicate) a genuine card
  – he must choose the same serial number → **traceable**

• Forging is easier to prevent
Background (6)

- **Emulating**

- **Not emulating**
  - the fake card is **physically** and **functionally** indistinguishable from a genuine card

- **Emulating**
  - the fake “card” is **functionally** indistinguishable from a genuine card (not physically, it can be a bulky electronic device)

- Emulating is less discreet but sufficient for a fraud (not for a mass fraud)
• $T1G =$ “Télécarte de première génération”

• Disposable $\rightarrow$ must be very cheap
• Designed in the early 80’s
• 1984: first T1G
• 1985: deployment
• 1998: end of production
• Much later: end of acceptability
T1G (2)

• Memory card
  – no PIN
  – no computation capabilities
• N-MOS technology
• EPROM memory (256 bits)
  – unary counting
• Synchronous protocol
• 50 or 120 units
• EPROM contents
  – \( I \) (permanent public data, including card identifier)
  – \( D \) (variable data, including balance)

• To prevent from forging, the permanent data \( I \) are “signed” by a (static) 16-bit MAC, \textit{not computed} by the card, called certificate

• The certificate does not prevent from cloning
T1G (4)

- Frauds on T1G are reported in the late 80’s
- Some of them (not all) are clone-based
  \(\rightarrow\) Need for a challenge-response protocol
- T2G (”Télécarte de seconde génération”) will include a “fonction anti-clone” (FAC, roughly a MAC)
- Works starts in 1989
  – ends in 1994 for “télécartes”
  – continues for other applications
T2G (1)

• *T2G* = “Télécarte de seconde génération”

• *Still* disposable → must *still* be very cheap
• Designed in the late 80’s
• 1993: first T2G
• 1994: deployment (in France and abroad)
• 2013: end of acceptability
  
  *(2015: end of acceptability of T3G, next and last generation)*
T2G (2)

- Memory card
  - light computation capabilities
- C-MOS technology
- E2PROM memory (340 bits)
  - binary counting
- Synchronous protocol
- 50 or 120 units
T2G (3)

• E2PROM contents
  – \( I \) (permanent public data, including card identifier)
  – \( D \) (variable data, including the balance)
  – \( S \) (secret key)

• To prevent from cloning, the data \( I \) and \( D \) are “signed” along with a challenge \( X \), by a (dynamic) MAC, \textit{computed} by the card

• This protocol is repeatedly executed during the phone call

• Typical sizes: 64 bits for each parameter
$T2G \ (4)$

$X$

$Y = \text{FAC} \ (I, \ D, \ S, \ X)$

$\cdots \cdots \cdots$

$X'$

$Y' = \text{FAC} \ (I, \ D', \ S, \ X')$
T2G (5)

• **General requirements**

  1) The chip must remain cheap
     → design the FAC with only **500 GE !!!**

     *(GE = logic Gate Equivalent)*

  2) The transaction time must be short
     → the number of rounds/iterations is “limited”

• Several versions of FAC have been designed
Technical requirement 1: The protocol is synchronous

→ E2PROM is read sequentially (bit by bit)

**FIG. 6**
FAC (2)

- Technical requirement 2: The number of GE is... 500!

→ ROM (≈ 6 GE/bit) and RAM (≈ 4 GE/bit) are very limited
FAC (3)

• Technical requirement 3: Clock frequency is low (typically 847 kHz)

→ E2PROM can be scanned only a few times
• Overall process
• Back to the 500 GE requirement

→ trade-off to find between:

– Complexity of Mix function
– State length
– Complexity of Change state function
Chip card sidelight on lightweight crypto  Marc Girault (Orange Labs)
CARDIS 2014  Paris - 5-7 November 2014
• **Mix function**

• A linear function of inputs

• Main ingredients:
  – inputs entered several times
  – sometimes after (easy-to-wire) permutation of bits
  – (easy-to-wire) LFSR
FAC (8)

- **State length** \((b \text{ bits})\)
- Recall: RAM bit \(\approx 6 \text{ GE}\)
- Depending on version, \(b = 4m (1 \leq m \leq 8)\)
- Result \(Y\) is (part of) last state
FAC (9)

- Change state function
- A non-linear $b$-bit permutation
- Main ingredient: 4-bit S-box
  - State bit $r0$ is XOR-ed with the output bit of Mix function
  - Other state bits are unchanged
- Up to four S-box, completed with rotations (of quartets)
Looking back 25 years after (1)

• **Overall process**

• Partly similar to the “absorbing phase” of a binary sponge – function:
  – All inputs are concatenated
  – Phase 1 output bit is XOR-ed with the state
  – Then the state enters a permutation
Looking back 25 years after (2)

- **Overall process**

- But it differs in that:
  - state is much smaller but...
  - ... the inputs are mixed in a “complex” not only padded
Looking back 25 years after (3)

- **Mix function**

- Evolution similar to the one of “message schedule” process in MDx-SHAx family:
  - inputs processed several times
  - sometimes after (easy-to-wire) bit-permutations
  - linear recurrences
Looking back 25 years after (4)

- **Change state** function
- 4-bit S-boxes happen to be a “natural” choice in lightweight crypto
  (see e.g. *Present*)
Conclusion

• Lightweight crypto was made necessary as soon as 1989 because:
  – mobile phones did not exist
  – money in public phones was undesirable
  – on-line architecture was not yet technically possible
  – prepaid chip phone cards had to be very cheap

• Lightweight crypto became a recognized research area 10-15 years later, with emergence of RFID
Credits

• Jean-Claude Paillès, David Arditti, Henri Gilbert, Jacques Burger