BAC TECH

Biometrics And Cryptography TECHnologies (made easy for you)

PUFFIN Workshop

Berlin, Nov 3, 2013

EURL au capital de 15.000€
SIREN 789 985 843 - RCS Aix-en-Provence - FRANCE

www.bactech.fr

31, Parc Club du Golf - CS 90519
350, avenue Guillibert de la Lauzière
13593 - Aix-en-Provence cedex 3

claude.barral@bactech.fr

Introduction

- I am very honored to have been invited to talk about a freely chosen subject:

  "PUF-Based Security for Smart Objects"

- My interest in embedded electronics security:
  - Past fifteen years in the smart cards industry, advanced hardware and software security research.
  - Currently trainer and consultant + academic activities
  - Multi-components smart cards, biometrics, cryptography…
- Registered expert for French and European funded projects
  - e.g. FP7 Unique

IEEE **Certified Biometrics Professional® (CBP) Program**

Agenda

- PUF & Biometrics
  - My very first contact with silicon PUFs
- PUF & Multi-components Smart Cards/Secure documents
  - Combining different PUF technologies
- PUF & Future (really?) Secured Communicating Solutions (a.k.a. Smart Objects)
- Secured Controllers vs. Application Processors
  - Underestimated applications of PUF
- Conclusion
  - Just my humble vision…

BAC TECH

Biometrics And Cryptography TECHnologies (made easy for you)

PUF & Biometrics

EURL au capital de 15.000€
SIREN 789 985 843 - RCS Aix-en-Provence - FRANCE

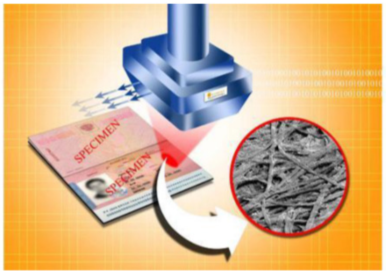
www.bactech.fr

31, Parc Club du Golf - CS 90519
350, avenue Guillibert de la Lauzière
13593 - Aix-en-Provence cedex 3

claude.barral@bactech.fr

Human ID vs. Material ID

- Human Biometrics
  - Two captures will never be identical
    - Hashing is useless
  - Matching upon “reasonable closeness”
- Material Identification
  - Intrinsic characteristics came from the raw material, the manufacturing tools, the material life cycle,…
  - Two measures will never be identical…
  - Deterministic Identification only after recovery upon “reasonable closeness” of measures
- Several common approaches
  - Error Correction, hamming distance…



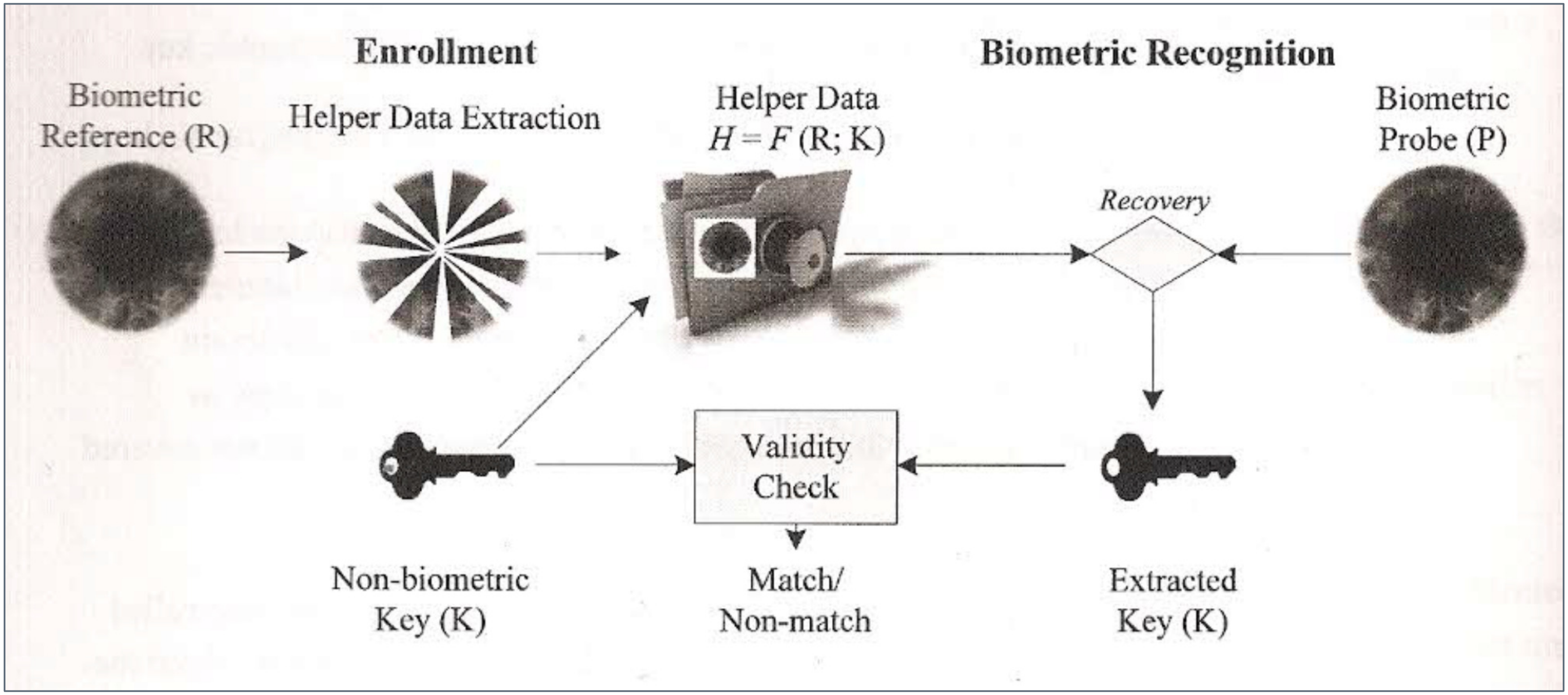
Coming from Fingerprint Match-on-Card…

- Reference fingerprint template never leaves the smart card secure memory
- Candidate fingerprint template sent to smart card for internal comparison and decision
- However, even internally, needs reference fingerprint template in clear for comparison: not satisfying
- Trying to match in the encrypted domain?
  - Fuzzy extraction
  - (fully) Homomorphic encryption
  - Cancellable transformation
  - Random obfuscation
  - …

My references

- Discussions with Yevgeniy Dodis about fuzzy extractor & secure sketch in 2004 after Eurocrypt
- **Security with Noisy Data: Private Biometrics, Secure Key Storage and Anti-Counterfeiting.**
  - Pim Tuyls, Boris Skoric, Tom Kevenaar (Eds.)
  - Springer, ISBN 978-1-84628-983-5
- This is where I learned about PUF…
- Effectively, technical issues very close to biometric extraction and matching of individuals

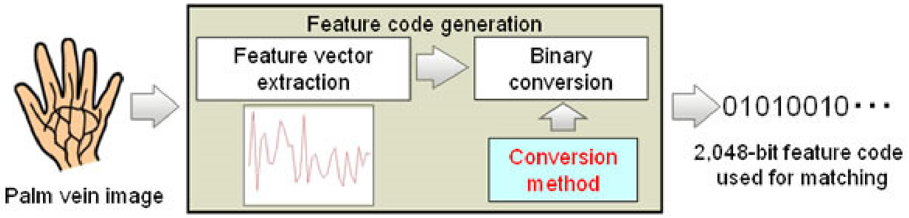
Conventional Biometric Cryptosystem



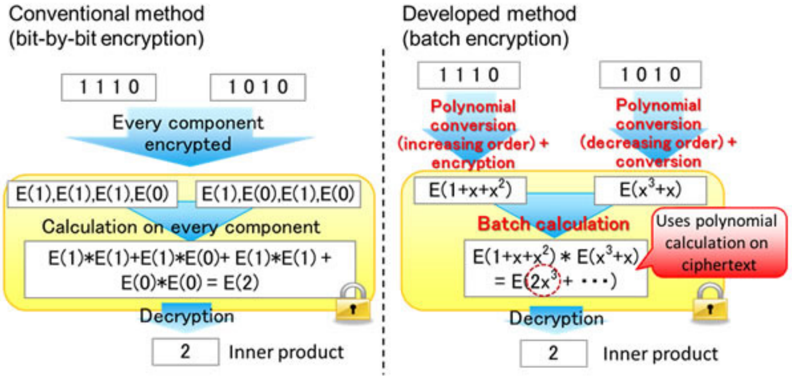
Credits: IEEE CPB program training material, 2012

Fujitsu recent press releases

- Fujitsu claims reproducible extraction of 2048 bits key from its PalmVein recognition technology (2013/08/05)



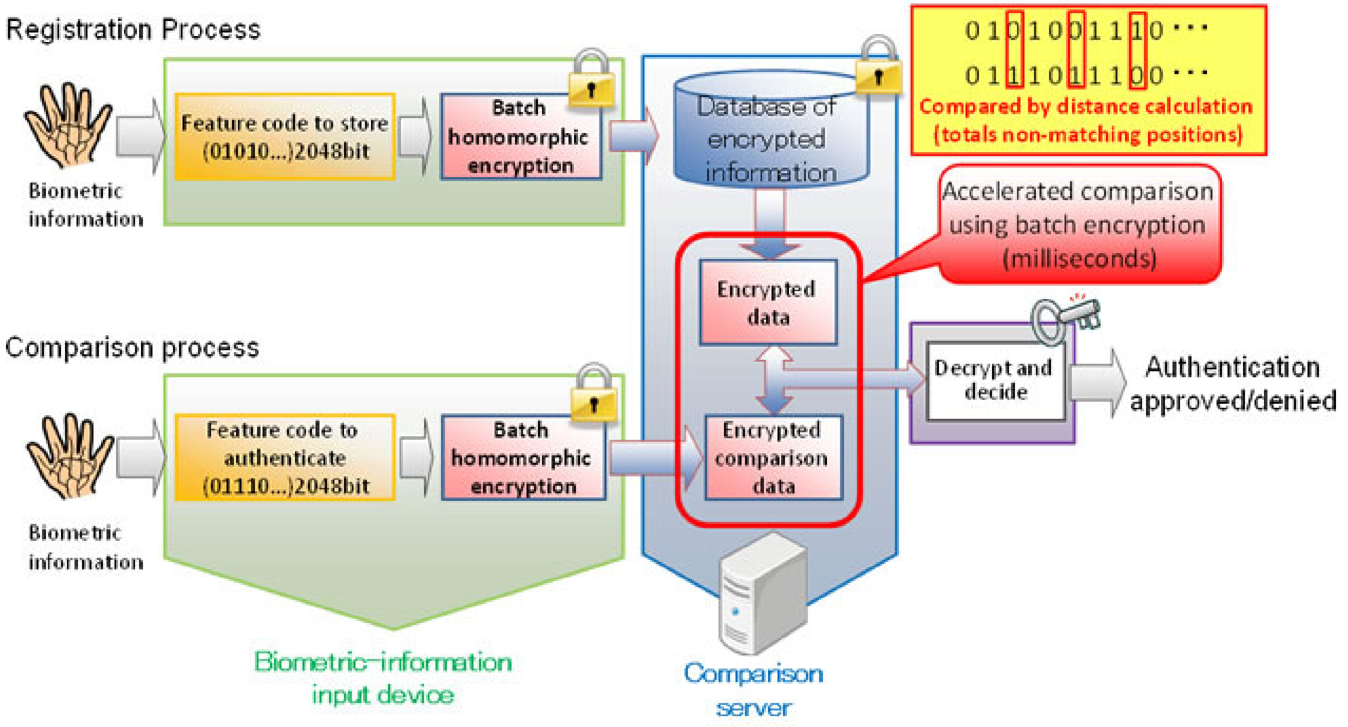
- Fujitsu then claims efficient fully homomorphic encryption (2013/08/28)


Conventional method (bit-by-bit encryption)
1 1 1 0
1 0 1 0
Every component encrypted
E(1),E(1),E(1),E(0)
E(1),E(0),E(1),E(0)
Calculation on every component
E(1)*E(1)+E(1)*E(0)+ E(1)*E(1) + E(0)*E(0) = E(2)
Decryption
2
Inner product
Developed method (batch encryption)
1 1 1 0
1 0 1 0
Polynomial conversion (increasing order) + encryption
Polynomial conversion (decreasing order) + conversion
E(1+x+x²)
E(x³+x)
Batch calculation
Uses polynomial calculation on ciphertext
E(1+x+x²) ∗ E(x³+x) = E(2x³+ ・・・)
Decryption
2
Inner product

Credits: Fujitsu, 2013

Combined product

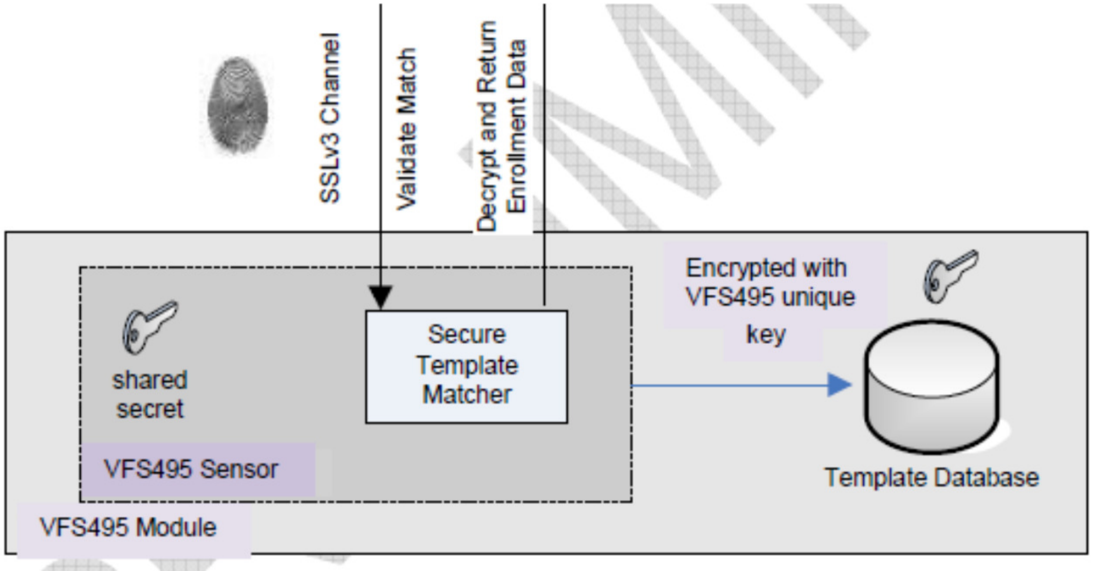
- Hamming distance, isn't it?


Registration Process
Biometric information
Feature code to store (01010...)2048bit
Batch homomorphic encryption
Database of encrypted information
0 1 0 1 0 0 1 1 1 0 ・・・
0 1 1 1 0 1 1 1 0 0 ・・・
Compared by distance calculation (totals non-matching positions)
Accelerated comparison using batch encryption (milliseconds)
Encrypted data
Comparison process
Biometric information
Feature code to authenticate (01110...)2048bit
Batch homomorphic encryption
Encrypted comparison data
Decrypt and decide
Authentication approved/denied
Biometric-information input device
Comparison server

Credits: Fujitsu, 2013

Silicon PUF and biometric sensors

- PUF feature claimed in fingerprint sensor:



- PUF (Physical Unclonable Function) – Generates unique 448 bit output for each VFS sensor. It is used to generate key material.

Credits: Validity Inc., 2013

BACTECH

Biometrics And Cryptography TECHnologies (made easy for you)

Multi-components Smart Cards

Controlled PUF vs. Uncontrolled

- Silicon PUF has the advantage of embedding its own “reader” and artificial intelligence
  - But you need silicon and processing capabilities…
- Optical PUF, coating PUF or other electronic PUF based on resistive/capacitive/inductive phenomenon are still of great interest
- New PUF approaches
  - Printed Electronics
    - Resistor, Capacitor, Inductor, Diode, Transistor…
    - Thin successive printed layers: charged, insulator…
  - RLC model of any basic active element: diode, transistor…

PUF as a tool for tamper-resistance

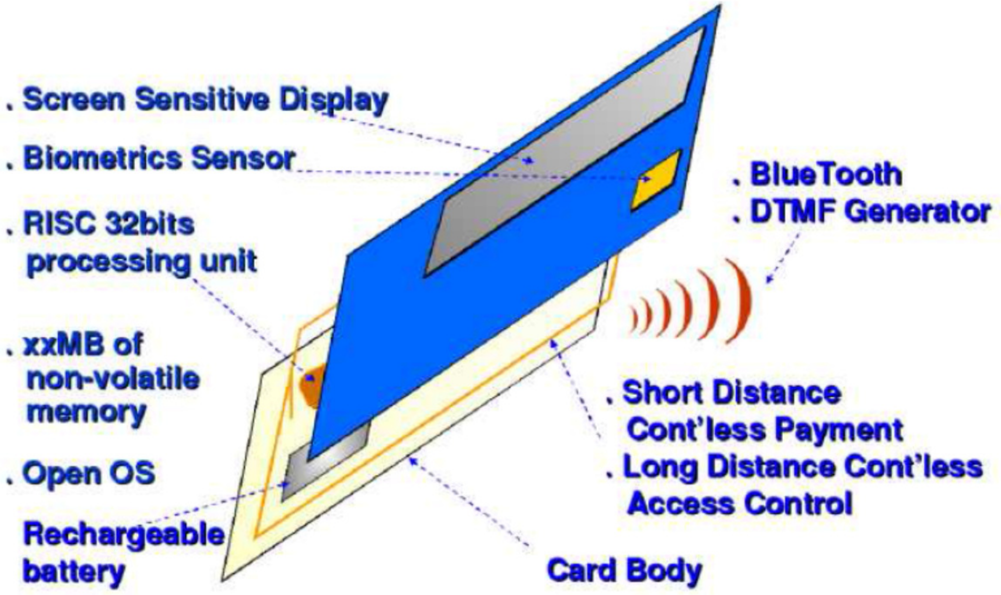
- Coating PUF came from this needed feature
  - Protecting decapsulation of smart card chip
- Bubble tags originally targeted to cost-effectively replace the active module onto the plastic body
  - Well, Unique ID but not processing capabilities!
  - Then, bubble tag as anti-counterfeiting of the plastic body with tag ID stored in smart card chip

Credits: Gemalto, 2006

Credits: ProofTag, 2011

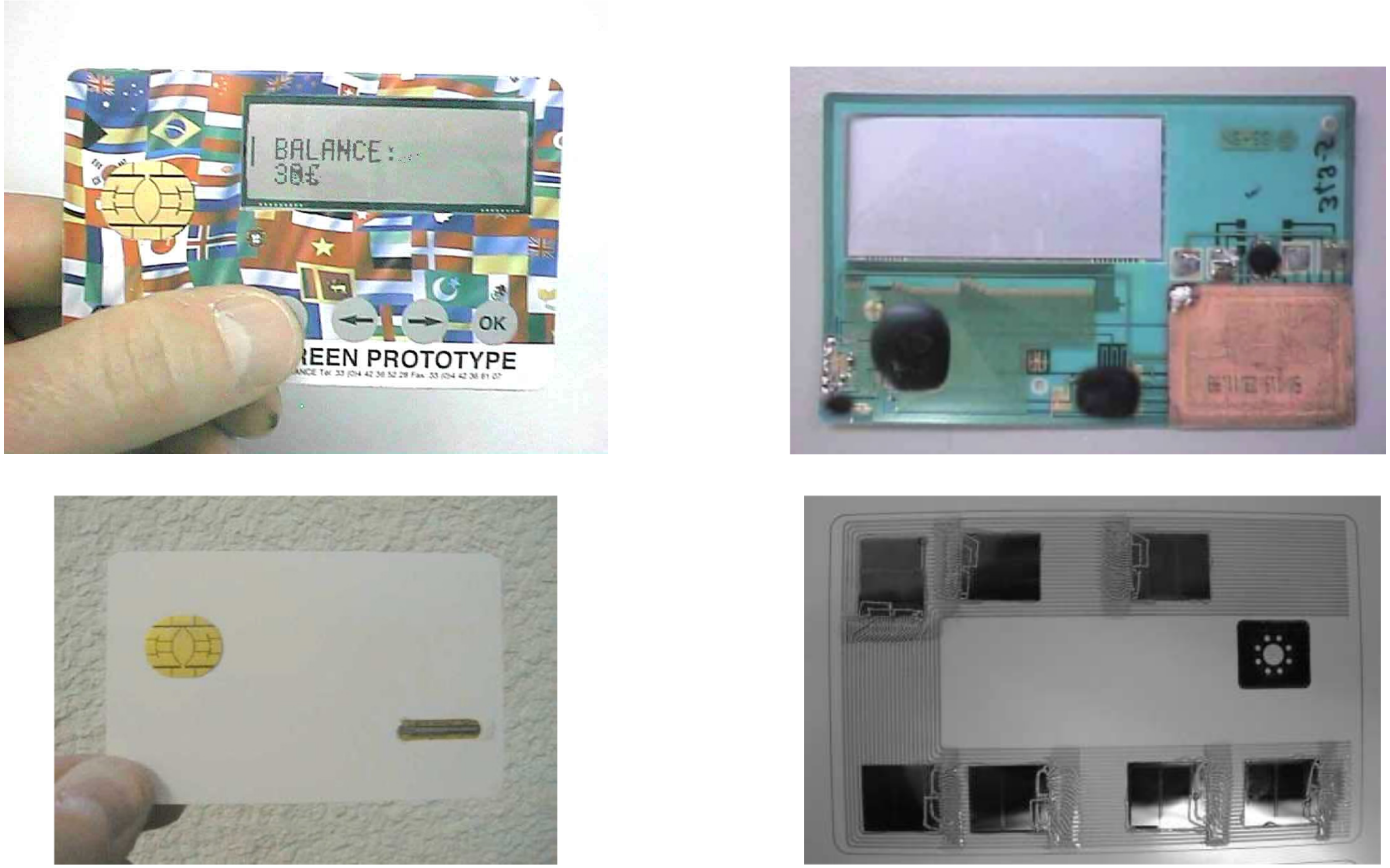
The Concept Card

- Smart card is longer only one piece of silicon in one piece of plastic!
- Contactless technology frees form factor constraints!


. Screen Sensitive Display
. Biometrics Sensor
. RISC 32bits processing unit
. xxMB of non-volatile memory
. Open OS
Rechargeable battery
. BlueTooth
. DTMF Generator
. Short Distance Cont'less Payment
. Long Distance Cont'less Access Control
Card Body

Credits: Gemplus, 1998

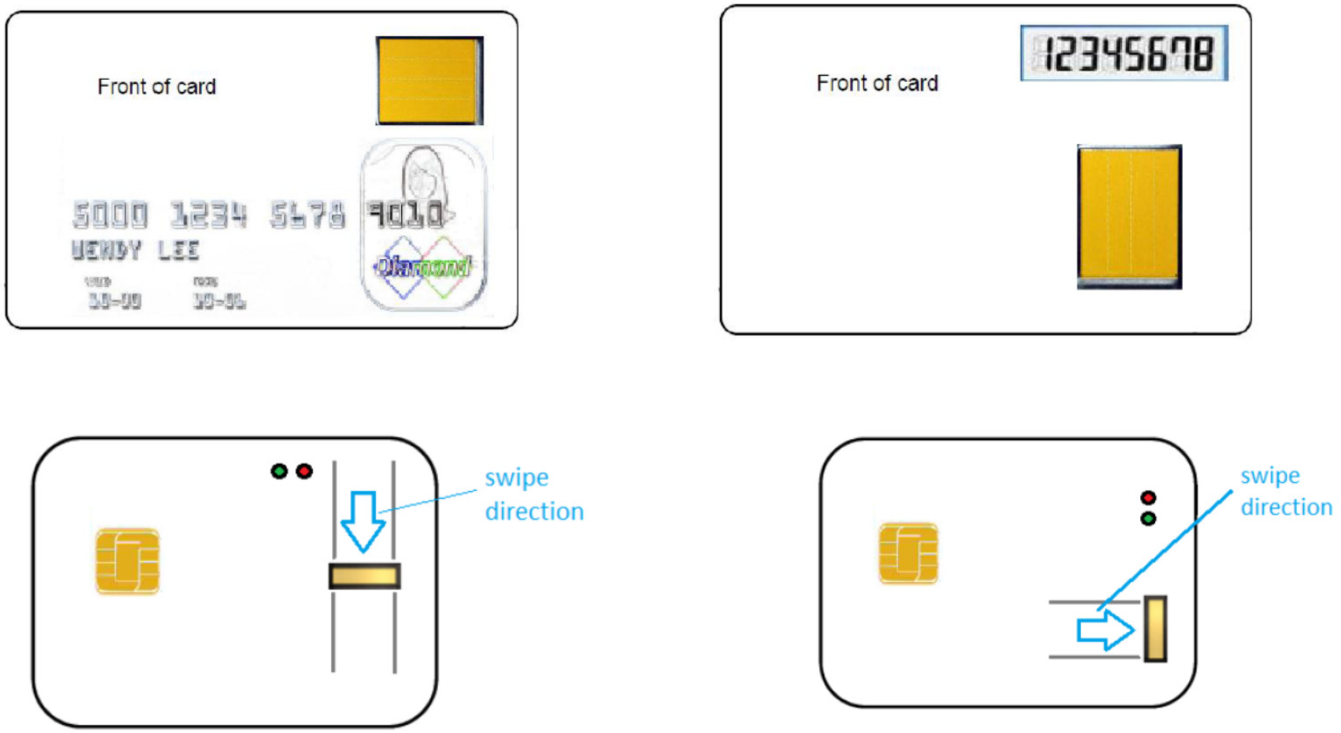
Examples



Credits: Gemplus, 1998-2001

Current ISO initiative

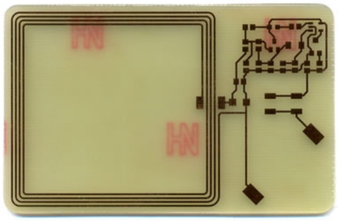
- ISO/IEC CD 17839: system on card

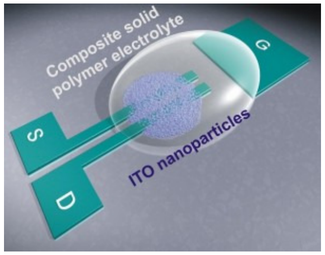


Credits: ISO/IEC 17839 Committee Draft Document, 2013

Electronic PUFs beyond silicon

- Dozens of unique and non-reproducible measurements from any semiconductor
- Remember RLC models of any basic electronic element
- Whatever is the technology
  - Etching
  - Printed Organic
- What about other effects/applications?
  - Piezoelectric
  - Pyro-electric
  - MEMS
  - Bio-electronic





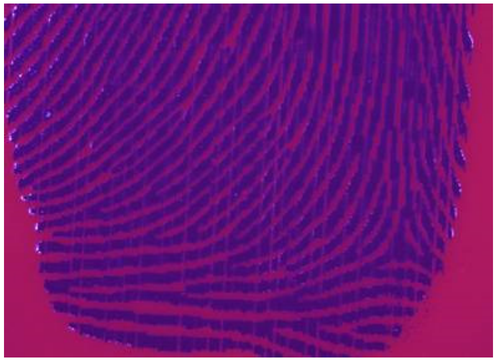
Credits: MaterialViews, 2012

Printed Electronics

- Ag-charged ink
  - Silver nanoparticles
  - Non-uniform
    - As Si doping…

Credits: EMSE, 2009

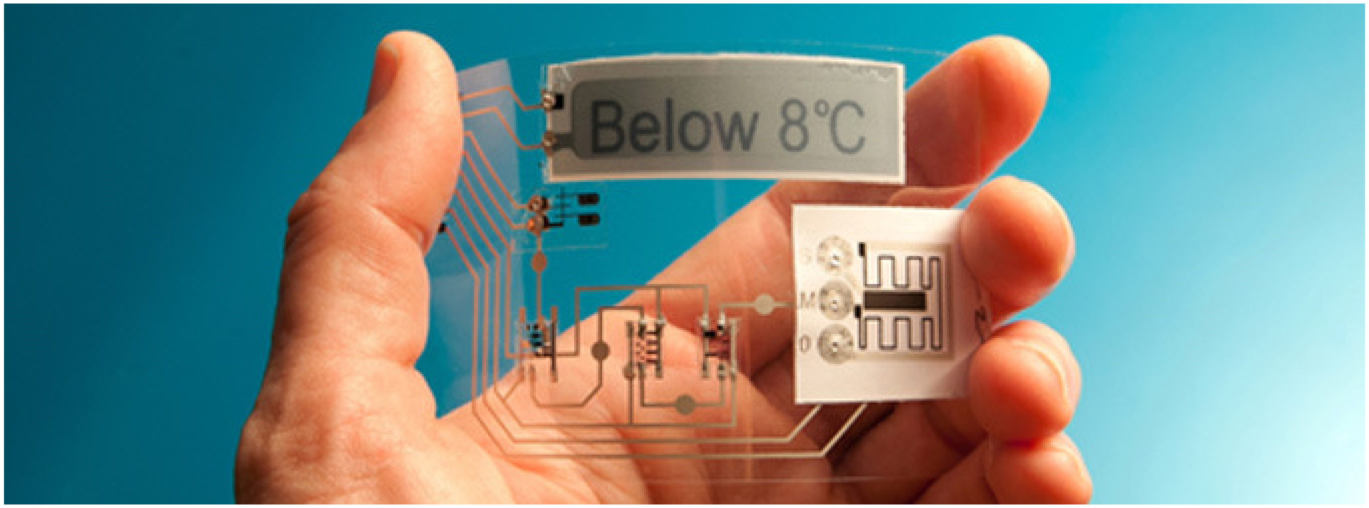
Credits: Google image…



Credits: EMSE, 2009

Organic/Plastic/Polymer Electronics

- Light Emitting Diodes
- Photovoltaic sensors
- Batteries
- …



Credits: ThinFilm.no, 2012

BAC TECH

Biometrics And Cryptography TECHnologies (made easy for you)

Secured Communicating Solutions (SCS)

EURL au capital de 15.000€
SIREN 789 985 843 - RCS Aix-en-Provence - FRANCE

www.bactech.fr

31, Parc Club du Golf - CS 90519
350, avenue Guillibert de la Lauzière
13593 - Aix-en-Provence cedex 3

claude.barral@bactech.fr

Future (really?) Smart Object: eWatches!

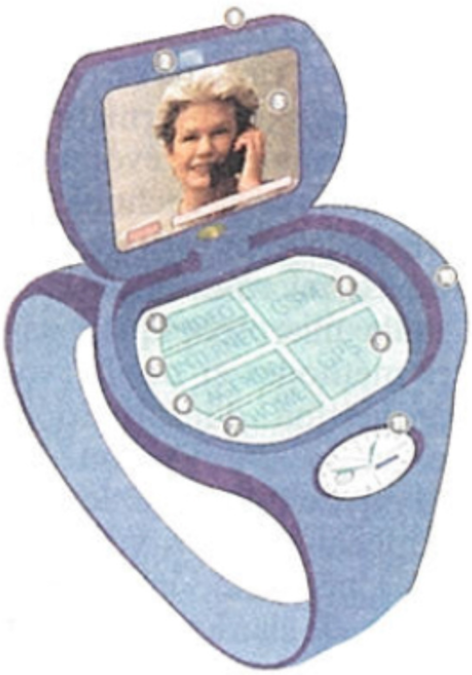
- What a hype!
  - Samsung Gear
  - Google Smart Watch
  - Apple iWatch
  - Microsoft
  - Sony
  - Well, what about Amazon, Facebook and so on…?

- Guess what?

Guess What?

- Here it ~~is~~ was:

La montre multimédia du futur



1 : Antenne GPS/GSM
2 : Caméra
3 : Écran tactile vidéo/PC
4 : Conférence vidéo
5 : Internet
6 : Agenda
7 : Liaison domotique
8 : GSM
9 : Localisation par satellite
10 : Capteur thermique intégré
11 : Heure-messagerie

Source : Gemplus.

Credits: ***PUF*** (Presse Universitaire de France), “La carte à puce”, 1999

Basic Components

- Display
  - Glass, plastic, Oled,…
  - Touchscreen
    - Possible measurement of touching finger characteristics?
      - “Bioelectrical PUF(?)” brings liveness detection
- Application processor
  - Additional secure element?
- Antenna(s)
- Battery
- Printed interconnections
- Camera, microphone (piezo), buzzer (piezo)

Hence plenty of elements to think “PUF”

- Smartwatch theft = Identity theft
- Threats of dissembling parts?
  - Replacement of the secure element
  - Replacement of the “personalized” touch sensing element
  - …
- Build a “security chain”
  - Let’s pick a challenge/response PUF technique
    - Each PUF response of an element is the challenge of the PUF feature in the next element
      - User biometrics > touchscreen > application processor > antenna > …

Other Smart Objects

- Personal Identification Device
  - http://www.ego-project.eu
  - Use Body Coupling Communication for pairing any other device
  - Needs close contact with user skin
    - Watch, wristband, necklace, ring
- KeyFob = contactless smart cards technology
  - Cars
  - Home
  - Virtualization: all these applications as a smartphone app.
    - e.g. My BMW remote, My Verisure (home burglar alarm)
    - Smartphone app => Smartwatch app
      - Back to smartwatch (chicken&egg?)

BAC TECH
Biometrics And Cryptography TECHnologies (made easy for you)

Secured Controllers vs. Application Processors

Back to Biometrics

- Coming from the security industry may not be an advantage to evaluate potential applications a new technology
- Fifteen years ago we focused on security application of fingerprint recognition and we “missed” user-convenience applications
  - There is a place for “weak-but-easy” security!
  - e.g. PIN replacement
  - Is iPhone5s fingerprint feature useless to security?
- Classical underestimation of capabilities out of our scope

PUF targeted Security Components

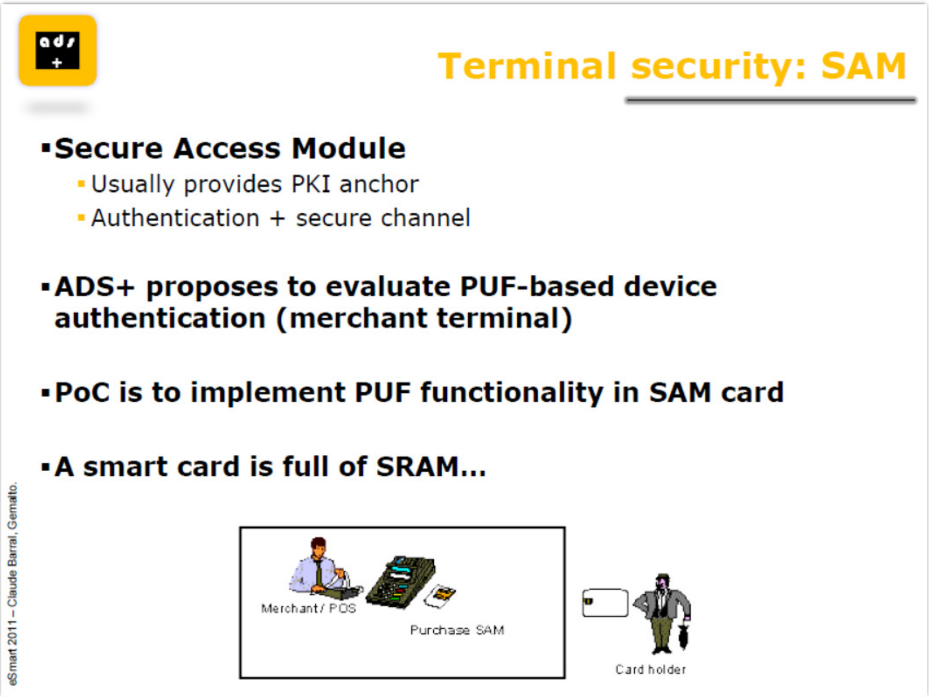
- Security devices are a niche within electronic market
- My feeling of initial marketing approach from a security manufacturer standpoint:
    - PUF Start-up companies:
        - Hide keys in low level electronic physics
        - No power supply = no keys = no attacks
    - My boss:
        - Additional cost
        - We have thirty years of experience and countermeasures to protect keys
        - => do not need PUF to write and recover keys!

PUF for Application Processors

- PUF is ideal to bring “weak-but-easy” security in any IT product
- Pure software approach using existing elements
- May combine PUF from different ICs within a same product
  - Main processor, graphic processor, baseband processor…
- Take better care of published attacks
  - e.g. Host2013
  - More sensitive for application processor since no real countermeasure against repeated RAM read/write, chip decapsulation…

Past initiative in secure transaction

- French funded research project with big players in the domain
  - French CB, Ingenico, Atos, Gemalto…



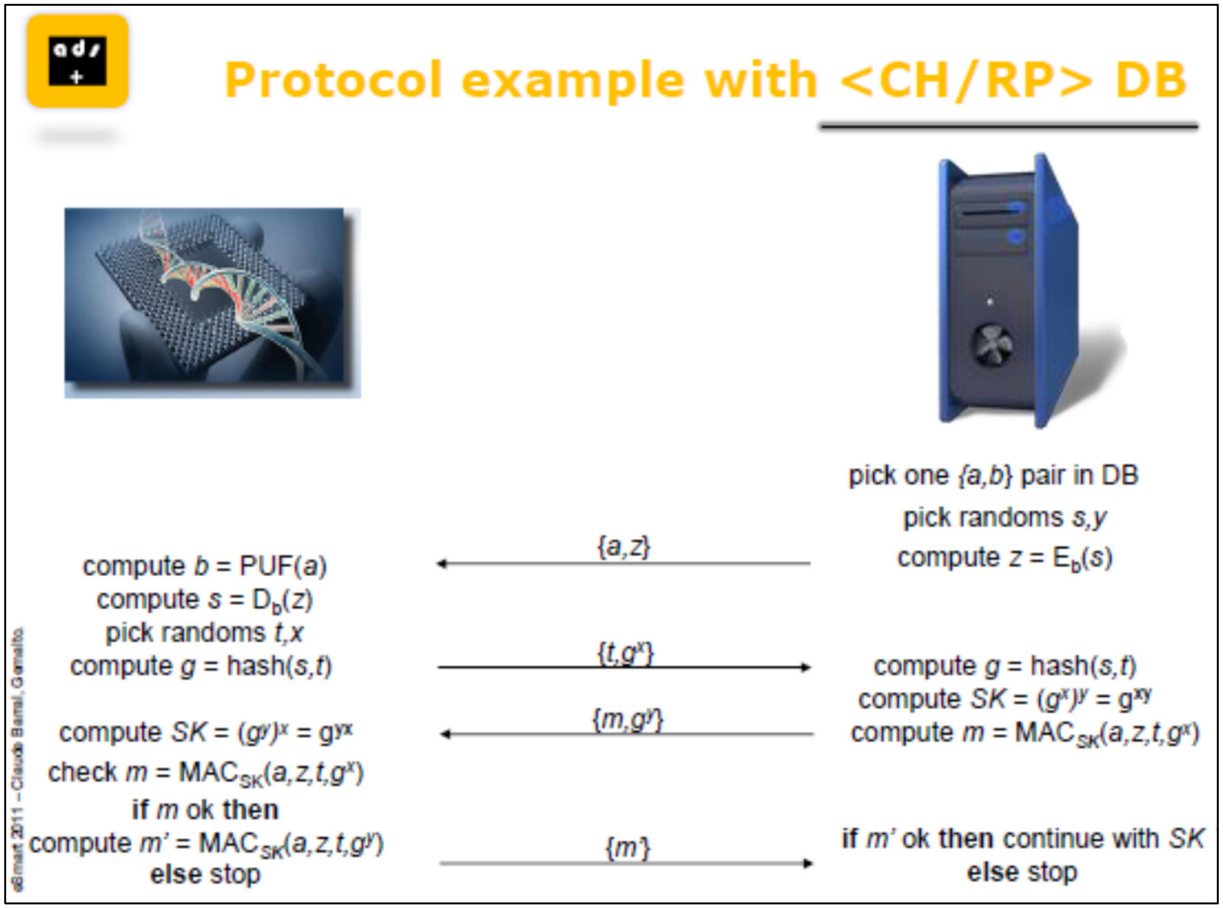
Terminal security: SAM

- **Secure Access Module**
  - Usually provides PKI anchor
  - Authentication + secure channel
- **ADS+ proposes to evaluate PUF-based device authentication (merchant terminal)**
- **PoC is to implement PUF functionality in SAM card**
- **A smart card is full of SRAM…**

eSmart 2011 – Claude Barral, Gemalto.

Credits: ADS+, eSmart2011 snapshot

Detailed Approach



Protocol example with <CH/RP> DB

pick one $\{a,b\}$ pair in DB
pick randoms s,y
compute $z = E_b(s)$

$\{a,z\}$ ←

compute $b = \mathrm{PUF}(a)$
compute $s = D_b(z)$
pick randoms t,x
compute $g = \mathrm{hash}(s,t)$

$\{t,g^x\}$ →

compute $g = \mathrm{hash}(s,t)$
compute $SK = (g^x)^y = g^{xy}$
compute $m = \mathrm{MAC}_{SK}(a,z,t,g^x)$

$\{m,g^y\}$ ←

compute $SK = (g^y)^x = g^{yx}$
check $m = \mathrm{MAC}_{SK}(a,z,t,g^x)$
if m **ok then**
compute $m' = \mathrm{MAC}_{SK}(a,z,t,g^y)$
else stop

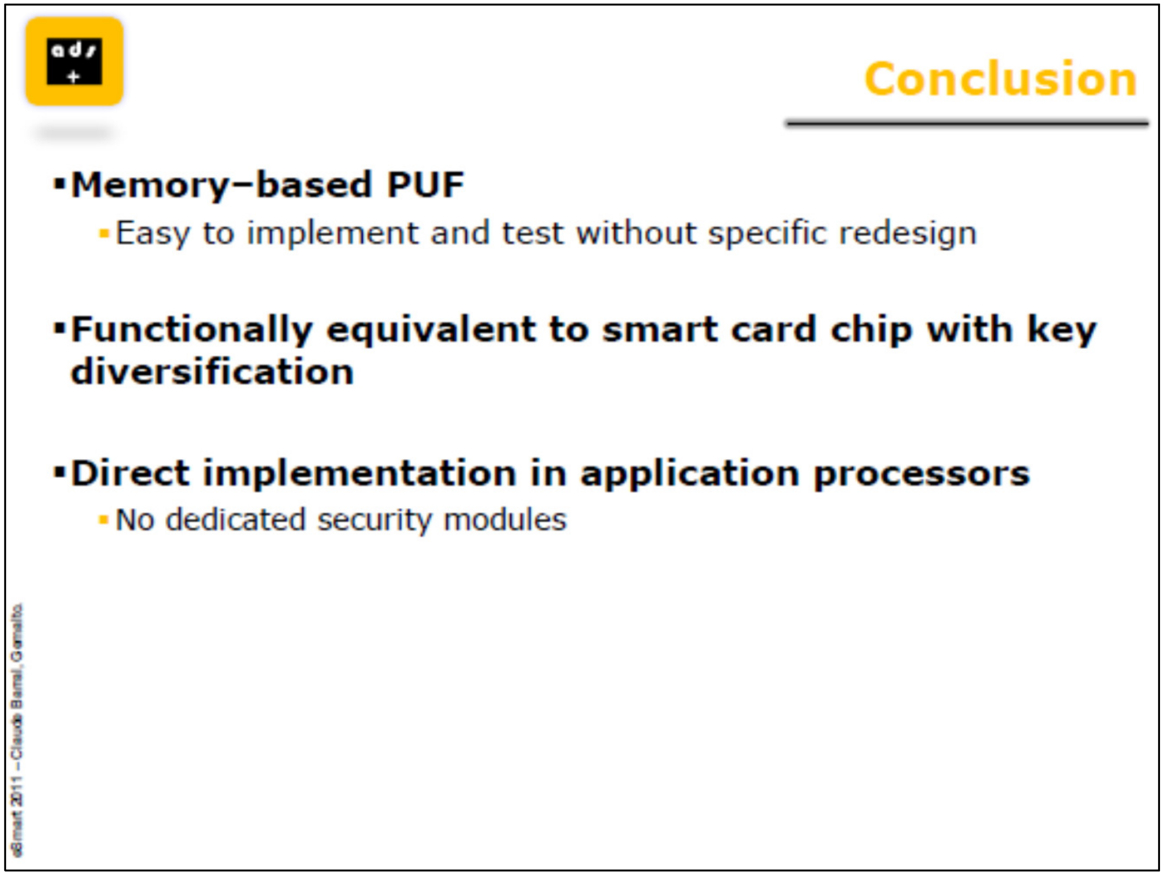
$\{m'\}$ →

if m' **ok then continue with** SK
else stop

eSmart 2011 – Claude Barral, Gemalto.

Credits: ADS+, eSmart2011 snapshot

ADS+/eSmart'2011 Conclusion



Conclusion

- **Memory–based PUF**
  - Easy to implement and test without specific redesign
- **Functionally equivalent to smart card chip with key diversification**
- **Direct implementation in application processors**
  - No dedicated security modules

eSmart 2011 – Claude Barral, Gemalto

Credits: ADS+, eSmart2011 snapshot

BAC TECH

Biometrics And Cryptography TECHnologies (made easy for you)

Conclusion

Let's dream…

- Secure PAN: Personal Area Network
  - Personal Guardian Angels
    - Network of wearable sensors for permanent health monitoring
- Beyond security of data, PUF may be used for intrinsic anti-collision techniques in RFID area
- User biometrics as a challenge for challenge/response PUF
  - Strong Human-Machine pairing
  - PUF and BCI (Brain-Computer Interfaces)
    - e.g. use unique brain signal as entry challenge for a PUF feature in the machine

Conclusion

- Very happy to see EU funded project about PUF technology for standard components
- Honored to have been short-listed as reviewing expert
  - …but disappointed being not confirmed ;-)
- PUF market is definitely not a niche in existing security products
- Cost-effective & near hassle-free implementation of a little bit of security in any electronic product
  - Complement other initiatives such as TPM, Secure elements
  - Once again, try not to compete with certified smart card chip industry and thirty-years old experience in protecting keys…

Conclusion

- Take care at non-silicon uncontrolled PUF needing silicon controller
- PUFFIN seems more research-oriented than UNIQUE
  - Smaller consortium: 3 academics, 1 start-up, no big players
  - May you need any help to evangelize your technology, please feel free to contact me
    - Chip manufacturers
    - Smart-Cards/Security solutions manufacturers
    - System integrators
    - Governmental entities
    - …

BACTECH

Biometrics And Cryptography TECHnologies (made easy for you)

Thank you

Any Questions?

EURL au capital de 15.000€
SIREN 789 985 843 - RCS Aix-en-Provence - FRANCE

www.bactech.fr

31, Parc Club du Golf - CS 90519
350, avenue Guillibert de la Lauzière
13593 - Aix-en-Provence cedex 3

claude.barral@bactech.fr