Introduction to Cryptology

Lecture-15
Identification Protocols
Physical Security

22.05.2023, v51

1

Cryptographic Identification Mechanisms/Protocols

1. Secret Key Mechanisms
2. Public Key Mechanisms

Required for every solid security system!

2

1. Secret-Key Identification Mechanisms

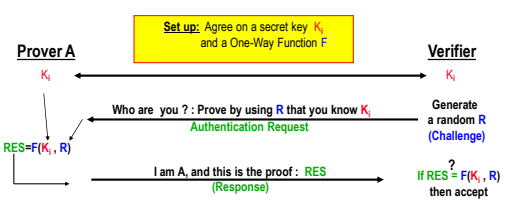
Require a secret key agreement!

3

Challenge-Response Identification Mechanisms

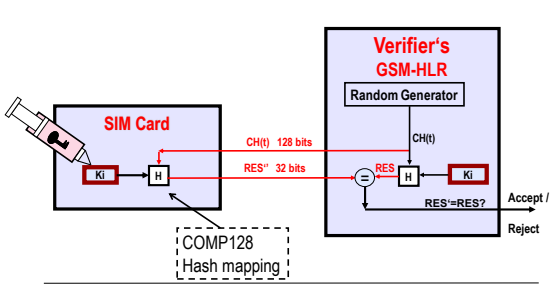
Explicit Secret Key Signature

Authenticity without Secrecy



4

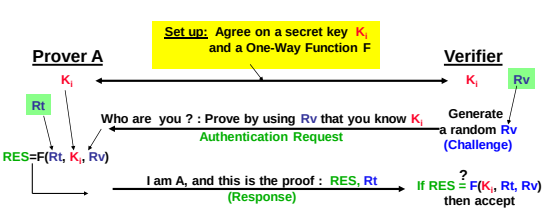
GSM Challenge-Response Identification (SIM-Card identification)



5

Improved Symmetric Challenge-Response Identification Mechanism

(Standard usage in modern network protocols)



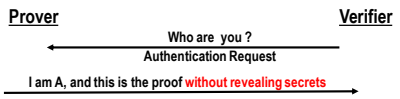
6

2. Public-Key Identification Protocols

No secret key agreement is necessary!

7

Identification Protocols/Mechanisms
Zero- Knowledge Iterative Proof (ZKIP)
Authenticity without Secrecy



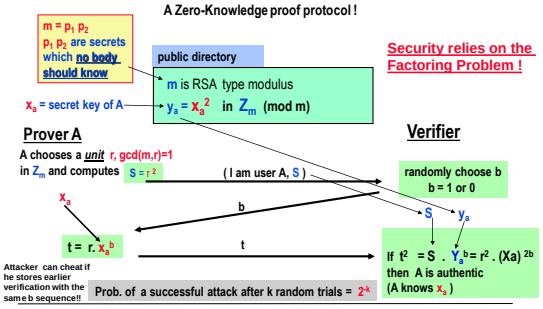
This protocol can be repeated many times for higher security !

The proof is called a **Zero-Knowledge** proof if:
Prover reveals no secrets (whatever) to the verifier !

8

Fiat-Shamir Proof-of-Identity Protocol (1986)

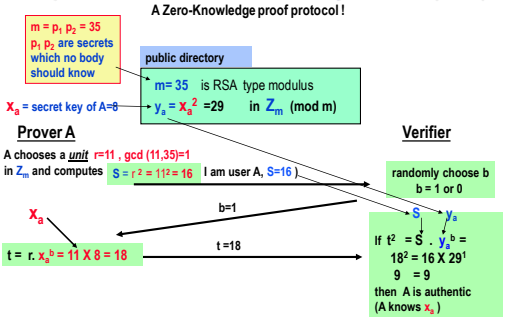
A Zero-Knowledge proof protocol !



9

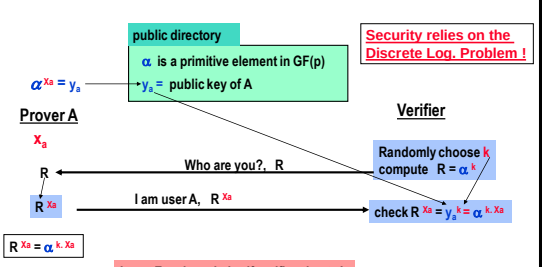
Example: Fiat-Shamir Proof-of-Identity Protocol (1986)

A Zero-Knowledge proof protocol !



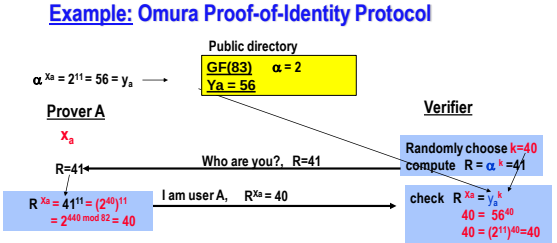
10

Omura Proof-of-Identity Protocol



11

Example: Omura Proof-of-Identity Protocol



12

Template of Schnorr's Identification/signature Scheme

Prover A

Secret key $x_A < q$

$y_A = \alpha^{x_A} \bmod p$

Open Directory (as DH public directory)

GF(p), Element **α** has order **q** such that **q** is prime which divides **p-1**

y_A: public key of signer A

verifier

User A sings a message M:

1. Random $k \in GF(q)$ $r = \alpha^k \bmod p$

A good and strong hash H function is required

2. Hash : $m = H(M \mid r)$

3. $Signature \Rightarrow$ $S = (k - x_A m) \bmod q$

Similarity to ElGamal Signature!

4. **A signed message M is : M, (S,m)**

5. $r' = \alpha^S y_A^m \bmod p$

6. $Compute\ H(M \mid r')$

7. **Verifiecation**

$if\ m = H(M \mid r')$

Then, M signed by A is authentic

Notice that $r' = \alpha^{k - x_A m}\ \alpha^{(x_A)m} = \alpha^k$

13

Physical Security

1. Why Physical Security
2. Physical Unclonability

14

Why Physical Security?
Why unclonable physical units?

- Commercial-economic reasons (Cloning)
- Identity (Privacy)
- Know-How protection (IP-Cores)
- Medical

- Automotive units

- E-Money ....
- Smart-Home, -City, -Gouvernement, Consumer, IoT ..

15

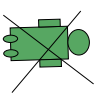
Popular Attack Scenarios
Physical Replacement/Substitution Attack

Customer

Intruder

False Unit

Legal Unit

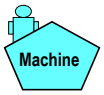


Examples: - False mobile base station attack (GSM Mobile system)
- False Internet host

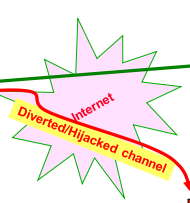
16

Popular Attack Scenarios
Tele-service attack: Channel Hijacking Attack

Customer



Machine

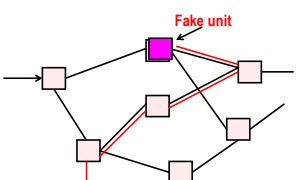


Legal Service Access

False Access

17

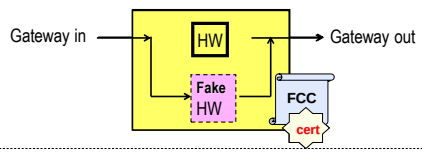
Popular Attack Scenarios
Network unit replacement attack



18

Popular Attack Scenarios
Replacement Attack- Hardware patch

- Manufacturer cheats!
- Attacker has successfully cloned the unit!



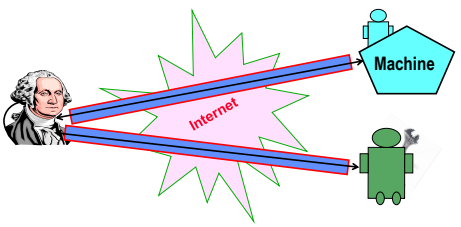
Requirements
1. Unit structure should be unclonable or clone-resistant!
2. Unit should be unchangeable "Tamper-Proof"!

Page : 19

19

Two Basic Requirements for Solid Security

1. Identify and trust each other (Mutual-Authentication)
2. Establish a secured link (secrecy)



Page : 20

20

Contemporary State of the Art

- Identify & Trust (Authentication) Physical Security
  - Physical uniqueness !! ?
  - Unclonable units !! ?
  - Electro-Mechanical identity (Mechatronic-Identity) !!?
    (Automobile, Production Machines, Robots ….)

- Secured link (secrecy)
  Relatively mature technology

Page : 21

21

State of the Art for basically clonable Physical Units

Page : 22

22

Practical GSM Security Gaps

International Mobile Equipment Identity
IMEI (non-secured)

Subscriber Identity Module
SIM (secured)

A5 Cipher
Broken 1999

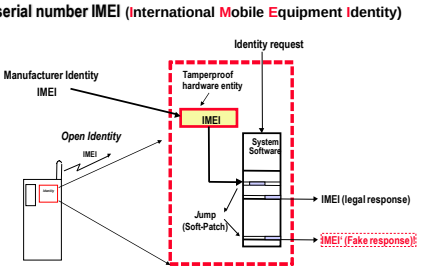
Cloned for some standard function
(150 000 challenges. Berkeley Univ.)
No collapse. System still solid!

Page : 23

23

Attack on GSM device Identity IMEI

Mobile serial number IMEI (International Mobile Equipment Identity)

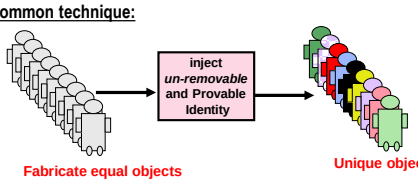


Page : 24

24

Physically Unique Units Production

Common technique:

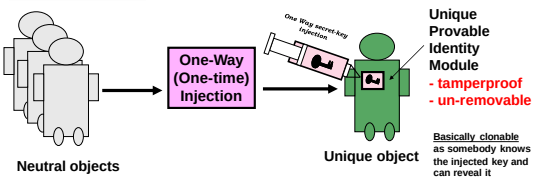


Page : 25

25

Personalizing Physical Entities : One-Way Injection

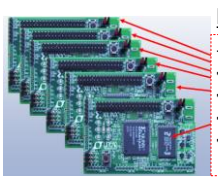
Mechanical simulation



Page : 26

26

Requirements on Physical Uniqueness in Production



Personalization requirements:

- Uniqueness
- Unclonable, Clone-Resistant
- Remotely and securely Identifiable
- Low cost
- Resilient security if cloned!
  (brake-one brake-all impossible!)

Page : 27

27

State of the Art in Unclonable Physical Units

DNA-like
Physically Unclonable Functions
(PUF's)

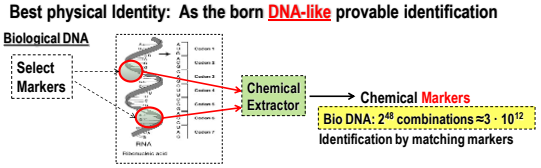
Bio-Inspired Provable Physical Identity
Make use of born uniqueness properties (DNA like)

Page : 28

28

Best physical Identity: As the born DNA-like provable identification

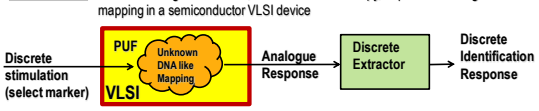
Biological DNA



Physical Unclonable Functions PUFs offer DNA like Identification Techniques

Ideal PUFs are: Born unpredictable and unclonable physical VLSI properties.

In other words: PUFs are analogue non-linear, hard to model or to copy, unpredictable huge mapping in a semiconductor VLSI device



Page : 29

29

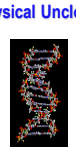
State of the Art: Unclonable Devices by:

Analog Physical Unclonable Functions (PUFs)

Since 2000 many proposals

optical PUF
coating PUF
Silicon PUF
optical fiber PUF
RF COA
LC-PUF
S-RAM PUF
Arbiter PUF
fluorescent PUF

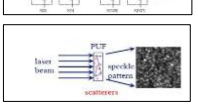
So far all have "Reproducibility" problems! Analog functions!!!



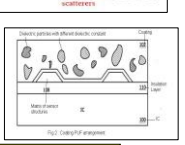
Unclonable
DNA-Chain

Delay PUF
Butterfly PUF
diode breakdown PUF
reconfigurable PUF
acoustic PUF
controlled PUF
phonchon PUF
...

Delay based



Optical



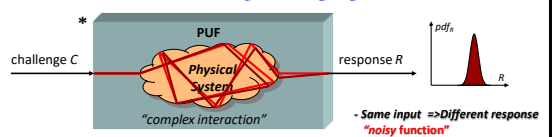
Coating PUF
(Capacity)

Born properties: Similar to the biological DNA

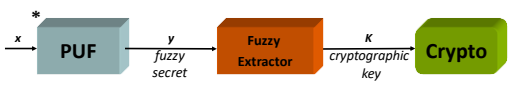
Page : 30

30

PUFs inconsistency and aging difficulties



Bad reproducibility due to : Operating conditions, quantization (Metastability), Aging, ...



Fuzzy Extractors: Complex, Costly (Sign. Proc + ECC)

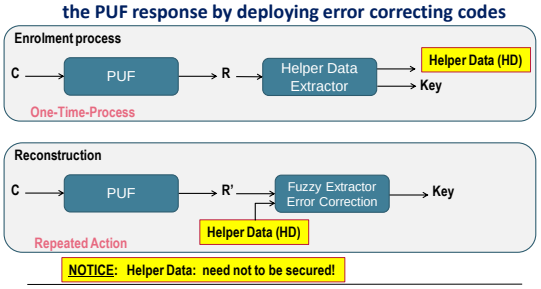
* Source: Roel Maes, ESAT/COSIC, K.U.Leuven, BCRYPT Workshop:

Page : 31

31

Fuzzy Extractor for (PUFs)

- **Fuzzy Extractor:** is used to correct errors in reproducing the PUF response by deploying error correcting codes



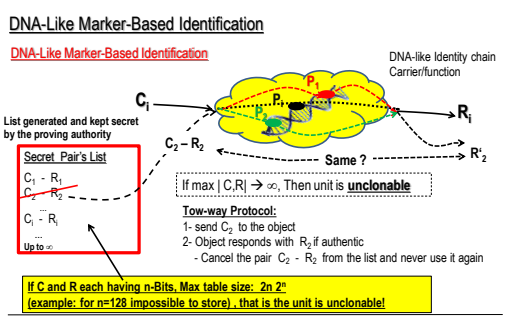
NOTICE: Helper Data: need not to be secured!

Page : 32

32

Bio-Inspired Identification Protocol

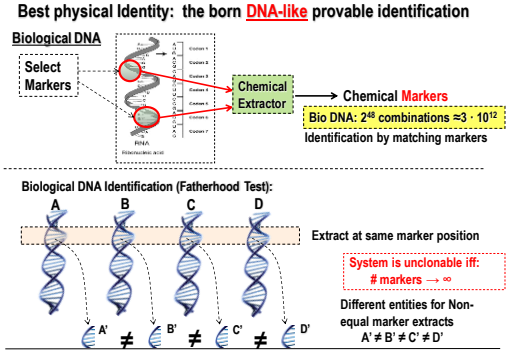
DNA-Like Marker-Based Identification



Page : 33

33

Best physical Identity: the born DNA-like provable identification



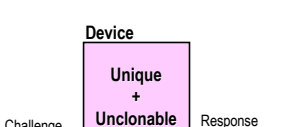
Page : 34

34

Selected Proposed Physical Unclonable Functions PUFs

Few promissing PUF´s

- Silicon PUF
- Intrinsic PUF
- Optical PUF
- Coating PUF



Identification module (Function)

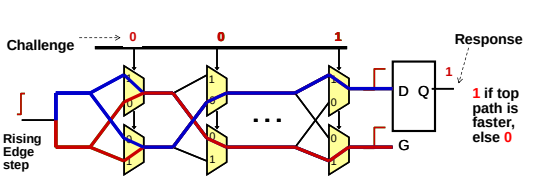
Identification by checking challenge-response behavior Like DNA

Page : 35

35

Silicon PUF
MUX Chain or Arbiter PUFs

Principle: Compare delay time in a chain.
Each physical chips exhibits own different delay time behaviour which identifies it



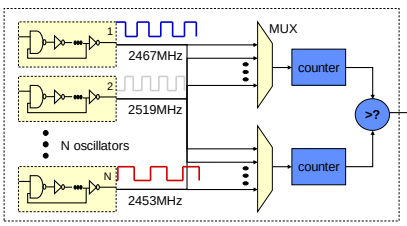
Source [8]

1.

Page : 36

36

Silicon PUF
Ring Oscillator Design Procedure



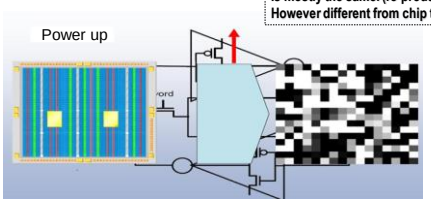
Compare frequencies of two oscillators. The faster oscillator is randomly determined by manufacturing variations

Page : 37

37

Intrinsic PUF(I-PUF)
S-RAM PUF

S-RAM initial state after power on
Is mostly the same. (re-production !!)
However different from chip to chip



Source [8]

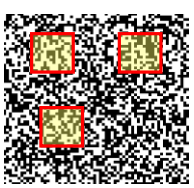
5.

Page : 38

38

Intrinsic PUF(I-PUF)
SRAM PUF : Intra-Chip Variation

Principle: Read some memory area to identify physical units
S-RAM initial state after power on is mostly the same. (re-production !!)
However different from chip to chip



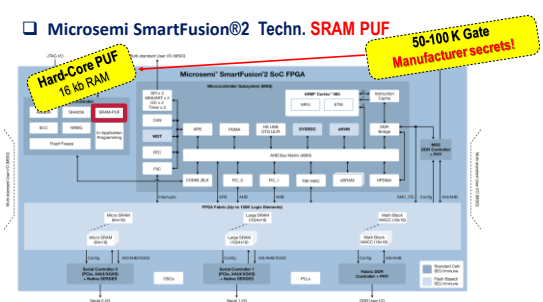
Source [8]

Page : 39

39

Real-Field SRAM PUF in the Market

- Microsemi SmartFusion®2 Techn. SRAM PUF



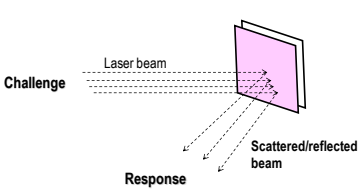
- Xilinx FPGA: SRAM PUF many IP-Cores … SRAM, Delay-based, …

Page : 40

40

Optical PUF

Principle: Difference in reflected and refracted ray of light on a surface



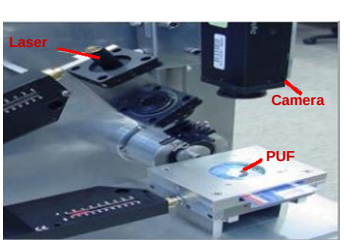
Source [8]

3.

Page : 41

41

Optical PUF
Practical set-up relatively complex

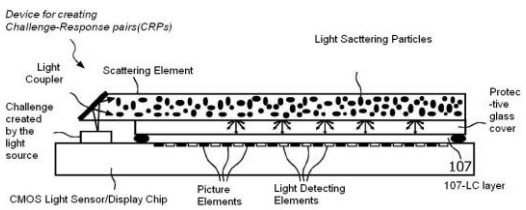


Source [8]

Page : 42

42

Optical PUF
Possible Integrated PUF



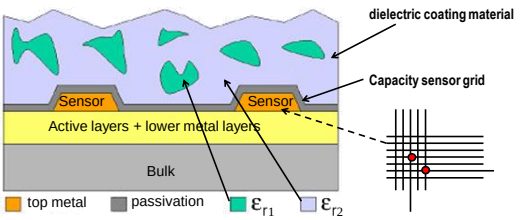
Source [8]

Page : 43

43

Coating PUF

Principle: Different capacity sensed at by different sensors

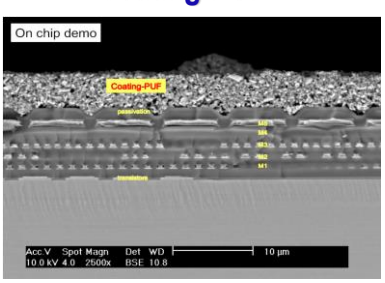


Source [8]

Page : 44

44

Coating PUF



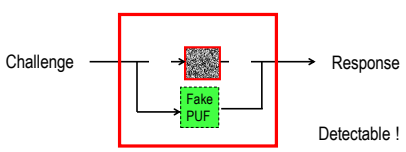
Source [8]

Page : 45

45

Possible attacks on PUFs

- Manufacturer cheats!



1. Manufacturer has to be trustable!
2. Tamper-Proof technology is required!

7.

Page : 46

46

All Analog PUFs are however,

1. Still complex and costly to produce
2. Sensitive to temperature and supply voltage etc.
3. Have long-term reproducibility "Aging" issues ! (non-Consistent in the long term!)

Still relatively limited for real field use!

7.

Page : 47

47