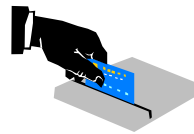




INSTITUTO  
SUPERIOR  
TÉCNICO



# Trusted Computing in Reconfigurable Systems





- Trusted computing
  - Trusted Computing Group
  - Introduction to Cryptography
    - ◆ History
    - ◆ Most used algorithms
  
- Implemented cores
  - AES implementation
  - SHA-1 implementation
  - Polymorphic implementation
  - Results
  
- Future work





INSTITUTO  
SUPERIOR  
TÉCNICO



# Trusted Computing in Reconfigurable Systems

## Trusted Computing Group

Group formed to create a new standard for trusted computing, in order to build more reliable computational systems.

Several features have been proposed:

- Secure I/O
- Memory curtain
- Sealed Storage
- Remote attestation





INSTITUTO  
SUPERIOR  
TÉCNICO



# Trusted Computing in Reconfigurable Systems

## Trusted Computing Group

### ➤ Secure I/O:

- The data coming to or from the I/O devices validated via checksum, to guarantee that the software has not been tampered with.

### ➤ Memory Curtaining:

- Only the software application with the appropriate key is able to access a given memory region

### ➤ Sealed Storage:

- The data is stored in memory encrypted.

### ➤ Remote attestation

- Each application has its own digital signature to ensure its identity when communicating with other applications.





## Trusted Computing Group

Drawbacks of the Trusted Computing Module:

- Lack of adaptability to new encryption algorithms
- Unknown knowledge of the internal design

Advantages of a reconfigurable approach :

- New algorithms and new features can be added with no cost
- Adaptable to different systems characteristics





INSTITUTO SUPERIOR TÉCNICO



# Trusted Computing in Reconfigurable Systems

## Cryptography - History and Usage

1900 BC is the 1<sup>st</sup> known usage of cryptography by the Egyptians – simple substitution scheme



Hieroglyphic encipherments of proper names and titles, with cipher hieroglyphs at left, plain equivalents at right.

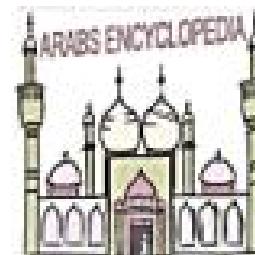
500 BC a new mathematical cryptographic scheme was used by Sun Tzu (a military strategist)

$$CRT(2,3,2)_{(357)} = ?? (23)$$

1 AD Julius Cesar used the simple letter shift cipher in the *Gallic Wars*

Msg: OMNIA GALLIA EST DIVISA IN PARTES TRES  
Enc: RPQLD JDOOLD HWV GLYLVD LQ SDUWHV WUHV

1412 AD an 14vol encyclopedia on Cryptanalysis is compiled by the Arabs



In the 2nd world war the enigma rotor machine is used (substitution scheme using a continuously changing alphabet)





INSTITUTO  
SUPERIOR  
TÉCNICO



# Trusted Computing in Reconfigurable Systems

## Cryptography - History and Usage

**In the 70's** with the development of complex electronic systems much more complex cryptographic systems have been created, such as Lucifer and DES.

**nowadays** a variety of cryptographic algorithms exist and they are present in almost every day actions:

- Accessing the internet
- E-shopping
- ATM machines
- Emails
- Buildings and public transportation access
- Pay TV
- Anti-car theft systems
- Private communications
- ...





INSTITUTO  
SUPERIOR  
TÉCNICO



# Trusted Computing in Reconfigurable Systems

## Cryptographic Systems

### ➤ Asymmetrical Encryption Algorithms

- Used mostly on to exchange private keys for the symmetrical algorithms
- There are two key: public key shared with every one else  
private Key kept private by the “receiver”
- Based on mathematical unresolved problems
- High computational requirements

### ➤ Symmetrical Encryption Algorithms

- Used to encrypt large blocks of data
- Only one key exists, that has to be kept secret between the users
- Lower computational requirements

### ➤ Hash functions

- Used to compact large blocks of data into a correlated small data block
- No keys are used
- Low computational requirements

### ➤ Digital Signature algorithms

- Used to guarantee the ownership of an data block (authentication)
- Based on asymmetric encryption algorithms





## Asymmetrical Encryption Algorithms

Most commonly used public algorithms are:

### ➤ RSA

- Key size = 512 to 2048 (1024)
- PK=(d,n) ; pK=(e,n)
- $p$  and  $q$  are prime numbers
- RSA has been up till now the most used asymmetric key algorithm (SSH, PGP)

$$e() = c = x^e \bmod n$$

$$d() = x = c^d \bmod n$$

$$\phi(n) = (p-1) \times (q-1)$$

$$n = p \times q$$

### ➤ ElGamal

- Security lays on the discrete logarithmic problem
- PK=(p,a) ; pK=(p,α,β)
- $p$  is a prime number
- Starting to have a wide use especially

$$e() = \begin{cases} y_1 = \alpha^k \bmod p \\ y_2 = (x\beta^k) \bmod p \end{cases}$$

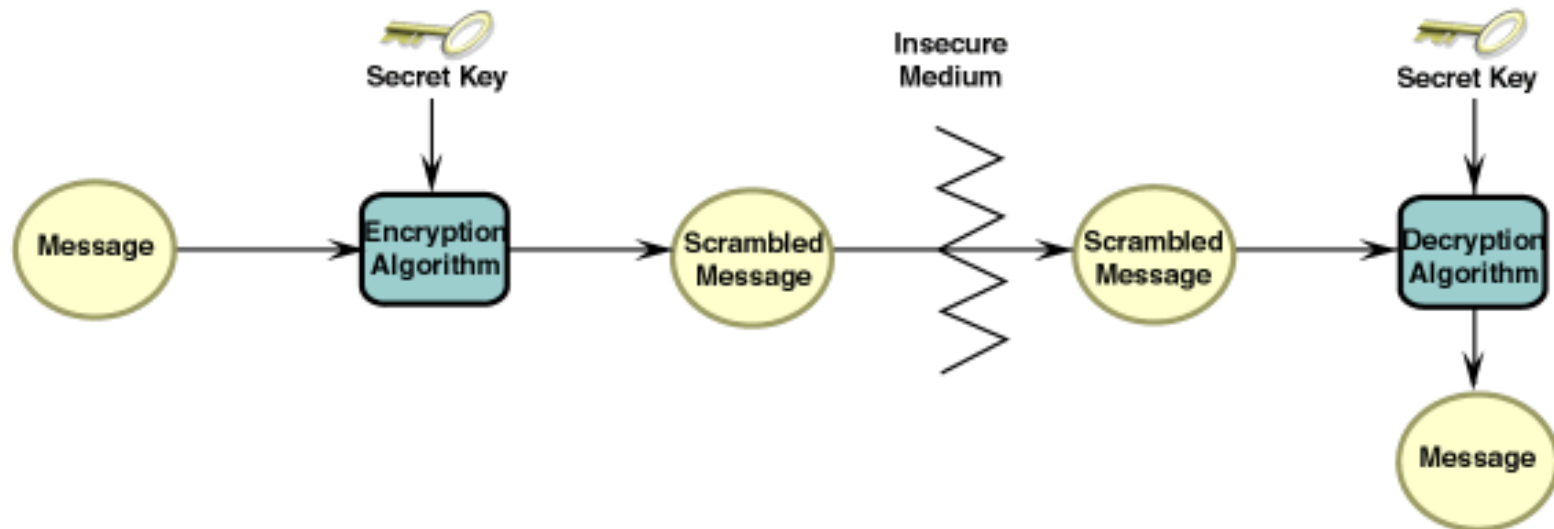
$$d() = (y_2 (y_1^a)^{-1}) \bmod p$$

$$\beta = \alpha^a \bmod p$$



## Symmetrical Encryption Algorithms

- These algorithms are used to encrypt the bulk of data (from a few bytes to several Giga bytes).
- The same key is used to encrypt and decrypt the message (symmetrical).
- Since only one key exists, it has to be kept private between the users
- Encryption/Decryption rates on a 30 MIPS machine:
  - 3DES - 49 Kbytes/s
  - AES - 232 Kbytes/s



## DES and 3DES

➤ DES (Data Encryption Standard) was one of the most used private key algorithms used.

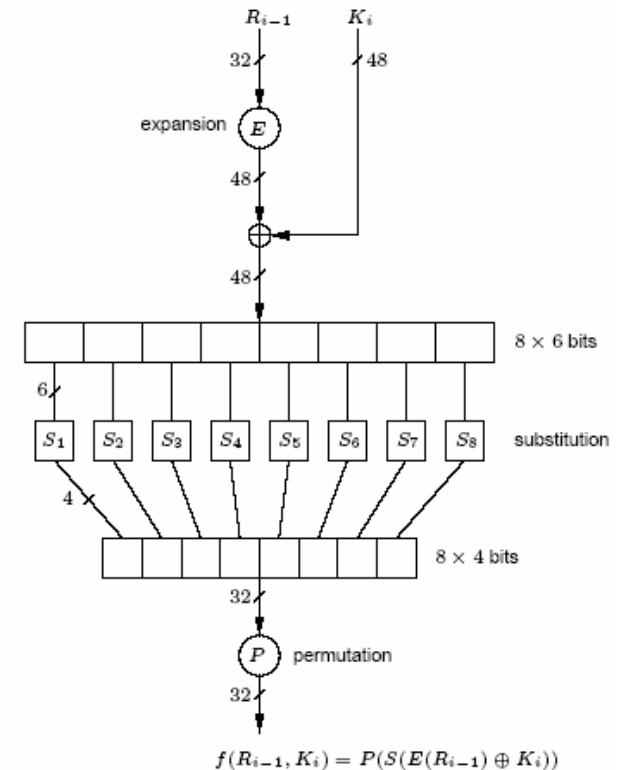
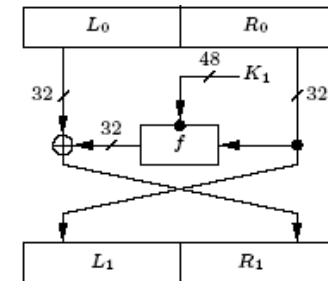
➤ Its main characteristics are:

- 256 bytes for the 8 S-boxes
- Uses fixed permutation networks
- 16 rounds
- 54-bit key
- 64-bit data blocks

➤ Currently the 3DES algorithm is used.

➤ 3DES simply repeats the DES algorithm 3 time, with a 108-bit or a 162-bit key.

➤ 3DES is fully compatible with DES





## Hash functions

### ➤ Hash function

- Hash functions are used to create a small data block, that is dependent of all the sent plaintext.
- In these algorithms a modification on the plaintext, will most likely produce a different result on the hash function result.
- The original plain text can not be retrieved from the hash result
- No key is used
- Reduced complexity
- Most common algorithms are: MD2, MD4, MD5, SHA-1
- High throughputs

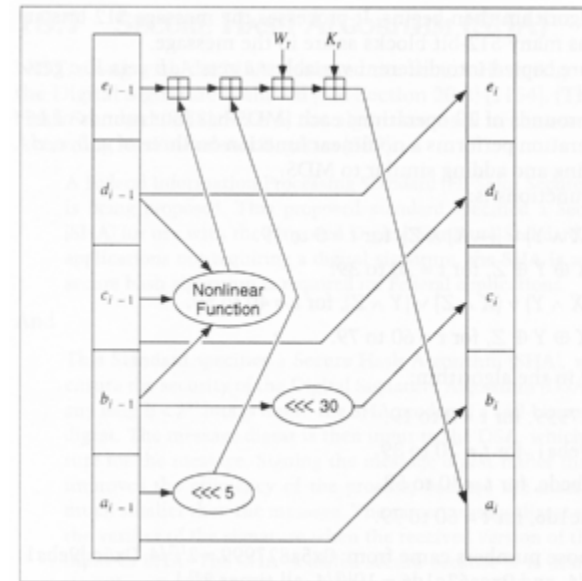


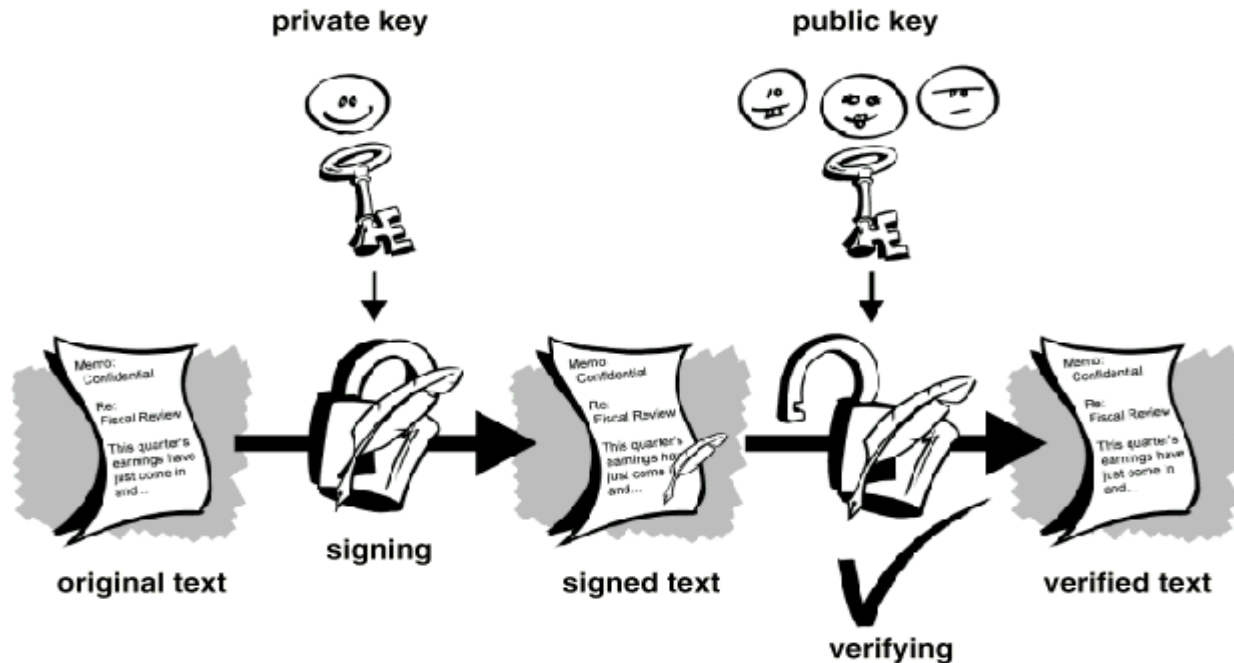
Figure 18.7 One SHA operation.

Example of one round of the SHA hash function.

- The Nonlinear functions are usually bitwise operations (OR, AND, XOR)
- Throughputs @ 30 MIPS:
  - MD5 - 656 Kbytes/s
  - SHA - 423 Kbytes/s

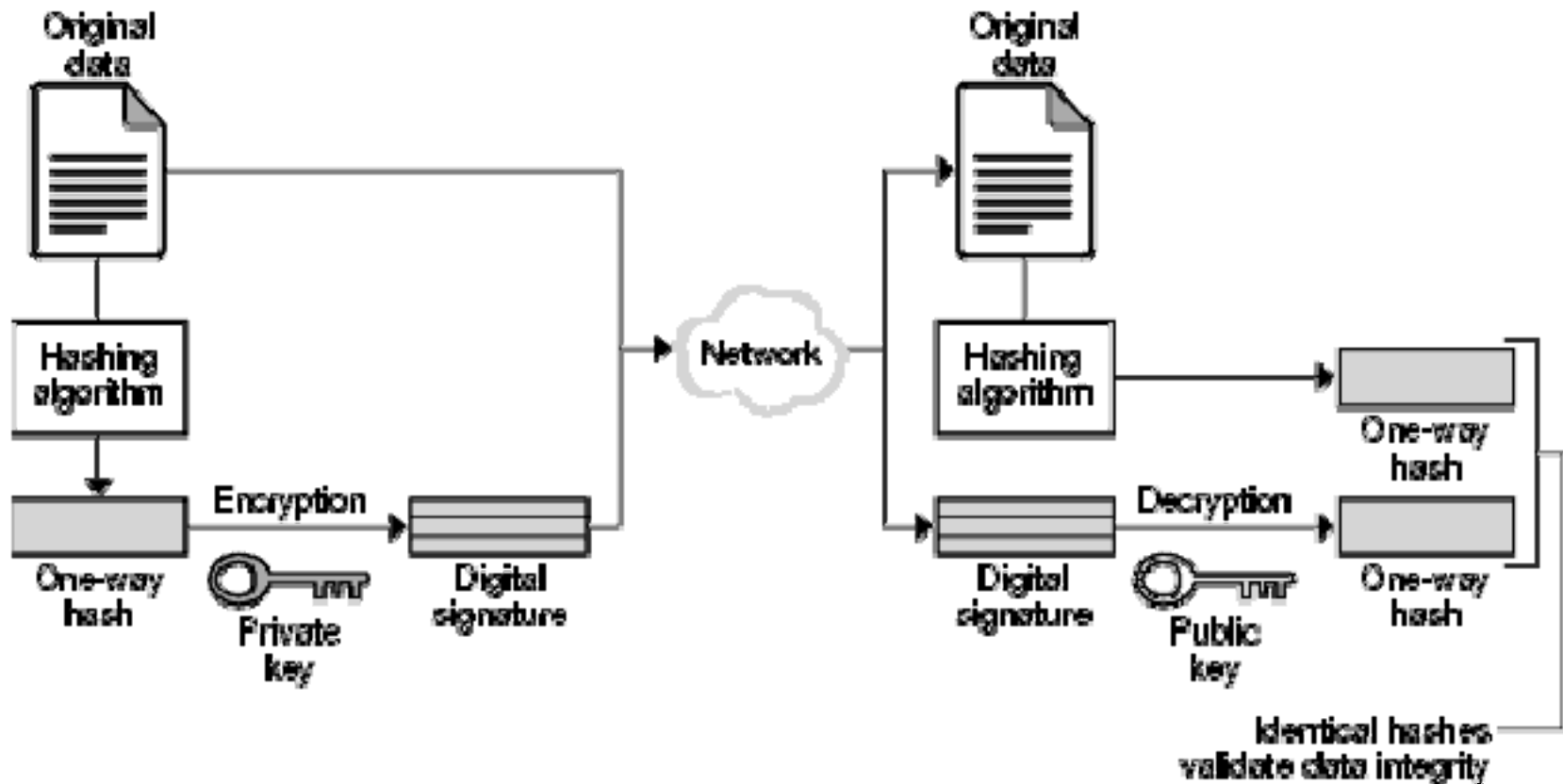
## Digital signatures

- Digital signatures are used to authenticate and to validate the ownership of a digital document.
- Private key algorithms are used, or based on. (computational demanding)
  - RSA, ElGamal, DSA (similar to the ElGamal Algorithm)



## Combining algorithms

- Digitally signing the all document, would be inefficient and could originate attacks to separate parts of the document.
- The *hashed* document is usually 128 to 160 bit long.





INSTITUTO  
SUPERIOR  
TÉCNICO



# Trusted Computing in Reconfigurable Systems

## AES Results

High efficiency gains to existing state-of-the-art

Higher Throughput/Slice ratio

- ◆ 200% for the folded loop AES core
- ◆ 560% for the unfolded loop AES core

36% faster than the known exiting AES cores: 34 Gbits/s

68% less reconfigurable logic

Half the output latency (for the loop unfolded AES core)

MOLEN implementation

Low FPGA utilization: 10% of a Virtex II Pro 20

High throughput: 1.2 Gbits/s

AES encryption speedup of 751 times

Minimal software integration costs





INSTITUTO  
SUPERIOR  
TÉCNICO



# Trusted Computing in Reconfigurable Systems

## SHA-1 Results

High efficiency gains to existing state-of-the-art

Higher Throughput/Slice ratio

- ◆ 29% better than the most efficient commercial core
- ◆ 59% better than the most recent academia related art

18% faster with less 5% area than the equivalent top commercial SHA-1 core  
1.4 Gbits with only 596 Slices

Permits for variable initialization vectors, i.e. can be used in HMAC protocols

MOLEN implementation

Low FPGA utilization: 4% of a Virtex II Pro 30

High throughput: 624 Mbits/s

SHA-1 encryption speedup of 155 times

Minimal software integration costs





INSTITUTO  
SUPERIOR  
TÉCNICO



# Trusted Computing in Reconfigurable Systems

## Polymorphic implementation MOLEN with an AES CCU

### Main characteristics:

Low FPGA utilization.

*10 % of a XCV2P20 for the AES CCU*

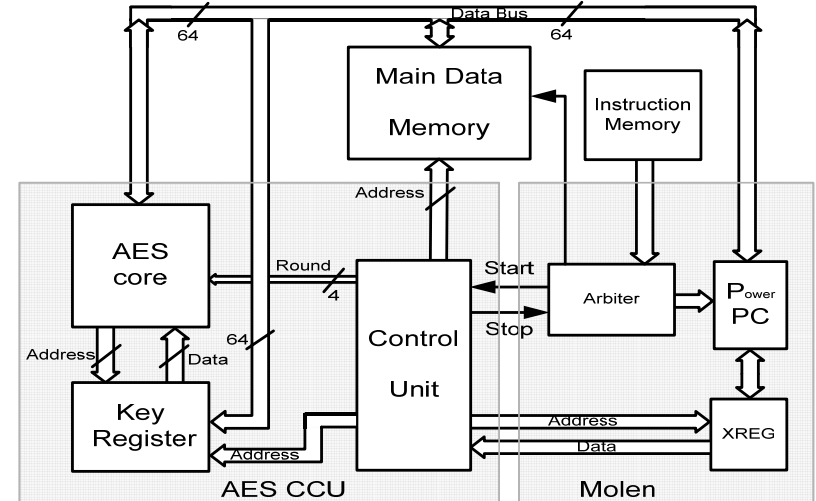
*5 % of a XCV2P30 for the SHA-1CCU*

Throughput of *1.2Gbits/s* for AES

Can be used in the 1 Gbits/s Ethernet network and applications.

Minimal software integration costs

A large range of encryption applications can be speedup just by being recompiled for the MOLEN processor with the AES core.





## AES core in the MOLEN processor

### Minimal Software integration costs:

#### *Original Software:*

Declaration: `void rijndaelEncryptData(){ instructions... }`

Usage : `rijndaelEncryptData(rounds,keys, data, mode);`

#### *Modified for MOLEN:*

Declaration: `#pragma call_fpga encrypt`

`void rijndaelEncryptData(){ /*implemented in Hardware*/ }`

Usage : `rijndaelEncryptData(rounds,keys, data, mode);`

### Significant Speedup for a minimal area cost:

- **10 % occupation** of a Virtex II Pro FPGA
- Encryption of a 128kbit file in **104 ns** (in MOLEN) instead of **78 ms** (in Software), **751 times Speedup**.





INSTITUTO  
SUPERIOR  
TÉCNICO



# Trusted Computing in Reconfigurable Systems

## Future work

- Improve the implementation of the most likely to be used in the future encryption algorithms.
- Improve the asymmetrical encryption algorithms, like RSA and its implementations in reconfigurable technology.
- Study efficient ways of implementing and integrating the memory curtaining into the existing systems.
- Explore how to adapt and efficiently use the Trusted Computing protocol in soft-cores and polymorphic computational approaches.
- Efficient implementation in multi-core systems
  - ◆ specially the memory curtaining mechanism with distributed memory systems
- Minimize the performance degradation due to the use of these additional security features.

