SECRICOM
Seamless Communication for Crisis Management

SECURE DOCKING STATION AND ITS PROTECTION AGAINST HARDWARE ATTACKS

26th April 2012

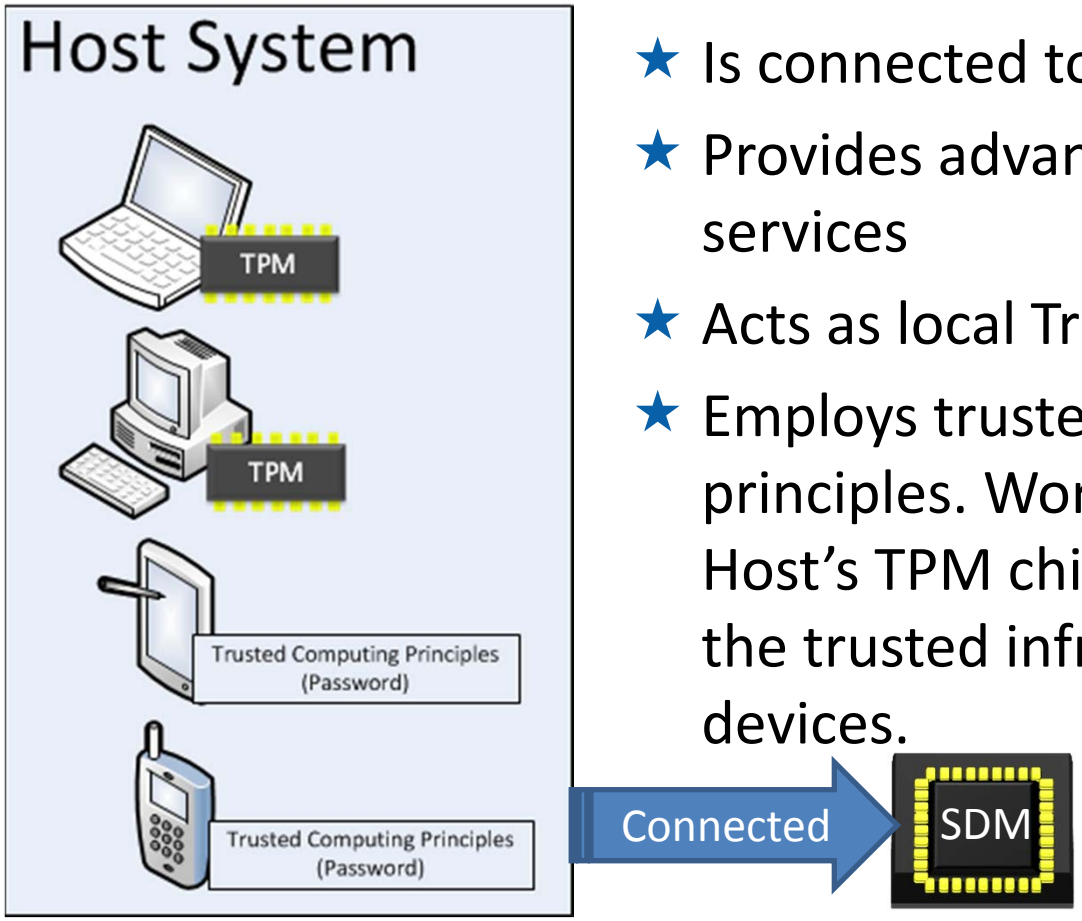
Overview

- ★ Motivation
- ★ SDM concept and objectives
- ★ SDM Hardware structure
- ★ SDM Hardware attacks
- ★ SDM AES attack countermeasures
- ★ SDM RSA crypto core Basic concept and attack countermeasures

Motivation

- How to offer strong security and trust in crisis management environments?
- Secure communication between emergency responders
- The emergency responders must be able to trust each other as well as trust their communication devices (regardless how different they might be).
- In crisis situations, agencies act under hostile, unsecure communication environments where communication can be interrupted or disturbed.
- Trusted Computing Group solutions (like TPM) are not adequate, since they require a reliable communication channel. Trust attestation services must be provided locally on agency devices and not remotely.
- Our goal: to provide to the user a local trust attestation device.

Secure Docking Module (SDM) Concept



The SDM:

- ★ is a hardware “smart card” like device
- ★ Is connected to a Host Machine
- ★ Provides advanced security and trust services
- ★ Acts as local Trusted third party.
- ★ Employs trusted computing principles. Works in cooperation with Host’s TPM chip (when available) or the trusted infrastructure of mobile devices.

Secure Docking Module Objectives

- **Development of the Secure Docking Module (SDM),**
  - Is a specialized security chip
  - Provides secure storage of trust measurements and credentials (keys)
  - Allows mobile agents to dock on to secure communication infrastructure
  - Ensures the trusted state of host device
  - Protected against Hardware malicious attacks
- **Secure Docking Module Purpose**
  - Validates the local software integrity of a Host platform through trust measurements.
  - Provides sufficient proof that the measurements are authentic, fresh and untampered
  - Binds a person and not only a device to the crisis communication system
  - Ease of use to an emergency scenario
  - Small overhead to the needed infrastructure for achieving strong security

SDM Hardware Attacks

- Traditional cryptanalysis Attacks fail for high bit length keys (RSA: 1024-2048 bit keys, AES: 128 bit keys)
- Semi invasive and Non invasive hardware attacks are easily mounted on unprotected Hardware and can compromise the system
  - ***Non invasive (Side channel attacks(SCA))***: successful in determining crypto keys using information leaking from a straightforward Hardware implementation of the algorithm (power, electromagnetic dissipation, timing e.t.c.)
    - ***Power Attack (PA):*** a hardware device's power trace is measured and exploited for secret information leakage either statically (Simple PA) or statistically (Differential PA)
  - ***Semi-Invasive (Fault Attack (FA))***: disturb a hardware device during cryptographic operation execution, analyze the faulty behavior of the disturbed device and as a result deduce sensitive information
    - ***Differential Fault attack (DFA):*** correlating the results of a correct algorithm execution with the results of a faulty execution…collecting enough measurements can reveal the key.

Low level SDM commands

★ **Memory store – save related operations**

- Store Hostnonce
- Store
- Store
- Store
- Store
- Store
- Store
- Store
- Store
- Store
- Store
- Store
- Store
- Save
- Save
- Save

VERIFY_CONFIG_AUTH

- •AES encrypt - decrypt
- •*Store HostID*
- •*Store KeyID*
- •*Store TPM quote*
- •*Store TPM quote signature*
- •*Store AuthToken*
- •*Find HostID*
- •*Find KeyID*
- •*Verify Authentication Token*
- •*Verify signature*
- •*Verify nonce*
- •*id platform config*

tion operations

erify SDMnonce
erify nonce
erify Auth Token
erify valid platform config.
erify Admin valid platform
nfig
erify Empty SDM

AES
Encryption-Decryption

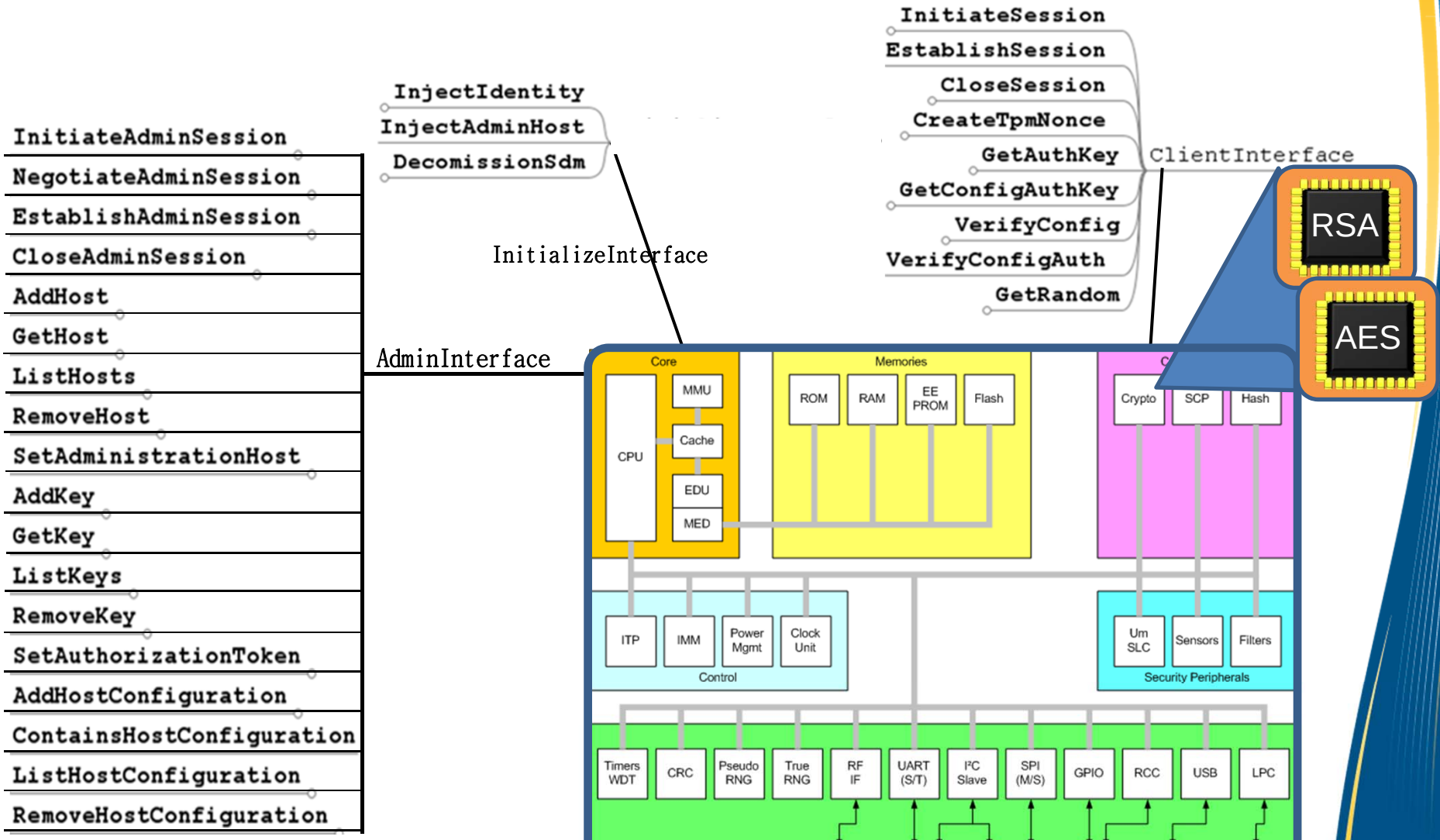
RSA
Encryption-Decryption

Hardware Attack Resistant

SDM Hardware unit related operations

- •Generate Random Number
- •Generate SHA-1 Hash value
- •Verify signature
- •Exponentiate (encrypt and decrypt)
- •Derive AES session key
- •AES encrypt – decrypt
- •Transmit Data

SDM concept – Hardware structure



SDM Architecture

AES Accelerator Countermeasures

- DFA protection:
  - Detection through spatial duplication
  - Detect errors and react to them:
    - Return a constant value or
    - Return a random value
  - Detection through spatial duplication
    - To instances of the algorithm are implemented, working in parallel thus detecting the existence of faults.
    - Blur erroneous ciphertext with scrambled values of detected error
- SCA protection:
  - Two instances of the algorithm are designed:
    - One instance computes a bit of each intermediate value
    - the other instances computes the complement bit of each intermediate value.
    - Provides constant hardware leakage characteristics (power dissipation, electromagnetic emission e.t.c)

M.Doulcier-Verdier, J-M. Dutertre, J. Fournier, J-B. Rigaud, B. Robisson & A. Tria, ***« A side-channel and fault attacks resistant AES cicuit working on duplicated complemented values »*** *in proc. of IEEE International Conference on Solid State circuits 'ISSCC 2011'.*

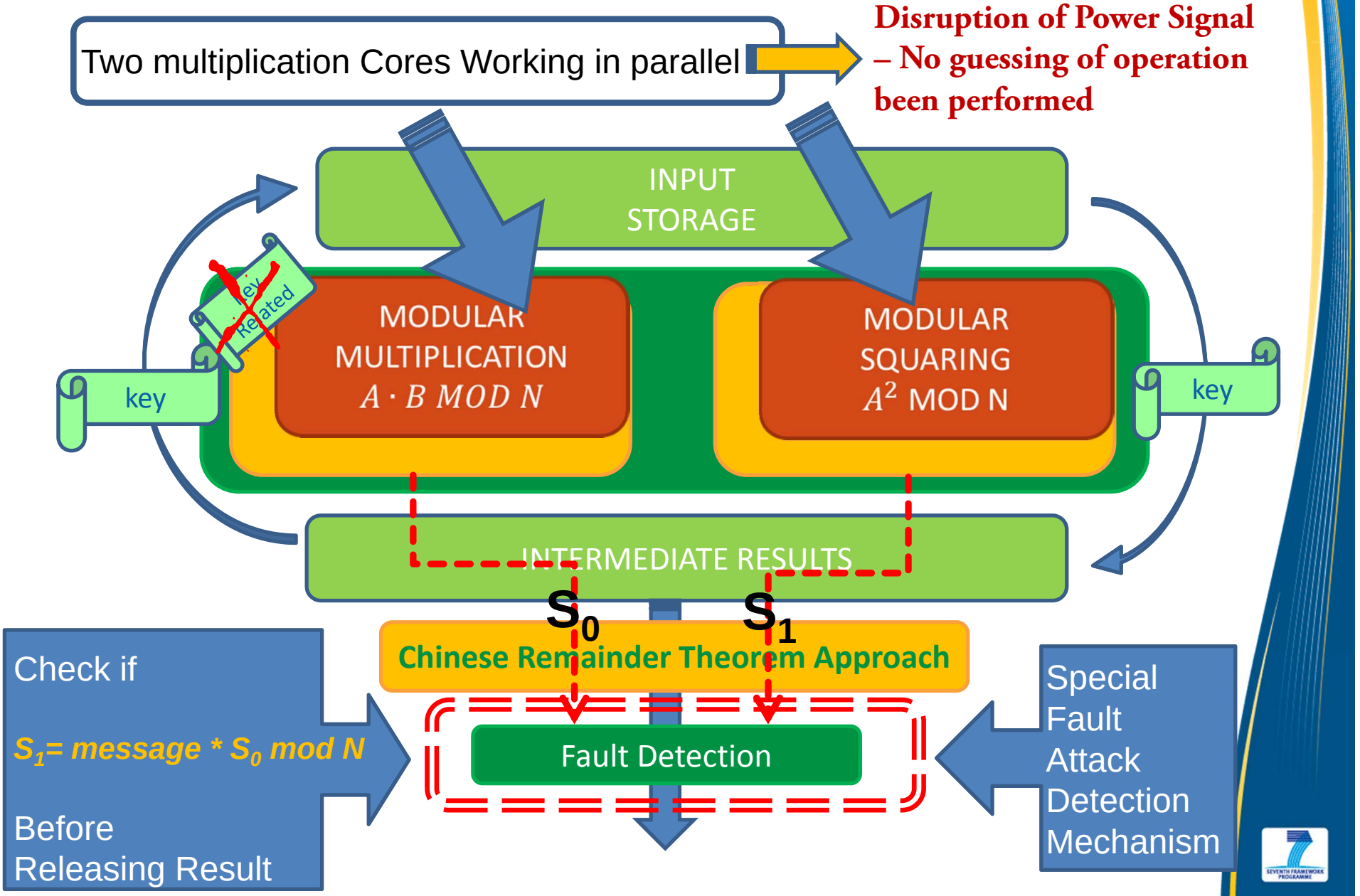
RSA Specifications

- ★ More than Reasonable speed
- ★ Support for the SDM functionality (expandable to the SDM key lengths)
- ★ Capable for encryption and decryption
- ★ Strongly protected against popular and disruptive Hardware attacks (Side Channel Attacks and Fault attacks)

RSA Protection Mechanism

- ★The SDM chip must be protected against simple and sophisticated Hardware attacks
- ★The Side channel attack countermeasures must be up to date and can be adapted for continuous protection against possible future attacks

The RSA core basic concept -protection support

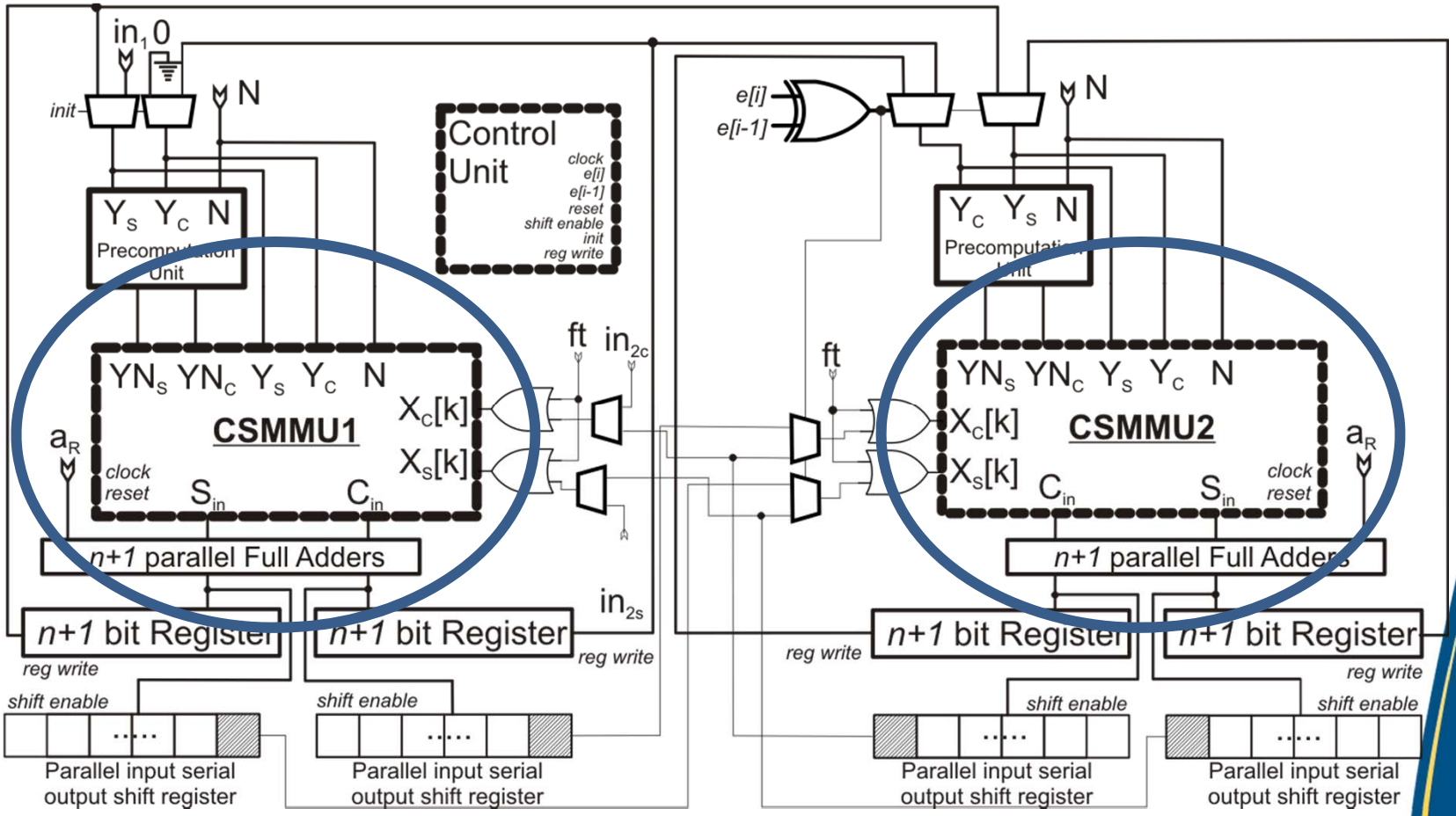


RSA Architecture Approaches

- Two approaches:
  - Non CRT RSA cryptographic core:
    - Traditional approach
    - Fully compatible with the SDM – TPM specifications:
      - Up to 2048 bit keys in non CRT form
  - CRT approach (the leap to the future):
    - Fast encryption – decryption
    - Small chip covered area
    - Modern RSA solution

RSA Architecture Basic Concept

★ *The Heart of the System*



- *Presented in 2010 IEEE International Symposium on Circuits and Systems (ISCAS 10), Paris, France*

END
Of
PRESENTATION

THANK YOU
QUESTIONS?


SEVENTH FRAMEWORK
PROGRAMME