

Design of an RSA Processor for Mitigating Insider Threats and Side-Channel Attacks

DR. SATYANARAYANA VOLLALA

Head and Associate Professor

Department of Computer Science & Engineering

International Institute of Information Technology, Naya Raipur



September 8, 2026

Insider Attack

Importance

Counteract for insider attacks

Type of Insider attack solutions

System of Multicore Crypto-Processor

Requirements Needs to be Addressed

Architecture of the multi-core crypto-processor

RSA Core0

RSA Core1, RSA Core2 & RSA Core3

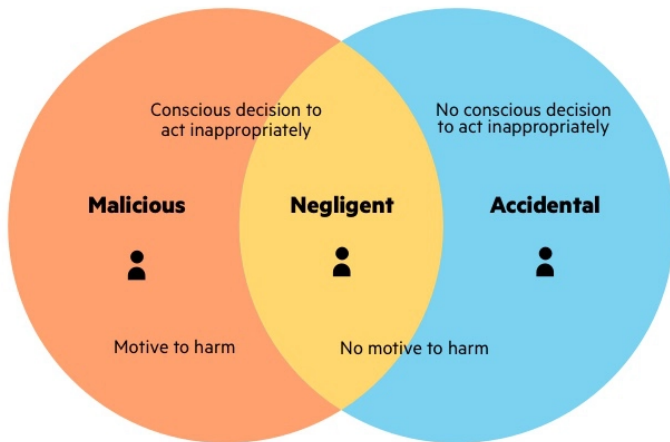
Scheduler & BRAM

Security parameters used in cypto-processor

Avoiding Attacks Caused by Trojan Placed by Insider Attacker

What is Insider Attack

An insider threat is a security risk that originates from within the targeted organization.



Insider intrusions are damaging to Information and Communication Technology (ICT) infrastructures and cause significant corporate risk of different forms, including:

- ▶ Brand risk
- ▶ Corporate trade secret disclosure risk
- ▶ Financial risk
- ▶ Legal compliance risk
- ▶ Operational and productivity risk

Counteract for insider attacks can be broadly categorized into three techniques based on time of action:

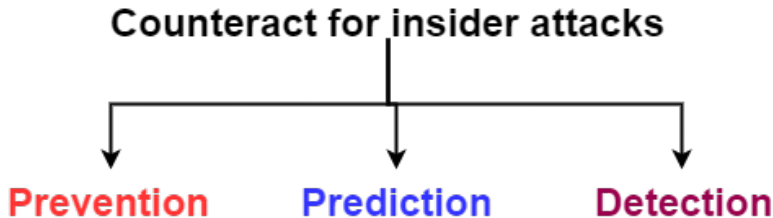


Figure 2: Counteract for insider attacks

The solutions to insider attacks have targeted four different aspects, out of which the first three are based on his:

1. Behaviour
2. Psychological study and
3. Network traffic pattern:
Solutions alarming the attacks based on these three aspects of an intruder are static and based on familiar incidents (that usually occurred before).
4. Technique that protects the information contained within the management frames transmitted via a network (e.g., IEEE 802.11 network).

- ▶ Prevent an insider attacker, trying to access or steal valuable information to avoid damage that can be caused by an insider attack.
- ▶ Storing the valuable information within the organization in an encrypted format.
- ▶ Secure the Key: Use of a large key size that is burnt into the chip.
- ▶ The system should be immune from the Trojan placed by an intruder during the development of the design in the foundry or placed at some access point within the organization.

There is a need for a strong system for Avoiding SCA caused by Trojan placed by insider attacker

- ▶ As software-based counteracts become more sophisticated and effective, hardware platforms are becoming a major attack source.
- ▶ The architecture has multiple crypto-processors which are selected randomly for cryptographic transformations and placed in a secured domain.
- ▶ The architecture restricts the monitoring of execution time, power consumption, and heat emission, which can help the intruder in guessing the key/plain-text.
- ▶ The architecture has its own sufficient memory space, and it is protected from illegal access.

Architecture of the multi-core crypto-processor

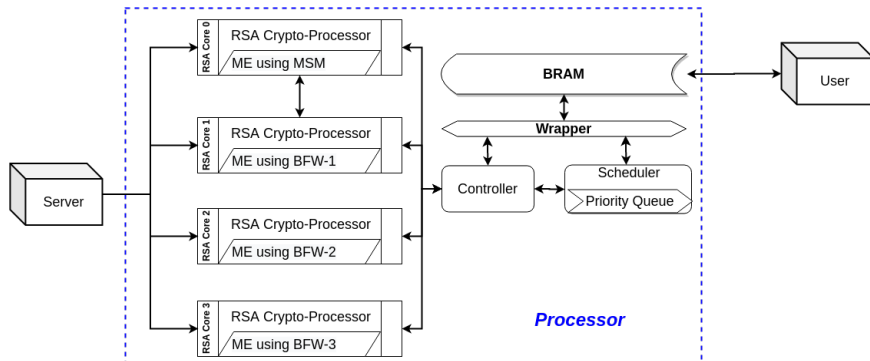


Figure 3: Overview of proposed multi-core crypto-processor

A quick revision of RSA Cryptosystem: Key Pair

► **Public Key** $\{n, e\}$

► **Private Key** $\{d\}$

Encryption $C = M^e \bmod n$

C: CipherText & M: Message

Decryption $M = C^d \bmod n$

$$M = (M^e)^d \bmod n \dots e \cdot d \cong 1 \bmod n$$

Table 1: An Example of **Square-And-Multiply** Method for $M^{89} \pmod{N}$

Exponent	Square	Multiply
e_i	Res = 1 <i>Initialization</i>	
1	$(1)^2 = 1$	$1 \times M = M$
0	$(M)^2 = M^2$	--
1	$(M^2)^2 = M^4$	$M^4 \times M = M^5$
1	$(M^5)^2 = M^{10}$	$M^{10} \times M = M^{11}$
0	$(M^{11})^2 = M^{22}$	--
0	$(M^{22})^2 = M^{44}$	--
1	$(M^{44})^2 = M^{88}$	$M^{88} \times M = M^{89}$

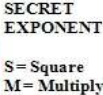
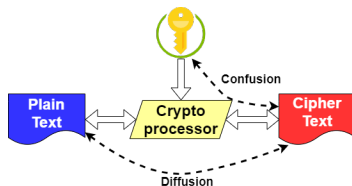
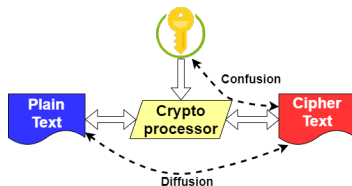


Figure 4: Simple Power Analysis

- **Confusion:** refers to making the relationship between **Cipher-text** and **Key** as complex and involved as possible.
- **Diffusion:** Relation between the **Plain-text** and the **Cipher-text** should be intractable.

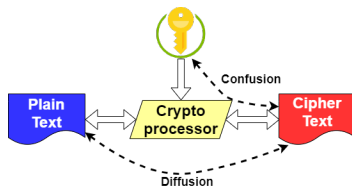


- **Confusion:** refers to making the relationship between **Cipher-text** and **Key** as complex and involved as possible.
- **Diffusion:** Relation between the **Plain-text** and the **Cipher-text** should be intractable.



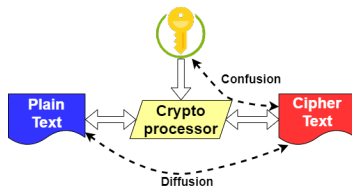
- Higher **Confusion** and **Diffusion**, create problems for the intruders to sniff the essential information.

- **Confusion:** refers to making the relationship between **Cipher-text** and **Key** as complex and involved as possible.
- **Diffusion:** Relation between the **Plain-text** and the **Cipher-text** should be intractable.



- Higher **Confusion** and **Diffusion**, create problems for the intruders to sniff the essential information.
- Avoiding **SCAs** only by the hardware means is not sufficient.
- **Crypto-algorithmic** way is required.

- ▶ **Confusion:** refers to making the relationship between **Cipher-text** and **Key** as complex and involved as possible.
- ▶ **Diffusion:** Relation between the **Plain-text** and the **Cipher-text** should be intractable.



- ▶ Higher **Confusion** and **Diffusion**, create problems for the intruders to sniff the essential information.
- ▶ Avoiding **SCAs** only by the hardware means is not sufficient.
- ▶ **Crypto-algorithmic** way is required.
- ▶ In our proposed techniques we have incorporated the **Confusion Mechanism** at two different levels.

RSA Core0 : Multiply & Square Module

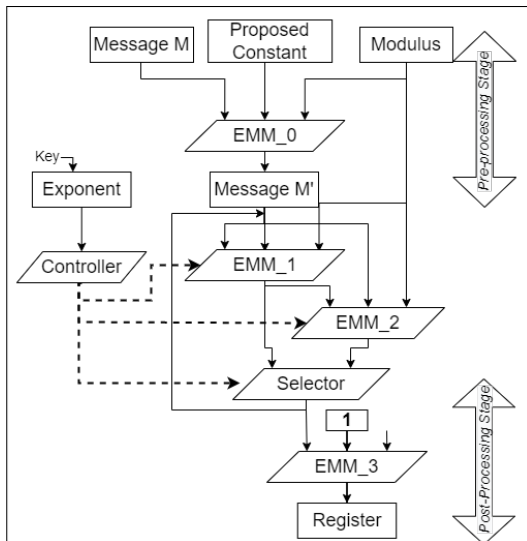


Figure 6: RSA Core0

Let $\{p_1 \ p_2\} = \{1 \ 1\}$ Multiplying Factor (MF) $\{M^2 \ M\} = M^3$

Let $\{p_1 \ p_2\} = \{1 \ 1\}$ Multiplying Factor (MF) $\{M^2 \ M\} = M^3$

$$89 = 1011001$$

Table 2: BFW with a Bit-Patter $\{1,1\}$ $M^{89} \bmod N$

Exponent		Square	Multiply
x_i	x_{i-1}	Res = 1 <i>Initialization</i>	
1	0	$(1)^2 = 1$	$1 \times = M$
0	1	$(M)^2 = M^2$	–
1	1	$(M^2)^2 = M^4$	FWD C
–	–	$(M^4)^2 = M^8$	$M^8 \times MF = M^{11}$
0	0	$(M^{11})^2 = M^{22}$	–
0	1	$(M^{22})^2 = M^{44}$	–
1	–	$(M^{44})^2 = M^{88}$	$M^{88} \times M = M^{89}$

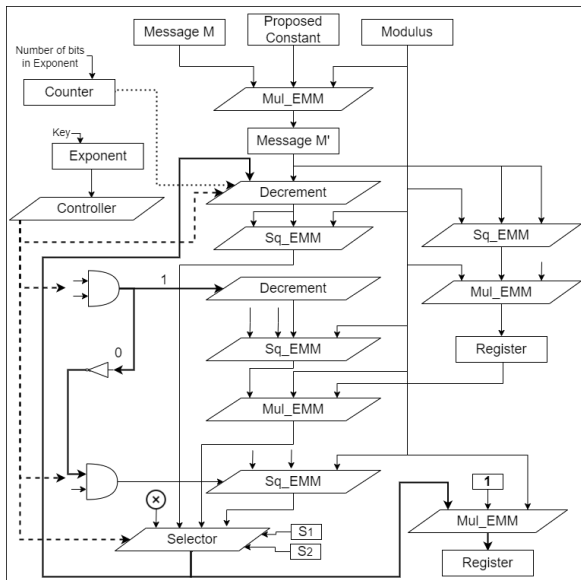


Figure 7: RSA Core1

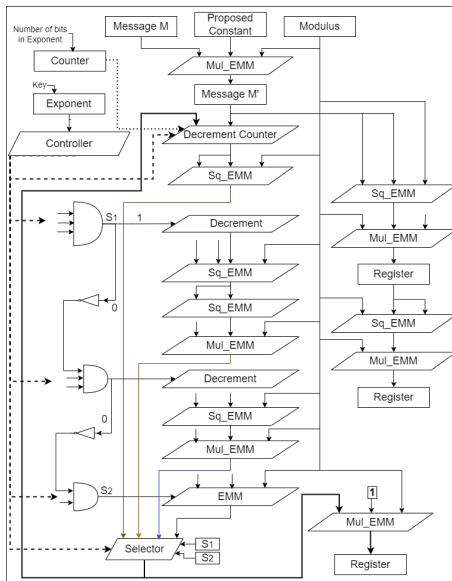


Figure 8: RSA Core2

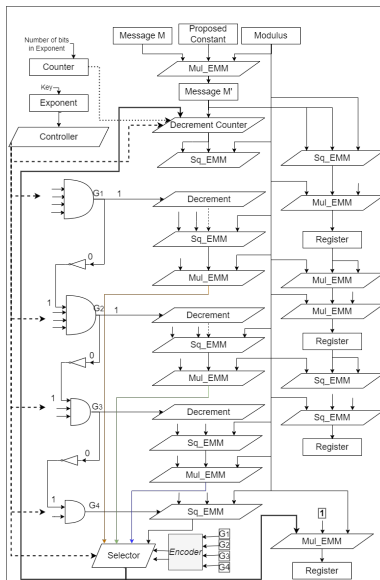


Figure 9: RSA Core3

- ▶ These RSA Cores are using BFW1, BFW2 and BFW3 modules.
- ▶ These modules performs a similar cryptographic transformations but its performance is better from the MSM module.
- ▶ The confusion factor is incorporated by specially designed controllers for each RSA Cores, which will send either of two, three or four consecutive bits instead of one Bit.

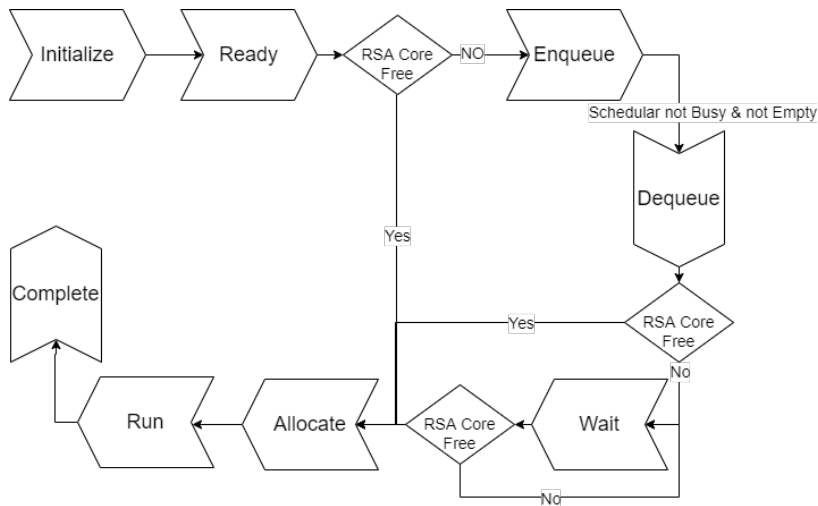


Figure 10: States of a Task Handled by Controller

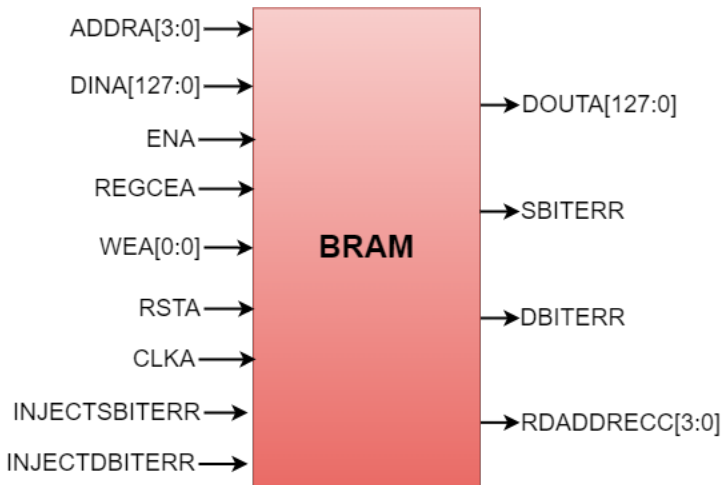


Figure 11: BRAM

Memory The very first layer of security is providing memory protection by using its own memory.

The crypto-processor is not depending on the underlying operating system(OS) for storing any kind of value.

Random The second layer of security is provided by the random selection of the RSA Core for cryptographic transformations.

Confusion All the RSA Cores have their unique way of performing modular exponentiation(ME).

The power and time required by each RSA Core are different.

Usually the intruder who is trying to sniff the secret information will plot a graph based on power and time consumption.

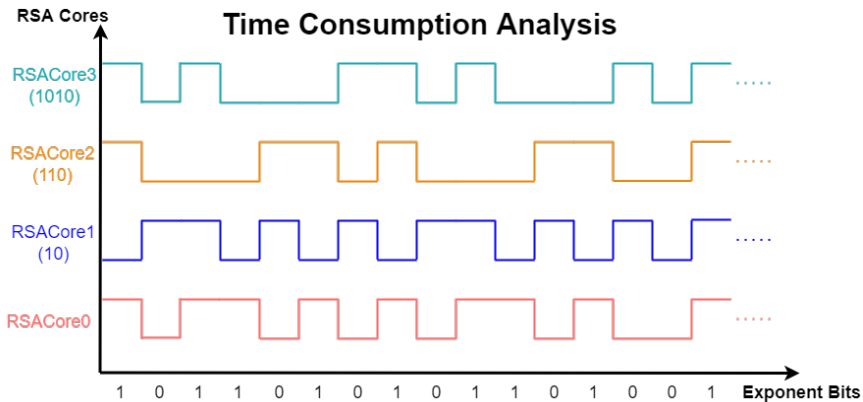


Figure 12: Time consumption by different RSA Cores

The designed architecture is immune from the Trojan placed by an intruder during the development of the design in the foundry or placed at some access point within the organization.

Table 3: Counteract techniques for SCA

Concept Used Counteract Technique	Hardware Based Methods		Algorithm Based Methods
	Power Hiding	Power Masking	Confusion Mechanism
Gornik et al.	Yes	No	No
Saha et al.	No	Yes	No
Ramezanpour et al.	No	Yes	No
Multi-Core Crypto-System	Can be implemented Externally		Yes

- ▶ The crypto-processors leak the various parameters while performing the cryptographic transformations.
- ▶ The presented multi-core crypto-processor is providing insider attack protection from Trojan which is placed by an insider close to a crypto-processor to steal the information using side channel attacks.

Thank You