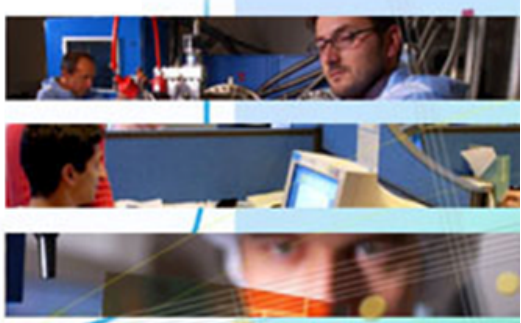
micro and nanoelectronics
microsystems
ambient intelligence
image chain
biology and health

Analyse cryptographique des altérations d'algorithmes : Applications au RSA

Alexandre Berzati

CEA-LETI Minatec et Université de Versailles

20 Janvier 2009



leti

cea

Outline

Introduction on RSA | Attack on "R2L" exp. | Attack on "L2R' exp. | Conclusion

1 Introduction on RSA

2 Attack on "R2L" exp.

3 Attack on "L2R' exp.

4 Conclusion

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Introduction

Description

Fault analysis on a standard RSA implementation by perturbating the public modulus

Motivation

Emphazing the importance of securing RSA public elements

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Outline

1 Introduction on RSA
- Fault Analysis Principle
- Previous work
- Overview of our attack

2 Attack on "R2L" exp.

3 Attack on "L2R' exp.

4 Conclusion

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

RSA Cryptosystem

- Public Key
  - Modulus N such that $N = p \cdot q$, p and q prime and kept secret
  - The exponent e such that $\gcd(e, \varphi(N)) = 1$, where $\varphi(.)$ denotes Euler's totient function and $\varphi(N) = (p-1) \cdot (q-1)$

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

RSA Cryptosystem

- Public Key
  - Modulus N such that $N = p \cdot q$, p and q prime and kept secret
  - The exponent e such that $\gcd(e, \varphi(N)) = 1$, where $\varphi(.)$ denotes Euler's totient function and $\varphi(N) = (p-1) \cdot (q-1)$

- Secret Key
  - The exponent d such that $e \cdot d \equiv 1 \bmod \varphi(N)$

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

RSA Cryptosystem

- Public Key
  - Modulus N such that $N = p \cdot q$, p and q prime and kept secret
  - The exponent e such that $\gcd(e, \varphi(N)) = 1$, where $\varphi(.)$ denotes Euler's totient function and $\varphi(N) = (p-1) \cdot (q-1)$
- Secret Key
  - The exponent d such that $e \cdot d \equiv 1 \bmod \varphi(N)$
- RSA functions
  - Encryption of a message $m \Rightarrow C \equiv m^e \bmod N$

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

RSA Cryptosystem

- Public Key
  - Modulus N such that $N = p \cdot q$, p and q prime and kept secret
  - The exponent e such that $\gcd(e, \varphi(N)) = 1$, where $\varphi(.)$ denotes Euler's totient function and $\varphi(N) = (p-1) \cdot (q-1)$

- Secret Key
  - The exponent d such that $e \cdot d \equiv 1 \bmod \varphi(N)$

- RSA functions
  - Encryption of a message $m \Rightarrow C \equiv m^e \bmod N$
  - Decryption of the cyphertext $C \Rightarrow \tilde{m} \equiv C^d \equiv m^{e \cdot d} \bmod N$

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

RSA Cryptosystem

- Public Key
  - Modulus N such that $N = p \cdot q$, p and q prime and kept secret
  - The exponent e such that $\gcd(e, \varphi(N)) = 1$, where $\varphi(.)$ denotes Euler's totient function and $\varphi(N) = (p-1) \cdot (q-1)$

- Secret Key
  - The exponent d such that $e \cdot d \equiv 1 \bmod \varphi(N)$

- RSA functions
  - Encryption of a message $m \Rightarrow C \equiv m^e \bmod N$
  - Decryption of the cyphertext $C \Rightarrow \tilde{m} \equiv C^d \equiv m^{e \cdot d} \bmod N$
  - Signature of a message $m \Rightarrow S \equiv \dot{m}^d \bmod N$

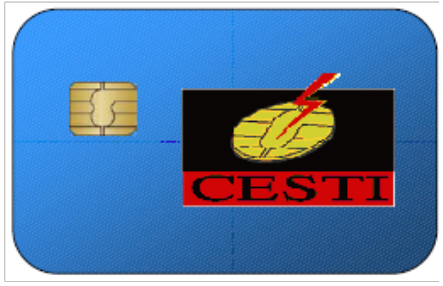
© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Fault Analysis Principle

- Differential Fault Analysis (*DFA*)
  - Identify the perturbation
  - Model faults
  - Differentiate correct and faulty outputs

Smart card input:
00101101 ... $\Longrightarrow$

Smart card output:
01010001 ... $\Longleftarrow$



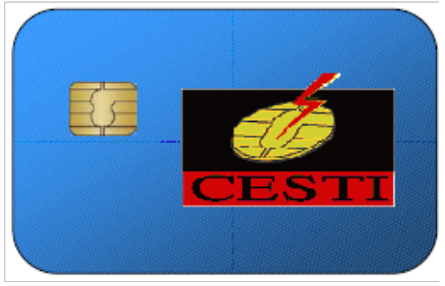
© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Fault Analysis Principle

- Differential Fault Analysis (*DFA*)
  - Identify the perturbation
  - Model faults
  - Differentiate correct and faulty outputs

Smart card input:
0010110100110010 . . . $\Longrightarrow$

Smart card output:
01010001 . . . $\Longleftarrow$



© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Fault Analysis Principle

- Differential Fault Analysis (*DFA*)
  - Identify the perturbation
  - Model faults
  - Differentiate correct and faulty outputs

Smart card input:
0010110100110010 . . . $\Longrightarrow$

Smart card output:
0101000110111011 . . . $\Longleftarrow$

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Outline

1 Introduction on RSA
- Fault Analysis Principle
- Previous work
- Overview of our attack

2 Attack on "R2L" exp.

3 Attack on "L2R' exp.

4 Conclusion

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

DFA on RSA Public Elements

- *On authenticated computing and RSA-based authentication* (Sei05), ACM-CCS 2005

- *Is it wise to publish your Public RSA Keys ?* (GS06), FDTC 2006
  - Corrupt the RSA signature scheme without recovering the secret exponent *d*
  - Rely on a specific fault model

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

DFA on RSA Public Elements

- *On authenticated computing and RSA-based authentication* (Sei05), ACM-CCS 2005

- *Is it wise to publish your Public RSA Keys ?* (GS06), FDTC 2006
  - Corrupt the RSA signature scheme without recovering the secret exponent *d*
  - Rely on a specific fault model

- *Why One Should Also Secure RSA Public Key Elements* (BCMCC06), CHES 2006
  - Recover the secret exponent *d*
  - In a variant the analysis doesn't rely on any fault model

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Outline

1 Introduction on RSA
- Fault Analysis Principle
- Previous work
- Overview of our attack

2 Attack on "R2L" exp.

3 Attack on "L2R' exp.

4 Conclusion

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Overview of our attack

- Our attack works by only modifying the public modulus *N*
  - Modification during the exponentiation

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Overview of our attack

- Our attack works by only modifying the public modulus *N*
  - Modification during the exponentiation
- Provides both partial and full secret key recovery:
  - Each faulty execution analysis makes the attacker recover a part of *d*
  - Cascading partial results leads to a full recovery of *d*

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Overview of our attack

- Our attack works by only modifying the public modulus *N*
  - Modification during the exponentiation
- Provides both partial and full secret key recovery:
  - Each faulty execution analysis makes the attacker recover a part of *d*
  - Cascading partial results leads to a full recovery of *d*
- Applies on Standard RSA functions that handles the secret key
  - Signature (with deterministic padding)
  - Decryption

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Overview of our attack

- Our attack works by only modifying the public modulus *N*
  - Modification during the exponentiation
- Provides both partial and full secret key recovery:
  - Each faulty execution analysis makes the attacker recover a part of *d*
  - Cascading partial results leads to a full recovery of *d*
- Applies on Standard RSA functions that handles the secret key
  - Signature (with deterministic padding)
  - Decryption
- Provides a faster attack algorithm

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Outline

1 Introduction on RSA

2 Attack on "R2L" exp.

- "Right-to-Left" Algorithm
- Fault Model
- Faulty Execution
- Fault Analysis

3 Attack on "L2R' exp.

4 Conclusion

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

RSA Exponentiation Algorithm

"Right-to-Left" Algorithm

Input: m, d, N
Output: $A = m^d \bmod N$

```
1 : A:=1;
2 : B:=m;
3 : for i from 0 upto (n − 1)
4 :     if (d_i == 1)
5 :         A := (A · B) mod N;
6 :     end if
7 :     B := B^2 mod N;
8 : end for
9 : return A;
```

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Outline

1 Introduction on RSA

2 Attack on "R2L" exp.

- "Right-to-Left" Algorithm
- Fault Model
- Faulty Execution
- Fault Analysis

3 Attack on "L2R' exp.

4 Conclusion

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Fault model

- Perturbation of the Standard RSA signature
  - Transient byte fault on the public modulus *N*
  - Fault injected on a square *j* steps before the end of the exponentiation
  - The time location of the fault is known by the attacker

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Fault model

- Perturbation of the Standard RSA signature
  - Transient byte fault on the public modulus N
  - Fault injected on a square j steps before the end of the exponentiation
  - The time location of the fault is known by the attacker

- The faulty result $\hat{N}$ can be model as:

$$\hat{N} = N \oplus \varepsilon$$

where $\varepsilon = R_8 \cdot 2^{8i}$, R_8 is a random byte value and $i \in [\![0; \frac{n}{8} - 1]\!]$

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Fault model

- Perturbation of the Standard RSA signature
  - Transient byte fault on the public modulus N
  - Fault injected on a square j steps before the end of the exponentiation
  - The time location of the fault is known by the attacker

- The faulty result $\hat{N}$ can be model as:

$$\hat{N} = N \oplus \varepsilon$$

where $\varepsilon = R_8 \cdot 2^{8i}$, R_8 is a random byte value and $i \in [\![0; \frac{n}{8} - 1]\!]$

- Then, the end of the exponentiation is executed with a faulty modulus $\hat{N}$

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Outline

1 Introduction on RSA

2 Attack on "R2L" exp.

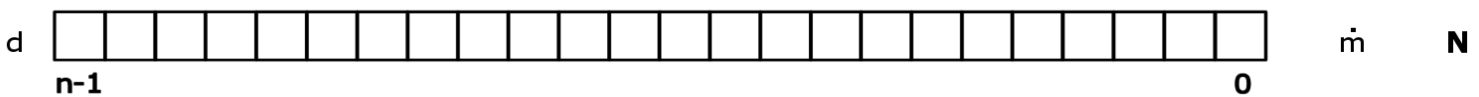
- "Right-to-Left" Algorithm
- Fault Model
- Faulty Execution
- Fault Analysis

3 Attack on "L2R' exp.

4 Conclusion

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

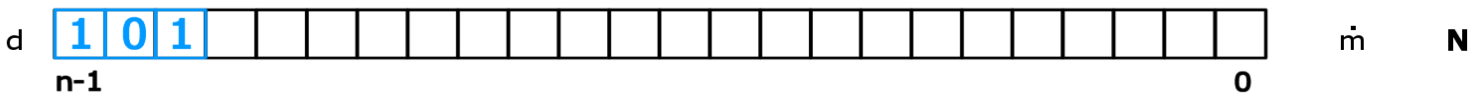
Faulty Execution of the *"Right-to-Left"* Algorithm



© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Faulty Execution of the *"Right-to-Left"* Algorithm

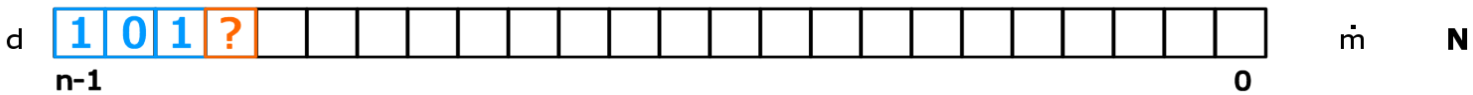
- A part of *d* is already known



© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Faulty Execution of the *"Right-to-Left"* Algorithm

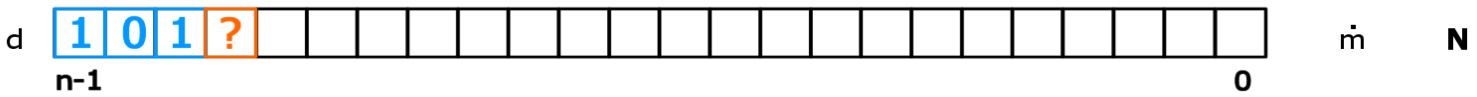
- A part of *d* is already known
- The attacker wants to recover *l* bits of *d*
  - *l* is a window length parameter



© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Faulty Execution of the *"Right-to-Left"* Algorithm

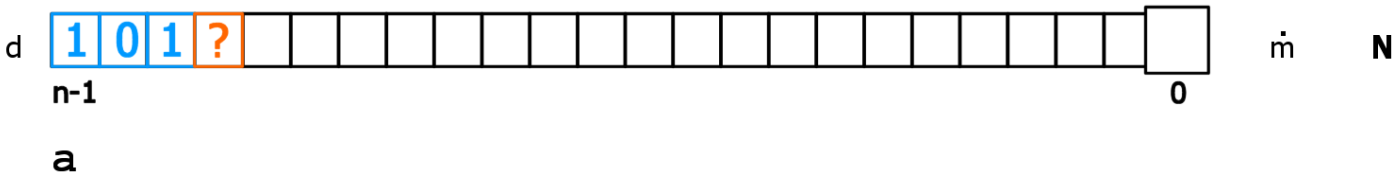
- A part of *d* is already known
- The attacker wants to recover *l* bits of *d*
  - *l* is a window length parameter
  - For this example $l = 1$



© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Faulty Execution of the *"Right-to-Left"* Algorithm

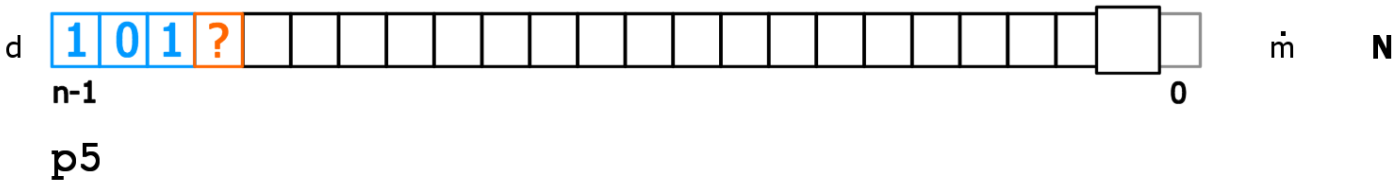
- Example of a faulty execution



© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Faulty Execution of the *"Right-to-Left"* Algorithm

- Example of a faulty execution



© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Faulty Execution of the *"Right-to-Left"* Algorithm

- Example of a faulty execution

a§7♪RSA Signature`]õ

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Faulty Execution of the *"Right-to-Left"* Algorithm

- Example of a faulty execution

çàjdn,vGrenobleàçjbkç

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Faulty Execution of the *"Right-to-Left"* Algorithm

- Example of a faulty execution

Ŝ 10th anniversary of CHES

- Consequences of the fault
  - The fault injection splits the faulty signature $\hat{S}$ into a correct part and a faulty one:

$$\hat{S} \equiv [(\dot{m}^{\sum_{i=0}^{(n-j-1)} 2^i \cdot d_i} \bmod N) \cdot (\dot{m}^{2^{(n-j-1)}} \bmod N)^{\sum_{i=(n-j)}^{n-1} 2^{[i-(n-j)+1]} \cdot d_i}] \bmod \hat{N}$$

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Faulty Execution of the *"Right-to-Left"* Algorithm

- Example of a faulty execution

Ŝ 10th anniversary of CHES

- Consequences of the fault
  - The fault injection splits the faulty signature $\hat{S}$ into a correct part and a faulty one:

$$\hat{S} \equiv [(\dot{m}^{\sum_{i=0}^{(n-j-1)} 2^i \cdot d_i} \bmod N) \cdot (\dot{m}^{2^{(n-j-1)}} \bmod N)^{\sum_{i=(n-j)}^{n-1} 2^{[i-(n-j)+1]} \cdot d_i}] \bmod \hat{N}$$

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Faulty Execution of the *"Right-to-Left"* Algorithm

- Example of a faulty execution

Ŝ 10th anniversary of CHES

- Consequences of the fault
  - The fault injection splits the faulty signature $\hat{S}$ into a correct part and a faulty one:

$$\hat{S} \equiv [(\dot{m}^{\sum_{i=0}^{(n-j-1)} 2^i \cdot d_i} \bmod N) \cdot (\dot{m}^{2^{(n-j-1)}} \bmod N)^{\sum_{i=(n-j)}^{n-1} 2^{[i-(n-j)+1]} \cdot d_i}] \bmod \hat{N}$$

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Outline

1 Introduction on RSA

2 Attack on "R2L" exp.

- "Right-to-Left" Algorithm
- Fault Model
- Faulty Execution
- Fault Analysis

3 Attack on "L2R' exp.

4 Conclusion

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Fault Analysis

- Result of the faulty execution

Ŝ 10th anniversary of CHES

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Fault Analysis

- Result of the faulty execution

ŝ 10th anniversary of CHES

- Attack principle

s r54_Correc+_519n4+ur3

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Fault Analysis

- Result of the faulty execution

ŝ 10th anniversary of CHES

- Attack principle

s r54_Correc+_519n4+ur3

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Fault Analysis

- Result of the faulty execution

```
ŝ 10th anniversary of CHES
```

- Attack principle

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Faulty Execution of the *"Left-to-Right"* Algorithm

- Under the same fault model the result of the perturbation is:

$$\hat{S} \equiv [(\dot{m}^{\sum_{i=j}^{(n-1)} 2^i \cdot d_i} \bmod N)^{2^j} \cdot (\dot{m}^{2^{(n-j-1)}} \bmod N)^{\sum_{i=0}^{j-1} 2^i \cdot d_i}] \bmod \hat{N}$$

- The extra squares modulo $\hat{N}$ defeat the *"Right-to-Left"* analysis

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Faulty Execution of the *"Left-to-Right"* Algorithm

- Under the same fault model the result of the perturbation is:

$$\hat{S} \equiv [(\dot{m}^{\sum_{i=j}^{(n-1)} 2^i \cdot d_i} \bmod N)^{2^j} \cdot (\dot{m}^{2^{(n-j-1)}} \bmod N)^{\sum_{i=0}^{j-1} 2^i \cdot d_i}] \bmod \hat{N}$$

- The extra squares modulo $\hat{N}$ defeat the *"Right-to-Left"* analysis

- Square roots are computable if $\hat{N}$ is prime or *B*-smooth

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Faulty Execution of the *"Left-to-Right"* Algorithm

- Under the same fault model the result of the perturbation is:

$$\hat{S} \equiv [(\dot{m}^{\sum_{i=j}^{(n-1)} 2^i \cdot d_i} \bmod N)^{2^j} \cdot (\dot{m}^{2^{(n-j-1)}} \bmod N)^{\sum_{i=0}^{j-1} 2^i \cdot d_i}] \bmod \hat{N}$$

- The extra squares modulo $\hat{N}$ defeat the *"Right-to-Left"* analysis
- Square roots are computable if $\hat{N}$ is prime or *B*-smooth
- We have to study the consistency of considering only prime faulty moduli

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Outline

1 Introduction on RSA

2 Attack on "R2L" exp.

3 Attack on "L2R' exp.

- "Left-to-Right" Algorithm
- Faulty Execution
- Fault Analysis

4 Conclusion

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Study of the new fault model

- Assumptions on the perturbation of the modulus
  - Transient fault on the public modulus N:

$$\hat{N} = N \oplus \varepsilon$$

    where $\varepsilon = R_{8k} \cdot 2^{8k \cdot i}$, R_{8k} is a k-byte random value and $i \in [\![0; \frac{n}{8k} - 1]\!]$
  - We consider only prime $\hat{N}$

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Study of the new fault model

- Assumptions on the perturbation of the modulus
  - Transient fault on the public modulus N:

$$\hat{N} = N \oplus \varepsilon$$

    where $\varepsilon = R_{8k} \cdot 2^{8k \cdot i}$, R_{8k} is a k-byte random value and $i \in [\![0; \frac{n}{8k} - 1]\!]$
  - We consider only prime $\hat{N}$

- Results obtained

Archi.	n bits	# of $\hat{N}$	# of prime $\hat{N}$	# of exp.	# of primes		
					Min.	Avg.	Max.
8-bit	1024	2^{15}	46.186	114890	18	46.26	79
8-bit	2048	2^{16}	46.176	57170	22	46.19	80
16-bit	1024	2^{22}	5911.83	17725	5621	5919.08	6212
32-bit	1024	2^{37}	$\approx 1,94 \cdot 10^8$				

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Study of the new fault model

- Assumptions on the perturbation of the modulus
  - Transient fault on the public modulus N:

$$\hat{N} = N \oplus \varepsilon$$

    where $\varepsilon = R_{8k} \cdot 2^{8k \cdot i}$, R_{8k} is a k-byte random value and $i \in [\![0; \frac{n}{8k} - 1]\!]$
  - We consider only prime $\hat{N}$

- Results obtained

Archi.	n bits	# of $\hat{N}$	# of prime $\hat{N}$	# of exp.	# of primes		
					Min.	Avg.	Max.
8-bit	1024	2^{15}	46.186	114890	18	46.26	79
8-bit	2048	2^{16}	46.176	57170	22	46.19	80
16-bit	1024	2^{22}	5911.83	17725	5621	5919.08	6212
32-bit	1024	2^{37}	$\approx 1,94 \cdot 10^8$				

- $\hat{N}$ has one chance over 709 to be prime on an 8-bit architecture

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Fault Analysis

- Attack principle
  - Precomputation of a dictionnary of prime faulty moduli
  - Choose a candidate pair $(d'_{(k)}, \hat{N}')$ and compute
    1. $S' \equiv \hat{S} \cdot \dot{m}^{-d'_{(k)}} \bmod \hat{N}'$
    2. Test if S' is a k-th quadratic residue modulo $\hat{N}'$, else the pair is rejected
    3. Check if $S \equiv (S')^{2^k} \cdot \dot{m}^{d'_{(k)}} \bmod N$ is satisfied to validate the candidate pair
  - Cascade the resolution using the already recovered part of d

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Fault Number

- Fault number

$$\#fault = \mathcal{O}\left(\frac{n^2}{1.441 \cdot l}\right) \text{ tries}$$

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Fault Number

- Fault number

$$\#fault = \mathcal{O}\left(\frac{n^2}{1.441 \cdot l}\right) \text{ tries}$$

  - Faulty moduli have to be prime to make the perturbation exploitable

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Fault Number

- Fault number

$$\#fault = \mathcal{O}\left(\frac{n^2}{1.441 \cdot l}\right) \text{ tries}$$

  - Faulty moduli have to be prime to make the perturbation exploitable
  - Number of iterations for a full key recovery

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Fault Number

- Fault number

$$\#fault = \mathcal{O}\left(\frac{n^2}{1.441 \cdot l}\right) \text{ tries}$$

  - Faulty moduli have to be prime to make the perturbation exploitable
  - Number of iterations for a full key recovery

- Additional Remark
  - The probability for $\hat{N}$ to be prime depends on the byte location of the fault

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

References

- DFA on RSA public elements
  - *Perturbating RSA Public Keys: an Improved Attack* (BCG08), CHES 2008
  - *Fault Attacks on RSA Public Keys: Left-To-Right Implementations are also Vulnerable* (BCDG09), CT-RSA 2009

- DFA on CRT based RSA
  - *(In)security Against Fault Injection Attacks on CRT-RSA Implementations* (BCG08), FDTC 2008

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Possible countermeasures

- Random mask on the exponent
  - The private exponent d is masked such that:

$$d_{mask} = d + k \cdot \varphi(N)$$

where k is a random value longer than the resolution window length l

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Possible countermeasures

- Random mask on the exponent
  - The private exponent d is masked such that:

$$d_{mask} = d + k \cdot \varphi(N)$$

    where k is a random value longer than the resolution window length l

- Mask the modulus N during the computation $\Rightarrow$ not a solution as itself
  - Lengthen the resolution and the number of faulty signatures to gather

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Possible countermeasures

- Random mask on the exponent
  - The private exponent d is masked such that:

    $$d_{mask} = d + k \cdot \varphi(N)$$

    where k is a random value longer than the resolution window length l

- Mask the modulus N during the computation $\Rightarrow$ not a solution as itself
  - Lengthen the resolution and the number of faulty signatures to gather

- Error detecting mechanism (Hardware or Software)

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

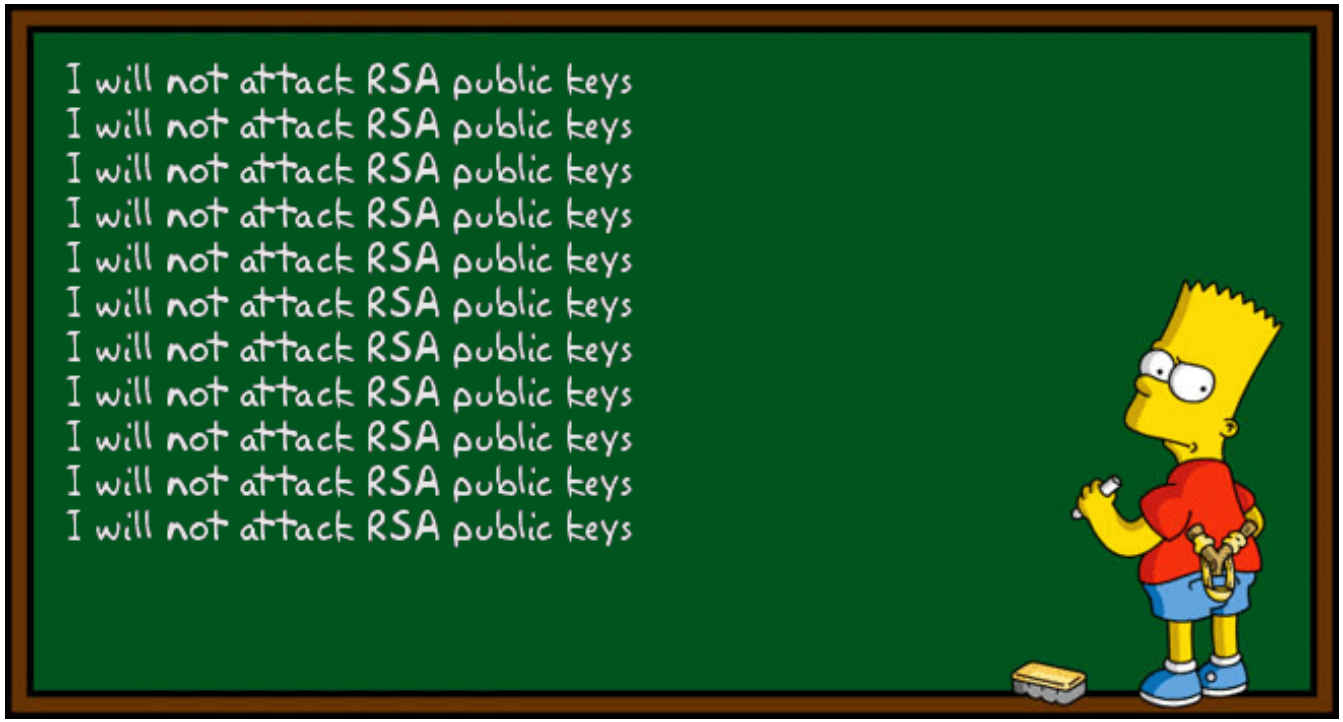
Conclusion

- Work in progress
  - Applications to elliptic curve cryptography

© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Conclusion

- Work in progress
  - Applications to elliptic curve cryptography
- Thank you for your attention !



© CEA 2009. All rights reserved
Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA