micro et nanoélectronique microsystèmes intelligence ambiante hiologie et santéchaîne de l'image



ren



(In)security Against Fault Injection Attacks on CRT-RSA Implementations

Alexandre Berzati, Cécile Canovas and Louis Goubin

E-mail : alexandre.berzati@cea.fr



leti







Outline

- Introduction
 - Previous work
 - Overview of our attack
- 2 Attack principle
 - Ciet & Joye Countermeasure
 - Fault Model
 - Faulty Execution
 - Fault Analysis



CEA 2008. Tous droits réservés Toute reproduction totale ou partielle sur queique support que ce soit ou ubisation du centenu de ce document est interdite sans à l'autrisation échite tréatible du CEA Un rights reserved. Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the point or writen constant of CEA



-

Introduction

Description

Fault analysis on a protected CRT-RSA implementation



© CEA 2008. Tous droits réservés.

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorization écnte préalable du CEA 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 protected CRT-RSA implementation

Motivation

Highlighting that protecting CRT-RSA against DFA is a challenging problem



CEA 2008. Tous droits réservés

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écnite préalable du CEA 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

Introduction

Previous work

Overview of our attack

2 Attack principle

- Ciet & Joye Countermeasure
- Fault Model
- Faulty Execution
- Fault Analysis





© CEA 2008. Tous droits réservés

Toute reproduction totale ou partielle sur queique support que ce soil ou ubisation du contenu de ce document est interdite sans l'autorisation écrite préalable du CEA 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 CRT-RSA



CEA 2008. Tous droits réservés.

Toute reproduction totale ou partielle sur quelque support que ce soit ou ubisation du contenu de ce document est interdite sans l'autorisation échte préalable du CEA 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 CRT-RSA
 - On the Importance of Checking Cryptographic Protocols for Faults (BDL97), EUROCRYPT'97



© CEA 2008. Tous droits réservés

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écnte préatable du CEA 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 CRT-RSA
 - On the Importance of Checking Cryptographic Protocols for Faults (BDL97), EUROCRYPT'97
 - Fault Attack on RSA with CRT: Concrete Results and Practical Countermeasures (ABF+02), CHES 2002



Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est intercite sans fautorisation écnte préalable du CEA. 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 writer consent of CEA.



- DFA on CRT-RSA
 - On the Importance of Checking Cryptographic Protocols for Faults (BDL97), EUROCRYPT'97
 - Fault Attack on RSA with CRT: Concrete Results and Practical Countermeasures (ABF+02), CHES 2002
 - Cryptanalysis of a Provably Secure CRT-RSA Algorithm (Wag04), ACM-CCS 2004

Toute reproduction totale ou particle sur quelque support que ce soit ou utilisation du contenu de ce document est interdité sans fautorisation acite préable du CEX 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 CEX



- DFA on CRT-RSA
 - On the Importance of Checking Cryptographic Protocols for Faults (BDL97), EUROCRYPT'97
 - Fault Attack on RSA with CRT: Concrete Results and Practical Countermeasures (ABF+02), CHES 2002
 - Cryptanalysis of a Provably Secure CRT-RSA Algorithm (Wag04), ACM-CCS 2004

Methods for protecting CRT-RSA



© CEA 2008. Tous droits réservés. In totale ou partie le sur queique support que ce soit ou utilisation du contenu de ce document est interdée sans queique support que ce soit ou utilisation du contenu de ce document est interdée sans queique du contenue de ce document est interdée sans queique du contenue de ce document est interdée sans queique du contenue de ce document est interdée sans queique du contenue de ce document est interdée sans queique du contenue de ce document est interdée sans queique du contenue de ce document est interdée sans queique du contenue de ce document est interdée sans queique du contenue de ce document est interdée sans queique du contenue de ce document est interdée sans queique du contenue de ce document est interdée sans queique du contenue de ce document est interdée sans queique du contenue de ce document est interdée sans queique du contenue de ce document est interdée sans queique du contenue de ce document est interdée sans queique du contenue de ce document est interdée sans queique du contenue du contenue



- DFA on CRT-RSA
 - On the Importance of Checking Cryptographic Protocols for Faults (BDL97), EUROCRYPT'97
 - Fault Attack on RSA with CRT: Concrete Results and Practical Countermeasures (ABF+02), CHES 2002
 - Cryptanalysis of a Provably Secure CRT-RSA Algorithm (Wag04), ACM-CCS 2004
- Methods for protecting CRT-RSA
 - Shamir's trick: Improved Method and Apparatus for Protecting Public Key Schemes from Timing and Fault Attacks (Sha97), Rump Session of Eurocrypt'97

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation échte préatable du CEA 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 CRT-RSA
 - On the Importance of Checking Cryptographic Protocols for Faults (BDL97), EUROCRYPT'97
 - Fault Attack on RSA with CRT: Concrete Results and Practical Countermeasures (ABF+02), CHES 2002
 - Cryptanalysis of a Provably Secure CRT-RSA Algorithm (Wag04), ACM-CCS 2004
- Methods for protecting CRT-RSA
 - Shamir's trick: Improved Method and Apparatus for Protecting Public Key Schemes from Timing and Fault Attacks (Sha97), Rump Session of Eurocrypt'97
 - Infective Computation: RSA Speedup with Residue Number System Immune Against Hardware Fault Cryptanalysis (YKLM01), ISISC 2001

CEA 2008. Tous droits réservés Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interde ans Taukrisation éntinte prévaible du CES. In infatts reserved. Any reproduction in whote or in part on any medium or use of the information contained herein is crohibited without the prior writte conserved of CES.

< □ < □ < □ >



- DFA on CRT-RSA
 - On the Importance of Checking Cryptographic Protocols for Faults (BDL97), EUROCRYPT'97
 - Fault Attack on RSA with CRT: Concrete Results and Practical Countermeasures (ABF+02), CHES 2002
 - Cryptanalysis of a Provably Secure CRT-RSA Algorithm (Wag04), ACM-CCS 2004
- Methods for protecting CRT-RSA
 - Shamir's trick: Improved Method and Apparatus for Protecting Public Key Schemes from Timing and Fault Attacks (Sha97), Rump Session of Eurocrypt'97
 - Infective Computation: RSA Speedup with Residue Number System Immune Against Hardware Fault Cryptanalysis (YKLM01), ISISC 2001
 - BOS Scheme: A New CRT-RSA Algorithm Secure Against Bellcore Attack (BOS03), ACM-CCS 2003



© CEA 2008. Tous droits réservés, ou utilisation du contenu de ce document est interdite sans l'autorisation écrite préalable du CEA.



Outline

Introduction

- Previous work
- Overview of our attack

2 Attack principle

- Ciet & Joye Countermeasure
- Fault Model
- Faulty Execution
- Fault Analysis



© CEA 2008. Tous droits réservés

Toute reproduction totale ou partielle sur queique support que ce soil ou ubisation du contenu de ce document est interdite sans l'autorisation écrite préalable du CEA 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 applies on a protected CRT-RSA implementation



CEA 2008. Tous droits réservés.

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écnte préatable du CEA 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 applies on a protected CRT-RSA implementation

Provides a full secret key recovery by factorizing the public modulus N



CEA 2008. Tous droits réservés

Toute reproduction totale ou partielle sur queique support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écnte préatable du CEA 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



Our attack applies on a protected CRT-RSA implementation

Provides a full secret key recovery by factorizing the public modulus N

Can be applied on CRT-RSA functions that handles the secret key d:

- Signature (with deterministic padding)
- Decryption

●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●
 ●</li

© CEA 2008. Tous droits réservés

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écrite préalable du CEA 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



Our attack applies on a protected CRT-RSA implementation

Provides a full secret key recovery by factorizing the public modulus N

Can be applied on CRT-RSA functions that handles the secret key d:

- Signature (with deterministic padding)
- Decryption

Based on a simple and practicable fault model

∃⇒



Outline

2 Attack principle

- Ciet & Joye Countermeasure
- Faulty Execution
- Fault Analysis



< A > < ∃ > ∢ ≣ ≯

CEA 2008. Tous droits réservés

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écrite tréalable du CEA



Ciet & Joye Algorithm — Practical Fault Countermeasures for Chinese Remaindering Based RSA (JC05), FDTC 2005

> Input: $\dot{m}, \{p, q, d_p, d_q\}$ Output: $S = \dot{m}^d \mod N$ Parameters: κ, l

1. For two κ -bit random integers r_1 and r_2 (a) $p^* = r_1 \cdot p$, (b) $q^* = r_2 \cdot q$, (c) $l_{q^*} = (q^*)^{-1} \mod p^*$, (d) $N = p \cdot q$. 2. Compute (a) $S_{p^*} \equiv \dot{m}^{d_p} \mod p^*$ and $s_2 \equiv \dot{m}^{d_q} \mod \varphi(r_2) \mod r_2$, (b) $S_{q^*} \equiv \dot{m}^{d_q} \mod q^*$ and $s_1 \equiv \dot{m}^{d_p} \mod \varphi(r_1) \mod r_1$. 3. Compute $S^* \equiv S_{q^*} + q^* \cdot l_{q^*} \cdot (S_{p^*} - S_{q^*}) \mod p^*$ 4. Compute (a) $c_1 \equiv (S^* - s_1 + 1) \mod r_1$ (b) $c_2 \equiv (S^* - s_2 + 1) \mod r_2$. 5. For a *l*-bit integer r_3 , set $\gamma = \lfloor \frac{(r_3 \cdot c_1 + (2^l - r_3) \cdot c_2)}{2^l} \rfloor$ 6. Return $S \equiv (S^*)^{\gamma} \mod N$

CEA 2008. Tous droits réservés

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation échte préatable du CEA All rights reserved. Any reproduction in whole er in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA



Outline

Introduction

- Previous work
- Overview of our attack

2 Attack principle

- Ciet & Joye Countermeasure
- Fault Model
- Faulty Execution
- Fault Analysis



◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →
◆□ →

© CEA 2008. Tous droits réservés

Toute reproduction totale ou partielle sur queique support que ce soil ou ubisation du contenu de ce document est interdite sans l'autorisation écrite préalable du CEA 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 CRT-RSA signature
 - Transient byte fault on Sp*



CEA 2008. Tous droits réservés.

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autoritation éche prévaible du CEA 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 CRT-RSA signature

• Transient byte fault on Sp*

The faulty result $\hat{S_{p^*}}$ can be model as:

$$\hat{S_{p^*}} = S_{p^*} \oplus \varepsilon$$

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

© CEA 2008. Tous droits réservés

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écnte préalable du CEA All rights reserved. Any reproduction in whote 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 CRT-RSA signature

• Transient byte fault on Sp*

The faulty result $\hat{S_{p^*}}$ can be model as:

$$\hat{S_{p^*}} = S_{p^*} \oplus \varepsilon$$

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

Then, the fault spreads over the computation:

- During the CRT Recombination
- Computation of the check values and gamma
- Final signature

CEA 2008. Tous droits réservés

< ⊒⇒

Toute reproduction totale ou partielle sur queique support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écrite préalable du CE 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 CE



Outline

Introduction

- Previous work
- Overview of our attack

2 Attack principle

- Ciet & Joye Countermeasure
- Fault Mode
- Faulty Execution
- Fault Analysis



© CEA 2008. Tous droits réservés

Toute reproduction totale ou partielle sur queique support que ce soil ou ubisation du contenu de ce document est interdite sans l'autorisation écrite préalable du CEA 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

Ciet & Joye Algorithm

Input: \dot{m} , {p, q, d_p , d_q] Output: $S = \dot{m}^d \mod N$ Parameters: κ , l

1. For two κ -bit random integers r_1 and r_2 (a) $p^* = r_1 \cdot p$, (b) $q^* = r_2 \cdot q$, (c) $l_{q^*} = (q^*)^{-1} \mod p^*$, (d) $N = p \cdot q$. 2. Compute (a) $S_{p^*} \equiv \dot{m}^{d_p} \mod p^*$ and $s_2 \equiv \dot{m}^{d_q} \mod \varphi(r_2) \mod r_2$, (b) $S_{q^*} \equiv \dot{m}^{d_q} \mod q^*$ and $s_1 \equiv \dot{m}^{d_p} \mod \varphi(r_1) \mod r_1$. 3. Compute $S^* \equiv S_{q^*} + q^* \cdot i_{q^*} \cdot (S_{p^*} - S_{q^*}) \mod p^*$ 4. Compute (a) $c_1 \equiv (S^* - s_1 + 1) \mod r_1$ (b) $c_2 \equiv (S^* - s_2 + 1) \mod r_2$. 5. For a *l*-bit integer r_3 , set $\gamma = \lfloor \frac{(r_3 \cdot c_1 + (2^l - r_3) \cdot c_2)}{2^l} \rfloor$ 6. Return $S \equiv (S^*)^{\gamma} \mod N$

DQC

CEA 2008. Tous droits réservés

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écrite préalable du CEA 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

Ciet & Joye Algorithm

Input: \dot{m} , {p, q, d_p , d_q] Output: $S = \dot{m}^d \mod N$ Parameters: κ , l

1. For two κ -bit random integers r_1 and r_2 (a) $p^* = r_1 \cdot p$, (b) $q^* = r_2 \cdot q$, (c) $i_{q^*} = (q^*)^{-1} \mod p^*$, (d) $N = p \cdot q$. 2. Compute (a) $S_{p^*}^* \equiv \dot{m}^{d_p} \mod p^*$ and $s_2 \equiv \dot{m}^{d_p} \mod \varphi(r_2) \mod r_2$, (b) $S_{q^*} \equiv \dot{m}^{d_p} \mod q^*$ and $s_1 \equiv \dot{m}^{d_p} \mod \varphi(r_1) \mod r_1$. 3. Compute $S^* \equiv S_{q^*} + q^* \cdot i_{q^*} \cdot (S_{p^*} - S_{q^*}) \mod p^*$ 4. Compute (a) $c_1 \equiv (S^* - s_1 + 1) \mod r_1$ (b) $c_2 \equiv (S^* - s_2 + 1) \mod r_2$ 5. For a *l*-bit integer r_3 , set $\gamma = \lfloor \frac{(r_3 \cdot c_1 + (2^l - r_3) \cdot c_2)}{2^l} \rfloor$ 6. Return $S \equiv (S^*)^{\gamma} \mod N$

CEA 2008. Tous droits réservés

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écrite préalable du CEA 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

Ciet & Joye Algorithm

Input: \dot{m} , {p, q, d_p , d_q] Output: $S = \dot{m}^d \mod N$ Parameters: κ , l

1. For two κ -bit random integers r_1 and r_2 (a) $p^* = r_1 \cdot p$, (b) $q^* = r_2 \cdot q$, (c) $i_{q^*} = (q^*)^{-1} \mod p^*$, (d) $N = p \cdot q$. 2. Compute (a) $\hat{S_{p^*}} \equiv \dot{m}^{d_p} \mod p^*$ and $s_2 \equiv \dot{m}^{d_q} \mod \varphi(r_2) \mod r_2$, (b) $S_{q^*} \equiv \dot{m}^{d_q} \mod q^*$ and $s_1 \equiv \dot{m}^{d_p} \mod \varphi(r_1) \mod r_1$. 3. Compute $\hat{S^*} \equiv S_{q^*} + q^* \cdot i_{q^*} \cdot (\hat{S_{p^*}} - S_{q^*}) \mod p^*$ 4. Compute (a) $c_1 \equiv (S^* - s_1 + 1) \mod r_1$ (b) $c_2 \equiv (S^* - s_2 + 1) \mod r_2$ 5. For a *l*-bit integer r_3 , set $\gamma = \lfloor \frac{(r_3 \cdot c_1 + (2^l - r_3) \cdot c_2)}{2^l} \rfloor$ 6. Return $S \equiv (S^*)^{\gamma} \mod N$

4) Q (4

CEA 2008. Tous droits réservés

oute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écrite préalable du CEA Il 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

Ciet & Joye Algorithm

Input: \dot{m} , {p, q, d_p , d_q] Output: $S = \dot{m}^d \mod N$ Parameters: κ , l

1. For two κ -bit random integers r_1 and r_2 (a) $p^* = r_1 \cdot p$, (b) $q^* = r_2 \cdot q$, (c) $l_{q^*} = (q^*)^{-1} \mod p^*$, (d) $N = p \cdot q$. 2. Compute (a) $\hat{S_{p^*}} \equiv \dot{m}^{d_p} \mod p^*$ and $s_2 \equiv \dot{m}^{d_q} \mod \varphi(r_2) \mod r_2$, (b) $S_{q^*} \equiv \dot{m}^{d_q} \mod q^*$ and $s_1 \equiv \dot{m}^{d_p} \mod \varphi(r_1) \mod r_1$. 3. Compute $\hat{S^*} \equiv S_{q^*} + q^* \cdot i_{q^*} \cdot (\hat{S_{p^*}} - S_{q^*}) \mod p^*$ 4. Compute (a) $\hat{c_1} \equiv (\hat{S^*} - s_1 + 1) \mod r_1$ (b) $c_2 \equiv (\hat{S^*} - s_2 + 1) \mod r_2$ 5. For a *l*-bit integer r_3 , set $\gamma = \lfloor \frac{(r_3 \cdot c_1 + (2^l - r_3) \cdot c_2)}{2^l} \rfloor$ 6. Return $S \equiv (S^*)^{\gamma} \mod N$

CEA 2008. Tous droits réservés

sute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écrite préatable du CEA I 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

Ciet & Joye Algorithm

Input: $\dot{m}, \{p, q, d_p, d_q\}$ Output: $S = \dot{m}^d \mod N$ Parameters: κ, l

1. For two κ -bit random integers r_1 and r_2 (a) $p^* = r_1 \cdot p$, (b) $q^* = r_2 \cdot q$, (c) $l_{q^*} = (q^*)^{-1} \mod p^*$, (d) $N = p \cdot q$. 2. Compute (a) $\hat{S_{p^*}} \equiv \dot{m}^{d_p} \mod p^*$ and $s_2 \equiv \dot{m}^{d_q} \mod \varphi(r_2) \mod r_2$, (b) $S_{q^*} \equiv \dot{m}^{d_q} \mod q^*$ and $s_1 \equiv \dot{m}^{d_p} \mod \varphi(r_1) \mod r_1$. 3. Compute $\hat{S^*} \equiv S_{q^*} + q^* \cdot i_{q^*} \cdot (\hat{S_{p^*}} - S_{q^*}) \mod p^*$ 4. Compute (a) $\hat{c_1} \equiv (\hat{S^*} - s_1 + 1) \mod r_1$ (b) $c_2 \equiv (\hat{S^*} - s_2 + 1) \mod r_2$ 5. For a *l*-bit integer r_3 , set $\hat{\gamma} = \lfloor \frac{(r_3 \cdot \hat{c_1} + (2^l - r_3) \cdot c_2)}{2^l} \rfloor$ 6. Return $S \equiv (S^*)^{\gamma} \mod N$

CEA 2008. Tous droits réservés.

sute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écrite préatable du CEA I 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

Ciet & Joye Algorithm

Input: $\dot{m}, \{p, q, d_p, d_q\}$ Output: $S = \dot{m}^d \mod N$ Parameters: κ, l

1. For two κ -bit random integers r_1 and r_2 (a) $p^* = r_1 \cdot p$, (b) $q^* = r_2 \cdot q$, (c) $l_{q^*} = (q^*)^{-1} \mod p^*$, (d) $N = p \cdot q$. 2. Compute (a) $\hat{S_{p^*}} \equiv \dot{m}^{d_p} \mod p^*$ and $s_2 \equiv \dot{m}^{d_q} \mod \varphi^{(r_2)} \mod r_2$, (b) $S_{q^*} \equiv \dot{m}^{d_q} \mod q^*$ and $s_1 \equiv \dot{m}^{d_p} \mod \varphi^{(r_1)} \mod r_1$. 3. Compute $\hat{S^*} \equiv S_{q^*} + q^* \cdot i_{q^*} \cdot (\hat{S_{p^*}} - S_{q^*}) \mod p^*$ 4. Compute (a) $\hat{c_1} \equiv (\hat{S^*} - s_1 + 1) \mod r_1$ (b) $c_2 \equiv (\hat{S^*} - s_2 + 1) \mod r_2$ 5. For a *l*-bit integer r_3 , set $\hat{\gamma} = \lfloor \frac{(r_3 \cdot c_1 + (2^l - r_3) \cdot c_2)}{2^l} \rfloor$ 6. Return $\hat{S} \equiv (\hat{S^*})^{\hat{\gamma}} \mod N$

CEA 2008. Tous droits réservés

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écrite préalable du CEA 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

Introduction

- Previous work
- Overview of our attack

2 Attack principle

- Ciet & Joye Countermeasure
- Fault Model
- Faulty Execution
- Fault Analysis



© CEA 2008. Tous droits réservés

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écrite préalable du CEA 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



Consequences of the fault

The faulty result $\hat{S_{p*}}$ has been modeled as:

$$\hat{S_{p^*}} = S_{p^*} \oplus R_8 \cdot 2^{8i}$$



CEA 2008. Tous droits réservés.

Toute reproduction totale ou partielle sur quelque support que ce soil ou utilisation du contenu de ce document est interdite sans l'autorisation écnte préalable du CEA 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



Consequences of the fault

The faulty result $\hat{S_{p^*}}$ has been modeled as:

$$\hat{S_{p^*}} = S_{p^*} \oplus R_8 \cdot 2^{8i}$$

Then, the fault infects the check values:

$$\begin{aligned} \hat{c}_1 &\equiv (\hat{S^*} - s_1 + 1) \mod r_1 \\ &\equiv 1 + R_8 \cdot 2^{8i} \mod r_1 \\ &\approx 1 + R_8 \cdot 2^{8i} \\ c_2 &\equiv (\hat{S^*} - s_2 + 1) \mod r_2 \\ &\equiv 1 \mod r_2 \end{aligned}$$

< 回
 < 回

© CEA 2008. Tous droits réservés

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écnte préalable du CEA 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



Consequences of the fault

The faulty result $\hat{S_{p^*}}$ has been modeled as:

$$\hat{S_{p^*}} = S_{p^*} \oplus R_8 \cdot 2^{8i}$$

Then, the fault infects the check values:

$$\begin{aligned} \hat{c_1} &\equiv (\hat{S^*} - s_1 + 1) \mod r_1 \\ &\equiv 1 + R_8 \cdot 2^{8i} \mod r_1 \\ &\approx 1 + R_8 \cdot 2^{8i} \\ c_2 &\equiv (\hat{S^*} - s_2 + 1) \mod r_2 \\ &\equiv 1 \mod r_2 \end{aligned}$$

So, the erroneous exponent $\hat{\gamma}$ can be written as:

$$\hat{\boldsymbol{\gamma}} = \lfloor \frac{(\boldsymbol{r}_3 \cdot \hat{\boldsymbol{c}}_1 + (2^l - \boldsymbol{r}_3) \cdot \boldsymbol{c}_2)}{2^l} \rfloor$$
$$= \lfloor \frac{\boldsymbol{R}_3 \cdot \boldsymbol{r}_3 \cdot 2^{8l}}{2^l} \rfloor + 1$$

© CEA 2008. Tous droits réservés

oute reproduction totale ou partielle sur quelque support que ce soit ou ubisation du contenu de ce document est interdite sans l'autorisation écrite préalable du CE Il 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 CE



Bit distribution of $R_8 \cdot r_3 \cdot 2^{8i}$

0	0	0 R ₈ ·r ₃	R _{8'} r ₃ ()	0	0
$\kappa + \ell$	l	+8i+8	8i			0



CEA 2008. Tous droits réservés.

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est intercitie sans l'autorisation écnte préatable du CEA 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



Bit distribution of $R_8 \cdot r_3 \cdot 2^{8i}$

	0	0		0	R _{8'} r₃		 	R _{8'} r ₃	0	 -	0	0
κ+	·l		1	l+8	8i+8	;		8	i			(

Result of the right shift by *I* bits if I > 8i:

0 0	0 R ₈ r ₃	R ₈ r ₃ 0	0 0
$\kappa + \ell$	$\ell + 8i + 8$	8i	0



CEA 2008. Tous droits réservés

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écnte préatable du CEA 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

Bit distribution of $R_8 \cdot r_3 \cdot 2^{8i}$

	0	0	 0	R _{8'} r₃		 	R _a r _a	0	 	0	0	
κ+	٠l		l+1	8i+8	;		8	i			()

Result of the right shift by *I* bits if I > 8i:





CEA 2008. Tous droits réservés

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écnte préatable du CEA 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

Bit distribution of $R_8 \cdot r_3 \cdot 2^{8i}$

	0	0	 0	R _{8'} r₃		R _{8'} r ₃	0	 0	0
κ+	٠l		l+1	8i+8	;	8	i		0

Result of the right shift by *I* bits if I > 8i:





© CEA 2008. Tous droits réservés

Toule reproduction totale ou partielle sur queique support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation échte préalable du CEA 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





	0	0	 0	R ₈ ∙r ₃		 R _{a'} r _a	0	 0	0
κ +	l		l+8	3i+8	3	8	i		0

Result of the right shift by *I* bits if I > 8i:



Result of the right shift by *I* bits if I < 8i and $I < \kappa$:

> © CEA 2008. Tous droits réservés locument est intercite sans l'autorisation écrite mégable du CEA

∢ ≣ ≯

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écrite préalable du CE. 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 CE.





© CEA 2008. Tous droits réservés duction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interda sans fautoristion échie présibile du CEA avect Any reproduction in white or in port on any medium or use of the information contained herein is rombited without the noncorrect of CEA.

∢ ≣ ≯





© CEA 2008. Tous droits réservés. e reproduction totale ou partielle sur quelque support que ce soit ou util sation du contenu de ce document est interda sans faultonsation écrite presideble du CEA pris reserved. Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the ency written consect of CEA

< ≣≯ < ≣≯





 $\Rightarrow \hat{\gamma}$ is a random value located on LSB or MSB.

CEA 2008. Tous droits réservés

< ≣≯ < ≣≯

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écrite préalable du CEA 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

First, one can advantageously notice that:

$$\hat{S}^{e} \mod N = \dot{m}^{d \cdot e \cdot \hat{\gamma}} \mod N$$
$$= \dot{m}^{\hat{\gamma}} \mod N$$

CEA 2008. Tous droits réservés.

Toute reproduction totale ou partielle sur quelque support que ce soil ou utilisation du contenu de ce document est interdite sans l'autorisation écnte préalable du CEA 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



First, one can advantageously notice that:

$$\hat{S}^{e} \mod N = \dot{m}^{d \cdot e \cdot \hat{\gamma}} \mod N$$
$$= \dot{m}^{\hat{\gamma}} \mod N$$

Then, the attacker tries to find $\hat{\gamma}$'s value to factorize the public modulus N



© CEA 2008. Tous droits réservés

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écnite préatable du CEA 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



First, one can advantageously notice that:

$$\hat{S}^{e} \mod N = \dot{m}^{d \cdot e \cdot \hat{\gamma}} \mod N$$
$$= \dot{m}^{\hat{\gamma}} \mod N$$

\blacksquare Then, the attacker tries to find $\hat{\gamma}$'s value to factorize the public modulus N

Attack algorithm

- 1. The attacker chooses a candidate value for $\hat{\gamma}$
- 2. The attacker computes:

$$q' = gcd\left((\hat{\mathbf{S}}^e - \dot{m}^{\hat{\mathbf{\gamma}}}) \mod N, N
ight)$$

3. Hence,

(a) if q' = 1, then the attacker tries again for another candidate, (b) $q' \neq 1$, then q' is a prime factor of N.

< ⊒⇒

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écrite préalable du CEA 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

Success probability for a fault that suits the model

$$\begin{aligned} \mathbf{Pr}(\text{success}) &= \mathbf{Pr} \left[\hat{c}_1 \approx 1 + R_8 \cdot 2^{8i} \, \& \, \hat{\gamma} \text{ is recoverable by brute force} \right] \\ &= \mathbf{Pr} \left[1 + R_8 \cdot 2^{8i} < r_1 \, \& \, \textit{length}(\hat{\gamma}) < B_f \right] \end{aligned}$$

CEA 2008. Tous droits réservés. Toute reproduction totale ou partielle sur quelque support que ce soit ou ubisation du contenu de ce document est intertois ans fautorisation échies préalable du CEA.

Leti

Success probability for a fault that suits the model

$$\begin{aligned} \mathbf{Pr}(\text{success}) &= \mathbf{Pr} \left[\hat{c}_1 \approx 1 + R_8 \cdot 2^{8i} \, \& \, \hat{\gamma} \text{ is recoverable by brute force} \right] \\ &= \mathbf{Pr} \left[1 + R_8 \cdot 2^{8i} < r_1 \, \& \, \textit{length}(\hat{\gamma}) < B_f \right] \end{aligned}$$

For n = 1024 bits, $\kappa = l = 80$ bits and $B_f = 40$ bits



CEA 2008. Tous droits réservés

Toute reproduction totale ou partielle sur quelque support que ce soil ou utilisation du contenu de ce document est interdite sans l'autorisation écnte préalable du CEA 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

letī

CEA LETI

Success probability for a fault that suits the model

$$\begin{aligned} \mathbf{Pr}(\text{success}) &= \mathbf{Pr} \left[\hat{c}_1 \approx 1 + R_8 \cdot 2^{8i} \, \& \, \hat{\gamma} \text{ is recoverable by brute force} \right] \\ &= \mathbf{Pr} \left[1 + R_8 \cdot 2^{8i} < r_1 \, \& \, \textit{length}(\hat{\gamma}) < B_f \right] \end{aligned}$$

For n = 1024 bits, $\kappa = l = 80$ bits and $B_f = 40$ bits • **Pr**(success) $\approx 5.4\%$ for a suitable fault

© CEA 2008. Tous droits réservés

Toute reproduction totale ou partielle sur quelque support que ce soil ou utilisation du contenu de ce document est interdite sans l'autorisation écnte préalable du CEA 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

leti

CEA LETI

Success probability for a fault that suits the model

$$\begin{aligned} \mathbf{Pr}(\text{success}) &= \mathbf{Pr} \left[\hat{c}_1 \approx 1 + R_8 \cdot 2^{8i} \, \mathbf{\&} \, \hat{\gamma} \text{ is recoverable by brute force} \right] \\ &= \mathbf{Pr} \left[1 + R_8 \cdot 2^{8i} < r_1 \, \mathbf{\&} \, \textit{length}(\hat{\gamma}) < B_f \right] \end{aligned}$$

For n = 1024 bits, $\kappa = l = 80$ bits and $B_f = 40$ bits

- $\Pr(\text{success}) \approx 5,4\%$ for a suitable fault
- The success probability increases by lengthening the brute force search

CEA 2008. Tous droits réservés

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écnte préalable du CEA 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

leti

GEALENI

Success probability for a fault that suits the model

$$\begin{aligned} \mathbf{Pr}(\text{success}) &= \mathbf{Pr} \left[\hat{c}_1 \approx 1 + R_8 \cdot 2^{8i} \, \mathbf{\&} \, \hat{\gamma} \text{ is recoverable by brute force} \right] \\ &= \mathbf{Pr} \left[1 + R_8 \cdot 2^{8i} < r_1 \, \mathbf{\&} \, \textit{length}(\hat{\gamma}) < B_f \right] \end{aligned}$$

For n = 1024 bits, $\kappa = I = 80$ bits and $B_f = 40$ bits

- $\Pr(\text{success}) \approx 5,4\%$ for a suitable fault
- The success probability increases by lengthening the brute force search



Leti



-

Conclusion

The proposed fault model can be extended to a less restrictive one



© CEA 2008. Tous droits réservés.

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écnte préatable du CEA 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



The proposed fault model can be extended to a less restrictive one

The attack has been extensively simulated using GMP Library



© CEA 2008. Tous droits réservés

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est intercitie sans l'autorisation écnte préatable du CEA 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



The proposed fault model can be extended to a less restrictive one

The attack has been extensively simulated using GMP Library

This attack works against a protected CRT-RSA implementation ...



© CEA 2008. Tous droits réservés. In totale ou partielle sur queique support que ce soit ou útisation du contenu de ce document est interdite anne administration échile anne ad the information excitation during the substitution and the second of CEA



The proposed fault model can be extended to a less restrictive one

The attack has been extensively simulated using GMP Library

This attack works against a protected CRT-RSA implementation ...

... but it can be avoided by

• Forcing the modular reduction during $\hat{c_1}$ computation

CEA 2008. Tous droits réservés

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans fautorisation écnte préatable du CE/ 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 consert of CE/



The proposed fault model can be extended to a less restrictive one

The attack has been extensively simulated using GMP Library

This attack works against a protected CRT-RSA implementation ...

... but it can be avoided by

- Forcing the modular reduction during $\hat{c_1}$ computation
- Replacing the final step by the proposed variant and returning

$$S = (\gamma \cdot S^* \oplus (\gamma - 1) \cdot r)$$

Practical Fault Countermeasures for Chinese Remaindering Based RSA (JC05), $_{\rm FDTC}$ 2005 $_{\rm CO5}$

CEA 2008. Tous droits réservés

э

Foute reproduction locale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écrite préalable du CE. Il 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 CE.



-

Conclusion

Thank you for your attention !



CEA 2008. Tous droits réservés.

≣⇒

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écnte préalable du CEA All rights reserved. Any reproduction in whote or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA