Physical Attacks against Cryptographic Implementations

Alexandre Berzati[1], Martin Gallezot[1], Alain Pomet[1]

INVIA, Arteparc Bat. D, Route de la Cote d'Azur, 13590 Meyreuil, France
{alexandre.berzati,martin.gallezot,alain.pomet}@invia.fr

1 Introduction

Since the advent of side channel attacks, classical cryptanalysis is no longer sufficient to ensure the security of cryptographic algorithms. In practice, the implementation of algorithms on electronic devices is a potential source of leakage that an attacker can use to completely break a system [KJJ99,BB03,GMO01]. The injection of faults during the execution of cryptographic algorithm is considered as an intrusive side channel method because secret information may leak from malicious modifications of the device's behavior [BDL97,BDL01,BS97]. In this context, the security of public key cryptosystems [BDL97,BDL01] and symmetric ciphers in both block [BS97] and stream modes [HS04] has been challenged. In this context, finding efficient countermeasures for cryptosystems against fault attacks is challenged by a constant discovery of flaws in designs. Even elements, such as public keys, that do not seem critical must be protected against physical attacks [BMM00,BCMCC06,KBPJJ08]. In this paper, we propose to distinguish potential source of leakage in designs that may lead to critical security flaws, even using provably secured cryptographic algorithms.
The rest of the paper is organized as follow. The example presented in Section 2 highlights the need for protecting both hardware and software against physical attacks. The Section 3 describes the different source of physical leakage referenced in the literature that must be considered as potential threats when designing secured systems.

2 A proof-of-concept example

Since its invention in 1977, the celebrated RSA primitive has remained unbroken from a mathematical point of view, and has been widely used to build provably secure encryption or signature protocols. However, the introduction in 1996 of a new model of attacks – based on fault injections – by Boneh, deMillo and Lipton suggests the use of specific countermeasures to obtain a secure RSA implementation. In the special case of CRT implementations – that is widely deployed in smart card industry – many protections have been proposed and most of them have been proven insufficient to ensure resistance against physical attacks and particularly fault injection attacks.

2.1 Description of CRT-RSA implementations

Standard RSA. Let N, the public modulus, be the product of two large prime numbers p and q. The length of N is denoted by n. Let e be the public exponent, coprime to $\varphi(N) = (p-1)\cdot(q-1)$, where $\varphi(\cdot)$ denotes Euler's totient function. The public key exponent e is linked to the private exponent d by the equation $e \cdot d \equiv 1 \bmod \varphi(N)$. The private exponent d is used to perform the following operations:

RSA Decryption: Decrypting a ciphertext C boils down to compute $\tilde{m} \equiv C^d \bmod N \equiv C^{\sum_{i=0}^{i=n-1} 2^i \cdot d_i} \bmod N$ where d_i stands for the i-th bit of d. If no error occurs during computation, transmission or decryption of C, then $\tilde{m}$ equals m.

RSA Signature: The signature of a message m is given by $S = \dot{m}^d \bmod N$ where $\dot{m} = \mu(m)$ for some hash and/or deterministic padding function μ. The signature S is validated by checking that $S^e \equiv \dot{m} \bmod N$.

CRT Optimization. The improvement brought by the Chinese Remainder Theorem concerns the computation of the modular exponentiation. In CRT mode, instead of computing the d-th exponentiation, two half exponentiations by $d_p \equiv d \bmod (p-1)$ and $d_q \equiv d \bmod (q-1)$ are done. Let $i_q \equiv q^{-1} \bmod p$ be the inverse of q in $\mathbb{Z}/p\mathbb{Z}$, the signature S is calculated with Garner's algorithm, denoted by CRT:

$$\begin{aligned} S &= \mathrm{CRT}(S_p, S_q) \\ &= S_q + q(i_q(S_p - S_q) \bmod p) \qquad (1) \\ \text{with} \quad &\begin{cases} S_p \equiv \dot{m}^{d_p} \bmod p, \\ S_q \equiv \dot{m}^{d_q} \bmod q. \end{cases} \end{aligned}$$

This trick speeds up the computation by computing two half exponentiations modulo a $n/2$-bit number instead of an exponentiation modulo a n-bit number. Because of the multiplication's quadratic complexity, the CRT computation is four times faster than the standard one. In both modes, the signature S is validated by checking if:

$$S^e \equiv \dot{m} \bmod N \qquad (2)$$

For performance purpose, this particular implementation of RSA is widely deployed on secured embedded systems such as smart cards. Even if these operations are totally secured in a mathematical point of view, the next chapter will show that extending the security of this secured protocol to an entire system (e.g.the combination of a smart card and a cryptographic algorithm) is not so straightforward.

2.2 How to exploit faulty computations

Bellcore's attack. In 1996, Bellcore researchers introduced the Differential Fault Analysis (DFA) by attacking the CRT based implementation of RSA. The principle is to induce malicious faults during the execution of the RSA and exploit the faulty result to recover secret information. They showed in [BDL97,BDL01] that if an error occurs while computing one of the two half exponentiations (*i.e.* S_p or S_q but not both) then, from the faulty signature $\hat{S}$ and the correct one S, it is possible to factor N. Indeed, assume that an error was provoked during the computation of S_p resulting in a faulty value $\hat{S_p}$, then the signature $\hat{S} = \text{CRT}(\hat{S_p}, S_q)$ is faulty too. Moreover, $\hat{S} \equiv S \bmod q$ but $\hat{S} \not\equiv S \bmod p$. So, only $q \mid (\hat{S} - S)$ and:

$$q = gcd((\hat{S} - S) \bmod N, N) \tag{3}$$

This result was reduced to the mere knowledge of the faulty signature by A. Lenstra [JLQ99], noticing that $\hat{S}^e \equiv \dot{m} \bmod q$ but $\hat{S}^e \not\equiv \dot{m} \bmod p$:

$$q = gcd((\hat{S}^e - \dot{m}) \bmod N, N) \tag{4}$$

Possible Countermeasure. The difficulty for designing efficient countermeasures does not rely only on the attack model to defeat. Indeed, a well-designed countermeasure has to provide a high security level but also reasonable performance. In that sense, computing twice an RSA signature cannot be considered as an efficient countermeasure. In [Sha97], A. Shamir presents a method to defeat DFA by randomizing the computation of S_p and S_q and adding a checking test before returning the signature. Let r be a κ-bit random value. The cryptographic device computes:

$$\begin{cases} S_{rp} \equiv \dot{m}^d \bmod (r \cdot p) \\ S_{rq} \equiv \dot{m}^d \bmod (r \cdot q) \end{cases} \tag{5}$$

Then, we check that no error occurs during the computation of the two half exponentiations:

1. **If** $S_{rp} \equiv S_{rq} \bmod r$, **return** $S = \text{CRT}(S_{rp}, S_{rq})$,
2. **Else**, **return** `Error detected`.

The main drawback of this method is that it requires the knowledge of d whereas, on a real cryptographic device that implements CRT-RSA, only $d_p \equiv d \bmod (p-1)$ and $d_q \equiv d \bmod (q-1)$ are available. That is why M. Joye, P. Paillier and S. Yen have proposed in [JPY01] an optimization of Shamir's countermeasure. Let r_1 and r_2 be two κ-bit random integers. The device computes:

$$\begin{aligned} S_p^* &\equiv \dot{m}^{d_p} \bmod (r_1 \cdot p),\ S_1 \equiv \dot{m}^{d_p \bmod \varphi(r_1)} \bmod r_1 \\ S_q^* &\equiv \dot{m}^{d_q} \bmod (r_2 \cdot q),\ S_2 \equiv \dot{m}^{d_q \bmod \varphi(r_2)} \bmod r_2 \end{aligned} \tag{6}$$

Both half exponentiations are checked separately before the CRT recombination:

1. **If** $S_1 \equiv S_p^* \bmod r_1$ **and** $S_2 \equiv S_q^* \bmod r_2$, **return** $S = \text{CRT}(S_p^*, S_q^*)$,
2. **Else**, **return** `Error detected`.

Thus, this optimization is resistant to fault injection during the two half exponentiations and only needs classical CRT parameters. Unfortunately, this countermeasure has been also broken by further attacks [ABF$^+$02] and many software architecture for protecting CRT-RSA implementations against faults have been proposed [YKLM01,BOS03].

3 Classification of Side-Channel Attacks against Cryptographic Implementations

In this context, new cryptanalytic attacks become possible which are known as physical cryptanalysis. Physical cryptanalysis includes two main families of attacks: side channel analysis and fault analysis. Side channel attacks exploit the physical leakage of the cryptographic computation. This leakage provides sensitive information that often makes it possible to recover the secret key even though the cryptosystem is proven secure. Regarding fault attacks, they consist in disrupting the cryptographic computation so that it produces erroneous results. These erroneous results are then analyzed in order to deduce information about the secret key.

Physical attacks performed against smart cards – or any secured embedded system – can further be divided into different categories depending on how they affect the physical integrity of the card:

3.1 Invasive Attacks

In this family of threat, the attacker is supposed to have a total physical control of the system to break. For instance, a smart card can be depackaged in order to extract its microchip. This enables probing attacks that directly examine the content of ROM or EEPROM or that spy the memory bus during a computation as well as destructive attacks that remove or modify some elements of the chip. Such attacks are complicated to mount in practice and require high-tech microelectronic equipment.

3.2 Semi-Invasive Attacks

In this model the attacker is supposed to have only a limited physical control of the system to break. The depackaging of the card can be used to facilitate physical cryptanalysis. It is in particular necessary to measure the electromagnetic radiations produced by the chip [GMO01,QS02] as well as to induce errors via light pulses [SA02]. For such a purpose, a partial depackaging may suffice to expose the chip without altering its integrity. These attacks requires less privileges than *invasive attacks* but quite expensive equipments.

3.3 Non-Invasive Attacks

Altering the physical integrity of the card is not mandatory for physical cryptanalysis. In particular, measuring the power consumption [KJJ99]. Hence, the well known Simple/Differential Power Analysis – that allows the attacker to retrieve secret informations from single/multiple power traces – can be considered as Non-Invasive Attacks. Moreover injecting faults using the malicious variation of a card input signals such as power and clock glitches [BS97] are non-invasive attacks. This attack model is the most powerful since the privileges given to the attacker are quite limited and that attack can be mount with an affordable high-tech microelectronic equipment.

4 Conclusion

References

[ABF$^+$02] C. Aumüler, P. Bier, W. Fischer, P. Hofreiter, and J.-P. Seifert. Fault Attack on RSA with CRT : Concrete Results and Practical Countermeasures. In B.S. Kaliski Jr., Ç.K. Koç, and C. Parr, editors, *Cryptographic Hardware and Embedded Systems (CHES 2002)*, volume 2523 of *Lecture Notes in Computer Science*, pages 260–275. Springer, 2002.

[BB03] D. Brumley and D. Boneh. Remote Timing Attacks are Practical. In *12th Usenix Security Symposium*, pages 1–14, 2003.

[BCMCC06] E. Brier, B. Chevallier-Mames, M. Ciet, and C. Clavier. Why One Should Also Secure RSA Public Key Elements. In L. Goubin and M. Matsui, editors, *Cryptographic Hardware and Embedded Systems (CHES 2006)*, volume 4249 of *Lecture Notes in Computer Science*, pages 324–338. Springer-Verlag, 2006.

[BDL97] D. Boneh, R.A. DeMillo, and R.J. Lipton. On the Importance of Checking Cryptographic Protocols for Faults. In W. Fumy, editor, *EUROCRYPT'97*, volume 1233 of *Lecture Notes in Computer Science*, pages 37–51. Springer-Verlag, 1997.

[BDL01] D. Boneh, R.A. DeMillo, and R.J. Lipton. "On the Importance of Eliminating Errors in Cryptographic Computations". *Journal of Cryptology*, 14(2):101–119, 2001.

[BMM00] I. Biehl, B. Meyer, and V. Müller. Differential Fault Attacks on Ellitic Curve Cryptosystems. In M. Bellare, editor, *Advances in Cryptology (CRYPTO 2000)*, volume 1880 of *Lecture Notes in Computer Science*, pages 131–146. Springer-Verlag, 2000.

[BOS03] J. Blömer, M. Otto, and J.-P. Seifert. A New CRT-RSA Algorithm Secure Against Bellcore Attack. In *ACM Conference on Computer and Communication Security (CCS 2003)*, pages 311–320. ACM Press, 2003.

[BS97] E. Biham and A. Shamir. Differential Fault Analysis of Secret Key Cryptosystems. In *Advances in Cryptology (CRYPTO 1997)*, 1997.

[GMO01] K. Gandolfi, C. Mourtel, and F. Olivier. Electormagnetic Analysis: Concrete Results. In *Cryptographic Hardware and Embedded Systems (CHES 2001)*, volume 2162, pages 251–261. Springer-Verlag, 2001.

[HS04] J. Hoch and A. Shamir. Fault Analysis of Stream Ciphers. In M. Joye and J.-J. Quisquater, editors, *Cryptographic Hardware and Embedded Systems (CHES 2004)*, volume 3156 of *Lecture Notes in Computer Science*, pages 240–253. Springer, 2004.

[JLQ99] M. Joye, A. Lenstra, and J.-J. Quisquater. "Chinese Remaindering Based Cryptosystems in the Presence of Faults". *Journal of Cryptology*, 12(4):241–245, 1999.

[JPY01] M. Joye, P. Paillier, and S.-M. Yen. Secure Evaluation of Modular Functions. In R.J. Hwang and C.K. Wu, editors, *2001 International Workshop on Cryptology and Network Security*, pages 227–229, Taipei,Taiwan, 2001.

[KBPJJ08] C.H. Kim, P. Bulens, C. Petit, and J.-J.Quisquater. Fault Attaks on Public Key Elements: Application to DLP-Based Schemes. In S. F. Mjölsnes, S. Mauw, and S. K. Katsikas, editors, *European PKI workshop Public Key Infrastructure (EuroPKI 2008)*, volume 5057 of *Lecture Notes In Computer Science*, pages 182–195. Springer, 2008.

[KJJ99] P. Kocher, J. Jaffe, and B. Jun. Differential Power Analysis. In *Advances in Cryptology (CRYPTO 1999)*, volume 1666, pages 388–397. Springer-Verlag, 1999.

[QS02] J.-J. Quisquater and D. Samyde. Eddy Current for Magnetic Analysis with Active Sensor. In *e-Smart 2002*, 2002.

[SA02] S.P. Skorobogatov and R.J. Anderson. Optical Fault Induction Attacks. In B.S. Kaliski Jr., Ç.K. Koç, and C. Parr, editors, *Cryptographic Hardware and Embedded Systems (CHES 2002)*, volume 2523 of *Lecture Notes in Computer Science*, pages 2–12. Springer-Verlag, 2002.

[Sha97] A. Shamir. "Improved Method and Apparatus for Protecting Public Key Schemes from Timing and Fault Attacks". *Presented at the Rump Session of Eurocrypt'97*, 1997.

[YKLM01] S.-M. Yen, D. Kim, S. Lim, and S. Moon. RSA Speedup with Residue Number System Immune Against Hardware Fault Cryptanalysis. In K. Kim, editor, *Information Security and Cryptology (ICISC 2001)*, volume 2288 of *Lecture Notes in Computer Science*, pages 397–413. Springer-Verlag, 2001.