Published in *Journal of Cryptology* **12(4):241–245, 1999.**

Chinese Remaindering Based Cryptosystems in the Presence of Faults

Marc Joye
UCL Crypto Group, Dép. de Mathématique, Université de Louvain
Chemin du Cyclotron, 2, B-1348 Louvain-la-Neuve, Belgium
mjoye@geocities.com

Arjen K. Lenstra
Citibank, N.A.
4 Sylvan Way, Parsippany, NJ 07054, U.S.A.
arjen.lenstra@citicorp.com

Jean-Jacques Quisquater
UCL Crypto Group, Lab. de Microélectronique, Université de Louvain
Place du Levant, 3, B-1348 Louvain-la-Neuve, Belgium
jjq@dice.ucl.ac.be

Abstract. We present some observations on public-key cryptosystems that use the Chinese remaindering algorithm. Our results imply that careless implementations of such systems could be vulnerable. Only one faulty signature, in some explained context, is enough to recover the secret key.

Key words. Public-key cryptosystems, Faulty computations, Chinese remaindering.

1. Introduction

In public-key cryptosystems two distinct computations can be distinguished: the computation that makes use of the secret, public key pair, and the one that only makes use of the public key. The former usually corresponds to the secret decryption or to the signature generation operation, the latter to the public encryption or to the signature verification operation. In this paper we restrict our attention to public key cryptosystems in which the former computation can be sped up using the Chinese remaindering algorithm. Examples of such cryptosystems are: RSA [16], LUC [19], KMOV [11], and Demytko's cryptosystem [6]. We show that devices implementing the signature generation of any of these cryptosystems may be tricked into revealing their secret key, if the following three conditions are met:

(1) the message as signed is known;

(2) a certain type of faulty behavior occurs during signature generation;

(3) the device outputs the faulty signature.

Leakage of the secret key can be averted by making sure that either of these three conditions will not be met. This can be done by adding enough random noise to the message to be signed, by making sure that the system works properly and that faulty behavior cannot be induced, by checking the correctness of the signature before outputting it, or by any combination of these three safety measures. We note that many devices already implement at least one of these countermeasures. Thus we feel confident that the practical impact of our observation is minimal. Therefore, if carefully implemented, Chinese remaindering based cryptosystems are not more vulnerable than usual cryptosystems.

We note that the same observation applies to decryption using the Chinese remaindering algorithm, if the decrypting party shows the faulty decryption to another party. The details of this ‘generalization’ are straightforward.

The analysis of cryptosystems in the presence of faults was launched by newspaper publications that cited a Bellcore press release *New Threat Model Breaks Crypto Codes*. Thereafter, several researchers reported some possible implications in both public-key [12], [3], [8], [9], [17], [20] and private-key [4], [9], [13] cryptography. The method presented in this paper improves the Bellcore’s result, later published in [5], in the following way. Their method requires two ‘Chinese remaindering’ signatures on the same message, one correct and one faulty, whereas our version requires the message and only a single faulty signature. Our version is therefore ‘more realistic’ and potentially more dangerous.

The problem of the presence of faults in cryptosystems can be turned into an active attack by inducing faulty behavior on computational devices. For example, this can be achieved by ROM overwriting, EEPROM modification, gate destruction, RAM remanence, etc… [1], [2], [7], [10], [14], [15]. Since these techniques are not fully published or described (and thus controversial), we do not elaborate or comment.

Our main objective is to dwell on the importance of a careful implementation of cryptosystems. Suppose you are in a context involving Trusted Third Parties (e.g., banks) and where thousands of signatures are produced each day. If, for some reason or other, a single signature is faulty, then the security of the whole system may be compromised.

2. Potential vulnerability of RSA using Chinese remaindering

Let p and q be two primes and let $n = pq$. Imagine a message m is signed with the secret exponent d using RSA: $s = m^d \bmod n$. Using the Chinese remaindering theorem, the value of s can be computed more efficiently from $s_p = m^d \bmod p$ and $s_q = m^d \bmod q$. Suppose an error occurs during the computation of s_p (we denote s'_p the faulty value), but not during the computation of s_q. Applying Chinese remaindering on s'_p ($\neq s_p$) and s_q will give the faulty signature s' for message m. Then, the computation of

$$\gcd({s'}^e - m \pmod{n}, n)$$

will give the secret factor q, where e is the public exponent.

Remarks. 1) If the attacker does not know the public modulus n, he may still be able to recover the secret parameter q. Indeed, if e is small, he has some probability to find q by trying to factorize ${s'}^e - m$ over the rational integers. This probability becomes non negligible if he possesses two or several faulty signatures, because in that case, he can recover q by computing $\gcd({s'_1}^e - m_1, \ldots, {s'_k}^e - m_k)$. Furthermore, from the knowledge of one or several valid signatures, the attacker can also recover p in a similar way.

2) A non-trivial factor of n may be derived in any scenario were exactly one of the

remainders used in the Chinese remaindering is incorrect. This includes, for instance, incorrect retrieval of (a possibly correctly computed) s_p. Thus, also the presence of a permanent failure, like a damaged wire, as opposed to a transient computational failure, may expose secret information.

3. Generalization to other cryptosystems

In this section, $n = pq$ denotes the RSA-modulus, and e and d are respectively the public and the secret exponents. The message to be signed is m, and the corresponding signature is s. Let

$$\mathcal{S} : \mathbb{Z}_n \to \mathbb{Z}_n, m \mapsto s = \mathcal{S}(m)$$

be an RSA-type signature function. If the signature s of message m is computed with the Chinese remaindering theorem, then the previous observation still applies.

Proposition 1 *If s' is a faulty signature such that $s' \not\equiv s \pmod{p}$ but $s' \equiv s \pmod{q}$, then*

$$\gcd(\mathcal{S}^{-1}(s') - m, n)$$

will give the secret factor q.

Proof. Since $s' \equiv s \pmod{q}$ and $s' \not\equiv s \pmod{p}$, we have $\mathcal{S}^{-1}(s') \equiv \mathcal{S}^{-1}(s) \equiv m \pmod{q}$ and $\mathcal{S}^{-1}(s') \not\equiv m \pmod{p}$. Hence, $\mathcal{S}^{-1}(s') - m \pmod{n}$ is divisible by q and not by p. □

Consequently, the observation of Section 2 works for all RSA-type cryptosystems.

Example 1. The LUC cryptosystem is based on Lucas sequences. The signature function is defined as $\mathcal{S}(m) = V_d(m, 1) \bmod n$, and the verification function as $\mathcal{S}^{-1}(s) = V_e(m, 1) \bmod n$, where $ed \equiv 1 \pmod{\operatorname{lcm}(p-1, p+1, q-1, q+1)}$. If $s' \not\equiv s \pmod{p}$ but $s' \equiv s \pmod{q}$, then

$$\gcd(V_e(s', 1) - m \pmod{n}, n)$$

will give q.

Example 2. The Demytko cryptosystem uses the x-coordinate of points on elliptic curves over the ring $\mathbb{Z}_n$. Such a curve will be denoted by $E_n(a, b)$. The x-coordinate of the multiple of a point can be computed thanks to the division polynomials (see [18, exercice 3.7]) considered as polynomials in $\mathbb{Z}_n[a, b, x]$. The signature function is defined as $\mathcal{S}(m) = \Phi_d(m)/\Psi_d(m)^2 \bmod n$, and the verification function as $\mathcal{S}^{-1}(s) = \Phi_e(s)/\Psi_e(s)^2 \bmod n$, where $ed \equiv 1 \pmod{\operatorname{lcm}\big(\#E_p(a,b), \#E_q(a,b), \#\overline{E_p(a,b)}, \#\overline{E_q(a,b)}\big)}$.[1] If $s' \not\equiv s \pmod{p}$ but $s' \equiv s \pmod{q}$, then

$$\gcd\left(\frac{\Phi_e(s')}{\Psi_e(s')^2} - m \pmod{n}, n\right)$$

will give q.

[1] $\overline{E_p(a,b)}$ denotes the complementary group of $E_p(a, b)$. See the original paper [6] for a detailed description.

Acknowledgements

We thank François Koeune for some useful comments.

References

[1] R. Anderson and M. Kuhn. Tamper resistance—a cautionary note. In *Proceedings of the Second USENIX Workshop on Electronic Commerce*, pp. 1–11. USENIX Association, Berkeley, 1996.

[2] R. Anderson and M. Kuhn. Low cost attacks on tamper resistant devices. In B. Christianson, B. Crispo, M. Lomas, and M. Roe, editors, *Security Protocols*, pp. 125–136. Lecture Notes in Computer Science, vol. 1361. Springer-Verlag, Berlin, 1998.

[3] F. Bao, R. H. Deng, Y. Han, A. Jeng, A. D. Narasimhalu, and T. Ngair. Breaking public key cryptosystems on tamper resistant devices in the presence of transient faults. In B. Christianson, B. Crispo, M. Lomas, and M. Roe, editors, *Security Protocols*, pp. 115–124. Lecture Notes in Computer Science, vol. 1361. Springer-Verlag, Berlin, 1998.

[4] E. Biham and A. Shamir. Differential fault analysis of secret key cryptosystems. In B. S. Kaliski Jr., editor, *Advances in Cryptology – CRYPTO '97*, pp. 513–525. Lecture Notes in Computer Science, vol. 1294. Springer-Verlag, Berlin, 1997.

[5] D. Boneh, R. A. DeMillo, and R. J. Lipton. On the importance of checking cryptographic protocols for faults. In W. Fumy, editor, *Advances in Cryptology – EUROCRYPT '97*, pp. 37–51. Lecture Notes in Computer Science, vol. 1233. Springer-Verlag, Berlin, 1997.

[6] N. Demytko. A new elliptic curve based analogue of RSA. In T. Helleseth, editor, *Advances in Cryptology – EUROCRYPT '93*, pp. 40–49. Lecture Notes in Computer Science, vol. 765. Springer-Verlag, Berlin, 1994.

[7] P. Gutmann. Secure deletion of data from magnetic and solid-state memory. In *Proceedings of Sixth USENIX Security Symposium*, pp. 77–89. USENIX Association, Berkeley, 1996.

[8] M. Joye and J.-J. Quisquater. Attacks on systems using Chinese remaindering. Technical Report CG-1996/9, UCL Crypto Group, Louvain-la-Neuve, November 1996.

[9] B. S. Kaliski Jr and M. J. B. Robshaw. Comments on some attacks on cryptographic devices. RSA Laboratories' Bulletin, no. 5, RSA Laboratories, Redwood City, July 1997.

[10] O. Kocar. Hardwaresicherheit von Mikrochips in Chipkarten. *Datenschutz und Datensicherheit*, vol. 20, no. 7, pp. 421–424, July 1996.

[11] K. Koyama, U. M. Maurer, T. Okamoto, and S. A. Vanstone. New public-key schemes based on elliptic curves over the ring $\mathbb{Z}_n$. In J. Feigenbaum, editor, *Advances in Cryptology – CRYPTO '91*, pp. 252–266. Lecture Notes in Computer Science, vol. 576. Springer-Verlag, Berlin, 1992.

[12] A. K. Lenstra. RSA signature generation in the presence of faults. Memo, Parsippany, September 1996.

[13] P. Paillier. Real life DFA is inherently limited. Presented at the rump session of EUROCRYPT ’97, 11–15th May 1997, Konstanz.

[14] I. Peterson. Chinks in digital armor—Exploiting faults to break smart-card cryptosystems. *Science News*, vol. 151, no. 5, pp. 78–79, February 1997.

[15] J.-J. Quisquater. The adolescence of smart cards. *Future Generation Computer Systems*, vol. 13, no. 1, pp. 3–7, June 1997.

[16] R. L. Rivest, A. Shamir, and L. M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, February 1978.

[17] A. Shamir. How to check modular exponentiation. Presented at the rump session of EUROCRYPT ’97, 11–15th May 1997, Konstanz.

[18] J. H. Silverman. *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 106. Springer-Verlag, New York, 1986.

[19] P. J. Smith and M. J. J. Lennon. LUC: a new public key system. In E. G. Douglas, editor, *Proceedings of the Ninth IFIP Symposium on Computer Security*, pp. 103–117. Elsevier, Amsterdam, 1993.

[20] Y. Zheng and T. Matsumoto. Breaking real-world implementations of cryptosystems by manipulating their random number generation. In *Pre-proceedings of the 1997 Symposium on Cryptography and Information Security*, 29th January–1st February 1997, Fukuoka.