UCL Crypto Group Technical Report Series

UCL
Université
catholique
de Louvain

# Faulty RSA encryption

M. Joye and J.-J. Quisquater

GROUPE CRYPTO

http://www.dice.ucl.ac.be/crypto/

Technical Report
CG–1997/8

Place du Levant, 3
B-1348 Louvain-la-Neuve, Belgium

Phone: (+32) 10 472541
Fax: (+32) 10 472598

# Faulty RSA encryption

M. Joye and J.-J. Quisquater

July 24, 1997

Département d'Électricité (DICE), Université catholique de Louvain
Place du Levant, 3, B-1348 Louvain-la-Neuve, Belgium
Email: {joye, jjq}@dice.ucl.ac.be

**Abstract.** The authors show that the presence of transient faults is dangerous when encrypting messages with the RSA cryptosystem. In particular, they show how a cryptanalyst can recover a plaintext without knowing the secret parameters.

## 1 Introduction

Simmons pointed out in [1] that the use of a common RSA [2] modulus is dangerous. Indeed, if the same message $m$ is encrypted with coprime public encryption keys $e_1$ and $e_2$, then it can easily be recovered as follows. Let $c_1 = m^{e_1} \bmod n$ and $c_2 = m^{e_2} \bmod n$ be the ciphertexts corresponding to message $m$. Since $\gcd(e_1, e_2) = 1$, there exist $u, v \in \mathbb{Z}$ such that $ue_1 + ve_2 = 1$. Therefore, message $m$ is recovered as

$$m = m^{ue_1+ve_2} \equiv c_1^u c_2^v \pmod{n}. \tag{1}$$

In the next Section, we will show that a similar technique enables to recover a plaintext in the presence of transient faults.

## 2 Faulty RSA encryption

We suppose that an error occurs during the computation of the ciphertext. More precisely, if $e = \sum_{i=0}^{t-1} e_i 2^i$ denotes the binary expansion of the public exponent $e$, we suppose that the $j^{\text{th}}$ bit of $e$ flips to its complementary value. So, the ciphertext corresponding to message $m$ will be $\hat{c} = m^{\hat{e}} \bmod n$ instead of $c = m^e \bmod n$, where

$$\hat{e} = \begin{cases} e + 2^j & \text{if } e_j = 0, \\ e - 2^j & \text{if } e_j = 1. \end{cases} \tag{2}$$

CG–1997/8

Let $\delta = \gcd(\hat{e}, e)$. Since $\delta = \gcd(e \pm 2^j, e)$, $\delta$ divides $2^j$. This implies $\delta = 1$ because $e$ is odd in the RSA cryptosystem. Consequently, the message $m$ can be recovered from $c$ and $\hat{c}$ by the common modulus attack previously described.

## 3 Extension to other systems

After its introduction in 1978, the RSA cryptosystem was extended to Lucas sequences to produce LUC [3]. It was also extended to elliptic curves by Koyama, Maurer, Okamoto and Vanstone, the so-called KMOV cryptosystem [4], and later by Demytko [5].

KMOV is homomorphic and is therefore susceptible to the common modulus attack. LUC and the Demytko's system apparently seem to be resistant because their non-homomorphic nature. However, Bleichenbacher, Joye and Quisquater [6] recently exhibited a chosen-message requiring only one message against LUC and the Demytko's system. So, these latter systems are also vulnerable to the common modulus attack. For LUC and KMOV, the encryption key $e$ must be odd; therefore the condition $\gcd(\hat{e}, e) = 1$ is always satisfied. This is not necessarily the case for the Demytko's system.

When several bits of the encryption exponent flip, the attack may still apply or not depending on the value of $\gcd(\hat{e}, e)$. Note also that using prime public encryption exponents is dangerous because, in that case, the attack is always applicable.

## References

[1] SIMMONS, G. J.: 'A 'weak' privacy protocol using the RSA cryptoalgorithm', *Cryptologia*, (Apr. 1983), **7**, (2), 180–182

[2] RIVEST, R. L., SHAMIR, A., and ADLEMAN, L.: 'A method for obtaining digital signatures and public-key cryptosystems', *Communications of the ACM*, (Feb. 1978), **21**, (2), 120–126.

[3] SMITH, P. J., and LENNON, M. J. J.: 'LUC: A new public key system', in *Ninth IFIP Symposium on Computer Security* (1993), Elsevier Science Publishers, pp. 103–117.

[4] KOYAMA, K., MAURER, U. M., OKAMOTO, T., and VANSTONE, S. A.: 'New public-key schemes based on elliptic curves over the ring $\mathbb{Z}_n$', in *Advance in Cryptology – Crypto '91* (1992), vol. 576 of *Lectures Notes in Computer Science*, Springer-Verlag, pp. 252–266.

[5] DEMYTKO, N.: 'A new elliptic curve based analogue of RSA', in *Advance in Cryptology – Eurocrypt '93* (1994), vol. 765 of *Lectures Notes in Computer Science*, Springer-Verlag, pp. 40–49.

[6] BLEICHENBACHER, D., JOYE, M., and QUISQUATER, J.-J.: 'A new and optimal chosen message attack on RSA-type cryptosystems', in *Information and Communications Security* (1997), vol. 1334 of *Lectures Notes in Computer Science*, Springer-Verlag, pp. 302–313.