Lietuvos matematikos rinkinys
Proc. of the Lithuanian Mathematical Society, Ser. A
DOI: 10.15388/LMR.A.2016.16

ISSN 0132-2818
Vol. **57**, 2016
pages 86–90

On the security of RSA textbook signature scheme on Paillier ciphertext

Aleksejus Mihalkovich, Eligijus Sakalauskas

Department of Fundamental Sciences, Kaunas University of Technology
Studentų str. 48, Kaunas, Lithuania
E-mail: aleksejus.michalkovic@ktu.lt, eligijus.sakalauskas@ktu.lt

Abstract. In this paper we consider Pailler encryption and RSA textbook signature. We show that due to valuable homomorphic property these algorithms can be used together to obtain a valid signature on a certain combination of ciphertexts. Our goal is to show that this combination of algorithms provide security against chosen plaintext and chosen ciphertext attacks.

Keywords: security analysis, e-signature, asymmetric encryption.

1 Introduction

Nowadays many algorithms of asymmetric encryption and digital signature are known. In our paper we consider two homomorphic cryptographic primitives, namely Pailler encryption and RSA textbook signature. The considered cryptographic primitives possess a homomorphic property. This valuable property allows us to apply these algorithms to distinct messages and obtain a valid result for a combination of these messages (sum or product).

Another important similarity between two protocols is the fact, that both algorithms use an integer n, which is a product of two primes p and q. Due to this similarity we are able to link these two algorithms together, i.e. we use Pailler encryption on the message m to obtain a ciphertext c, which is then signed using RSA textbook signature. This combination of two schemes can be used to create e-money or in e-voting.

Though is was previously shown in [3], that RSA textbook signature scheme is existentially forgeable, we consider the resistance of the combination of it with Pailler encryption to chosen plaintext and chosen ciphertext attacks (CPA and CCA respectively).

2 Mathematical background

In this section we provide brief overview of cryptographic primitives mentioned above. Note however, that we shall be using the Carmichael function $\lambda(\cdot)$ in stead of Euler totient function $\phi(\cdot)$. The following steps are performed once and are used in both cryptographic primitives:

- Generate two large distinct primes p and q of the roughly same size;
- Compute $n = pq$ and $\lambda(n) = \mathrm{lcm}(p-1, q-1)$.

2.1 Pailler encryption

In Pailler asymmetric encryption protocol the public key $PuK = n$, and the private key $PrK = \lambda(n)$.

Assume, that a message to be encrypted is encoded by an integer m. The encryption is performed as follows [4]:

- Select a random number $r \in \boldsymbol{Z}_{n^2}^*$;
- Compute the ciphertext $c = (1+n)^m r^n \bmod n^2$. Note, that $c \in \boldsymbol{Z}_{n^2}^*$.

Note, that since the multiplicative order $ord_{n^2}(1+n) = n$ it is reasonable to turn a message to an integer $m \in \boldsymbol{Z}_n$.

The plaintext message m is computed using an identity:

$$m = \frac{c^{\lambda(n)} \bmod n^2 - 1}{n} \lambda^{-1}(n) \bmod n.$$

Note, that division is performed over set of integers $\boldsymbol{Z}$.

2.2 RSA textbook signature scheme

The main idea of this paper is to link two cryptographic primitives by using the same value n for both Pailler encryption and RSA textbook signature. The steps to execute the latter are presented below [5]:

2.2.1 Key generation algorithm

- Select a random integer e, $1 < e < \lambda(n)$, such that $\gcd(e, \lambda(n)) = 1$. It reasonable to consider values of e having a short bit-length and small Hamming weight. A common value of e is $2^{16} + 1$;
- Find a value of d satisfying the congruence $ed \equiv 1 \bmod \lambda(n)$, i.e. compute the modular multiplicative inverse of e modulo $\lambda(n)$.

The public key $PuK = (n, e)$, and the private key $PrK = d$.

2.2.2 Signature generation

Compute the signature $s = c^d \bmod n$. Note, that $s \in \boldsymbol{Z}_n^*$.

2.2.3 Signature verification

Let $s \in \boldsymbol{Z}_n^*$ be a signature to be verified.

- Compute $\widetilde{c} = s^e \bmod n$;
- Verify if $c = \widetilde{c}$. The output of the verification function $Ver_{RSA}(s)$ is "Yes" if the identity holds and "No" otherwise.

2.3 Homomorphic properties

A useful feature of the Paillier cryptosystem is its homomorphic property [4]:

$$Enc_{Pai}(m_1) \cdot Enc_{Pai}(m_2) = Enc_{Pai}\big((m_1 + m_2) \bmod n\big) = Enc_{Pai}(m),$$

when $m = (m_1 + m_2) \bmod n$, for all $m, m_1, m_2 \in \boldsymbol{Z}_n$, where $Enc_{Pai}(m)$ denotes the Paillier encryption of the message m.

The proof of this relation can be found in [4].

Due to this property Paillier encryption scheme allows computations (multiplications) to be performed on ciphertext values, as the product of ciphertexts corresponds to the sum of plaintexts.

Furthermore, RSA signature scheme also has a homomorphic property:

$$Sig_{RSA}(c_1) \cdot Sig_{RSA}(c_2) = Sig_{RSA}\big((c_1 \cdot c_2) \bmod n\big) = Sig_{RSA}(c),$$

when $c = (c_1 \cdot c_2) \bmod n^2$, for all $c, c_1, c_2 \in \boldsymbol{Z}^*_{n^2}$, where $Sig_{RSA}(c)$ denotes the RSA signature on the ciphertext c.

The proof of this property follows directly from the definition of RSA signature.

Hence, the product of two signatures is equal to the signature on the product of ciphertexts.

The main advantage of homomorphic property of both algorithms is the fact that users can combine their messages m_1, m_2, etc. to obtain a ciphertext of a sum of these messages without actual knowledge of the whole message $m = \sum_k m_k$. Furthermore, users can also obtain a valid signature on a product of ciphertexts c_1, c_2 without actual knowledge of the whole ciphertext $c = \prod_k c_k$.

3 Security proof

Let us assume that the message m is encrypted using Pailler algorithm obtaining ciphertext c which is signed by RSA signature.

According to [3, 4], we assume, that Paillier encryption scheme is indistinguishable encryption under a chosen-plaintext attack if random encryption number r is chosen as random element in $\boldsymbol{Z}^*_n$. We assume, that in this case Paillier encryption is performed correctly and we will follow this assumption. Then ciphertext c corresponding to the message m is uniformly distributed in $\boldsymbol{Z}^*_{n^2}$ if r is uniformly distriuted in $\boldsymbol{Z}^*_n$.

In [1], authors introduced RSA Full–Domain–Hash (FDH) function, which can be applied for signing with RSA signature scheme. It was shown in [1] and [2] that this scheme is provably secure, i.e. existentially unforgeable under adaptive chosen-message attacks in the random oracle model, assuming that inverting RSA is hard, i.e. extracting a root modulo a composite integer, is hard.

We now prove the following proposition:

Proposition 1 *If Paillier encryption and RSA signature has the same modulus n and message $m \in \boldsymbol{Z}_n$, then ciphertext $c = Enc_{Pai}(m)$ obtained by Paillier encryption taken modulo n, is in RSA FDH, i.e. $c \equiv z \bmod n$, $z \in \boldsymbol{Z}^*_n$.*

Proof. It is clear, that $z \in \boldsymbol{Z}^*_n$, since $\gcd(z, n) = 1$ iff $\gcd(c, n^2) = 1$. Hence the composition of function $f(\cdot)$ and $Enc_{Pai}(m)$ represents the following mapping

$$f\big(Enc_{Pai}(m)\big) : \boldsymbol{Z}_n \times \boldsymbol{Z}_n^* \to \boldsymbol{Z}_n^*$$

and this function range is equal to RSA domain.

Now we have to show that if Paillier encryption is correct, then for any $m \in \boldsymbol{Z}_n$, value z is uniformly distributed in $\boldsymbol{Z}_n^*$ for distinct uniform values of r. This comes from the following two facts:

- Pailler encryption function $Enc_{Pai}(m)$ is a bijection and hence the value of c is distributed uniformly in $\boldsymbol{Z}_{n^2}^*$;
- Since there are exactly n distinct values of c less than n^2 that give the same residue modulo n, the values of z are uniformly distributed in $\boldsymbol{Z}_n^*$.

Hence function f is an n-to-1 mapping $\boldsymbol{Z}_{n^2}^* \to \boldsymbol{Z}_n^*$ and the composition $f(Enc_{Pai}(m))$ can be interpreted as a H-function and as a artificial random oracle if random number r in correct Paillier encryption scheme can be treated as random. □

This implies that element z as a function of r is strongly universal as defined by Wegman and Carter in [7]. In [6] Vaudenay defines this property as a perfect 1-wise decorrelation (as denoted by the author). Vaudenay showed in [6], that in this case our scheme is secure against chosen plaintext attack (CPA) and chosen ciphertext attack (CCA) respectively (Theorem 7). Hence we have proved, the following proposition:

Proposition 2 *If Paillier encryption and RSA signature have the same modulus n and message $m \in \boldsymbol{Z}_n$, then RSA signature s on ciphertext c is existentially unforgeable under CPA in the random oracle model.*

The security of RSA signature now relies on the multiplicative order of z, which is denoted by $ord_n(z)$. To simplify the security analysis, we can use Sophie Germain primes $p\prime$ and $q\prime$ (hence $p = 2p\prime + 1$ and $q = 2q\prime + 1$ are primes) to construct the modulus n. In this case the maximal multiplicative order of $\boldsymbol{Z}_n^*$ is defined by the value of the Carmichael function $\lambda(n) = 2p\prime q\prime$. The latter expression is also the canonical representation of $\lambda(n)$, i.e. only 8 distinct divisors of $\lambda = \lambda(n)$ exist. Hence there are only 8 possible values of $ord_n(z)$, since, due to Lagrange theorem, $ord_n(z)$ divides λ. To ensure security of RSA signature we have to exclude small values of λ, i.e. 1 and 2, which is possible by checking if the following congruences hold:

$$c \equiv 1 \bmod n,$$
$$z^2 \equiv 1 \bmod n.$$

In case of at least one correct identity the ciphertext c has to be recalculated, i.e. Pailler encryption algorithm is executed with a different value of r. We assume, that none of latter congruences hold. In this case an element z generates a significantly large subgroup $\langle z \rangle$ of cardinality $ord_n(z)$.

4 Conclusions

In this paper we considered Pailler asymmetric encryption and RSA texbook signature. We have shown that by using the same modulus n we obtain a ciphertext c,

which reduced modulo n is in RSA FDH. Hence the operation of reduction modulo n can be interpreted as a hash function. Furthermore, since RSA FDH is existentially unforgeable, we have shown that a combination of considered algorithms provides security against CPA in random oracle model.

References

[1] M. Bellare and Ph. Rogaway. The exact security of digital signatures-how to sign with rsa and rabin. In *Advances in Cryptology-Eurocrypt'96*, pp. 399–416. Springer, 1996.

[2] J. Coron. On the exact security of full domain hash. In *Advances in Cryptology-CRYPTO 2000*, pp. 229–235. Springer, 2000.

[3] J. Katz and Y. Lindell. *Introduction to Modern Cryptography.* CRC Press, 2014.

[4] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Advances in Cryptology-EUROCRYPT'99*, pp. 223–238. Springer, 1999.

[5] R. Rivest, Shamir A and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, **21**(2):120–126, 1978.

[6] S. Vaudenay. Decorrelation: a theory for block cipher security. *J. Crypt.*, **16**(4):249–286, 2003.

[7] M.N. Wegman and J.L. Carter. New hash functions and their use in authentication and set equality. *J. Comput. Syst. Sci.*, **22**(3):265–279, 1981.

REZIUMĖ

Apie RSA parašo ant Pajė šifrogramos saugumą

A. Mihalkovich, E. Sakalauskas

Darbe nagrinėjamas Pajė asimetrinis šifravimas ir RSA parašas. Kadangi abu algoritmai turi homomorfiškumo savybę, tai šie algoritmai gali būti panaudoti kartu teisėtam parašui ant tam tikros šifrogramų kambinacijos gauti. Mūsų tikslas yra parodyti, jog šių algoritmų kombinacija užtkrina atsparumą pasirinktos žinutės ir pasirinktos šifrogramos atakoms.

Raktiniai žodžiai: saugumo analizė, elektroninis parašas, asimetrinis šifravimas.