M.A. Asbullah, and M.R.K. Ariffin, "Rabin-*p* Cryptosystem: Practical and Efficient Method for Rabin based Encryption Scheme" *International Journal of Computer Mathematics,* 2014. (Submitted: 22.08.2014).

A Practical and Efficient Method for Rabin based Encryption Scheme

[1]Muhammad Asyraf Asbullah and [2]Muhammad Rezal Kamel Ariffin

[1]Al-Kindi Cryptography Research Laboratory, Institute for Mathematical Research, Universiti Putra Malaysia, Serdang, 43400, Malaysia.
[1,2]Department of Mathematics, Faculty of Sciences, Universiti Putra Malaysia, Serdang, 43400, Malaysia

[1]ma_asyraf@upm.edu.my, [2]rezal@upm.edu.my

Abstract: In this work, we introduce a new, efficient and practical scheme based on the Rabin cryptosystem without using the Jacobi symbol, message redundancy technique or the needs of extra bits in order to specify the correct plaintext. Our system involves only a single prime number as the decryption key and does only one modular exponentiation. Consequently, this will practically reduce the computational efforts during decryption process. We demonstrate that the decryption is unique and proven to be equivalent to factoring. The scheme is performs better when compared to a number of Rabin cryptosystem variants.

Keywords: Encryption; Rabin Cryptosystem; Factoring Problem; Chinese Remainder Theorem; Coppersmith's Theorem.

1. Introduction

In principle, the Rabin scheme is really efficient, because only a square is required for encryption; furthermore, it is shown to be as hard as factoring problem. Alas, the Rabin cryptosystem suffer from two major drawbacks; the foremost one is because the Rabin's decryption produces four possible candidates, thus introduces ambiguity or unclearness to decide the correct message out of four possible values. Another drawback is from the fact that its equivalence relation to factorization. On one side, the Rabin cryptosystem gives confidence as the security of breaking such system is proven to be as difficult as factoring compare to RSA. On the other side, the computational equivalence relation of the Rabin cryptosystem and the integer factorization problem makes the scheme vulnerable to an adversary that can launch a stronger attack, namely the chosen ciphertext attack. In summation, any scheme that inherits the properties of a security reduction that is equivalent to factoring is not very

practicable as cipher systems [26]. These two disadvantages of the Rabin encryption scheme prevented it from widespread practical use.

1.1 Related work

In spite of the situation of four-to-one mapping of Rabin's decryption, and the vulnerability to chosen ciphertext attacks, several attempts were made to solve this problem adequately. It is very interesting to witness continuous efforts in searching for a practical and optimal Rabin cryptosystem by numerous scholars. We put forward the summary for Rabin's variants as follows.

Williams [11] proposed an implementation of the Rabin cryptosystem using the Jacobi symbol. Subsequently, the utility of the Jacobi symbol as extra information to define the correct square root accompanied with Rabin cryptosystem was also proposed by [13]. Next is the extra bits methodology. It is a very attractive approach to solve the uniqueness problem in the Rabin decryption procedure. It appeared in current literature such as extra bits introduced by [18] and also utilized together with the Dedikind Sums Theorem in [7].

In [3] a redundancy to the message was proposed, which intends to append the plaintext with the repeating of least significant bits of the message with a pre-defined length. In [19, 29] and [15] the authors proposed a Rabin-type cryptosystem with alternative modulus choice of $N = p^2q$. The combination of Rabin cryptosystem with a specific padding method was proposed by [14], [19] by using Optimal Asymmetric Encryption Padding (OAEP) [17] and Rabin-SAEP [5]. Note that the message output by decryption process for this padding scheme is unique but the decryption may fail with small probability.

1.2 Motivation and Contributions

It is of practical considerations that motivated researchers to turn the Rabin scheme to be useful and practical as RSA since it possess practical qualities. In general, all the existing variation seems to apply some additional features, for instance; implementing some padding, adding redundancy in the message or manipulate some mathematical pattern, with the target to get a unique decryption result but at the same time losing its computational advantage over RSA. In order to engage this problem and to overcome all the mentioned shortcomings, further analytical work is needed to refine those existing work.

In this work, we revisit Rabin cryptosystem and propose a new efficient and practical scheme which has the following characteristics; i) a cryptosystem that can be proven equivalent to factoring, ii) preserve the performance of Rabin encryption while producing a unique message after decryption, iii) improve decryption efficiency by using only one modular exponentiation as oppose to typical Rabin-based decryption that use two one modular exponentiation, iv) the decryption key using only a single prime number instead of two, and finally v) resilient to a side channel attack namely the Novak's attack by avoiding the need for CRT computation.

2. Preliminaries

2.1 Public Key Encryption.
2.2 Rabin Cryptosystem
2.3 Drawbacks of Previous Strategies

In this section, we initiate a list that describes the drawback of the previous strategies to overcome the Rabin weaknesses. Hence we established conditions that need to be avoided on any attempt to refine the Rabin scheme.

2.3.1 The Use of Jacobi Symbol.

See [5, 25].

2.3.2 Message Redundancy and Padding Mechanism

2.3.3 The Use of CRT

(see [23])

2.4 Methodology

Now, we outlined the methodology to overcome the drawbacks of the Rabin cryptosystem and all its variants. Firstly, we put the condition on the modulus of type $N = p^2q$ to be used. We then impose restriction on the plaintext m and ciphertext c space as $m \in \mathbb{Z}_{p^2}$ and $c \in \mathbb{Z}_{p^2q}$, respectively. From the plaintext-ciphertext expansion such restriction leads to a system that is not a length-preserving for the message.

Let m, c be the plaintext and ciphertext and $c(m)$ be the function of c taking m as its input. Say, for instance, in RSA the plaintext and ciphertext spaces are the same, thus we denote the mapping as $c(m): \mathbb{Z}_{pq} \to \mathbb{Z}_{pq}$. Note that this situation could be an advantage for the RSA scheme since RSA encryption has no message expansion. This is not, however true for all cryptosystems. For example, the plaintext-ciphertext mapping for Okamoto-Uchiyama Cryptosystem [28] is $c(m): \mathbb{Z}_p \to \mathbb{Z}_{p^2q}$, Pailier cryptosystem [22] and the scheme by [8] is $c(m): \mathbb{Z}_{pq} \to \mathbb{Z}_{(pq)^2}$, Rabin-SAEP [5] mapping is $c(m): \mathbb{Z}_{\frac{pq}{2}} \to \mathbb{Z}_{pq}$ and Schmidt-Samoa cryptosystem [15] is $c(m): \mathbb{Z}_{pq} \to \mathbb{Z}_{p^2q}$.

The maximum space size is determined by the plaintext space. One way to do it would be to tell the user a maximum number of bits for the plaintext messages. If we view the message as merely the keys for a symmetric encryption scheme, meaning that the message is indeed a short message, then this is fine as many others schemes also implement this approach. Thus, we argue that the restriction of message space would be a hindrance is not an issue.

3 Our Proposed Scheme: Rabin-p Cryptosystem

In this section, we provide the details of the proposed cryptosystem namely Rabin-p Cryptosystem. Rabin-p is named after the Rabin cryptosystem with the additional p symbolizing that the proposed scheme only uses a single prime p as the decryption key. The proposed cryptosystem defined as follows.

Algorithm 3.1: Key Generation
INPUT: The size k of the security parameter.
OUTPUT: The public key N and the private key p.

1. Generate random and distinct k -bit primes p, q such that $p, q \equiv 3 \pmod 4$ where $2^{k-1} < p, q < 2^k - 1$.
2. Compute $N = p^2q$.
3. Return the public key N and the private key p.

Algorithm 3.2: Encryption
INPUT: The plaintext m and the public key N.
OUTPUT: A ciphertext c.

1. Choose plaintext $m < 2^{2k-2}$ such that $\gcd(m, N) = 1$
2. Compute $c \equiv m^2 \pmod N$.
3. Return the ciphertext c.

Remark 3.1 We observe that the message space is restricted to the range $m < 2^{2k-2}$. It shows that the message $m < 2^{2k-2} < \frac{p^2}{2} < p^2$.

Algorithm 3.3: Decryption
INPUT: A ciphertext c and the private key p.
OUTPUT: The plaintext m.

1. Compute $w \equiv c \pmod{p}$
2. Compute $m_p \equiv w^{\frac{p+1}{4}} \pmod{p}$.
3. Compute $i = \frac{c-m_p^2}{p}$.
4. Compute $j \equiv \frac{i}{2m_p} \pmod{p}$.
5. Compute $m_1 = m_p + jp$.
6. If $m_1 < \frac{p^2}{2}$, then return $m = m_1$.
7. Else return $m = p^2 - m_1$.

Remark 3.2 The decryption algorithm needs only a single prime number as its key and it operates with single modular exponentiation operation. This situation would give impact on the overall computational advantage of the proposed scheme against other Rabin variants.

3.1 Proof of Correctness

The decryption output by Algorithm 3.3 is correct and produces the unique m. We shall break down the proof of correctness to several lemmas. We proceed with the proof of correctness as follows.

Suppose $c \equiv m^2 \pmod{p^2q}$ then $c - m^2 \equiv 0 \pmod{p^2q}$. Note that, if $c - m^2$ is divisible by p^2q then it is certainly divisible by p^2. From Remark 3.1 the message $m < 2^{2k-2} < \frac{p^2}{2} < p^2$. Thus, it is sufficient to solve for $c \equiv m^2 \pmod{p^2}$.

Lemma 3.3 Let $c \equiv m^2 \pmod{p^2}$ then exist two distinct square roots; $\pm m \pmod{p^2}$.

Proof: Suppose $m_1 \neq m_2$ such that $m_1^2 \equiv m_2^2 \equiv c \pmod{p^2}$. Then

$$m_1^2 - m_2^2 \equiv (m_1 + m_2)(m_1 - m_2) \equiv 0 \pmod{p^2} \quad (1)$$

Note that $p^2 | (m_1 + m_2)(m_1 - m_2)$, thus consider $p | (m_1 + m_2)(m_1 - m_2)$ as

well. If $p|(m_1 + m_2)$ and $p|(m_1 - m_2)$, then p would divide $(m_1 + m_2) + (m_1 - m_2) = 2m_1$ and $(m_1 + m_2) - (m_1 - m_2) = 2m_2$. Since $p \equiv 3 \pmod 4$ is odd prime, then $p \nmid 2$ so p would divide both m_1 and m_2. Consider $m_1^2 \equiv c \pmod{p^2}$ thus $m_1^2 = c + lp^2$ for some integer l. If $p|m_1$ then $p|m_1^2$ therefore $p|c$. Observe that $\gcd(c, p) = 1$ therefore $p \nmid c$. Hence $p \nmid m_1$. The same goes for $p \nmid m_2$.

Now, consider in the case if $p|(m_1 + m_2)$ or $p|(m_1 - m_2)$ but not both. Since $p^2|(m_1 + m_2)(m_1 - m_2)$, therefore either $p^2|(m_1 + m_2)$ *or* $p^2|(m_1 - m_2)$. This concludes $m_1 \equiv m_2 \pmod{p^2}$ and $m_1 \equiv -m_2 \pmod{p^2}$.■

Lemma 3.4 Suppose m_p is a solution to $w \equiv c \pmod p$. Let j be a solution to $2m_p j \equiv i \pmod p$ such that $i = \frac{c - m_p^2}{p}$. Then $m = m_p + jp$ is a solution to $c \equiv m^2 \pmod{p^2}$. Furthermore $-m \pmod{p^2}$ is another solution. Let $m_1 \equiv m \pmod{p^2}$ and $m_2 \equiv -m \pmod{p^2}$ then $m_1 + m_2 = p^2$.

Proof: Suppose we are given the ciphertext c as described in the encryption process (i.e. 3.4.2), and need to solve for its square root modulo $N = p^2 q$. Let $c \equiv m^2 \pmod N$, and since $p|N$, then we have $w \equiv m^2 \equiv c \pmod p$. From here, since $m < p^2$ thus it is sufficient just solving $w \equiv c \pmod p$.

We begin by solving $w \equiv c \pmod p$. Let m_p is a solution to $w \equiv c \pmod p$ such that $w \equiv m_p^2 \pmod p$. It thus suffices to find for m_p the values $m = m_p + jp$ for some integer j that we will find later. Suppose that $m = m_p + jp$ is a solution for $w \equiv c \pmod p$, then we have

$$c \equiv m_p^2 + 2m_p jp \pmod{p^2} \qquad (2)$$

So, the above congruence can be rearranged as $2m_p jp \equiv c - m_p^2 \pmod{p^2}$. Note that from $w \equiv m_p^2 \pmod p$, we have $c - m_p^2 \equiv 0 \pmod p$ which means that $c - m_p^2$ is a multiple of p, say ip for some integer i. From here, we could simply compute $i = \frac{c - m_p^2}{p}$. We then rewrite this equation as $2m_p jp \equiv ip \pmod{p^2}$. Hence, p factors immediately cancelled out from $2m_p jp \equiv ip \pmod{p^2}$ since it implies that $2m_p j \equiv i \pmod p$. Hence, we compute $j \equiv \frac{i}{2m_p} \pmod p$.

To conclude, we have a solution $m = m_p + jp$ for $c \equiv m^2 \pmod{p^2}$. Observe that $-m \pmod{p^2}$ is also another solution and we simply can write it as $p^2 - m$. In addition, if we set $m_1 = m$ then $m_2 \equiv p^2 - m$, thus $m_1 + m_2 = p^2$.■

Now, the following lemma shows that the decryption algorithm will output a unique solution as follows.

Lemma 3.5 Let $m < 2^{2k-2}$. Then the decryption algorithm will output the unique m.

Proof: Observe that the upper bound for m is $2^{2k-2} - 1 < 2^{2k-2} < \frac{p^2}{2}$. Consider $m_1 + m_2 = p^2$ with p^2 is an odd integer. Then either m_1 or m_2 is less than $\frac{p^2}{2}$ that satisfies the upper bound of $m < 2^{2k-2}$. Observe that p^2 is an odd integer, then by definition $\frac{p^2}{2}$ is not an integer. Since that m_1 and m_2 need to be integers, thus $m_1, m_2 \neq \frac{p^2}{2}$.

Suppose we consider both m_1 and m_2 are less than $\frac{p^2}{2}$, then we should have $m_1 + m_2 < p^2$ therefore we have a contradiction (i.e the fact that $m_1 + m_2 = p^2$). On the other hand, if we consider both m_1 and m_2 are greater than $\frac{p^2}{2}$, then we should have $m_1 + m_2 > p^2$ yet we reach the same contradictory statement. Thus, one of m_1 or m_2 must be less than $\frac{p^2}{2}$.

Suppose $m_1 < \frac{p^2}{2}$ then there must exist a real number ϵ_1 such that $m_1 + \epsilon_1 = \frac{p^2}{2}$. On the other site, since we let $m_1 < \frac{p^2}{2}$, then m_2 must be greater than $\frac{p^2}{2}$. Suppose $m_2 > \frac{p^2}{2}$ then there must exist a real number ϵ_2 such that $m_2 - \epsilon_2 = \frac{p^2}{2}$. If we add up these two equations, we should have

$$(m_1 + \epsilon_1) + (m_2 - \epsilon_2) = \frac{p^2}{2} + \frac{p^2}{2} = p^2 \qquad (4)$$

But since we have $m_1 + m_2 = p^2$, thus $(\epsilon_1 - \epsilon_2)$ should be equal to zero, meaning that $\epsilon_1 = \epsilon_2$. Finally, we conclude that only one of $m_1$or m_2 are less than $\frac{p^2}{2}$ and will be outputted by the decryption algorithm as the unique m.■

4 Analysis and Discussion

4.1 Equivalent to Factoring $N = p^2q$

Proposition 4.1 Breaking the scheme is reducible to factoring the modulus $N = p^2q$.

Proof: (⇒) Suppose we have an algorithm with the ability to factor the modulus $N = p^2q$, then we can solve the message m from the ciphertext c output by the proposed scheme simply by following the outlined decryption algorithm. Therefore the proposed scheme is reducible to factoring. ■

Proposition 4.2 Factoring the modulus $N = p^2q$ is reducible to breaking the scheme.

Proof: (⇐) Conversely, suppose there exists an algorithm that break the proposed scheme; that is able to find the message m from the ciphertext c then there exists an algorithm to solve the factorization of the modulus $N = p^2q$. Implying that someone who can decrypt the message m from the ciphertext c must also be able to factor $N = p^2q$. The factoring algorithm is defined as follows.

Algorithm 4.1: Factoring Algorithm
INPUT: A ciphertext c and N
OUTPUT: The prime factors p^2, q

1. Choose integer $2^{2k-1} < \bar{m} < 2^{2k} - 1$
2. Compute $\bar{c} \equiv \bar{m}^2 \pmod N$.
3. Ask the decryption of ciphertext $\bar{c}$.
4. Receive the output $m' < 2^{2k-2}$
5. Compute $\gcd(\bar{m} \pm m', N) = p^2$.
6. Compute $\frac{N}{p^2} = q$.
7. Return The prime factors p^2, q. ■

4.2 Coppersmith's Technique

Coppersmith [6] introduced a significantly powerful theorem for finding small roots of modular polynomial equations using the LLL algorithm.

Theorem 4.3 [6] Let N be an integer of unknown factorization. Let $f_N(x)$ be a univariate, a monic polynomial of degree δ. Then we can find all solutions x_0 for the equation $f_N(x) \equiv 0 \pmod N$ with $|x_0| < N^{\frac{1}{\delta}}$ in polynomial time.

Proposition 4.4 Let $c \equiv m^2 \left(mod\, N\right)$ from the ciphertext. If $m < 2^{\frac{3n}{2}}$ then m can be found in polynomial time.

Proof: Suppose $c \equiv m^2 (\mathrm{mod}\, N)$. Consider the univariate, monic polynomial $f_N(x) \equiv x^2 - C \equiv 0 (\mathrm{mod}\, N)$, hence $\delta = 2$. Thus, by applying the Coppersmith's method; the root $x_0 = m$ can be recovered if $m < N^{\frac{1}{\delta}} = N^{\frac{1}{2}} \approx 2^{\frac{3n}{2}}$. Therefore, to avoid this attack, we need to set $m > 2^{\frac{3n}{2}}$. ■

Theorem 4.5 [2] Let N be an integer of unknown factorization, which has a divisor $b > N^{\beta}$. Furthermore, let $f_b(x)$ be a univariate, a monic polynomial of degree δ. Then we can find all solutions x_0 for the equation $f_b(x) \equiv 0 (\mathrm{mod}\, b)$ with $|x_0| < \frac{1}{2} N^{\frac{\beta^2}{\delta}}$ in polynomial time.

Proposition 4.6 Let $c \equiv m^2 \left(\mathrm{mod}\, p^2\right)$ such that p^2 is an unknown factor for N. If $m < 2^{\frac{2n}{3}}$ then m can be found in polynomial time.

Proof: Suppose $c \equiv m^2 \left(\mathrm{mod}\, p^2\right)$ such that p^2 is an unknown factor for N. Consider $f_{p^2}(x) \equiv x^2 - c \equiv 0 (\mathrm{mod}\, p^2)$ with $p^2 \approx N^{\frac{2}{3}} \approx 2^{2n}$. We can find a solution $x_0 = m$ if $m < \frac{1}{2} N^{\frac{\beta^2}{\delta}} < N^{\frac{\left(\frac{2}{3}\right)^2}{2}} = N^{\frac{2}{9}} \approx 2^{\frac{2n}{3}}$.■

4.3 Chosen Ciphertext Attack

Notice that the factoring algorithm mentioned by Algorithm 3.4 could provide a way to launch a chosen ciphertext attack upon the proposed scheme in polynomial time, hence resulting in the system totally insecure in this sense. Therefore, in order to provide security against this kind of attack, we could consider implementing any hybrid technique with symmetric encryption. The result from [9] is suitable for our scheme in order to achieve chosen ciphertext security, with the cost of a hash function. We may also apply the chosen ciphertext secure hybrid encryption transformation that was proposed in [16].

4.4 Side Channel Attack

See [21, 31, 4 or 27]. Alternatively, Novak's attack on CRT [23].

5 Conclusion

Rabin- p cryptosystem is purposely designed without using the Jacobi symbol, redundancy in the message and avoiding the demands of extra information for finding the correct plaintext. Decryption outputs a unique plaintext without any

decryption failure. In addition, decryption only requires a single prime. Furthermore, the decryption procedure only computes a single modular exponentiation instead of two modular exponentiation executed by other Rabin variants. As a result, this reduces computational effort during decryption process. Some possible attacks such as Coppersmith's technique, chosen ciphertext attack and side channel attack have been analyzed. Still, none can successfully affect the proposed strategy. Finally, we show that Rabin-p cryptosystem is performs better when compared to a number of Rabin variants.

References

[1] A. Lenstra, and E. R. Verheul, Selecting cryptographic key sizes, Journal of cryptology. 14(4) (2001), 255-293.

[2] A. May, *New RSA vulnerabilities using lattice reduction methods*, PhD diss., University of Paderborn, 2003.

[3] A. Menezes, C. van Oorschot, and A. Vanstone, *Handbook of applied cryptography*, CRC Press, Washington, 1997.

[4] D. Brumley, and D. Boneh, *Remote timing attacks are practical*, Computer Networks 48 (2005), 701-716.

[5] D. Boneh, *Simplified OAEP for the RSA and Rabin functions*, Advances in Cryptology—CRYPTO 2001. Springer Berlin Heidelberg, 2001.

[6] D. Coppersmith, *Small solutions to polynomial equations, and low exponent RSA vulnerabilities*, Journal of Cryptology. 10(4) (1997), 233-260.

[7] D. Freeman, O. Goldreich, E. Kiltz, A. Rosen, and G. Segev, *More constructions of lossy and correlation-secure trapdoor functions*, Journal of cryptology. 26(1) (2013), 39-74.

[8] D. Galindo, S. Martýn, P. Morillo, and J. Villar, *A practical public key cryptosystem from Paillier and Rabin schemes*, Public Key Cryptography—PKC 2003. Springer Berlin Heidelberg, 2003.

[9] D. Hofheinz, and E. Kiltz, *Secure hybrid encryption from weakened key encapsulation*, Advances in Cryptology—CRYPTO 2007. Springer Berlin Heidelberg, 2007.

[10] G. Castagnos, A. Joux, F. Laguillaumie, and P. Nguyen, *Factoring pq^2 with quadratic forms: nice cryptanalyses*, Advances in Cryptology—ASIACRYPT 2009. Springer Berlin Heidelberg, 2009.

[11] H. C. Williams, *A modification of the RSA public-key encryption procedure*, IEEE Transactions on Information Theory. 26(6) (1980), 726-729.

[12] K. Kurosawa, and Y. Desmedt *A new paradigm of hybrid encryption scheme*, Advances in Cryptology—Crypto 2004. Springer Berlin Heidelberg, 2004.

[13] K. Kurosawa, T. Ito, and M. Takeuchi, *Public key cryptosystem using a reciprocal number with the same intractability as factoring a large number*, Cryptologia. 12(4) (1988), 225-233.

[14] K. Kurosawa, W. Ogata, T. Matsuo, and S. Makishima, *IND-CCA public key schemes equivalent to factoring* $n = pq$, Public Key Cryptography—PKC 2001. Springer Berlin Heidelberg, 2001.

[15] K. Schmidt-Samoa, *A new Rabin-type trapdoor permutation equivalent to factoring*, Electronic Notes in Theoretical Computer Science. 157(3) (2006), 79-94.

[16] M. Abe, R. Gennaro, and K. Kurosawa, *Tag-KEM/DEM: A new framework for hybrid encryption*, Journal of Cryptology. 21(1) (2008), 97-130.

[17] M. Bellare, and P. Rogaway, *Optimal asymmetric encryption*, Advances in Cryptology—EUROCRYPT'94. Springer Berlin Heidelberg, 1995.

[18] M. Elia, M. Piva, and D. Schipani, *The Rabin cryptosystem revisited*. arXiv preprint (2011). Available at *arXiv:1108.5935*.

[19] M. Nishioka, H. Satoh, and K. Sakurai, *Design and analysis of fast provably secure public-key cryptosystems based on a modular squaring,* Information Security and Cryptology—ICISC 2001. Springer Berlin Heidelberg, 2002.

[20] M. O. Rabin, *Digitalized signatures and public-key functions as intractable as factorization*, Technical Report (1979).

[21] P. Kocher, *Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems*, Advances in Cryptology—CRYPTO'96. Springer Berlin Heidelberg, 1996.

[22] P. Paillier, *Public-key cryptosystems based on composite degree residuosity classes*, Advances in cryptology—EUROCRYPT'99. Springer Berlin Heidelberg, 1999.

[23] R. Novak, *SPA-based adaptive chosen-ciphertext attack on RSA implementation*, Public Key Cryptography—PKC2002. Springer Berlin Heidelberg, 2002.

[24] R. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM. 21(2) (1978), 120-126.

[25] S. D. Galbraith, *Mathematics of public key cryptography*. Cambridge University Press, 2012.

[26] S. Müller, *On the security of Williams based public key encryption scheme*, Public Key Cryptography—PKC2001. Springer Berlin Heidelberg, 2001.

[27] T. Messerges, E. Dabbish and R. Sloan, *Power analysis attacks of modular exponentiation in smartcards*, Cryptographic Hardware and Embedded Systems. Springer Berlin Heidelberg, 1999.

[28] T. Okamoto, and S. Uchiyama, *A new public-key cryptosystem as secure as factoring*, Advances in Cryptology—EUROCRYPT'98. Springer Berlin Heidelberg, 1998.

[29] T. Takagi, *Fast RSA-type cryptosystem modulo* $p^k q$, Advances in Cryptology—CRYPTO'98. Springer Berlin Heidelberg, 1998.

[30] W. Diffie, and M. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory. 22(6) (1976), 644-654.

[31] W. Schindler, *A timing attack against RSA with the Chinese Remainder Theorem*, Cryptographic Hardware and Embedded Systems—CHES 2000. Springer Berlin Heidelberg, 2000.