Security Features of an Asymmetric Cryptosystem based on the Diophantine Equation Hard Problem and Integer Factorization Problem

M.R.K.Ariffin[1,2,[a]], M.A.Asbullah[1,2,[b]], and N.A.Abu[1,3,[c]]

[1] Al-Kindi Cryptography Research Laboratory, Institute for Mathematical Research, Universiti Putra Malaysia (UPM), Selangor, Malaysia
[2] Department of Mathematics, Faculty of Science, Universiti Putra Malaysia (UPM), Selangor, Malaysia
[3] Faculty of Information Technology and Communication, Unitversiti Teknikal Malaysia (UTeM), Melaka, Malaysia

[a]rezal@math.upm.edu.my,[b]ma_asyraf@putra.upm.edu.my,[c]nura@utem.edu.my

Abstract. The Diophantine Equation Hard Problem (DEHP) is a potential cryptographic problem on the Diophantine equation $U = \sum_{i=1}^{n} V_i x_i$. A proper implementation of DEHP would render an attacker to search for private parameters amongst the exponentially many solutions. However, an improper implementation would provide an attacker exponentially many choices to solve the DEHP. The AA_β-cryptosystem is an asymmetric cryptographic scheme that utilizes this concept together with the factorization problem of two large primes and is implemented only by using the multiplication operation for both encryption and decryption. With this simple mathematical structure, it would have low computational requirements and would enable communication devices with low computing power to deploy secure communication procedures efficiently.

Keywords: Diophantine equation hard problem (DEHP), integer factorization problem, asymmetric cryptography, passive adversary attack

1 Introduction

The discrete log problem (DLP) and the elliptic curve discrete log problem (ECDLP) has been the source of security for cryptographic schemes such as the Diffie Hellman key exchange procedure, El-Gamal cryptosystem and elliptic curve cryptosystem (ECC) respectively [6], [10]. As for the world renowned RSA cryptosystem, the inability to find the e-th root of the ciphertext C modulo N from the congruence relation $C \equiv M^e \pmod{N}$ coupled with the inability to

---

factor $N = pq$ for large primes p and q is its fundamental source of security [11]. Recently, suggestions have been made that the ECC is able to produce the same level of security as the RSA with shorter key length. Thus, ECC should be the preferred asymmetric cryptosystem when compared to RSA [16]. Hence, the notion "cryptographic efficiency" is conjured. That is, to produce an asymmetric cryptographic scheme that could produce security equivalent to a certain key length of the traditional RSA but utilizing shorter keys. However, in certain situations where a large block needs to be encrypted, RSA is the better option than ECC because ECC would need more computational effort to undergo such a task [14]. Thus, adding another characteristic toward the notion of "cryptographic efficiency" which is it must be less "computational intensive". As such, in order to design a state-of-the-art public key mechanism, the above two characteristics must be adhered to apart from other well known security issues. In 1998 the cryptographic scheme known as NTRU was proposed with better "cryptographic efficiency" relative to RSA and ECC [9]. Much effort has been done to push NTRU to the forefront [8].

The cryptographic scheme in this paper is based on what is defined as the Diophantine Equation Hard Problem (DEHP). It is coupled together with the well known integer factorization problem of two large primes. The DEHP is a new form of cryptographic problem based on the Diophantine equation of the form $U = \sum_{i=1}^{n} V_i x_i$. The authors propose that the DEHP as outlined in this paper is also another cryptographic problem that has secure cryptographic qualities coupled with the above described "cryptographic efficiency" qualities.

The layout of this paper is as follows. In Section 2, the Diophantine Equation Hard Problem (DEHP) will be described. The mechanism of the AA $_\beta$-cryptosystem will be detailed in Section 3. Continuing in Section 4, will be discussion on the security features of this cryptosystem. In Section 5 lattice based attacks on the scheme is discussed. Section 6 will be devoted in discussing the consequences of improper design utilizing the DEHP. That is, the possibility of succumbing to a passive adversary attack. The underlying principle and reduction proofs regarding the intractability of the scheme is proposed in Section 7. A numerical example of the scheme as well as an illustration of the DEHP will also be given in this section. Finally, we conclude the paper by comparing "cryptographic efficiency" characteristics against RSA,ECC and NTRU schemes in Section 8.

2 The Diophantine equation hard problem (DEHP)

The DEHP is based upon the linear diophantine equation which is of the form $U = \sum_{i=1}^{n} V_i x_i$. The following definitions would give a precise idea regarding the DEHP.

Definition 1. *Let $U = \sum_{i=1}^{n} V_i x_i^*$ where the integers U and $\{V_i\}_{i=1}^{n}$ are known. We define the sequence of integers $\{x_i^*\}_{i=1}^{n}$ as the preferred integers used to obtain*

U. The sequence $\{x_i^*\}_{i=1}^n$ are particular elements from the set of solutions of $U = \sum_{i=1}^n V_i x_i^*$ that contains infinitely many elements. The problem to determine the sequence $\{x_i^*\}_{i=1}^n$ is known as the DEHP.

Definition 2. *From Definition 1, for $n = 2, V_1 = 1$ and $V_2 = 1$ the DEHP is known as the AA $_\beta$-DEHP-2 (see Section 7).*

Definition 3. *The Diophantine equation given by $U = \sum_{i=1}^n V_i x_i^*$ is defined to be prf-solved when the sequence of integers $\{x_i^*\}_{i=1}^n$ are found in order to obtain U. The DEHP or the AA $_\beta$-DEHP-2 is solved when U is prf-solved.*

Example 1. Let $x_1 = 6143959510671614040, x_2 = 6143959507200090613$ be the preferred solutions for the equation $12287919017871704653 = x_1 + x_2$ where x_1 and x_2 are 2n-bits long (i.e. this example $n = 32$). An attacker would be faced with the AA $_\beta$-DEHP-2 (see Section 7) of determining the preferred integer $x_1 = t$ in order to determine the remaining preferred integer $x_2 = 12287919017871704653 - t$ that form the *prf*-solution set for the above Diophantine equation. Since it is known that x_1 is 64-bits long, the possible values of t resides within the interval $(2^{63}, 2^{64} - 1)$. In other words, there are 2^{64} possible values that x_1 might be.

3 The AA $_\beta$-Cryptosystem

We will now define parameters needed for the renewed AA_β-cryptosystem. The communication model is between two parties A (Along) and B (Busu).

Definition 4. *The ephemeral secret keys for Along are three integers. The integers a_1, a_2 and a_3 are 2n-bits long. The relation between the integers is:*

$$a_1 + a_2 \equiv 0 (mod \ a_1 - a_2) \tag{1}$$

and

$$a_2 + a_3 \equiv v (mod \ a_1 - a_2) \tag{2}$$

where v is $0.8125n$-bits long.

Definition 5. *Let p and q be two prime numbers of n-bit length. Along's public keys are given by*

$$e_{A1} = a_1 + a_2 = pq \tag{3}$$

and

$$e_{A2} = a_1 + a_3 \tag{4}$$

Definition 6. *Along's private key is given by*

$$d_{A1} = a_1 - a_2 = p \tag{5}$$

$$d_{A2} = v \tag{6}$$

Definition 7. *Busu will generate two ephemeral session keys: k_1 and k_2. The keys k_1 and k_2 are $\frac{n}{6}$-bits long.*

Definition 8. *The message that Busu will relay to Along is a $\left(\frac{4n}{5}\right)$-bit integer m.*

Definition 9. *Busu will produce the following ciphertext:*

$$C = k_1 e_{A1} + k_2 e_{A2} + m \tag{7}$$

Proposition 1. $(C(mod\ d_{A1}))(mod\ d_{A2}) = m.$

Proof. We begin with:

$$(C(\mathrm{mod}\ d_{A1})) = k_2 v + m \tag{8}$$

because $k_2 v + m < d_{A1}$. Then,

$$(k_2 v + m(\mathrm{mod}\ d_{A2})) = m \tag{9}$$

because $m < d_{A2}$. $\square$

3.1 The AA $_\beta$ - public key cryptography scheme

We will now discuss the AA $_\beta$-cryptosystem. It is as follows: the scenario is that Busu will send an encrypted message to Along. Along will provide Busu with his public key pair e_{A1} and e_{A2}. Busu intends to send the integer plaintext $P = m$ as in Definition 8. Busu will then proceed to generate the ciphertext C. Then Busu transmits the ciphertext C to Along. Upon receiving the ciphertext from Busu, Along by Proposition 1, can retrieve the integer plaintext $P = m$.

4 Security Features

In this section we will focus on the obvious objective of an attacker. That is to retrieve the plaintext or the private key or both. Discussion would begin by discussing the objective of trying to obtain the plaintext from the ciphertext followed by the objective to obtain the private key embedded within the public key.

4.1 To obtain the plaintext from the ciphertext

As defined in Definition 9, the plaintext resides within C. Thus, the attacker has to *prf*-solve C via the preferred integers k_1 and k_2 the AA $_\beta$-DEHP-1 (see Section 7) given by

$$C = k_1 e_{A1} + k_2 e_{A2} + m \tag{10}$$

The ability to determine the keys k_1 or k_2 would infer that the attacker has also the ability to determine m in the first instance.

4.2 To obtain the private key from the public key via the Diophantine equations

The attacker has to *prf*-solve e_{A1} and e_{A2} via the preferred integers a_1, a_2 and a_3 the AA $_\beta$-DEHP-2 (see Section 7). In congruent with the ability to obtain the plaintext from the ciphertext as discussed above, the ability to determine the keys a_1, a_2 and a_3 would infer that the attacker has also the ability to determine m in the first instance.

5 Lattice based attacks

In this section we put forward two possible attacks via lattices and show that why such attacks will not yield any information detrimental to the scheme.

5.1 Attack with Coppersmith method in the univariate case

We will reproduce Coppersmith's theorem for the benfit of the reader.

Theorem 1. *(Coppersmith) Let N be an integer of unknown factorization, which has a divisor $b \geq N^\beta$. Furthermore, let $f_\beta(x)$ be an univariate, monic polynimial of degree δ. Then we can find all solutions x_0 for the equation $f_\beta \equiv 0 (mod\ b)$ with*

$$\mid x_0 \mid \leq \frac{1}{2} N^{\frac{\beta^2}{\delta} - \epsilon}$$

in polynomial time in $(logN, \delta, \frac{1}{\epsilon})$.

Case 1. We begin by observing $e_{A1} = pq$ where p and q are of equal length. Suppose p is prime integer that satisfies $p > (pq)^\beta$. It is clear that $\beta = \frac{1}{2}$. Let us now observe the polynomials $x - e_{A2}$ and $e_{A1} = pq$ which have a small common root v modulo p. By the polynomial $f_p(x) = x^2 - e_{A2}x + (pq)$ we have the parameter $\delta = 2$. The parameter $\frac{1}{2} N^{\frac{\beta^2}{\delta} - \epsilon}$ is an $(\frac{n}{4})$-bit integer while the parameter v is a $0.8125n$-bit integer. Thus, the bound is much smaller than the root.

Case 2. A more efficient method would be just to observe the polynomial $f_p(x) = x - e_{A2}$. Hence, $\delta = 1$. The parameter $\frac{1}{2} N^{\frac{\beta^2}{\delta} - \epsilon}$ is an $(\frac{n}{2})$-bit integer while the parameter v is a $0.8125n$-bit integer. Thus, the bound is still much smaller than the root.

5.2 Gaussian heuristic

We will look at the the lattice L spanned by $(1, 0, e1), (0, 1, e2), (0, 0, C)$. Observe that the vector $V = (k1, k2, -m)$ is in L. If V is short, then the LLL algorithm will be able to detect V. This is critical since by the usage of the vector $V = (k1, k2, -m)$ it is obvious that the length of m is dominant when compared to

k1 and k2 hence length of V is approximately m. And by the above information m is certainly dominant in the vector V=(k1,k2,-m). Now let us check whether V is really short or not. The Gaussian heuristic for the lattice L is given by:

$$\sigma(L) = \sqrt{(\frac{3}{2\pi e})}C^{1/3} \tag{11}$$

One can see that $\sigma(L)$ is approximately $(\frac{2n}{3})$-bits, while the length of the vector V is $(\frac{4n}{5})$-bits. The Gaussian heuristic is much smaller than the length of the vector V. Thus, the vector V is not considered to be short and cannot be detected by the LLL algorithm.

6 Improper design via the DEHP

It is important to note that, an improper design of an asymmetric cryptosystem via the DEHP would lead to succesful passive adversary attacks. To illustrate this fact, we will produce the following two examples.

6.1 A key exchange mechanism based on the DEHP

Let Along and Busu utilize private 2 X 2 non-singular matrices $\mathbf{A}$ and $\mathbf{B}$ respectively. A base generator $\mathbf{G}$ will be made public. It is a 2 X 2 singular matrix. The parameter $\mathbf{E}_A = \mathbf{AG}$ and $\mathbf{E}_B = \mathbf{GB}$ will be exchanged between Along and Busu. Then Along will compute $\mathbf{EAB} = [\mathbf{A}]\mathbf{E}_B$, while Busu will compute $\mathbf{EBA} = \mathbf{E}_A[\mathbf{B}]$. Now both parties have the same key (i.e. key exchange). If the assumption is that the attacker has to obtain either $\mathbf{A}$ or $\mathbf{B}$ from either $\mathbf{E}_A$ or $\mathbf{E}_B$ this would be the DEHP, since $\mathbf{G}$ is singular. However, an attacker could still compute $\mathbf{A}^{'} \neq \mathbf{A}$ but $\mathbf{A}^{'}\mathbf{G} = \mathbf{AG}$ and as a result is able to compute $\mathbf{A}^{'}\mathbf{E}_B = \mathbf{EAB}$. Thus rendering the scheme insecure. The following is a numerical example.

Example 2. Let

$$\mathbf{G} = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}, \mathbf{A} = \begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}, \mathbf{B} = \begin{pmatrix} 7 & 8 \\ 9 & 10 \end{pmatrix}$$

Along will generate

$$\mathbf{E}_A = \begin{pmatrix} 7 & 14 \\ 14 & 28 \end{pmatrix}$$

and Busu will generate

$$\mathbf{E}_B = \begin{pmatrix} 25 & 28 \\ 50 & 56 \end{pmatrix}$$

The shared key computed by both parties is

$$\mathbf{AGB} = \begin{pmatrix} 175 & 196 \\ 350 & 392 \end{pmatrix}$$

An attacker intercepting $\mathbf{E}_A$ could construct the matrix

$$\mathbf{A}' = \begin{pmatrix} 7 & 0 \\ 14 & 0 \end{pmatrix}$$

It could be observed that $\mathbf{AGB} = \mathbf{A}'\mathbf{GB}$. Hence, a passive adversary attack has been successfully executed.

6.2   Improper integer size

Observe the equation given by

$$e_A = a_1 + a_2 g_1 \tag{12}$$

where e_A and g_1 are public parameters. Let g_1 be of length $2n$-bits, while the private parameters a_1 and a_2 are n-bits long.Because of this improper choice of size, one can obtain

$$a_2 = floor(\frac{e_A}{g_1}) \tag{13}$$

7   The Underlying Security Principle

We will now observe the underlying security principles that the AA_β-cryptosystem is based upon.

7.1   The AA_β-DEHP-1

Determine the preferred integer either (k_1 or k_2) such that $m = C - k_1 e_{A1} (\text{mod } e_{A2})$ or $m = C - k_2 e_{A2} (\text{mod } e_{A1})$.

7.2   The AA_β-DEHP-2

Determine the preferred integers (a_1, a_2, a_3) belonging to the public keys e_{A1} and e_{A2}.

7.3   The integer factorization problem

Let p and q be two large primes. From $e_{A1} = a_1 + a_2 = pq$ obtain $d_{A1} = p$.

7.4   Security reduction

Proposition 2. *AA_β-DEHP-2 $\equiv_T$ Factoring $e_{A1} = pq$.*

Proof. Let θ_1 be an oracle that factors the product of primes. Call $\theta_1(e_{A1})$ to obtain p and q. Then we are able to construct $a_1 = \frac{p(q+1)}{2}$, $a_2 = \frac{p(q-1)}{2}$ and $a_3 = e_{A2} - a_1$. Hence, the preferred integers (a_1, a_2, a_3) are obtained Thus, AA_β-DEHP-2 $\leq_T$ Factoring $e_{A1} = pq$. Let θ_2 be an oracle that obtains the preferred integers (a_1, a_2, a_3). Then obtain $p = a_1 - a_2$ and $\frac{e_{A1}}{p} = q$. Thus, Factoring $e_{A1} = pq \leq_T AA_\beta$-DEHP-2. Hence, AA_β-DEHP-2 $\equiv_T$ Factoring $e_{A1} = pq$. $\square$

Proposition 3. *Decryption $\leq_T$ Factoring $e_{A1} = pq$.*

Proof. Let θ_1 be an oracle that factors the product of primes. Call $\theta_1(e_{A1})$ to obtain p and q. Then determine $v \equiv e_{A2}(\bmod p)$. Now, decryption can occur. $\square$

7.5   Indistinguishability

Proposition 4. *The AA_β public key cryptosystem is IND-CPA.*

Proof. The AA_β public key cryptosystem is a probabilistic cryptosystem. A probabilitic encryption scheme is IND-CPA [16]. Thus the AA_β public key cryptosystem is IND-CPA. $\square$

7.6   Example

We will now provide a clear numerical illustration of the AA_β-cryptosystem for $n = 32$-bits. Along will generate the following secret keys: $a_1 = 6143959510671614040$, $a_2 = 6143959507200090613$, $a_3 = 5113460585870913605$ and $v = 66857602$. Along's public keys are $e_{A1} = 12287919017871704653$ and $e_{A2} = 11257420096542527645$. Observe that e_{A1} is product of two 32-bit primes ($p = 3471523427$ and $q = 3539633039$). Along's private keys are $d_{A1} = 3471523427$ and $d_{A2} = 66857602$. In the meantime Busu will generate $k_1 = 33$ and $k_2 = 32$. The message is $M = 39152991$. The ciphertext generated by Busu is $C = 765738770679166291180$. Finally, $(C(\bmod d_{A1}))(\bmod d_{A2}) = 39152991$. $\square$

8   Conclusion

The AA_β-cryptosystem has the capacity to become a novel public key cryptosystem whose hard mathematical problem is based upon the difficulty of the DEHP and the integer factorization problem of two large primes. Just like the RSA, where the e-th root problem is considered much more difficult than factoring the product of primes, the DEHP could also be considered much more difficult than factoring the product of primes (due to the exponential number of possibilities for the private parameters). The minimum key length for optimum security should be set to $n = 512$-bits. On another note, it is known that the implementation of RSA and ECC is $O(n^3)$ operations where n is the length of the message block [5],[8],[17]. By this fact we can have the following table of comparison.

Algorithm	Encryption Speed	Decryption Speed	Expansion
RSA	$O(n^2)$	$O(n^3)$	1 - 1
ECC	$O(n^3)$	$O(n^3)$	1 - 2 (2 parameter ciphertext)
NTRU	$O(n^2)$	$O(n^2)$	varies
AA_β	$O(n^2)$	$O(n^2)$	1 - 2.7

Table 2

Encryption / decryption speed and message expansion table for message block of length n

One can also note another advantage. That is, since encrypt and decrypt procedures are the basic arithmetic operation of multiplication, the scheme could encrypt messages of large block size with ease. As a result this algorithm is advantageous relative to RSA or ECC (because of better speed) and ECC (because of less computational effort to encrypt/decrypt messages of large block size).

Acknowledgments

References

[1]   M. R. K. Ariffin and N. A. Abu, AA_β-cryptosystem: A chaos based public key cryptosystem, *Int. Jour. Cryptology Research.* vol. 1, no. 2 (2009), pp. 149–163.

[2]   AM. R. K. Ariffin, N. A. Abu and A. Mandangan, Strengthening the AA_β-cryptosystem, *Proc. Second International Cryptology Conference 2010.* (2010), pp. 16–26.

[3]   S. R. Blackburn, The Discrete Log Problem Modulo 1: Cryptanalyzing the Ariffin - Abu cryptosystem, *J. Mathematical Cryptology*, vol. 4, no. 2, (2010), pp. 193–198.

[4]   CR. Bose, Novel Public Key Encryption Techniques Based on Multiple Chaotic Systems, *Physic Review Letters.* vol. 95, issue 9 (2005).

[5]   A. E. Cohen and K. K. Parhi, Implementation of Scalable Elliptic Curve Cryptosystem Crypto-Accelerators for GF(2m), *Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers 1.* (2004), pp. 471–477.

[6]   W. Diffie and M. E. Hellman, New Directions in Cryptography, *IEEE Transactions on Information Theory.* vol. 22, no. 26 (1976), pp. 644–654.

[7]   J. Hoffstein, J. Pipher and J. H. Silverman, An Introduction to Mathematical Cryptography. *New York: Springer.* (2008), pp. 352–358.

[8]   J. Hermans *et. al.*, Speed Records for NTRU, *CT-RSA 2010, LNCS 5985.* (2010), pp. 73–88.

[9]   J. Hoffstein, J. Pipher, J. H. Silverman. NTRU: A Ring Based Public Key Cryptosystem in Algorithmic Number Theory (ANTS III) Lecture Notes in Computer Science 1423, *Springer-Verlag, Berlin.* (1998), pp. 267–288.

[10] N. Koblitz, Elliptic Curve Cryptosystems, *Math. Comp.* vol. 48, no. 177 (1987), pp. 203–209.

[11] R. L. Rivest, A. Shamir and L. Adleman, A method for obtainning digital signatures and public key cryptosystems, *Commun. ACM.* vol. 21, issue 2 (1978), pp. 120–126.

[12] M. Naor and M. Yung, Public-key cryptosystems provably secure against chosen ciphertext attacks., *Proc.22nd Annual ACM Symposium on Theory of Computing*(1990), pp.427–437.

[13] B. Schneier, Key length in Applied Cryptography. *New York: John Wiley & Sons.* (1996), pp. 151–168.

[14] M. Scott, When RSA is better than ECC. (2008, November 15) [Online]. Available: HTTP://WWW.DERKEILER.COM/NEWSGROUPS/SCI.CRYPT/2008-11/MSG00276.HTML

[15] S. S. Wagstaff, Cryptanalysis of Number Theoretic Ciphers, *Divisibility and Arithmetic.* (2003), pp. 27–42.

[16] S. Vanstone, ECC holds key to next generation cryptography. (2006, March 18) [Online].Available: HTTP://WWW.DESIGN-REUSE.COM/ARTICLES/7409/ECC-HOLD-KEY-TO-NEXT-GEN-CRYPTOGRAPHY.HTML

[17] J. Wolkerstorfer and W. Bauer, A PCI-Card for Accelerating Elliptic Curve Cryptography, *Proceedings of Austrochip 2002, Graz, Austria, October 4,* (2002).