A NEW EFFICIENT ASYMMETRIC CRYPTO SYSTEM BASED
ON THE INTEGER FACTORIZATION PROBLEM

M.R.K. ARIFFIN

Abstract. A new asymmetric cryptosystem based on the Integer Factorization
Problem is proposed. It posses an encryption and decryption speed of
$O(n^2)$, thus making it the fastest asymmetric encryption scheme available. It
has a simple mathematical structure. Thus, it would have low computational
requirements and would enable communication devices with low computing
power to deploy secure communication procedures efficiently.

1. Introduction

By textbook convention 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 (DHKE) procedure, El-Gamal
cryptosystem and elliptic curve cryptosystem (ECC) respectively [2], [8]. 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 $C \equiv M^e (mod\ N)$ coupled
with the inability to factor $N = pq$ for large primes $p$ and $q$ is its fundamental
source of security [11]. It has been suggested 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 [10]. 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 [13].
Thus, adding another characteristic toward the notion of “cryptographic efficiency”
which is it must be less “computational intensive” and be able to transmit large
blocks of data (when needed). In 1998 the cryptographic scheme known as NTRU
was proposed with better ”cryptographic efficiency” relative to RSA and ECC [5]
[6] [7]. NTRU has a complexity order of $O(n^2)$ for both encryption and decryption
as compared to DHKE, EL-Gammal, RSA and ECC (all have a complexity order
of $O(n^3)$). As such, in order to design a state-of-the-art public key mechanism, the
following are characteristics that must be “ideally” achieved (apart from other well
known security issues):

(1) Shorter key length. If possible shorter than ECC 160-bits.
(2) Speed. To have speed of complexity order $O(n^2)$ for both encryption and decryption.

(3) Able to increase data set to be transmitted asymmetrically. That is, not to be restricted in size because of the mathematical structure.

(4) Simple mathematical structure for easy implementation.

In this paper, we produce a newly designed asymmetric cryptosystem based on the Integer Factorization Problem. The scheme does not require “expensive” operations. It only requires multiplication and addition for encryption and for decryption it only utilizes multiplication together with a one time modular reduction.

The layout of this paper is as follows. In Section 2, we define the Diophantine Equation Hard Problem (DEHP) which is the source of “mathematical hardness” integrated within the ciphertext equation. The new asymmetric cryptosystem will be detailed in Section 3. In Section 4, the authors detail the decryption process and provide a proof of correctness. An example will also be presented. Continuing in Section 5, we will discuss algebraic attacks. An analysis of lattice based attack will be given in Section 6. Section 7 will be about the underlying security principles of the AA$\beta$ scheme. A table of comparison between the AA$\beta$ scheme against RSA, ECC and NTRU is given in Section 8. Finally, we shall conclude in Section 9.

2. THE DIOPHANTINE EQUATION HARD PROBLEM (DEHP)

In this section we begin by producing a diophantine equation of the form

$$C = Ax + By$$

where $(A, B, C)$ are known integers while $(x, y)$ are unknown integers. Another condition is that $\gcd(A, B) = 1$. We will observe the following 2 cases:

2.1. Case 1. Let the public parameters $(A, B)$ be of length $n$-bits and the secret parameters $(x, y)$ also be of length $n$-bits.

The general solution for $(x, y)$ is given by

- $x = x_0 + Bt$
- $y = y_0 - At$

Since the size if the unknown parameters $(x, y)$ are $n$-bits, from the following inequality

$$2^n - 1 - x_0 < t < 2^n - 1 - x_0$$

and by the fact that $2^n - 1 < B < 2^n - 1$, the interval that the variable $t$ belongs to is approximately given by

$$\frac{2^n}{B} > \frac{2^n}{2^n - 1} \approx 1$$

As a result an attacker could be able to determine the value of $t$ and solve for the unknown pair $(x, y)$ in polynomial time.

2.2. Case 2. Let the public parameters $(A, B)$ be of length $n$-bits and the secret parameters $(x, y)$ be of length $2n$-bits. The general solution for $(x, y)$ is given by

- $x = x_0 + Bt$
- $y = y_0 - At$
A NEW EFFICIENT ASYMMETRIC CRYPTO SYSTEM BASED ON THE INTEGER FACTORIZATION PROBLEM

Since the size if the unknown parameters \((x, y)\) are \(2n\)-bits, from the following inequality
\[
\frac{2^{2n-1}-x_0}{B} < t < \frac{2^{2n}-1-x_0}{B}
\]
and by the fact that \(2^{n-1} < B < 2^n - 1\), the interval that the variable \(t\) belongs to is approximately given by
\[
\frac{2^{2n}}{B} > \frac{2^{2n}}{2^n-1} \approx 2^n
\]
As a result an attacker could not be able to determine the value of \(t\) and solve for the unknown pair \((x, y)\) in polynomial time for sufficiently large \(n\).

2.3. Definition (DEHP). The Diophantine Equation Hard Problem (DEHP) is the problem to determine the preferred solution set \((x, y)\) from
\[
C = Ax + By
\]
where \((A, B, C)\) is known and \((x, y)\) is unknown. A correct implementation of DEHP will be executed as describe in Case 2 above. If the preferred solution set is obtained then the equation \(C\) is said to be \(prf\)-solved.

3. A new asymmetric algorithm based on Integer Factorization Problem

Let us begin by stating that the communication process is between A (Along) and B (Busu), where Busu is sending information to Along after encrypting the plaintext with Along’s public key.

- Key Generation by Along

INPUT: Generate a pair of random \(n\)-bit prime numbers \(p\) and \(q\), an \(n\)-bit odd integer \(k_1, k_2 = \frac{q-k_1}{2}\) and a random \(2n\)-bit integer \(u\). Another condition is that \(p > 2^{n-1} + 2^{n-2}\).
OUTPUT: The public key \(e_1\) and \(e_2\) where

\[
\begin{align*}
& e_1 = u + p(k_1 + k_2) \\
& e_2 = u - pk_2
\end{align*}
\]
and the private key pair \((p, d)\) where \(d \equiv v^{-1} \pmod{p}\) and \(v \equiv u \pmod{p}\).

- Encryption by Busu

INPUT: The public key \((e_1, e_2)\) and the message \(M\) where \(M\) is an \(n\)-bit integer within the interval \((2^{n-1}, 2^n - 1)\) and \(M < 2^{n-1} + 2^{n-2}\). As a result \(M < p\).
OUTPUT: The ciphertext \(C = Xe_1 - Ye_2\).

- Decryption by Along

INPUT: The private key pair \((p, d)\) and the ciphertext \(C\).
OUTPUT: The plaintext \(M\).

4. Decryption

**Proposition 4.1.** \(Cd \equiv M \pmod{p}\).
We now proceed to give a proof of correctness.

Proof. \(Cd \equiv X - Y \equiv M \pmod{p}\). Observe that, modular reduction does not occur since \(M < p\). \(\square\)

4.1. Example. Let \(n = 16\). Along will choose the primes \(p = 65287\) and \(q = 40829\). Then Along chooses the following private parameters:

(1) \(k_1 = 46381\)
(2) \(k_2 = -2776\)
(3) \(u = 3096817651\)
(4) \(d = 49913\)

The public keys will be

(1) \(e_1 = 5943657286\)
(2) \(e_2 = 3278054363\)

Busu’s message will be \(M = 43963\) with the following accompanying parameters

(1) \(X = 281474976710656\)
(2) \(Y = 281474976666693\)

The ciphertext will be \(C = 750300520815394662808057\). To decrypt is arbitrary. \(\square\)

5. Algebraic Attacks

5.1. Computing with X. To find \(X = X_0 + e_2j\), we should find an integer \(j\) such that \(2^{3n-1} < X < 2^{3n} - 1\). This gives

\[
\frac{2^{3n-1} - X_0}{e_2} < j < \frac{2^{3n} - 1 - X_0}{e_2}.
\]

We know that \(2^{2n-1} < e_2 < 2^{2n} - 1\). Then the difference between the upper and the lower bound is

\[
\frac{2^{3n} - 1 - X_0}{e_2} - \frac{2^{3n-1} - X_0}{e_2} \approx \frac{2^{3n}}{e_2} - \frac{2^{3n} - 1}{2^{2n} - 1} \approx 2^n.
\]

Hence the difference is very large and finding the correct \(j\) is infeasible.

Remark 5.1. If one attempts to compute with \(Y\) the above scenario when computing with \(X\) would appear.

5.2. Euclidean division attack. From \(C = Xe_1 - Ye_2\), the size of each public parameter within \(C\) ensures that Euclidean division attacks does not occur. This can be easily deduced as follows:

(1) \(\lfloor \frac{C}{e_1} \rfloor \neq X\)
(2) \(\lfloor \frac{C}{e_2} \rfloor \neq Y\)
A NEW EFFICIENT ASYMMETRIC CRYPTOSYSTEM BASED ON THE INTEGER FACTORIZATION PROBLEM

6. ANALYSIS ON LATTICE BASED ATTACK

With reference to the $AA_{B}$ scheme in [1] which has gone through square lattice attack, the ciphertext equation in this article is of the same structure. Recall that the structure of the ciphertext $AA_{B}$ scheme is as follows:

$$C = Ue_{A1} + V^2e_{A2}$$

where both $(U, V^2)$ are of size $4n$-bits, while both $(e_{A1}, e_{A2})$ are of size $3n$-bits. That is, the unknown parameters are larger by $n$-bits from the known parameters. It is by this fact that the square lattice attack as described in [1] failed upon the $AA_{B}$ scheme.

Now, observe that the ciphertext in this article also has its unknown parameters to be larger by $n$-bits than the known parameters. It is arbitrary to replicate the empirical evidence by executing the LLL algorithm upon the scheme in this article to see that the square lattice attack will not succeed.

7. UNDERLYING SECURITY PRINCIPLES

7.1. The public key Integer Factorization Problem. Observe that one can obtain $e_1 - e_2 = pq$. This is obviously the Integer Factorization Problem.

7.2. The ciphertext DEHP. To find the preferred solution set $(X, Y)$ such that $C = Xe_{1} - Ye_{2}$.

8. TABLE OF COMPARISON

The following is a table of comparison between RSA, ECC, NTRU and the scheme in this article. Let $|E|$ denote public key size.

| Algorithm         | Encryption Speed | Decryption Speed | Ratio $M:C$ | Ratio $M:|E|$ |
|-------------------|------------------|------------------|-------------|-------------|
| RSA               | $O(n^3)$         | $O(n^3)$         | 1 : 1       | 1 : 2       |
| ECC               | $O(n^3)$         | $O(n^3)$         | 1 : 2       | 1 : 2       |
| NTRU              | $O(n^2)$         | $O(n^2)$         | Varies [5]  | N/A         |
| Scheme in this paper | $O(n^2)$         | $O(n^2)$         | 1 : 5       | 1 : 4       |

Table 1. Comparison table for input block of length $n$

9. CONCLUSION

The asymmetric scheme presented in this paper provides a secure avenue for implementors who need encryption and decryption speed of complexity order $O(n^2)$.

REFERENCES

1. M.R.K.Ariffin, M.A.Asbullah and N.A.Abu A New Efficient Asymmetric Cryptosystem Based on the Square Root Problem.[Online]. Available: HTTP://ARXIV.ORG/PDF/1207.1157V2 2012.
2. W. Diffie and M. E. Hellman, “New Directions in Cryptography,” Proc. IEEE Transactions on Information Theory, pp. 644–654, 1976.
3. S.D.Galbraith, Mathematics of Public Key Cryptography, Cambridge University Press, 2012.
4. J. Hoffstein, J. Pipher and J. H. Silverman, An Introduction to Mathematical Cryptography. New York: Springer, 2008.
5. J. Hoffstein, D. Lieman, J. Pipher and J. H. Silverman, *NTRU: A Public Key Cryptosystem*, NTRU Cryptosystems Inc. [Online]. Available: http://grouper.ieee.org/groups/1363/lattPK/submissions/ntru.pdf 2008.
6. J. Hermans et. al., “Speed Records for NTRU,” *CT-RSA 2010, LNCS 5985*, pp. 73–88, 2010.
7. J. Hoffstein, J. Pipher, J. H. Silverman. “NTRU: A Ring Based Public Key Cryptosystem in Algorithmic Number Theory,” *Lecture Notes in Computer Science 1423*, pp. 267–288, 1998.
8. N. Koblitz, “Elliptic Curve Cryptosystems,” *Math. Comp.*, pp. 203–209, 1987.
9. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*, CRC Press, 1996.
10. M. O. Rabin, Digitalized signatures and public-key functions as intractable as factorization, Tech. Report MIT/LCS/TR-212, MIT Laboratory for Computer Science, 1979.
11. R. L. Rivest, A. Shamir and L. Adleman, “A method for obtaining digital signatures and public key cryptosystems,” *Commun. ACM*, pp. 120–126, 1978.
12. B. Schneier, *Key length in Applied Cryptography*. New York: Wiley & Sons, 1996.
13. M. Scott, When RSA is better than ECC,[Online]. Available: http://www.derkeiler.com/Newsgroups/sci.crypt/2008-11/msg00276.html 2008.
14. S. S. Wagstaff, *Cryptanalysis of Number Theoretic Ciphers*, Chapman & Hall, 2003.
15. H. C. Williams, A modification of the RSA public key encryption procedure, *IEEE Trans. Inf. Theory* 26 (1980), no. 6, 726729.
16. S. Vanstone, *ECC holds key to next generation cryptography*,[Online]. Available: http://www.design-reuse.com/articles/7409/ecc-hold-key-to-next-gencryptography.html 2006.

**Al-Kindi Cryptography Research Laboratory, Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM, Serdang, Selangor, MALAYSIA**

**Current address:** Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, 43400 UPM, Serdang, Selangor, MALAYSIA

**E-mail address:** rezal@putra.upm.edu.my