AA_β Public Key Cryptosystem - An Asymmetric Cryptosystem based on the Diophantine Equation Hard 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@putra.upm.edu.my,[b]ma_asyraf@putra.upm.edu.my,[c]nura@utem.edu.my

1 Introduction

We begin with 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. We begin by stating first the public parameter θ which is an n-bit prime number and $\theta > 2^{n-1} + 2^{n-2}$.
Now, Along's secret parameters are:

1. An n-bit integer d.
2. A $4n$-bit integer δ.

The following are public values that could be obtained from the published public key set.

1. A $4n$-bit integer α_1 where $\alpha_1 d \equiv \theta (\text{mod } \delta)$.
2. A $2n$-bit prime integer α_2.
3. A $4n$-bit integer α_3 where $\alpha_3 d \equiv 1 (\text{mod } \delta)$.

The following are Along's published public keys:

1. Along's public key 1: $e_{A1} = \theta$.
2. Along's public key 2: $e_{A2} = \alpha_3\theta - \alpha_1 :\approx 5n$-bits.
3. Along's public key 3: $e_{A3} = \alpha_2\alpha_3 :\approx 6n$-bits.

Remark 1. Observe that $\gcd(e_{Ai}, e_{Aj}) = 1$.

Busu's secret parameters are:

1. The message components are given by the integers:
   - $m_1 : n$-bits
   - $m_2 : 5n$-bits
   - $m_3 : n$-bits where $m_3 < 2^{n-1} + 2^{n-2}$
2. The message given by an even integer $M = m_1 m_2 m_3$.

2 Encryption

The encryption of the message is given by the ciphertext $C = m_1 e_{A1} + m_2 e_{A2} + m_3 e_{A3}$ which is approximately $10n$-bits. The length of the message is $7n$-bits. The ratio size between message and ciphertext is approximately $1 : 1.4$.

3 Decryption

To begin decryption do:

$$W_1 \equiv Cd \equiv (m_1\theta d + m_3\alpha_2)(\mathrm{mod}\delta)$$

which is exactly $W_1 = m_1\theta d + m_3\alpha_2$. Continuing, compute:

$$W_2 \equiv W_1 \equiv m_3\alpha_2(\mathrm{mod}\ \theta)$$

Then retrieve

$$m_3 \equiv \alpha_2^{-1} W_2(\mathrm{mod}\ \theta)$$

Thus, Along now has the m_3. He can proceed to obtain m_1 and then m_2 trivially.□

We now proceed to give a proof of correctness.

Proof. Let $\gamma_1 = m_1\theta d + m_3\alpha_2$. Since $\gamma_1 < \delta$, we have $W_1 = \gamma_1$. Let $\gamma_2 \equiv \alpha_2^{-1} W_2 \equiv m_3(\mathrm{mod}\ \theta)$. Since $m_3 < \theta$, $\gamma_2 = m_3$. Obtaining m_1 and m_2 is trivial.□

4 Example

Let $n = 32$. Along's secret parameters are:

1. $d = 2729352959$
2. $\delta = 123602780311578972764937793425044807559$

Along's public values are:

1. $\alpha_1 = 380251062454108988000178013603826576675$
2. $\alpha_2 = 11565865260296943587$
3. $\alpha_3 = 231603566871861480588581594612440061 21$

Along's public keys are:

1. $e_{A1} = 3654483977$
2. $e_{A2} = 84639152034675516843337808666649159252657846542$
3. $e_{A3} = 267869564824412276378056513521652795772741039119819696027$

Busu's secret message parameters are:

1. $m_1 = 3343624388$

2. $m_2 = 1006071385193363690376938086628136144034563233508$
3. $m_3 = 2555991201$

Thus, the message is $M = 859816223972687713801499739799615973590374638100333875816849227790 4$. The ciphertext is given by
$C = 851530289291177040439672831000688513528159545256534693320086371662722172050511811171621$
35418839.

Upon receiving the ciphertext Along will compute

$$W_1 = Cd(\text{mod } \delta) = 629128188801826767657698953187 1$$

and

$$W_2 = W_1(\text{mod } \theta) = 3639866374$$

Along will then proceed to compute

$$m_3 \equiv \alpha_2^{-1} W_2(\text{mod } \theta) = 2555991201.$$

Continuing, Along will do

$$m_1 = \frac{C - m_3 e_{A3}(\text{mod } e_{A2})}{e_{A1}} = 3343624388$$

Finally, Along can obtain

$$m_2 = \frac{C - m_1 e_{A1} - m_3 e_{A3}}{e_{A2}} = 1006071385193363690376938086628136144034563233508$$

Along can now construct the message.□

5 Analysis on lattice based attack

We will now look at the the lattice L_1 spanned by the matrix:

$$M = \begin{pmatrix} 1 & 0 & 0 & e_{A1} \\ 0 & 1 & 0 & e_{A2} \\ 0 & 0 & 1 & e_{A3} \\ 0 & 0 & 0 & C \end{pmatrix}$$

Observe that the vector $V = (m_1, m_2, m_3, 0)$ is in L_1. If V is short, then the LLL algorithm will be able to detect V. Now let us check whether V is really short or not. The Gaussian heuristic for the lattice L_1 is given by:

$$\sigma(L_1) = \sqrt{(\frac{4}{2\pi e})} C^{1/4}$$

One can see that $\sigma(L_1)$ is approximately $\frac{5n}{2}$-bits, while the length of the vector V is approximately $5n$-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 Analysis on extended lattice based attack

We will now look at the lattice L_2 spanned by the matrix:

$$M = \begin{pmatrix} 1\ 0\ 0\ e_{A1}K \\ 0\ 1\ 0\ e_{A2}K \\ 0\ 0\ 1\ e_{A3}K \\ 0\ 0\ 0\ -CK \end{pmatrix}$$

Observe that the vector $V = (m_1, m_2, m_3, 0)$ is in L_2. If V is short, then the LLL algorithm will be able to detect V. Now let us check whether V is really short or not. The Gaussian heuristic for the lattice L_2 is given by:

$$\sigma(L_2) = \sqrt{(\frac{4}{2\pi e})}(CK)^{1/4}$$

Choose K such that $\sigma(L_2) > \|V\|$. Hence, K has to satisfy

$$K > (\frac{\pi \exp(1)}{2})^2 \cdot \frac{2^{4n}}{C}$$

An experiment was conducted to visualize this method. The LLL algorithm outputs a basis matrix in the form

$$ML = \begin{pmatrix} a_{11}\ a_{12}\ a_{13}\ 0 \\ a_{21}\ a_{22}\ a_{23}\ 0 \\ a_{31}\ a_{32}\ a_{33}\ 0 \\ a_{41}\ a_{42}\ a_{43}\ K \end{pmatrix}$$

Continuing the attck by **utilizing the method as introduced by Abderrahmane in Draft 4**, the parameters m_1, m_2, m_3 did not appear.

6.1 Example with extended lattice based attack

In this example Maple 13 was used. We will use the parameters in the earlier example in Section 4. Observe the lattice L_2 spanned by the matrix:

$$M = \begin{pmatrix} 1\ 0\ 0\ e_{A1}K \\ 0\ 1\ 0\ e_{A2}K \\ 0\ 0\ 1\ e_{A3}K \\ 0\ 0\ 0\ -CK \end{pmatrix}$$

the length of the vector $V = (m_1, m_2, m_3, 0)$ is
$\| V \| \approx 100607138519336369037693808662813765386252950499 6$.
We will use $K = 2^{37n}$ which would result in the length of the vector $V = (m_1, m_2, m_3, 0)$ is shorter than the gaussian heuristic of the lattice L_2.

The LLL algorithm outputs:

$$ML = \begin{pmatrix} -4561287656758210484974982277 3 & -6560587702754182404791901291 6 & \lambda_1 & 0 \\ 8139920034089290547537056088 7 & -9780033294833833354030300892 9 & \lambda_2 & 0 \\ 1547732058407404781196213134 0 & 6069551379617859720737156815 8 & \lambda_3 & 0 \\ -2030031355007717847779998566 5 & -2069605101321612982153298951 5 & \lambda_4 & -K \end{pmatrix}$$

where $\lambda_1 = 20729588397567664249$, $\lambda_2 = 30902119429224734484$, $\lambda_3 = 3178899003952635616806100179912637842 35$ and $\lambda_4 = 6539362605867270281$. Continuing the procedure by Abderrahmane we focus on the equation:

$$m_3 = \lambda_1 x_1 + \lambda_2 x_2 + \lambda_3 x_3$$

because m_3 is the shortest parameter among the three secret parameters from Busu.

Now consider the equation:

$$[\frac{\lambda_1}{2^{4n}}]x_1 + [\frac{\lambda_2}{2^{4n}}]x_2 + [\frac{\lambda_3}{2^{4n}}]x_3 \approx 1$$

Then we consider the matrix:

$$MK_1 = \begin{pmatrix} 1 & 0 & [\frac{20729588397567664249}{2^{4n}}] \\ 0 & 1 & [\frac{30902119429224734484}{2^{4n}}] \\ 0 & 0 & -[\frac{3178899003952635616806100179912637842 35}{2^{4n}}] \end{pmatrix}$$

which is

$$MK_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

Applying the LLL algorithm on MK_1 we get:

$$ML_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

Which gives us $x_1 = 1, x_2 = 0, x_3 = 0$. Finally, one can have $m_1^{'} = 4561287656758210484974982277 3$, $m_2^{'} = 6560587702754182404791901291 6$ and $m_3^{'} = 20729588397567664249$.□

Remark 2. An interesting observation is that $ML(3,1)e_{A1} + ML(3,2)e_{A2} + ML(3,3)e_{A3} = C$.

7 Euclidean division attacks

From $C = k_1 e_{A1} + k_2 e_{A2} + k_3$, the size of each public parameter within C ensures that Euclidean division attacks does not occur.

8 The work by Herrman and May

With reference to the work by Herrman and May: Solving Linear Equations Modulo Divisors: On Factoring Given Any Bits as cited by Prof. Abderrahmane Nitaj in Draft 1 - 3.

We quote the objective of the work by Hermann and May as stated in their abstract and introduction: "to find solutions for linear equations modulo an unknown divisor p of a known composite $N = pq$. From:

$$f(x_1, ..., x_n) = a_1x_1 + ... + a_nx_n = 0(\text{mod } N) \tag{1}$$

for some N with unknown factorization. Equation (3) has many solutions $(y_1, ..., y_n) \in \mathbb{Z}_N^n$. It is stated that if X_i are upper bounds such that $|y_i| \leq X_i$ then one can roughly expect a unique solution when $\prod_i X_i \leq N$. And the work by Hermann and May suggests a technique to obtain the solution set.

The design in this article is not related to the problem of finding the secret prime composites p and q of the public value $N = pq$. Nevertheless, it would be interesting to state its equivalent statement.

8.1 The Hermann and May AA_β statement

The equivalent statement for the proposed AA_β-cryptosystem is "to find a **"solution"** for a linear equation modulo an unknown **"composite"** δ (and its corresponding d) from a known **"summation composite"** α_1 and α_3" such that $\alpha_1 d \equiv \theta(\text{mod } \delta)$ and $\alpha_3 d \equiv 1(\text{mod } \delta)$ - that is, to find the prf-solution for α_1 and α_3.

9 Modulo public key type attack

Conducting a modulo operation using any public key would result in modular reduction of the remaining terms.

10 Table of Comparison

The following is a table of comparison between RSA, ECC, NTRU and AA_β.

Algorithm	Encryption Speed	Decryption Speed	Message Expansion
RSA	$O(n^3)$	$O(n^3)$	1-1
ECC	$O(n^3)$	$O(n^3)$	1-2 (i.e. 2 parameter ciphertext)
NTRU	$O(n^2)$	$O(n^2)$	Varies
AA_β	$O(n^2)$	$O(n^2)$	1-1.4

Table 1. Comparison table for input block of length n

11 Conclusion

The DEHP, is proposed to be another source of cryptographic primitive, that if utilized correctly could give rise to other possible asymmetric algorithms differing from classical algorithms based on integer factorization, discrete log problem (DLP), elliptic curve discrete log problem (ECDLP), e -th root modulo N, square root problem and others. Its speed and fixed message expansion ratio makes it "advantageous" to other well known asymmetric algorithms as given in Table 1.

Acknowledgments

The authors would like to thank Dr. Yanbin Pan of Key Laboratory of Mathematics Mechanization Academy of Mathematics and Systems Science, Chinese Academy of Sciences Beijing, China, Dr. Gu Chunsheng of School of Computer Engineering, Jiangsu Teachers University of Technology, Jiangsu Province, China and the most recent commenter Prof. Dr. Abderrahmane Nitaj of Département de Mathématiques, Université de Caen, France for valuable comments and discussion.