A new security notion for asymmetric encryption Draft #19

Muhammad Rezal Kamel Ariffin[1,2]

[1] Al-Kindi Cryptography Research Laboratory,
Institute for Mathematical Research,
[2] Department of Mathematics, Faculty of Science,
Universiti Putra Malaysia (UPM), Selangor, Malaysia
rezal@upm.edu.my

Abstract. A new practical asymmetric design is produced with desirable characteristics especially for environments with low memory, computing power and power source.

KEYWORDS: asymmetric security, diophantine equations

1 Key Generation

1. Generate random n-bit primes $p_0, p_1, p_2, p_3, p_5, p_6, s, u, v, e$ and where $u > v$ and $p_0 \equiv 3 \pmod 4$.
2. Compute root for $P(x) = p_2 x^u + (p_5 - p_6)x^v - p_3 \pmod{p_0}$, denoted by r. If roots does not exist, try with new parameters. Observe that we will have $p_2 r^u + p_5 r^v \equiv p_6 r^v + p_3 \pmod{p_0}$. We denote $t \equiv p_6 r^v + p_3 \pmod{p_0}$.
3. Compute $e_1 \equiv st(1 - \frac{1}{p_1}) \pmod{p_0}$.
4. Compute $e_2 \equiv sp_2 r^u \pmod{p_0}$.
5. Compute $e_3 \equiv sp_3 \pmod{p_0}$.
6. Compute $e_4 \equiv \frac{t}{p_1 r^v} \pmod{p_0}$.
7. Compute $e_5 \equiv p_5 \pmod{p_0}$.
8. Compute $e_6 \equiv p_6 \pmod{p_0}$.
9. Keep (p_2, p_3, s, u, v, r) secret and publish $(e_1, e_2, e_3, e_4, e_5, e_6)$ as public keys.
10. The integer p_0 can be published but is of no use during encryption (we will see in Section 4).

Remark 1. We can have the congruence relation:

$$e_2 e_6 + e_3 e_4 + e_1 e_5 - e_1 e_6 - e_3 e_5 - e_2 e_4 \equiv 0 \pmod{p_0}$$

2 Encryption

1. Message is $b_0 \approx 2^{n-1}$ and $b_1, b_2 \approx 2^{jn-1}$.
2. Compute $b_3 = b_0^2 - b_1 - b_2$.
3. Compute $C_1 = b_1 e_1 + b_2 e_2 + b_3 e_3$ and $C_2 = b_1 e_4 + b_2 e_5 + b_3 e_6$.
4. Send (C_1, C_2) to recipient.

3 Decryption

1. Compute $((\frac{C_1}{s}+C_2(r^v))\frac{1}{t})^{\frac{p_0+1}{4}} \equiv \pm b_0 \pmod{p_0}$.
2. Let $b_{01} = +b_0 \pmod{p_0}$ and $b_{02} = -b_0 \pmod{p_0}$
3. Solve the system of equations:

$$b_{0i}^2 = b_1 + b_2 + b_3 \quad (1)$$
$$C_1 = b_1e_1 + b_2e_2 + b_3e_3 \quad (2)$$
$$C_2 = b_1e_4 + b_2e_5 + b_3e_6 \quad (3)$$

for $i = 1, 2$. Either $i = 1$ or $i = 2$ will obtain $(b_1, b_2) \in \mathbb{Z}$.

Proposition 1. *The decryption procedure is correct.*

Proof. $((\frac{C_1}{s}+C_2(r^v))\frac{1}{t})^{\frac{p_0+1}{4}} \equiv (\frac{t}{t})(b_1+b_2+b_3)^{\frac{p_0+1}{4}} \equiv (b_0^2)^{\frac{p_0+1}{4}} \equiv \pm b_0 \pmod{p_0}$.

To obtain $(b_1, b_2) \in \mathbb{Z}$ from the system of equations $(1) - (3)$ is trivial. Only the correct root b_{0i} would provide integral solutions. □

4 Desirable properties

This section must be treated with caution. It is only meaningful if there does not exist "trivial" attacks on the scheme.
In this section we list down some "desirable" properties induced within the key generation procedures that disallows an adversary to construct "usable" information; either to reconstruct the plaintext or the private keys.

1. The ratio plaintext to ciphertext is $2j+1 : 2(j+1)$. As j gets larger the ratio is $\approx 1:1$.
2. From (C_1, C_2), determine (b_0, b_1, b_2). From section 2, this is impossible because of $b_1b_2b_3 \approx 2^{3jn} > C_1 \approx 2^{(j+1)n}$ and $b_2b_3 \approx 2^{2jn} > C_2 \approx 2^{(j+1)n}$ (refer to article by Hermann and May).
3. From section 2 it can be viewed as the problem to solve 3 unknowns in 2 equations.
4. From e_1 determine the pair (s, t). That is from $e_1 = st(1-\frac{1}{p_1})+p_0k$ determine (s, t). We conjecture that this is much harder than the question from $N = st$ determine (s, t).
5. At the moment if (s, t) is obtained, the adversary can obtain the value:
   (a) $p_2r^u \pmod{p_0}$ from e_2.
   (b) $p_3 \pmod{p_0}$ from e_3.
6. From point 3 and 4, if the pair is (s, t) is obtained, in order to proceed to find the root of the equation $P(x) = p_2x^u + (p_5 - p_6)x^v - p_3 \pmod{p_0}$, the following are still unknown: (p_2, u, v).
7. Observe that $(e_1 \pm e_4) \not\equiv (e_2 \pm e_5) \not\equiv (e_3 \pm e_6) \not\equiv 1 \pmod{p_0}$. Thus, $C_1 \pm C_2 \not\equiv b_1 + b_2 + b_3 \equiv b_0^2 \pmod{p}$.

8. From the matrix relation $C_0 X = Y$, where:

$$C_0 = \begin{pmatrix} e_1 & e_4 \\ e_2 & e_5 \\ e_3 & e_6 \end{pmatrix}, X = \begin{pmatrix} s \\ r \end{pmatrix}, Y = \begin{pmatrix} t' \\ t' \\ t' \end{pmatrix}$$

where t' is chosen at random, the matrix C_0 is a non square matrix. Hence, non-invertible.
9. Choose at random $d'_1, d'_2 \in \mathbb{Z}_{p_0}$. Let $e_1 d'_1 + e_4 d'_2 \equiv t' \pmod{p_0}$. The probability that:
(a) $e_2 d'_1 \pm e_5 d'_2 \equiv t' \pmod{p_0}$
(b) $e_3 d'_1 \pm e_6 d'_2 \equiv t' \pmod{p_0}$
is negligible.
10. Observe that the determinant of C_0 is $det(C_0) = e_2e_6 + e_3e_4 + e_1e_5 - e_1e_6 - e_3e_5 - e_2e_4$. Thus, $det(C_0) \equiv 0 \pmod{p_0}$ (see Remark 1). Hence, the encryption procedure should not utilize the modular p_0 operation (would result in decryption failure - since the inverse of C_0 modulo p_0 does not exist.
11. Determine $(s', r', t') \in \mathbb{Z}_{p_0}$ such that $((\frac{C_1}{s'} + C_2(r'))\frac{1}{t'}) \equiv \pm b_0 \pmod{p_0}$.