A new security notion for asymmetric encryption Draft #18 Ver 1.0

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 $p_1, p_2, p_3, p_4, p_5, s, u, v$ and where $u > v$ and $p_1 \equiv 3 \pmod 4$.
2. Compute root for $P(x) = p_2x^u + (p_4 - p_5)x^v - p_3 \pmod{p_1}$, denoted by r. If roots does not exist, try with new parameters. Observe that we will have $p_2r^u + p_4r^v \equiv p_5r^v + p_3 \pmod{p_1}$. We denote $t \equiv p_5r^v + p_3 \pmod{p_1}$.
3. Compute $e_1 \equiv st \pmod{p_1}$.
4. Compute $e_2 \equiv sp_2r^u \pmod{p_1}$.
5. Compute $e_3 \equiv sp_3 \pmod{p_1}$.
6. Compute $e_4 \equiv p_4 \pmod{p_1}$.
7. Compute $e_5 \equiv p_5 \pmod{p_1}$.
8. Keep (p_2, p_3, s, u, v, r) secret and publish $(e_1, e_2, e_3, e_4, e_5, p_1)$ as public keys.

Remark 1. We can have the congruence relation:

$$(e_2 - e_1)e_5 + (e_1 - e_3)e_4 \equiv 0 \pmod{p_1}$$

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 $C_1 = b_1e_1 + b_2e_2 + b_3e_3$ and $C_2 = b_2e_4 + b_3e_5$.
4. Send (C_1, C_2) to recipient.

3 Decryption

1. Compute $((\frac{C_1}{s} + C_2(r))\frac{1}{t})^{\frac{p+1}{4}} \equiv \pm b_0 \pmod{p_1}$.
2. Let $b_{01} = +b_0 \pmod{p_1}$ and $b_{02} = -b_0 \pmod{p_1}$
3. Solve the system of equations:

$$b_{0i}^2 = b_1 + b_2 + b_3 \tag{1}$$
$$C_1 = b_1 e_1 + b_2 e_2 + b_3 e_3 \tag{2}$$
$$C_2 = b_2 e_4 + b_3 e_5 \tag{3}$$

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. $((\frac{C_1}{s} + C_2(r))\frac{1}{t})^{\frac{p+1}{4}} \equiv (\frac{t}{t})(b_1 + b_2 + b_3)^{\frac{p+1}{4}} \equiv (b_0^2)^{\frac{p+1}{4}} \equiv \pm b_0 \pmod{p_1}$.

To obtain $(b_1, b_2) \in \mathbb{Z}$ from the system of equations $(1) - (3)$ is trivial.□

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. From (C_1, C_2), determine (b_0, b_1, b_2). From section 2, this is impossible because of $b_1 b_2 b_3 \approx 2^{3jn} > C_1 \approx 2^{(j+1)n}$ and $b_2 b_3 \approx 2^{2jn} > C_2 \approx 2^{(j+1)n}$ (refer to article by Hermann and May).
2. From section 2 it can be viewed as the problem to solve 3 unknowns in 2 equations.
3. From e_1 determine the pair (s, t). That is from $e_1 = st + p_1 k$ determine (s, t). We conjecture that this is much harder than the question from $N = st$ determine (s, t).
4. At the moment if (s, t) is obtained, the adversary can obtain the value:
   (a) $p_2 r^u \pmod{p_1}$ from e_2.
   (b) $p_3 \pmod{p_1}$ from e_3.
5. From point 3 and 4, if the pair is (s, t) is obtained, in order to proceed to find the root of the equation $P(x) = p_2 x^u + (p_4 - p_5)x^v - p_3 \pmod{p_1}$, the following are still unknown: (p_2, u, v).
6. Observe that $e_1 \not\equiv (e_2 \pm e_4) \not\equiv (e_3 \pm e_5) \not\equiv 1 \pmod{p_1}$. Thus, $C_1 \pm C_2 \not\equiv b_1 + b_2 + b_3 \equiv b_0^2 \pmod{p}$.
7. Let $e_1 d_1' \equiv t' \pmod{p_1}$. The probability that:
   (a) $e_2 d_1' \pm e_4 d_2' \equiv t' \pmod{p_1}$
   (b) $e_3 d_1' \pm e_5 d_2' \equiv t' \pmod{p_1}$
   is negligible.
8. Determine $(s', r', t') \in \mathbb{Z}_{p_1}$ such that $((\frac{C_1}{s'} + C_2(r'))\frac{1}{t'}) \equiv \pm b_0 \pmod{p_1}$.