# A new security notion for asymmetric encryption Draft #14

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 primes $p, p_1, p_2, t_1, t_2, k_1, g_1$ n-bits.
2. Generate $e$ where $gcd(e, p-1) = 1$. Compute $d_0 \equiv e^{-1} \pmod{p}$.
3. Compute $A = p_1 - t_1$, $B = p_2 - t_2$ and $u = gcd(B, p-1)$.
4. Compute $a \equiv g_1^A \pmod{p}$.
5. Compute $d_B = \frac{u}{B} \pmod{\frac{p-1}{u}}$.
6. Compute $g_2 \equiv a^{d_B} \pmod{p}$. That is $g_1^A \equiv g_2^{\frac{B}{u}} \pmod{p}$.
7. Generate random $v$ n-bits. Compute $k_2 = vu + t_2$.
8. Compute $w \equiv g_1^{p_1-k_1} g_2^{\frac{k_2-t_2}{u}} - g_1^{k_1-t_1} g_2^{\frac{p_2-k_2}{u}} \pmod{p}$.
9. Compute $e_1 \equiv g_1^{k_1-t_1} \pmod{p}$ and $e_2 \equiv g_2^{\frac{k_2-t_2}{u}} \pmod{p}$.
10. Compute $a_1 \equiv \frac{1-e_1}{w} \pmod{p}$ and $a_2 \equiv \frac{e_2-1}{w} \pmod{p}$.
11. Compute $e_3 \equiv a_1 g_1^{p_1-k_1} + a_2 g_2^{\frac{p_2-k_2}{u}} \pmod{p}$.
12. Compute $d_1 \equiv a_1 g_2^{\frac{p_2-k_2}{u}} + a_2 g_1^{p_1-k_1} \pmod{p}$
13. Publish $(e_1, e_2, e_3)$.
14. Keep $(d_0, d_1, p)$ private.

*Remark 1.* We can re-write $e_2, e_3$ and $d_1$ as follows:

1. $e_2 \equiv g_1^{Ad_B \frac{k_2-t_2}{u}} \pmod{p}$.
2. $e_3 \equiv \frac{1}{w}\left(g_1^{p_1-k_1} - g_2^{\frac{p_2-k_2}{u}}\right) \pmod{p}$
3. $d_1 \equiv \frac{1}{w}\left(g_2^{\frac{p_2-k_2}{u}} - g_1^{p_1-k_1}\right) + 1 \pmod{p}$

*Remark 2.* We can have the congruence relation:

$$e_3 + d_1 - 1 \equiv 0 \pmod{p}$$

## 2 Encryption

1. Message is $b_0 \approx 2^{n-1}$ and $b_1, b_2 \approx 2^{en}$.
2. Compute $b_3 = b_0^e - b_1 - b_2$.
3. Compute $C_1 = b_1 + b_2(e_2e_3) + b_3(e_1e_3)$ and $C_2 = b_2e_1 + b_3e_2$.
4. Send $(C_1, C_2)$ to recipient.

## 3 Decryption

1. Compute $(C_1 + C_2(1 - d_1))^{d_0} \equiv b_0 \pmod{p}$.
2. Solve the system of equations:

$$b_0^e = b_1 + b_2 + b_3 \tag{1}$$
$$C_1 = b_1 + b_2(e_2e_3) + b_3(e_1e_3) \tag{2}$$
$$C_2 = b_2e_1 + b_3e_2 \tag{3}$$

to obtain $(b_1, b_2)$.

**Proposition 1.** *The decryption procedure is correct.*

*Proof.* $(C_1 + C_2(1 - d_1))^{d_0} \equiv (b_1 + (a_1b_3 - a_2b_2)(g_1^{p_1-t_1} - g_2^{\frac{p_2-t_2}{u}}) + (a_1b_2 - a_2b_3)(g_1^{p_1-k_1}g_2^{\frac{k_2-t_2}{u}} - g_1^{k_1-t_1}g_2^{\frac{p_2-k_2}{u}}) + C_2)^{d_0} \equiv (b_1 + b_2 + b_3)^{d_0} \equiv (b_0^e)^{d_0} \equiv b_0 \pmod{p}$

To obtain $(b_1, b_2)$ is trivial.□