A new security notion for asymmetric encryption Draft #21

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 basic number theoretic properties and its difficulty is not reduced to either the integer factorization problem, discrete log problem or any known number theoretic cryptographic primitive.

KEYWORDS: asymmetric security, base-exponent hard problem

1 Key Generation

1. Generate a random n-bit prime p and n-bits odd primes $(g, x) \in \mathbb{Z}_p$.
2. Compute $e_1 \equiv gx \pmod{p}$.
3. Compute $e_2 \equiv g^x \pmod{p}$.
4. Compute $y \equiv (e_1(1-x)-x)^{-1} \pmod{p-1}$.
5. Compute $e_3 \equiv x^{xy} \pmod{p}$.
6. Keep (g, x, y) secret and publish (e_1, e_2, e_3, p) as public keys.

2 Encryption

1. Message is $m \in \mathbb{Z}_p$.
2. Generate random ephemeral $r, s, t \in \mathbb{Z}_p$.
3. Compute $C_1 \equiv m + r^s(e_3^{s+t})^{-1} \pmod{p}, C_2 \equiv r^{s(1+e_1)}e_1^{s+t} \pmod{p}$ and $C_3 \equiv r^{se_1}e_2^{s+t} \pmod{p}$.
4. Send (C_1, C_2, C_3) to recipient.

3 Decryption

1. Compute $m \equiv C_1 - (\frac{C_3}{C_2^x})^y \pmod{p}$.

Proposition 1. *The decryption procedure is correct.*

Proof. $C_1 - (\frac{C_3}{C_2^x})^y \equiv m + r^s(e_3^{s+t})^{-1} - r^s(e_3^{s+t})^{-1} \equiv m \pmod{p}$.□

Proposition 2. *The secret parameter $x \in \mathbb{Z}_p$ is unique.*

Proof. Let $x_1, x_2 \in \mathbb{Z}_p$ where $x_1 \neq x_2$ such that

$$e_3^{w_1} \equiv e_1^{x_1} e_2^{-1} \equiv x_1^{x_1} \equiv x_2^{x_2} \equiv e_1^{x_2} e_2^{-1} \equiv e_3^{w_2} \pmod{p}$$

where $w_1 y_1 \equiv 1 \pmod{p-1}$ and $w_2 y_2 \equiv 1 \pmod{p-1}$. That is,

$$e_3^{w_1} \equiv e_3^{w_2} \pmod{p}$$

This means $w_1 \equiv w_2 \pmod{p-1}$. But since $w_1, w_2 \in \mathbb{Z}_{p-1}$, we have $p-1 \mid (w_1 - w_2)$ only when $w_1 = w_2$ This implies $e1(1-x_1) - x_1 \equiv e_1(1-x_2) - x_2 \pmod{p-1}$, will end up as $x_1 \equiv x_2 \pmod{p-1}$. Since $x_1 - x_2 < p-1$ we have $x_1 = x_2$.□

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 (e_1, e_2) an adversary will have to solve the relation (i.e. obtain x) $e_1^x \equiv e_2 x^x \pmod{p}$. This is not the DLP. The question is can the adversary find $x \in \mathbb{Z}_p$ in polynomial time such that $e_1^x - e_2 x^x \equiv 0 \pmod{p}$?
2. Let us view the 3 public keys as follows; From the system of relations

$$e_1 \equiv gx \pmod{p} \tag{1}$$
$$e_2 \equiv g^x \pmod{p} \tag{2}$$
$$e_3 \equiv x^{xy} \pmod{p} \tag{3}$$

   where $(g, x) \in \mathbb{Z}_p$. We have $e_i : \mathbb{Z}_p^2 \longmapsto \mathbb{Z}_p$ for $i = 1, 2, 3$.
3. From item (2), is this problem a particular case of trying to solve a system of multivariate polynomials?
4. We have the relation $e_1 \equiv (e_2 e_3^v)^u \pmod{p}$, where $u \equiv x^{-1} \pmod{p-1}$ and $v \equiv y^{-1} \pmod{p-1}$. Thus, this relation is not of the DLP format.
5. From (C_2, C_3), the adversary can obtain the relation: $C_2 C_3^{-1} \equiv r^s (e_1 e_2^{-1})^{s+t} \pmod{p}$. It is desirable for the adversary to try to obtain (r, s, t) to extract m from C_1. Solving this relation is not the DLP.
6. Only if $s \equiv 0 \pmod{p-1}$, then the relation $C_2 C_3^{-1} \equiv (e_1 e_2^{-1})^{s+t} \pmod{p}$. Hence, would be reduced to the DLP.
7. Even if one attempts to solve independently from just either C_2 or C_3, both are not in the DLP format.
8. One can observe that the structure of C_2 or C_3 is the same as the second ciphertext parameter of the El-Gamal cryptosystem.

9. Another way to reduce the problem to DLP is to find functions F_1, F_2 such that $F_1(C_2)F_2(C_3) \equiv H^t \pmod{p}$ where H is a publicly available parameter.
10. We name the cryptographic primitive the ***base-exponent hard problem*** (BEHP).
11. BEHP is situated in $(e_1, e_2, e_3, C_2, C_3)$.
12. In C_1 the cryptographic primitive follows the El-Gammal strategy.