A new security notion for asymmetric encryption Draft #20

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 $(g, x, G) \in \mathbb{Z}_p$.
2. Compute $y_0 \equiv (2x - Gx)^{-1} \pmod{p-1}$.
3. Compute $y_1 \equiv (1 - Gx)(2x - Gx)^{-1} \pmod{p-1}$.
4. Compute $e_1 \equiv gx \pmod{p}$.
5. Compute $e_2 \equiv g^x \pmod{p}$.
6. Compute $e_3 \equiv G^{-1} \pmod{p-1}$.
7. Compute $e_4 \equiv x^{xy_0} g^{xy_1} \pmod{p}$.
8. Keep (g, x, y_0, y_1) secret and publish (e_1, e_2, e_3, e_4, 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 $C_1 \equiv m + r^{s+e_1} e_4^t \pmod{p}, C_2 \equiv r^{2s+e_1} e_1^t \pmod{p}$ and $C_3 \equiv r^{s+e_1-e_1e_3} e_2^t \pmod{p}$.
4. Send (C_1, C_2, C_3) to recipient.

3 Decryption

1. Compute $m \equiv C_1 - (\frac{C_2^x}{C_3^{Gx}})^{y_0} \pmod{p}$.

Proposition 1. *The decryption procedure is correct.*

Proof. $C_1 - (\frac{C_2^x}{C_3^{Gx}})^{y_0} \equiv m + r^{s+e_1} e_4^t - r^{s+e_1} e_4^t \equiv m \pmod{p}$.□

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.
2. Let us view the problem in item (1) as follows; From the system of relations

$$e_1 = gx \pmod{p} \tag{1}$$
$$e_2 = g^x \pmod{p} \tag{2}$$

   where $(g, x) \in \mathbb{Z}_p$. We have $e_i : \mathbb{Z}_p^2 \longmapsto \mathbb{Z}_p$. The question is can the adversary find $x \in \mathbb{Z}_p$ in polynomial time such that $e_1^x - e_2 x^x \equiv 0 \pmod{p}$?
3. From item (2), is this problem a particular case of trying to solve a system of multivariate polynomials?
4. From (C_2, C_3), the adversary can obtain the relation: $C_2 C_3^{-1} \equiv r^{s+e_1 e_3}(e_1 e_2^{-1})^t \pmod{p}$. 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.
5. Only if $s + e_1 e_3 \equiv 0 \pmod{p-1}$, then the relation $C_2 C_3^{-1} \equiv r^{s+e_1 e_3}(e_1 e_2^{-1})^t \pmod{p}$ would be reduced to the DLP.
6. Even if one attempts to solve independently from just either C_2 or C_3, it is still not the DLP.
7. 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.
8. We name the cryptographic primitive the ***base-exponent hard problem*** (BEHP).
9. BEHP is situated in $(e_1, e_2, e_4, C_2, C_3)$.
10. In C_1 the cryptographic primitive follows the El-Gammal strategy.