Security Analysis of IDComby identity-based encryption scheme

Pavlo Kravchenko

Abstract - **We propose a fully functional combine identity-based encryption scheme. We show that our scheme has chosen plaintext security in the random oracle model assuming a variant of the computational Diffie-Hellman problem. IDComby combines the best aspects of identity-based encryption and public key encryption.**

Keywords – **Identity based encryption, semantic security, pairing, IND-ID-CPA, random oracle model.**

A public key encryption scheme was asked for by Shamir in 1984 where the public key can be an arbitrary string. Shamir's motivation for identity-based encryption was to make the certificate management in e-mail systems more simple. Nevertheless there are two negative points in this scheme: the first is that the private key escrow is inherent in this system – i.e., a PKG can decrypt its clients' messages without difficulties or efforts; and the second is that the PKG must send client private keys using secure channels and ipso facto making private key distribution rather difficult.

Our scheme, which was present in 2009, we called IDComby. We combine the best aspects of identity-based encryption and public key encryption in it. In this paper we are going to describe the security of our scheme in random oracle model.

An combine identity-based encryption scheme IDComby is specified by six randomized algorithms: Setup, SetKeyPair, Certify, Extract, Encrypt, Decrypt.

The clear proof of security for our IDComby scheme makes use of a weaker notion of security that is known as semantic security (also known as semantic security against a chosen plaintext attack). Semantic security is similar to chosen ciphertext security (IND-ID-CCA) except for the fact that the adversary is more limited; it cannot issue decryption queries while attacking the challenge public key. The public key system is said to be semantically secure if no polynomial time adversary can win the game with an essential advantage. As shorthand we say that a semantically secure public key system is IND-CPA secure. Semantic security captures our intuition that given a ciphertext the adversary learns nothing about the corresponding plaintext.

We allow the adversary to issue chosen private key extraction queries in semantic security for identity based systems (denoted IND-ID-CPA). In the same way, the adversary is challenged on a public key ID of her choice.

We refer to such an adversary A as an IND-ID-CPA adversary. As we did above, the advantage of an IND-ID-CPA adversary A against the scheme B is the following function of the security parameter k:

$$\mathrm{Adv}_{\varepsilon,A}(k) = |\Pr[b = b'] - \frac{1}{2}|.$$

We say that the IBE system B is semantically secure if for any polynomial time IND-ID-CPA adversary A the function $\mathrm{Adv}_{\varepsilon,A}(k)$ is negligible. As shorthand, we say that B is IND-ID-CPA secure.

To analyze the security of our scheme, we use an idealized security model, which introduced Bellare and Rogaway. This model is called the random oracle model.

Next, we study the security of this basic scheme. The following theorem shows that IDComby is a semantically secure identity based encryption scheme (IND-ID-CPA) assuming BDH is hard.

We prove following theorem:

Theorem: Suppose the hash functions H_1, H_2 are random oracles. Then IDComby is a semantically secure identity based encryption scheme (IND-ID-CPA) assuming BDH is hard in groups generated by Ω. Concretely, suppose there is an IND-ID-CPA adversary A that has advantage $\varepsilon(k)$ against the scheme IDComby. Suppose A makes at most $q_E > 0$ private key extraction queries and $q_{H_2} > 0$ hash queries to H_2. Then there is an algorithm B that solves BDH in groups generated by G with advantage at least:

$$\mathrm{Adv}_{G,B}(k) \geq \frac{2\varepsilon(k)}{e(1+q_E)\cdot q_{H_2}}$$

The running time of B is O(time(A)).

To prove the theorem we first define a related Public Key Encryption scheme (not an identity based scheme), called BasicPub. BasicPub is described by three algorithms: keygen, encrypt, decrypt.

We prove Theorem in two steps. We first show that an IND-ID-CPA attack on IDComby can be converted to a IND-CPA attack on BasicPub. This step shows that private key extraction queries do not help the adversary. We then show that BasicPub is IND-CPA secure if the BDH assumption holds.

Pavlo Kravchenko – Kharkiv National University of Radioelectronics, Lenina Str., 14, Kharkiv, 61166, UKRAINE, E-mail: kravchenkopo@gmail.com