T-79.515 Cryptography: Special Topics
Some ID-PKC signcryption schemes

Lauri Tarkkala

March 25, 2003

1 Introduction

The traditional method for transmitting sensitive information over untrusted networks has been to first sign it with a cryptographic key and encrypt it with another cryptographic key. These traditional sign-then-encrypt schemes are composed of a separate signature scheme and an encryption scheme such that the encryption scheme could be applied without the signature scheme.

A signcryption scheme, originally introduced by Zheng in [3], combines these two operation tightly, thereby achieving improved efficiency [3]. An informal way to describe a signcryption way is to say that it is a cryptographic protocol which digitally signs messages and then encrypts them in such a manner, that the signing and encryption operations are not totally disjoint.

Identity based public key cryptography (ID-PKC) was originally proposed by Shamir in 1984 [4]. The idea is that the public key corresponding to an identity can be derived from a canonical representation of that identity in a deterministic manner. This requires that there must exist some additional secret information which provides the randomness in the key. A KGC (Key Generation Center) is used to create the "public parameters" of the system and the secret keys for each identity. ID-PKC was surveyed in [5].

This survey presents the basic security notions for identity-based signcryption schemes (signcryption schemes based on ID-PKC) and surveys a set of signcryption schemes and their security properties.

2 A Simple Example

A signcryption scheme can be constructed from any non-interactive one-round authenticated key-agreement protocol. Such a construction will lack the forward secrecy and non-repudiation properties. The protocol by Zheng [3] is presented here is a nice example, although it is not an identity-based scheme.

A set of global parameter must be generated by a trusted party. These are a pair of large primes p, q and a generator g s.t. $q|p-1$, ord $g \in Z_p^* = q$ and the difficulty of solving the decisional Diffie-Hellman problem in $< g > \subseteq Z_p^*$ is exponential in the security parameter k. Let h be a hash function with range at least 2^{2k}. Let **mac** be a keyed hash function. Let (E, D) be the encryption and decryption functions of a symmetric encryption scheme.

A private key is an integer $x \in Z_q^*$ and the corresponding public key $y = g^x \bmod p$. Denote the keys of A as x_A and y_A.

The $\mathbf{Signcrypt}(m, x_A, B)$ operation which signs and encrypts a message from A to B proceeds as follows:

- A chooses randomly $r \in Z_q^*$.
- $k = h(y_B^x \bmod p)$. Split k into k_1, k_2 s.t. $k = k_1 || k_2$ and k_1 is a key for (E, D) and k_2 is a key for kh.
- $r = \mathbf{mac}_{k_2}(m)$.
- $s = x(r + x_A)^{-1} \bmod q$
- $C = E_{k_1}(m)$.
- $\varphi = (C, r, s)$

The **Unsigncrypt**(m, x_B, A) operation which validates and decrypts a message from A to B proceeds as follows:

- $k = h((y_A g^r)^{sx_b} \bmod p)$
- Split k into k_1 and k_2 as above.
- m = $D_{k_1}(C)$
- Accept if $r = \mathbf{mac}_{k_2}(m)$.

Note that $(y_A g^r)^{sx_b} = g^{(x_A+rx)/x(x_A+r)*x_b} = g^{x_b x} = y_B^x$.

3 Security Model

Definition 3.1 The protocols **Setup**, **Keygen**, **Signcrypt** and **Unsigncrypt** are said to be an identity based signcryption scheme (ID-SC) if the following conditions hold:

- **Setup**(k). The setup algorithm computes a set of public parameters *params* upon input k (the security parameter).
- **Keygen**(ID). The keygen algorithm computes private key d_{ID} upon input ID (canonical representation of identity ID) and *params*.
- **Signcrypt**(m, d_A, B). The signcryption algorithm creates an encrypted and signed representation (φ) of message m upon input d_A (secret key of signer), B (canonical representation of identity B), m and *params*.
- **Unsigncrypt**(φ, d_B, A). The unsigncryption algorithm decrypts (producing m) and verifies the signature in the ciphertext φ given as input the ciphertext (φ), the secret key of the recipient (d_B), the canonical representation of identity of the signer (A) and *params*.

The (deterministic) public key derivation algorithms are interpreted be embedded in the signcryption and unsigncryption operations in this definition.

The definition above is based on the one presented in [2]. It was re-iterated here to give a framework for presenting the security notions.

Definition 3.2 Let (**Setup**, **Keygen**, **Signcrypt** and **Unsigncrypt**) be a signcryption scheme. Let $\mathcal{A}$ be an adversary which has access to a **Signcrypt** oracle (given two identities and a message, outputs the signed ciphertext φ), **Keygen** oracle (given an identity ID outputs d_{ID}), an **Unsigncrypt** oracle (given two identities and a signed ciphertext outputs the validity of the signature and the message m) and the public parameters *params*.

The scheme is said to be indistinguishable against adaptive chosen ciphertext attacks if $\mathcal{A}$ after a polynomial number of oracle queries cannot generate a pair of messages (M_0, M_1) and identities (A, B) such that when challenged with a ciphertext $C = \mathbf{Signcrypt}(M_b, d_A, B)$, $\mathcal{A}$s advantage in guessing b correctly after another polynomial number of oracle queries is negligible (ie. if the guess of $\mathcal{A}$ is b' then (2Pr[b' = b] - 1) is negligible). The adversary $\mathcal{A}$ is not allowed to query the oracle for the secret keys of A or B or the unsigncrypt oracle for C at any time.

The above property requires in essence that a polynomial amount of valid keypairs, valid (message, ciphertext, keypairs) triplets do not help in deriving any information from a correctly signed ciphertext, unless the secret key is available, or the plaintext is known a priori.

Definition 3.3 Let (**Setup**, **Keygen**, **Signcrypt** and **Unsigncrypt**) be a signcryption scheme. The adversary $\mathcal{A}$ has again access to the same oracles as in the previous definition.

The scheme is said to be secure against existential forgery for adaptive chosen message attacks if a polynomially bounded adversary $\mathcal{A}$ cannot after a polynomial number of oracle queries with non-negligible probability generate a triple (φ', A, B) such that **Unsigncrypt**(φ, d_A, B) accepts the signature on φ'. The adversary is not allowed to query the secret key of B from an oracle.

!Please note that [2] allows the adversary to compute the private key of the signer and the public key of the recipient. I believe this to be a typo, and have hence corrected the definition, which now only allows the adversary to hold the decryption key, but not the signing key.

Definition 3.4 Let G_1 and G_2 be groups of prime order q, $e : G_1 \times G_1 \rightarrow G_2$ be a bilinear map and P be a generator of G_1. G_1 is an additive group and G_2 is a multiplicative group. The *Bilinear Diffie-Hellman problem* (BDHP) in (G_1, G_2, e) is to compute $e(P,P)^{abc}$ given (P, aP, bP, cP). The *Decisional Bilinear Diffie-Hellman problem* (DBDH(G_1, P)) is to decide whether $h = e(P,P)^{abc}$ given (P, aP, bP, cP) and $h \in G_2$.

4 Modifying Zhengs Scheme for ID-SC

Nalla and Reddy have used the principles inherent in Zhengs scheme and constructed a similar ID-SC scheme. They acknowledge that they do not yet know whether the scheme is secure or not, but are working on a formal security proof. The scheme is defined in terms of the algorithms **Setup**, **Keygen**, **Signcrypt** and **Unsigncrypt**.

The **Setup**(k) randomized algorithm is run by the KGC and given the security parameter k it generates the parameters:

- An additive group G_1 of prime order q
- A multiplicative group G_2 of prime order q (same as above).
- A generator P of G_1.
- A bilinear map $e : G_1 \times G_1 \to G_2$ such that the Bilinear Diffie-Hellman Problem in (G_1, G_2, e) is a hard problem.
- A master key $s \in F_q^*$
- A public parameter $P_{pub} = sP$.
- A hash function $H_1 : \{0,1\}^* \to G_1$.
- A hash function $H_2 : \{0,1\}^* \to Z_q^*$.
- A hash function $H_3 : Z_q^* \to \{0,1\}$.

All parameters except s are public.

The **Keygen**(ID) which computes the key-pair given an identity ID is a simple hash $Q_{ID} = H_1(ID)$ of the canonical representation of the identity. The private key is $d_{ID} = sH_1(ID)$.

The **Signcrypt**(m, d_A, B) proceeds as follows:

- Let $Q_A = H_1(A)$.
- Let $Q_B = H_1(B)$.
- Randomly choose $x \in Z_q^*$.
- Compute $R = xQ_B \in G_1$.
- Compute $S = xP + H_2(m)Q_A \in G_1$.
- Let $k_1 = H_3(e(R, P_{pub})e(Q_B, H_2(m)d_A))$
- Let $C = k_1 \oplus m$.
- Output the signed ciphertext as $\varphi = (R, S, C)$.

The **Unsigncrypt**$(\varphi = (R, S, C), d_A, B)$ proceeds as follows:

- Let $Q_A = H_1(A)$.
- Let $Q_B = H_1(B)$.
- Let $k_2 = H_2(e(d_B, S))$.
- Let $m = k_2 \oplus C$.
- Accept the signature iff $e(R, P_{pub})e(d_B, Q_A)^{H_2(m)} = e(d_B, S)$.

Note that

$$\begin{gathered} e(R, P_{pub})e(d_B, Q_A)^{H_2(m)} = \\ e(xQ_B, sP)e(sQ_B, H_2(m)Q_A) = \\ e(sQ_B, xP)e(sQ_B, H_2(m)Q_A) = \\ e(sQ_B, xP + H_2(m)Q_A) = \\ e(d_B, S). \end{gathered}$$

The scheme is defined for constant-sized blocks, as it uses k_1 as a pseudo-random key stream used to pad the plaintext. A trivial extension would be to use a symmetric cipher and use k_1 as a key get around this limitation.

5 A Secure Identity Based Signcryption Scheme

Libert and Quisquater propose a secure ID-SC scheme in [2]. In this version I will refer to this scheme as the Libert-Quisquater scheme. The elementary (un-optimized) version of the scheme is presented here. The scheme is an improvement on the Malone-Lee signcryption scheme [6], but is quite similar to the scheme by Nalla and Reddy shown above. The Libert-Quisquater scheme consists of the algorithms **Setup**, **Keygen**, **Signcrypt** and **Unsigncrypt**.

The **Setup**(k) randomized algorithm is run by the KGC and given the security parameter k it generates the parameters:

- An additive group G_1 of prime order q
- A multiplicative group G_2 of prime order q (same as above).
- A generator P of G_1.
- A bilinear map $e : G_1 \times G_1 \to G_2$.
- A master key $s \in F_q^*$
- A public parameter $P_{pub} = sP$.
- A hash function $H_1 : \{0,1\}^* \to G_1$.
- A hash function $H_2 : G_2 \to \{0,1\}^n$.
- A hash function $H_3 : \{0,1\}^* \times G_2 \to F_q$.
- A symmetric cryptosystem (E, D).

All parameters except s are public.

The **Keygen**(ID) which computes the key-pair given an identity ID is simple. The public key is $Q_A = H_1(A)$ and the private key $d_A = sQ_A = sH_1(A)$ (note that G_1 is an additive group).

The **Signcrypt**(m, d_A, B) algorithm proceeds as follows:

- Let $Q_B = H_1(B) \in G_1$.
- Randomly choose $x \in F_q^*$.
- Let $k_1 = e(P, P_{pub})^x$.
- Let $k_2 = H_2(e(P_{pub}, Q_B)^x)$.
- Compute the ciphertext $c = E_{k_2}(m)$.
- Let $r = H_3(c, k_1)$
- Let $S = xP_{pub} - rd_A \in G_1$.
- Output (c, r, S) as the ciphertext φ.

The **Unsigncrypt**$(\varphi = (c, r, S), d_A, B)$ proceeds as follows:

- Let $Q_A = H_1(A) \in G_1$.
- Let $k_1 = e(P, S)e(P_{pub}, Q_A)^r$.
- Let $\tau = e(S, Q_B)e(Q_A, d_B)^r$.
- Let $k_2 = H_2(\tau)$.
- Decrypt the plaintext $m = D_{k_2}(c)$.
- Accept iff $r = H_3(c, k_1)$.

Note that the following equations hold due to bilinearity.

$$\begin{gathered} e(P,S)e(P_{pub},Q_A)^r = \\ e(P, xP_{pub} - rd_A)e(rP_{pub}, rQ_A) = \\ e(P, xP_{pub})e(P, rd_A)^{-1}e(P_{pub}, rQ_A) = \\ e(P, xP_{pub})e(P, rd_A)^{-1}e(P, srQ_A) = \\ e(P, P_{pub})^x. \end{gathered}$$

$$\begin{gathered} e(S, Q_B)e(Q_A, d_B)^r = \\ e(xP_{pub} - rd_A, Q_B)e(Q_A, d_B)^r = \\ e(xP_{pub}, Q_B)e(rsQ_A, Q_B)^{-1}e(Q_A, sQ_B)^r = \\ e(P_{pub}, Q_B)^x e(Q_A, Q_B)^{-rs}e(Q_A, Q_B)^{rs} = \\ e(P_{pub}, Q_B)^x. \end{gathered}$$

Theorem 5.1 *In the random oracle model, let $\mathcal{A}$ be an adversary attempting to distinguish messages using a chosen ciphertext attack, as described in Definition 1. If $\mathcal{A}$ is able to distinguish the encryptions of messages M_0 and M_1 with advantage ε in running time t and performing at most q_{H_1} H_1 operations, at most q_R H_3 operations, at most q_r* **Signcrypt** *operations and q_U* **Unsigncrypt** *operations, then there exists an algorithm $\mathcal{B}$ that can solve the Decisional Bilinear Diffie-Hellman problem in time $\mathcal{O}(t + (8q_R^2 + 4q_U)T_\varepsilon)$ with advantage $Adv(\mathcal{B})^{DBDH(G_1,P)} > 2(\varepsilon - q_U/2^{k-1})/q_{H_1}^4$ where T_ε denotes the computation time of the bilinear map.*

Libert and Quisquater provide a proof of this theorem. The proof is approximately three pages and is omitted here. See Appendix A in [2] for the complete proof. Libert and Quisquater also argue that the scheme is secure against existential forgeries under the adaptive chosen message attacks. Their argument is that the problem of breaking Hess' scheme can be reduced to breaking the Libert-Quisquater scheme and Hess' scheme has been proven to be secure against existential forgeries under adaptive chosen message attacks.

6 Conclusion

This survey presented three signcryption schemes. One due to Zheng, one due to Nalla and Reddy and one due to Libert-Quisquater. The skeleton of all three schemes is highly similar, although their security properties differ. Based on the Libert-Quisquater work one can state that efficient and secure Identity Based Signcryption schemes exist.

References

[1] D. Nalla, K. C. Reddy. Signcryption scheme for Identity-Based Cryptosystems. Available at "http://eprint.iacr.org/2003/044/".

[2] B. Libert, J. Quisquater. New identity based signcryption schemes from pairings. Available at "http://eprint.iacr.org/2003/023/".

[3] Y. Zheng. Digital Signcryption or how to achieve cost(signature & encryption) ¡¡ cost(signature) + cost(encryption). In Advances in Cryptology, CRYPTO 97, LNCS 1294, pp. 165-179, Springer-Verlag, 1997.

[4] A. Shamir. Identity Based Cryptosystems and Signature Schemes. Advances in Cryptology - CRYPTO 84, LNCS 0196, Springer-Verlag, 1984.

[5] T. Issaeva. ID-Based Cryptography. Available at "http://www.tcs.hut.fi/Studies/T-79.515/surveys/L3.ps.gz".

[6] J. Malone-Lee. Identity Based Signcryption. Available at "http://eprint.iacr.org/2002/098/".

[7] F. Hess. Efficient Identity Based Signature Schemes based on Pairings. To appear in Proc. of SAC 2002.