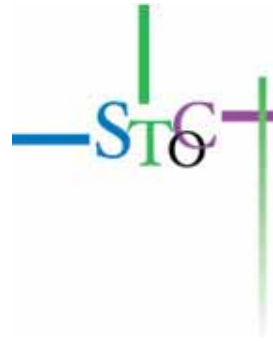


An Efficient ID-Based Verifiably Encrypted Signature Scheme Based on Hess's Scheme

2007.5.8

Kwon, Saeran and Lee, Sang-Ho
Dept. of Computer Science and Engineering
EWha Womans University, Seoul, Korea
sranie@ewhain.net



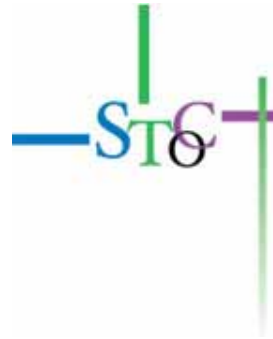
Traditional Public Key Cryptography

- Main Difficulty is to guarantee a user's public key is indeed linked to right owner
- Solution
 - Certificate issued by a trusted certification authority (CA)
 - But it needs administrative infrastructure and management for certifications
 - Also pre-enrollment of all users is needed



ID-Based Public Key Cryptography (ID-PKC)

- Concept was formulated by Adi Shamir in Crypto'84
- Efficiently implemented by Boneh-Franklin (Crypto'01)
- In ID-PKC, entity's public key is derived from identity information such as e-mail address, name, or IP address
- Private key is generated by a trusted authority called the Private Key Generator (PKG)
 - After verifying user, the PKG hands user's private key through secure channel
- Eliminate certificates & related problems



Identity Based Cryptography



Request key for Alice@hotmail.com



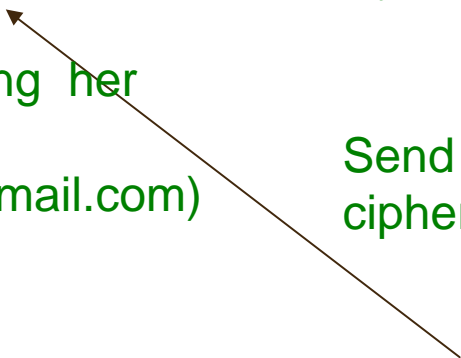
PKG
(Private Key Generator)

Issue private key $sH(\text{Alice@hotmail.com})$

Parameters,
master 's secret key is **s**,
hash function : **H**

Decrypt C using her
private key
 $sH(\text{Alice@hotmail.com})$

Send
ciphertext C



Encrypt message M into
ciphertext C with M, receiver's
identity Alice@hotmail.com,
and *params*



Fair Exchange Problem

Fair Exchange Problem

- Various business is conducted over the Internet under the distributed community
 - Electronic checks, electronic airplane ticket, e-mail, electronic contract signing
- Fair exchange problem becomes of a greater importance
 - During the exchange of items, either each party involved in the protocol gets the other's item, or neither of the parties does, even if the protocol is halted by any reason.

Verifiably Encrypted Signature

- When to deal with the fair exchange problem
 - Use optimistic fair exchange protocol
 - A trusted third party (TTP) does not participate in the actual exchange protocol in normal cases
 - The TTP is needed in only abnormal case where one player crashes or attempts to cheat.
 - It is called an off-line TTP.
 - Verifiably encrypted signature scheme (VESS)
 - building block of optimistic fair exchange protocol

Verifiably Encrypted Signature

- Verifiably encrypted signature scheme (VESS)
 - Alice wants to show Bob that she has signed a message, but does not want Bob to possess her signature.
 - Encrypt her signature using the public key of a TTP.
 - Bob can verify that Alice has signed the message, but cannot deduce any information about her signature.
 - If Alice is unable or unwilling to reveal her signature, Bob can ask the TTP to reveal Alice's signature.

Related Works for VES (in certificate-based PKI)

- Asokan et al. [Eurocrypt'98] introduced formally a fair exchange protocol relying on a TTP in an optimistic way.
- Boneh et al. [Eurocrypt'03] proposed non-interactive VES via aggregation of BLS short signature based on the bilinear pairing on GDH group.
- Zhang et al. [Indocrypt'03] constructed a VES based on their signature scheme [PKC'04] using hash functions such as SHA-1 or MD5.
- Recently, Lu et al. [Eurocrypt'06] also gave a VES based on Waters's signature scheme [Eurocrypt'05], which is secure especially in the standard model.

Related Works for VES (in ID-based PKI)

- Z. Zhang et al. [ICICS'05] gave an provably secure optimistic fair exchange protocol and an ID-based VESS derived from an ID-based signature scheme of Sakai-Ogishi-Kasahara modified by Bellare et al. [Eurocrypt'04].
- Gu & Zhu [CISC'05] and J. Zhang & Zou [EUC'06] proposed ID-based VES schemes based on Hess's signature scheme, respectively.

Our Proposed VES Scheme

- We propose an ID-based VES scheme based on Hess's signature scheme
- Efficiency and size of our scheme

	Size	VE_Sign	VE_Verify	Adjudication
C.Gu	$Z_q \times 3G_1$	$2\hat{e} + 5M / 5M$	$3\hat{e} + 1M$	$1\hat{e} + 1M$
J.Zhang	$Z_q \times 2G_1$	$1\hat{e} + 4M$	$4\hat{e} + 2M$	$1\hat{e} + 1M$
Proposed	$2G_1$	$1\hat{e} + 4M$	$4\hat{e} / 3\hat{e}$	$1\hat{e} + 1M$
	$Z_q \times 2G_1$	$1\hat{e} + 3M$	$3\hat{e} / 2\hat{e}$	$1M$

Notation: Z_q a finite field of prime order q , G_1 a GDH group of prime order q
 M scalar multiplication in $(G_1, +)$, e^\wedge pairing operation in $(G_1, +)$
 Optimized cases at the right side of general cases

Our Proposed VES Scheme

- **Setup** : Two groups $(G_1, +)$ and (G_2, \cdot) of prime order q ,
Bilinear map $e: G_1 \times G_1 \rightarrow G_2$,
 P a generator of G_1 ,
Three hash functions: $H_1: \{0, 1\}^* \rightarrow G_1^*$,
 $H_2: \{0, 1\}^* \times G_2 \rightarrow Z_q^*$
 $H_3: \{0, 1\}^* \times G_1 \times G_1 \rightarrow G_1^*$,
PKG's master key $s \in Z_q^*$ and public key $P_{pub} = sP$,
Adjudicator TTP's private key x and public key $PK = xP$,
System parameters $\Omega = (G_1, G_2, q, e, P, P_{pub}, PK, H_1, H_2, H_3)$.

Our Proposed VES Scheme

- **Extract** : Given an identity $ID \in \{0, 1\}^*$, the PKG computes user's public key $Q_{ID} = H_1(ID)$ and generates the user's private key $D_{ID} = sQ_{ID}$ with its master key s , then gives D_{ID} to the user by a secure channel.
- **Sign** : Given a private key D_{ID} and a message m , choose an arbitrary point P_1 , pick $k \in \mathbb{Z}_q^*$ at random and output a signature $\sigma = (r, V)$, where $r = e(P_1, P)^k$, $h = H_2(m, r)$, and $V = hD_{ID} + kP_1$.
- **Verify**: Given $\sigma = (r, V)$ of an identity ID for a message m , compute $h = H_2(m, r)$, and accept the signature if and only if $r = e(V, P) \cdot e(Q_{ID}, P_{pub})^{-h}$.

Our Proposed VES Scheme

- **VE_Sign:** Given a private key D_{ID} of identity ID , a message m and adjudicator's public key PK ,
 - choose $k \in \mathbb{Z}_q^*$ at random,
 - compute $U = kP$, $P_1 = H_3(ID, U, PK)$, $h = H_2(m, e(P_1, U))$,
 - compute $V = hD_{ID} + kP_1 + kPK$,
 - output the VES $\sigma = (V, U)$.
- **VE_Verify:** Given a VES $\sigma = (V, U)$ of identity ID for message m ,
 - compute $P_1 = H_3(ID, U, PK)$ and $h = H_2(m, e(P_1, U))$,
 - accept the signature if and only if
$$e(P, V) = e(Q_{ID}, P_{pub})^h \cdot e(U, P_1 + PK).$$

Our Proposed VES Scheme

- **Adjudication** : Given the adjudicator's secret key x , and a valid VES $\sigma' = (V', U)$ of ID for message m ,
 - compute $V = V' - xU$, $r = e(P_1, U)$ along with $P_1 = H_3(ID, U, PK)$,
 - output $\sigma = (r, V)$.

Since $xU = xkP = kPK$ and $r = e(P_1, U) = e(P_1, P)^k$,

$\sigma = (r, V)$ is an signature by Hess's scheme-1.

Note 1 : **(Extract, Sign, Verify)** constitutes Hess's scheme-1 in [SAC'02]

Note 2 : If including $r = e(P_1, U) = e(P_1, P)^k$ in the VES,
the running time is reduced while the size of messages extends.

Security Model of VES

- **Security against a signer with private key:** A dishonest signer should not be able to produce a VES which are verified but can not be decrypted into an ordinary signature by the adjudicator.
- **Security against signing without private key:** An adversary without a private key for the target ID should not be able to produce a valid VES on any message. Then, the adjudicator justly can not extract an ordinary signature from the VES because it means to forge the original signature scheme.

Security Model of VES

- **Security against a verifier:** A verifier should not be able to transfer any VES he got from the signer into an ordinary signature, without explicitly asking the adjudicator to do it.
- **Security against the adjudicator:** The adjudicator should not be able to produce a valid signature on a message m of a signer without asking the signer to generate a VES on m .

Security Proof of Our VES

- **Theorem1.** Under the formal model, our verifiably encrypted signature scheme based on Hess's signature scheme-1 is provably secure in the random oracle model, if assuming that the CDH problem is hard

Security Proof of Our VES

- **Security against a signer :**
 - If $\sigma = (V, U)$ satisfies $e(P, V) = e(Q_{ID}, P_{pub})^h \cdot e(U, P_1 + PK)$ along with the values $P_1 = H_3(ID, U, PK)$ and $h = H_2(m, e(U, P_1))$ ahead computed, the adjudicator always can extract the ordinary signature $\sigma = (r, V)$ by $V = V' - xU$ as the follows:

$$\begin{aligned}
 e(P, V) &= e(P, V') \cdot e(P, -xU) = e(P, V') \cdot e(PK, -U) \\
 &= e(Q_{ID}, P_{PUB})^h \cdot e(U, P_1)
 \end{aligned}$$

- When r is set as $e(U, P_1)$, we get $r = e(V, P) \cdot e(Q_{ID}, P_{pub})^{-h}$ where $h = H_2(m, r)$.

Security Proof of Our VES

- **Security against a verifier :**
 - If A draws out valid signature $\sigma = (r, V)$ whose corresponding VES $\sigma' = (V, U)$ has not been queried to O_{Adj} , and ID has not been queried to O_{Ext} , then we can construct a forger algorithm F to solve the CDH problem through making use of A .
 - Let $X = aP, Y = bP \in G_1$ be a random instance of the CDH problem.
 - F takes $z \in Z_q^*$ at random and sets $PK = zY$ and then initializes A with $P_{pub} = X$ and PK .
 - **Queries on oracle H_1 :** when identity ID is submitted to H_1 , F flips a coin $T \in \{0, 1\}$ that yields 0 or 1. For random chosen $w \in Z_q^*$, if $T = 0$, $H_1(ID)$ is defined as being $wP \in G_1$, or if $T = 1$, $H_1(ID)$ is defined as being $wY \in G_1$.

Security Proof of Our VES

- **Security against a verifier :**
 - *Key extraction queries on oracle O_{ext}* : When A requests the private key of ID to oracle O_{Ext} , if $T = 1$, F outputs "failure" and halts. If $T = 0$, F returns wX .
 - *VES queries on oracle O_{Vsig}* :
 - (1) If $T = 0$ i.e. $Q_{ID} = wP$, F randomly chooses a $k_i \in \mathbb{Z}_q^*$ and set $U_i = k_i P$. Also for a query (ID, U_i, PK) to H_3 oracle, F picks a $v_i \in \mathbb{Z}_q^*$ randomly and define the hash value $H_3(ID, U_i, PK) = P_{1i}$ as $v_i P$. Then set $V_i = h_i wX + k_i v_i P + k_i PK$. Then (U_i, V_i) is returned to A as a valid VES.
 - (2) If $T = 1$ i.e. $Q_{ID} = wY$, then F randomly chooses $t_i, k_i, h_i \in \mathbb{Z}_q^*$, and then sets $V_i = t_i P_{pub}$, $U_i = k_i P_{pub}$ and defines the hash value $H_3(ID, U_i, PK) = P_{1i}$ as $k_i^{-1} (t_i P - h_i Q_{ID}) - PK \in G_1$.

Security Proof of Our VES

- **Security against a verifier :**
 - Suppose A outputs a fake signature $\sigma = (m, r, V)$ for an identity ID .
 - If $T = 0$, then F outputs "failure" and stops.
 - Otherwise, F finds out k for which $U = kP_{pub}$.
 - Then $e(P, V - V) = e(U, PK) = e(kP_{pub}, zY) = e(kX, zY)$.
 - At last, get $abP = (kz)^{-1}(V - V)$ for the CDH instance $X=aP$, $Y=bP$.

Security Proof of Our VES

- **Security against the adjudicator :**
 - If adjudicator A forges a valid $\sigma = (r, V)$ on m not queried to O_{Vsig} , we can construct a forger algorithm F to forge an Hess-type signature through making use of A .
 - For a query on O_{Vsig} under message m , F chooses $t_i, k_i, h_i \in \mathbb{Z}_q^*$ at random, and then sets $V_i = t_i P_{pub}$, $U_i = k_i P_{pub}$ and defines $H_3(ID, U_i, PK) = P_{1i}$ as $k_i^{-1}(t_i P - h_i Q_{ID}) - PK \in G_1$.

Security Proof of Our VES

- **Security against the adjudicator :**
 - Next, F computes $e(U_i, P_{1i}) = r_i$ and defines $H_2(m_i, r_i)$ as h_i . If $H_3(ID, U_i, PK)$ or $H_2(m_i, r_i)$ is already defined, F halts. Otherwise, (V_i, U_i) can be verified and adjudicator A accepts it as a valid VES.
 - When A outputs a forgery $(m, \sigma = (r, V))$, where m has not been queried to O_{Vsig} , then F just outputs the same (m, σ) returned from A .
 - F succeeds in generating a valid forgery if A succeeds.

- In this paper,
 - We constructed an efficient ID-based verifiably encrypted signature scheme based on Hess's signature scheme.
 - It is more profitable for communication requirements due to the smaller size than other schemes of same kind
 - We showed the formal security proof of our VES scheme in a random oracle model.