Control and Cybernetics

vol. **38** (2009) No. 3

Anonymous signer verifiable encrypted signature from bilinear pairing*

by

Jacek Pomykała and Tomasz Trabszys

Faculty of Mathematics, Informatics and Mechanics
University of Warsaw, Poland
e-mail: pomykala@mimuw.edu.pl

Abstract: In this paper we propose and prove the security of the new cryptographic primitive called the Anonymous Signer Verifiable Encrypted Signature (ASVES), joining the idea of the group signature and the verifiable encrypted signature. It satisfies the traditional requirements of the group signature (unforgeability, anonymity, unlinkability, traceability) and the opacity condition known from the verifiable encrypted signatures. The corresponding scheme may be applied for the fair exchange protocols. Our construction is based on bilinear pairings, defined in the Gap Diffie-Hellman groups.

Keywords: anonymous signer, verifiable encrypted signature, GDH group, bilinear pairing.

1. Introduction

The contemporary e-commerce is strongly affected by the mutual exchange of information between the different parties. The fair exchange protocols admit the satisfactory solution for the corresponding requirements by means of the cryptographic ingredients. A good example is the electronic fair contract signing, where none of the participated parties is expected to have any advantage over the other (see Asokan, Shoup and Vaidner, 1998).

In this connection the verifiable encrypted signatures (Boneh and Gentry, 2003) turned out to play a significant role. They allow one party to be sure about the correct (encrypted) signature of the other one, before signing the agreed contract. Such functionality is usually solved by the passive participation of the trusted party (Trustee), in the corresponding protocol. The suitable signature is encrypted by Trustee's public key in a way that allows for its verification by the other party. In case it is necessary, the Trustee intervenes in the decryption of the corresponding signature.

*Submitted: May 2008; Accepted: December 2008.

On the other hand, the functionality of the group signature (Chaum and van Heyst, 1991) is related to the "provable" representation of the group membership. Group members can sign the messages on behalf of the group. The signers are anonymous, but in the exceptional cases the trusted party (called the Manager) may reveal their identities. The application of group signatures or blind signatures (Chaum, 1983) in e-commerce allows for protecting the personal data and user's anonymity in electronic transactions (see also Lysyanskaya and Ramzan, 1998).

The current state of electronic commerce also implies new challenges such as protection of user's profiles or identities (see Dodis et al., 2004) when visiting the www sites (see the onion routing protocols for example). Here we shall be focused on the anonymous channels in application to contract signing.

In the paper we shall define and prove the security of the new cryptographic primitive called the Anonymous Signer Verifiable Encrypted Signature (ASVES), that joins the idea of the group signature (see Bellare, Micciancio and Warinschi, 1999; Bellare, Shi and Zhang, 2005) and the verifiably encrypted signature (see Boneh and Gentry, 2003). It satisfies the traditional requirements of the group signature (unforgeability, anonymity, unlinkability, traceability) and the opacity condition known from the verifiable encrypted signatures. The corresponding scheme may be applied for the fair exchange protocols (with joint or separate functionalities of the corresponding Trustees). We will refer here to the idea of anonymous role-based signing rights delegations investigated in Yao and Tamassia (2006). Our construction is based on the structure of the Gap Diffie-Hellman groups (see Joux, 2004). The corresponding security analysis is related to Boneh and Gentry (2003) and Yao and Tamassia (2006).

2. Related work

The proposed cryptographic protocols work in the Gap Diffie-Hellman Groups (GDH groups). The first construction of the Gap Diffie Hellman group has been proposed in Joux (2004). In Boneh, Lynn and Shacham (2001) and Lysyanskaya (2002) the first examples of digital signatures working in the GDH group were given. The group signature scheme has been introduced by Chaum and van Heyst (1991). The security of the group signature scheme for dynamic groups was studied in details in Bellare, Shi and Zhang (2005). Provably secure verifiably encrypted signatures have been investigated in Boneh and Gentry (2003). The anonymous-signer signature scheme based on the BLS short signature (Boneh, Lynn and Shacham, 2001) has been considered in Yao and Tamassia (2006). The security proof of the proposed ASVES protocol is based on the ideas of Boneh and Gentry (2003). For the efficient construction of the derandomized Weil pairing in the GDH groups we refer the reader to Pomykała and Źrałek (2008). The first ID-based verifiable encrypted signature based on bilinear pairing has been proposed in Cheng, Liu and Wang (2005). The anonymous-signer signature scheme based on the BLS short signature schemes

has been considered in Yao and Tamassia (2006). Our security proof of the new primitives applies the ideas of Boneh and Gentry (2003). For the effectivity in the construction of the derandomized Weil pairing in the GDH groups we refer the reader to Pomykała and Źrałek (2008).

3. Notations and assumptions

In this paper we shall consider the bilinear map $e : G_1 \times G_1 \to G_2$ where $G_1 = (G_1, +)$ is additive and $G_2 = (G_2, \cdot)$ multiplicative group of prime order p (respectively). We assume that e satisfies the following conditions:

- **Bilinear:** $e(aR, bQ) = e(R, Q)^{ab}$, $\forall R, Q \in G_1$ and $\forall a, b \in Z_q^*$
- **Non-degenerate:** $e(P, P)$ is a generator of G_2
- **Computable:** there exists an efficient algorithm to compute $e(\cdot, \cdot)$.

Computational Diffie-Hellman problem (CDH)

Given the triple (P, Q, R) compute the point $S \in G_1$ such that the discrete logarithm of S in the base R coincides with the discrete logarithm of Q in the base P.

Decisional Diffie-Hellman problem (DDH)

Given a quadruple (P, Q, R, S) decide whether the discrete logarithm of S in the base R coincides with the discrete logarithm of Q in the base P.

The bilinear map e implies that the corresponding DDH problem is tractable in G_1. However, if the corresponding CDH problem still remains intractable, the group G_1 is called the gap Diffie-Hellman group. The explicit examples of such bilinear pairings are Weil or Tate pairings. The derandomization of the Weil pairing is proposed in Pomykała and Źrałek (2008).

4. Anonymous Signer Verifiable Encrypted Signature (ASVES)

There are four parties participating in the protocol: Signer, Manager, Trustee and Verifier. Similarly as in the Verifiably Encrypted Signature Scheme, the Trustee plays the passive role in the protocol (i.e. it decrypts the signature only if it is required). For instance, in the fair exchange protocols Trustee is engaged only if at least one of the parties signing the contract is a dishonest one. The role of Manager is similar as in the group signature schemes. The trapdoor information he knows might be used to reveal the anonymity of the Signer. We point out below the consecutive steps, followed by the protocol:

1. Setup of the system:
   Having as an input the public data, the tuple (G, e, P, H, h) is generated as output, where P is a random nonzero element of the group G and $H : G \to G$, $h : \{0,1\}^* \to G$ are the corresponding secure hash functions.

2. Long-term key generation:
   The Certificate Authority generates the pairs of private/public keys: (u, uP) for the Signer, (t, T) for the Trustee and (s, Ω) for the Manager, where $T = tP$ and $\Omega = sP$.
3. Short-term key generation:
   The Signer generates the list of random values $x \in Z_q^*$, computes the one-time public signing keys $Y = xuP$ and the verification keys $X = xP$. The private short-term key would be $y = xu$.
4. Certification:
   The Manager uses the verification key X to check if $e(P, Y) = e(X, U)$, where $U = uP$. If so, he generates the certificate $(Y, sH(Y))$ and sends it to the Signer. The Manager stores the tuple (U, X, Y) in his $one - time$ *signing permits* record. The Signer stores his short-term key y with its certificate $(Y, sH(Y))$.
5. Signing:
   Given the message $m \in \{0, 1\}^*$, the Signer generates a random $v \in Z_q^*$ and computes the signature of m: $[m, Y, V, W]$, where $W = yh(m) + sH(Y) + vT$ and $V = vP$, $Y = xuP$, $y = xu$.
6. E-verification:
   To verify the encrypted signature $[m, Y, V, W]$ any user checks if $e(P, W) = e(Y, h(m))e(\Omega, H(Y))e(V, T)$, where Y is the Signer's short-term public key.
7. Signature recovery:
   The Trustee computes the proper (decrypted) signature: $W' = yh(m) + sH(Y) = W - tV$ and sends it to the Verifier (if required).
8. Verification:
   Any Verifier can check the validity of the ordinary (decrypted) signature. Namely, the decrypted signature is accepted if and only if $e(P, W') = e(Y, h(m))e(\Omega, H(Y))$. In fact, it is the verification of the role signature from the ASAS scheme.

The scheme consists of the corresponding eight algorithms:

ASVES =(Setup, Keygen, ShortKeygen, Certify, Sign, E-verify,
Recover, Verify.)

5. Security of ASVES

Let us consider the role signature defined in Yao and Tamassia (2006, section 3.3). In this paper we are not considering roles, so assume that $roleinfo = \epsilon$. The Signer with permanent private and public key (u, uP), having one-time private and public keys pair (y, Y) and certificate of the public key $C = sH(Y)$, would generate the following role signature:

$$[m, Y, W] = [m, Y, yh(m) + C].$$

It is a special case of the anonymous-signer aggregate signature(ASAS) scheme (Yao and Tamassia, 2006) — with only one message and signer. Hence for the security of the ASAS scheme we will refer to Yao and Tamassia (2006, Theorem 4), which claims:

- correctness
- unforgeability
- anonymity
- unlinkability
- exculpability
- traceability.

Definitions of the above properties are presented in Yao and Tamassia (2006). We note that our ASVES scheme combines the above signature with the BLS short signature scheme (Boneh, Lynn and Shacham, 2001). BLS is used for encrypting signatures. In what follows, we prove the security properties of the ASVES scheme, reducing them to the corresponding properties of the ASAS scheme.

5.1. Validity

Validity of the signature

If the ASVES signature is generated according to the protocol, then the following equation holds:

$$\begin{aligned} e(P,W) &= \\ &= e(P, yh(m) + sH(Y) + vT) = e(P, yH(m))e(P, sH(Y))e(P, vT) = \\ &= e(Y, h(m))e(\Omega, H(Y))e(V, T). \end{aligned}$$

Correctness of the *Signature recovery* procedure

Assume that $\omega = (Y, V, W)$ satisfies the verification:

$$e(P,W) = e(Y, H(m))e(\Omega, H(Y))e(V,T)\ ,$$

so when considering the decrypted signature $\sigma = (Y, W')$, $W' = W - tV$, we have:

$$e(P,W') = e(P,W)/e(P,tV) = e(P,W)/e(V,T) = e(Y,H(m))e(\Omega,H(Y)).$$

■

5.2. Traceability

Consider the proof of correctness of the *Signature recovery* procedure. After obtaining the verifiable encrypted signature $\omega = (Y, V, W)$, the Trustee can compute ordinary (decrypted) signature $\sigma = (Y, W')$. Now the Manager can

identify the Signer by consulting his $one-time\ signing\ permits$ record. The Manager finds a tuple $(U, X, \tilde{Y})$, where $Y = \tilde{Y}$ and U is a public key of the Signer. Signer with the public key U cannot deny his signature because the Manager can provide the proof by showing that the equation $e(P, Y) = e(U, X)$ holds. We remind here that $Y = uxP$, $U = uP$, $X = xP$ (see 3. of section 4). Computing such a X, knowing P, U, Y is called a reversion of the Diffie-Hellman Problem, which is equivalent (see Chen, Zhang and Kim, 2003) to the computational Diffie-Hellman Problem. This completes the argument. ■

5.3. Exculpability

We will show here that the Manager is not able to sign on behalf of the non-involved member. In fact we are going to show even a stronger statement, that The Manager with the Trustee are not able to sign on behalf of the member.

Let $\omega = (Y, V, W)$ be the signature forged by the Manager and the Trustee on behalf of a member with a public key U. Hence, the Trustee could also obtain ordinary (decrypted) signature $\sigma = (Y, W') = (Y, yH(m) + sH(Y))$. According to Theorem 4 in Yao and Tamassia (2006), the ASAS scheme (σ) is secure against exculpability and this completes the argument. ■

5.4. Unforgeability, anonymity, unlinkability

Let us introduce a forger $\mathcal{B}$, who would simulate the challenger and interact with a forger $\mathcal{A}$. Forger $\mathcal{A}$ would be able to break each time one of the properties of our ASVES scheme: unforgeability, anonymity, unlinkability, traceability (definitions are given in Yao and Tamassia, 2006) in the random oracle model. Then we are going to show that the forger $\mathcal{B}$ would be able to break one of the corresponding properties of the anonymous-signer aggregate signature (ASAS) scheme (Yao and Tamassia, 2006) respectively.

$\mathcal{B}$ interacts with $\mathcal{A}$ as follows:

- Setup: $\mathcal{B}$ generates a pair of private and public keys (t, T), which serves as the Trustee's keys.
- Hash Queries: $\mathcal{A}$ requests a hash on some message m or hash value on some element $g \in G_1$. $\mathcal{B}$ makes a query to its own hash oracle and gives the value back to $\mathcal{A}$.
- VerSign Queries: $\mathcal{A}$ requests a signature for some message m. $\mathcal{B}$ queries its own signing oracle for a signature of m, obtaining $\sigma = (Y, S)$. It chooses random $v \in Z_q^*$, computes $V = vP$ and returns to $\mathcal{A}$ the triple $\omega = (Y, V, S + tV)$.
- Decryption Queries: $\mathcal{A}$ requests decryption of $\omega = (R, V, W)$. $\mathcal{B}$ checks that the signature is valid, computes $W' = W - tV$ and returns $\sigma = (R, W')$.

- Output: $\mathcal{A}$ outputs either:
  - unforgeability: a forge $\omega = (R, V, W)$ for some message m. $\mathcal{B}$ computes $W' = W - tV$ and $\sigma = (R, W')$ is a valid ASAS signature.
  - anonymity: $\mathcal{B}$ asks for a challenge ASAS signature $\sigma = (Y, S)$. It chooses random $v \in Z_q^*$, computes $V = vP$ and waits for $\mathcal{A}$ to ask for a challenge ASVES signature. When it does, $\mathcal{B}$ responds with $\omega = (Y, V, S + vT)$ and at the end outputs the identity which has been returned by $\mathcal{A}$.
  - unlinkability: $\mathcal{B}$ can challenge the ASAS scheme unlinkability property as follows: After receiving a challenge pair $(\sigma_k^1, \sigma_k^2) = ((Y_k^1, S_k^1), (Y_k^2, S_k^2))$ it chooses random $v_1, v_2 \in Z_q^*$, computes $V_i = v_i P$ and as a challenge for $\mathcal{A}$ chooses $(\omega_1^i, \omega_2^i) = ((Y_k^1, V_1, S_k^1 + v_1 T), (Y_k^2, V_2, S_k^2 + v_2 T))$. If $\mathcal{A}$ would have a significant probability of guessing if those signatures belong to the same user, so would have $\mathcal{B}$.

Therefore, if ASAS scheme has the properties of unforgeability, anonymity, unlinkability so has our ASVES scheme. ■

5.5. Opacity

Opacity requires that given a verifiably encrypted signature it should be difficult to extract an ordinary signature on the same message. Extracting ASAS from ASVES signature is actually the 3-element Aggregate Extraction Problem, studied in Boneh at al. (2003) and proven to be equivalent to the Diffie-Hellman Assumption in Coron and Naccache (2003).

As a conclusion we are now in a position to formulate the following theorem:

THEOREM 5.1 *The proposed anonymous-signer verifiable encrypted signature scheme satisfies the following requirements: validity, traceability, exculpability, unforgeability, anonymity, unlinkability and opacity in the random oracle model under the CDH assumption.*

References

ASOKAN, N., SHOUP, V. and VAIDNER, M. (1998) Optimistic fair exchange of digital signatures. In: K. Nyberg , ed., *Advances in Cryptology — EUROCRYPT'98*. **LNCS 1403**, Springer Berlin/Heidelberg, 591—606.

BELLARE, M., MICCIANCIO, D. and WARINSCHI, B. (1999) Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions. In: E. Biham, ed., *Advances in Cryptology - EUROCRYPT'03*. **LNCS 2656**, Springer Berlin/Heidelberg, 614–629

Bellare, M., Shi, H. and Zhang, Ch. (2005) Foundations of Group Signatures: The Case of Dynamic Groups. In: A. Menezes, ed., *Topics in Cryptology - CT-RSA'05*. **LNCS 3376**, Springer Berlin/Heidelberg, 136–153.

Boneh, D., Gentry, C., Lynn, B. and Shacham, H.(2003) Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In: E. Biham, ed., *Advances in Cryptology - EUROCRYPT'03*. **LNCS 2656**, Springer Berlin/Heidelberg, 416–432.

Boneh, D., Lynn, B. and Shacham, H. (2001) Short Signatures from the Weil Pairing. In: C. Boyd, ed., *Advances in Cryptology - Asiacrypt'01*. **LNCS 2248**, Springer Berlin/Heidelberg, 514–532.

Chaum, D. (1983) Blind signatures and untraceable payments. In: D. Chaum, R.L. Rivest and A.T. Sherman, eds. *Advances in Cryptology, Proc. of Crypto 82*. Plenum, 199–203.

Chaum, D. and van Heyst, E. (1991) Group signatures. In: D.W. Davies, ed., *Advances in Cryptology — EUROCRYPT '91*. **LNCS 547**, Springer Berlin/Heidelberg, 257–265.

Chen, X., Zhang, F. and Kim, K. (2003) A new ID-based group signature scheme from bilinear pairings. http://eprint.iacr.org/2003/116.

Cheng, X., Liu, J. and Wang, X. (2005) Identity-based aggregate and verifiably encrypted signatures from bilinear pairing. In: O. Gervasi et al., eds., *Computational Science and Its Applications – ICCSA 2005*. **LNCS 3483**, Springer Berlin/Heidelberg, 1046–1054.

Coron, J. and Naccache, D. (2003) Boneh et al.'s k-Element Aggregate Extraction Assumption Is Equivalent to The Diffie-Hellman Assumption. In: C. Laih, ed., *Advances in Cryptology - Asiacrypt'03*. **LNCS 2894**, Springer Berlin/Heidelberg, 392–397.

Dodis, Y., Kiayias, A., Nicoli, A. and Shoup, V. (2004) Anonymous Identification in Ad Hoc Groups. In: Ch. Cachin and J. Camenisch, eds., *Advances in Cryptology - EUROCRYPT 2004*. **LNCS 3027**, Springer Berlin/Heidelberg, 609–626.

Joux, A. (2004) A one-round protocol for tripartite Diffie-Hellman. *Journal of Cryptology* **17** (4), 263–276.

Lysyanskaya, A. (2002) Unique signatures and verifiable random functions from the DH-DDH separation. In: M. Yung, ed., *Advances in Cryptology — CRYPTO 2002*. **LNCS 2442**, Springer Berlin/Heidelberg, 597–612.

Lysyanskaya, A. and Ramzan, Z. (1998) Group blind digital signatures: a scalable solution to electronic cash. In: R. Hirschfeld, ed., *Financial Cryptography (FC '98)*. **LNCS 1465**, Springer Berlin/Heidelberg, 184–197.

Pomykała, J. and Źrałek, B. (2008) A model of Id-based proxy signature scheme. In: *Proc. of the 6th Collaborate Electronic Communications & Commerce Tech. and Research Conference*, Madrid, 25-27 June 2008.

Yao, D. and Tamassia, R. (2006) Cascaded Authorization with Anonymous-Signer Aggregate Signatures. *Information Assurance Workshop*, 21-23 June 2006, IEEE, 84–91.