STUDIA UNIV. BABEŞ–BOLYAI, INFORMATICA, Volume **XLVII**, Number 2, 2002

AN EFFICIENT ID-BASED GROUP SIGNATURE SCHEME

CONSTANTIN POPESCU

Abstract. We present an efficient group signature scheme which make use of elliptic curves identity-based signature scheme. The performance of the generated group signature scheme is similar to the performance of the underlying ID-based signature scheme.

Keywords: Group Signature, ID-based Signature schemes, elliptic curves

1. Introduction

The concept of identity-based cryptography is due to Shamir [10]. An identity based crypto-system [2, 10] is a system that allows a publicly known identifier (email address, IP address, name) to be used as the public key component of a public/private key pair in a crypto-system. The scheme assumes the existence of a trusted authority whose sole purpose is to compute for each user the private key associated with the identifier they want to use as public key. The scheme is ideal for closed groups of users. Several ID-based signature schemes have been proposed in the last years [7, 9, 10]. Some of these schemes use Elliptic Curve (EC) algorithms and are therefore particularly efficient.

A group signature, introduced by Chaum and van Heyst [5], allows any member of a group to digitally sign a document such that a verifier can confirm that it came from the group but does not know which individual in the group signed the document. The scheme assumes the existence of a group manager whose sole purpose is to compute for each user a private key that the user should use when signing a message on behalf on the group. A user verifies a signature with the group public key that is usually constant and unique for the whole group (i.e. independent of the members). Many group signature schemes have been proposed [1, 3, 6, 8, 12]. However all of them are much less efficient that regular signature schemes (such as DSA or RSA). Designing an efficient group signature scheme is still an open research problem. In this paper we show that ID-based signature schemes [7] can be used to implement an efficient group signature scheme. Such group signature has the same performance than the performance of the ID-based

2000 *Mathematics Subject Classification.* 94A60.

1998 *CR Categories and Descriptors.* D.4.6. [**Software**]: Operating Systems – *Security and Protection.*

signature scheme it is derived from. This makes our proposal very attractive since it is probably the most efficient group signature scheme that exists today.

2. Identity-Based Signature Scheme

An identity based crypto-system [2, 10] is a system that allows a publicly known identifier to be used as the public key component of a public/private key pair for the purposes of digital signature [7, 9, 10], encryption [2] and key agreement [11]. The private key component is computed by the trusted authority and sends to the corresponding node via a secure and authentic channel.

Definition 1. *An identity based signature scheme is a digital signature scheme specified by the following four algorithms:*

SETUP*: An algorithm, executed by the trusted authority, that takes a random parameter l as input and generates from it system parameters and master key. System parameters is publicly known, while master key is only known to the trusted authority.*

EXTRACT*: An algorithm, executed by the trusted authority, that takes as input system parameters, master key and an arbitrary $ID_i \in \{0,1\}^*$, provided by a user, U_i, and returns a private key x_i. ID_i is an arbitrary string that is used as a public key and x_i is the corresponding private key.*

SIGN*: An algorithm that takes as input system parameters, x_i and a message, $m \in \{0,1\}^*$ and returns a signature σ.*

VERIFY*: An algorithm that takes as input a message $m \in \{0,1\}^*$ and its signature σ, the system parameters and a public key ID_i.* ***VERIFY*** *outputs* 0 *if the signature is invalid and* 1 *if the signature is valid.*

A secure ID-based signature scheme must at least satisfy the following properties:

Correctness: Signatures produced by a user using **SIGN** must be accepted by **VERIFY.**

Unforgeability: It is computationally hard for everyone that do know the secret key x_i of U_i to forge his signatures. As a consequence, it must be computationally hard for everyone to retrieve from system parameters the corresponding master key.

Coalition-resistance: A colluding subset of users, that have received their private key from the same trusted authority and system parameters, cannot generate a valid signature that the trusted authority cannot link to one of the colluding users.

3. ID-based Signatures from Pairings on Elliptic Curves

In this section we review the ID-based signature scheme from [7] which makes use of bilinear pairings on elliptic curves.

3.1. **Setup.** We use the same notation as in [7]:

(1) We let G_1 be an additive group of prime order q and G_2 be a multiplicative group of the same order q.
(2) We assume the existence of a bi-linear map $\widehat{e}$ from $G_1 \times G_1$ to G_2 with the property that the discrete logarithm problems in both G_1 and G_2 are hard. Typically, G_1 will be a subgroup of the group of points on an elliptic curve over a finite field, G_2 will be a subgroup of the multiplicative group of a related finite field and the map $\widehat{e}$ will be derived from the Weil or Tate pairing on the elliptic curve.
(3) We also assume that an element $P \in G_1$ satisfying $\widehat{e}(P,P) \neq 1_{G_2}$ is known. We refer to [2, 7] for a fuller description of how these groups, maps and other parameters should be selected in practice for efficiency and security.
(4) We let ID_i be a string denoting the identity of a user U_i and H_1, H_2 and H_3 be public cryptographic hash functions. We require $H_1 : \{0,1\}^* \to G_1$, $H_2 : \{0,1\}^* \to \mathbb{Z}_q$ and $H_3 : G_1 \to \mathbb{Z}_q$.
(5) A trusted authority chooses a random integer $s \in \mathbb{Z}_q$ which is a system-wide master secret.
(6) We also assume that the value $P_{pub} = s \cdot P$ is publicly known.

3.2. **Extract.** A user's public key for signature verification is $Q_{ID_i} = H_1(ID_i)$, while his secret key for signature generation is $D_{ID_i} = s \cdot Q_{ID_i}$. These keys are the same as in the encryption scheme of [7]. If desired, encryption and signature keys can be separated simply by concatenating the string ID_i with extra bits which identify the keys' intended functions.

3.3. **Sign.** To sign a message $m \in \{0,1\}^*$, a user U_i uses the following algorithm:

- Chooses a random $k \in \mathbb{Z}_q^*$.
- Computes $(R,S) \in G_1 \times G_1$, where

$$\begin{aligned} R &= k \cdot P \\ S &= k^{-1}\left(H_2(m) \cdot P + H_3(R) \cdot D_{ID_i}\right). \end{aligned}$$

  Here k^{-1} is the inverse of k in $\mathbb{Z}_q^*$.
- Output the signature (R,S).

3.4. **Verify.** Checking whether a pair (R,S) is a valid signature on a message $m \in \{0,1\}^*$ with respect to the public key Q_{ID_i} can be done as follow:

- Computes $\widehat{e}(U,V)$, where (U,V) is a purported signature on message m.
- Check whether $\widehat{e}(U,V) = \widehat{e}(P,P)^{H_2(m)} \cdot \widehat{e}(P_{pub}, Q_{ID_i})^{H_3(R)}$.
- The signature is accepted if these values in G_2 match and rejected otherwise.

4. Group Signature Scheme

A group signature, introduced by Chaum and van Heyst [5], allow any member of a group to sign on behalf of the group. Group signatures are publicly verifiable and can be verified with respect to a single group public key. Only a designated group manager, can revoke the anonymity of a group signature and find out the identity of the group member who issued a given signature. Furthermore, group signatures are unlinkable which makes it computationally hard to establish whether or not multiple signatures are produced by the same group member. At the same time, no one, including the group manager, can misattribute a valid group signature.

Group signature schemes are defined as follows. (See [4] for more details).

Definition 2. *A group signature scheme is a digital signature scheme comprised of the following:*

(1) ***Setup****: On input of a security parameter* 1^l *this probabilistic algorithm outputs the initial group public key* PK *and the secret key* SK *for the group manager.*
(2) ***Join****: An interactive protocol between the group manager and a user that results in the user becoming a new group member.*
(3) ***Sign****: An interactive protocol between a group member and a user whereby a group signature on a user supplied message is computed by the group member.*
(4) ***Verify****: An algorithm for establishing the validity of a group signature given a group public key and a signed message.*
(5) ***Open****: An algorithm that, given a signed message and a group secret key, determines the identity of the signer.*

A secure group signature scheme must satisfy the following properties:

(1) *Correctness*: Signature produces by a group member using **Sign** must be accepted by **Verify**.
(2) *Anonymity*: Given a signature, identifying the actual signer is computationally hard for everyone but the group manager.
(3) *Unlinkability*: Deciding whether two different signatures were computed by the same group member is computationally hard.
(4) *Unforgeability*: Only group members are able to sign messages on behalf of the group.
(5) *Exculpability*: Even if the group manager and some of the group members collude, they cannot sign on behalf of non-involved group members.
(6) *Traceability*: The group manager can always establish the identity of the member who issued a valid signature.
(7) *Coalition-resistance*: A colluding subset of group members cannot generate a valid group signature that cannot be traced.

5. Our Group Signature Scheme from a ID-based Signature

In this section we present how a ID-based signature scheme [7] can be used to implement an efficient group signature scheme. If we consider that, in the ID-based signature scheme [7], all users that get a private key (from their ID) from the same system and master key parameters form a group, the concepts of ID-based signatures and group signatures are very similar. In this description, the group manager is also a trusted authority.

5.1. **The scheme.**

- **Setup:** The group manager executes the steps from the subsection 3.1. The initial group public key is

$$PK = (q, P, P_{pub}, Q_{ID_i}, H_1, H_2, H_3, \widehat{e})$$

and the secret key is $SK = s$.

- **Join**: Suppose now that a user U_i wants to join the group. We assume that communication between the group member and the group manager is secure, i.e., private and authentic. To obtain his membership certificate, each user U_i must perform the following protocol with the group manager:
  - The user U_i sends ID_i to the group manager.
  - The group manager computes $S_i = s \cdot Q_{ID_i}$ and then S_i is communicated secretly to the user U_i.
- **Sign**: In our scheme, ID_i is the public component of a RSA signature public/private key pair generated by the user itself. This public/private key pair will be referred as (ID_i, d_i) in the remainder of this paper. First, the user U_i signs a message $m \in \{0,1\}^*$ with its RSA private key d_i and the corresponding RSA signature scheme:

$$SigRSA = m^{d_i} \, (mod \; n) \, ,$$

where n is an RSA-like modulus. Then, the group member U_i can generate anonymous and unlinkable group signatures on a message $m \in \{0,1\}^*$ as follows:
  - Chooses a random $k \in \mathbb{Z}_q^*$.
  - Computes $(R, S) \in G_1 \times G_1$, where

$$\begin{aligned} R &= k \cdot P \\ S &= k^{-1} \left(H_2 \left(m \right) \cdot P + H_3 \left(R \right) \cdot S_i \right) , \end{aligned}$$

    where k^{-1} is the inverse of k in $\mathbb{Z}_q^*$.
  - The group signature Sig is then the concatenation of the previously generated signatures $SigRSA$, (R, S) with the U_i's public key ID_i

$$Sig = m^{d_i} \, (mod \; n) \, ||x_R||x_S||ID_i$$

where x_R is the x-coordinate of R and x_S is the x-coordinate of S.

- **Verify**: First, a user verifies that the signature was generated by the group by verifying using the algorithm specified in Section 3.4 that (R, S) is valid and therefore the user U_i is an authorized member of the group:

$$\begin{aligned}\widehat{e}(R,S) &= \widehat{e}\left(k\cdot P, k^{-1}\left(H_2(m)\cdot P + H_3(R)\cdot S_i\right)\right)\\ &= \widehat{e}(P, H_2(m)\cdot P + H_3(R)\cdot S_i)\\ &= \widehat{e}(P,P)^{H_2(m)}\cdot\widehat{e}(P_{pub}, Q_{ID_i})^{H_3(R)}\end{aligned}$$

  where we have used the bi-linearity properties of $\widehat{e}$. Second, a user verifies that the signature was generated by U_i and not by the group manager by verifying using the U_i's public key ID_i and the corresponding RSA signature that $SigRSA$ is valid:

$$m = SigRSA^{ID_i}\,(mod\ n)\,.$$

  Since the group manager does not know the private key d_i it will not be able to generate a valid $SigRSA$.
- **Open**: The group manager knows for each ID_j the identity of the user U_j that is associated with it. This binding is established during the **Join** phase. As a result, it is easy for a group manager, given a message and a valid group signature Sig, to determine the identity of the signer.

5.2. **Security Considerations.** In this section, we access the security of the group signature scheme defined in Section 5 according to the security properties defined in Section 4.

Correctness: This property is guaranteed since the ID-based signature scheme [7] must guaranteed it too.

Unforgeability: This property is guaranteed since the ID-based signature scheme [7] must guaranteed it too.

Anonymity: In our scheme, a group signature is the concatenation of the identity based signature with the user's public key (i.e. ID). Therefore if the underlying identity based signature provides anonymity and if the user's public key does not reveal any information about the user, anonymity is guaranteed by the group signature scheme.

Unlinkability: In our scheme, a group signature is the concatenation of the identity based signature with the user's public key (i.e. ID). As a result, all the signatures generated by a user will contains his public key. Therefore unlinkability is not provided. However if the underlying identity-based signature provides unlinkability and if a user uses a different public/private key pair for each signature, unlinkability is then provided. This solution might not be very practical if the user has to sign a lot of messages (because it needs to get and store a lot of public/private key pairs) but is acceptable otherwise.

Exculpability: In our group signature scheme, a group member can not sign on behalf of other members because it does not know the other members' private keys. The group manager knows each users' private key S_i, but he do not knows the users' RSA private key d_i. Therefore, exculpability is provided.

Traceability: Since, in our proposal, the group manager generates each member private keys from their public keys, it can easily identify the actual signer of a valid signature by looking at the public key component in the group signature. Traceability is therefore provided.

Coalition-resistance: This property is guaranteed since the ID-based signature scheme [7] must guaranteed it too.

Our ID-based group signature scheme has a performance cost since it adds one RSA signature. Furthermore even with this extra cost, we believe that our scheme is still more efficient that any existing group signatures.

6. Conclusion

This paper describes an efficient group signature scheme from an elliptic curves identity based signature scheme. The generated group signature can handle large groups since the group public key and parameters are constant and do not depend on the group members. The security of such a group signature depends on the security of the ID based signature scheme it was derived from. The generated group signature performance is similar to the performance of the underlying ID based signature scheme.

References

[1] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, A practical and provably secure coalition-resistant group signature scheme, Advances in Cryptography, CRYPT0 2000, vol. 1880, Lecture Notes in Computer Science, Springer Verlag, pp. 255-270, 2000.

[2] D. Boneh and M. Franklin, Identity based Encryption from Weil pairing, Advances in Cryptography CRYPT0 2001, Springer-Verlag, Lecture Notes in Computer Science, vol. 2139, pp. 213-229, 2001.

[3] J. Camenisch, M. Stadler, Efficient group signature schemes for large groups, Advances in Cryptology, CRYPTO'97, Lecture Notes in Computer Science, vol. 1070, Springer-Verlag, 1296, pp. 410-424, 1997.

[4] J. Camenisch and M. Michels, A group signature with improved efficiency, Advances in Cryptography, ASIACRYPT'98, Springer-Verlag, Lecture Notes in Computer Science, vol. 1514, pp. 160-174, 1998.

[5] D. Chaum and E. Van Heyst, Group signatures, Advances in Cryptography, EUROCRYPT'91, Springer-Verlag, Lecture Notes in Computer Science, vol. 547, pp. 257-265, 1991.

[6] L. Chen and T.P. Pedersen, New group signature schemes, Advances in Cryptography, EUROCRYPT'95, Springer-Verlag, Lecture Notes in Computer Science, vol. 950, pp. 171-181, 1995.

[7] K. Paterson, Id-based signatures from pairings on elliptic curves, Tech. Rep., IACR Cryptology ePrint Archive: Report 2002/004, http://eprint.iacr.org/2002/004/, 2002.

[8] C. Popescu, Group signature schemes based on the difficulty of computation of approximate e-th roots, Proceedings of Protocols for Multimedia Systems (PROMS 2000), Poland, pp. 325-331, 2000.
[9] R. Sakai, K. Ohgishi, and M. Kasahara, Cryptosystems based on pairing, Proceedings of Symposium on Cryptography and Information Security, Japan, Okinawa, pp. 26-28, 2000.
[10] A. Shamir, Identity-based cryptosystems and signature schemes, Advances in Cryptography, CRYPTO'84, Springer-Verlag, Lecture Notes in Computer Science, vol. 196, pp. 47-53, 1984.
[11] N. P. Smart, An Identity based Authenticated Key Agreement Protocol based on the Weil Pairing, Tech. Rep., IACR Cryptology ePrint Archive: Report 2001/111, http://eprint.iacr.org/2001/111/, 2001.
[12] Y.M. Tseng and J.K. Jan, A novel id-based group signature, Workshop on Cryptology and Information Security, Tainan, pp. 159-164, 1998.

University of Oradea, Department of Mathematics, Str. Armatei Romane 5, Oradea, Romania
E-mail address: cpopescu@uoradea.ro