An Identity-based Ring Signature Scheme with Enhanced Privacy

Chandana Gamage, Ben Gras, Bruno Crispo, and Andrew S Tanenbaum
Vrije Universiteit Amsterdam, The Netherlands
{chandag,beng,crispo,ast}@cs.vu.nl

Abstract. There are many applications in which it is necessary to transmit authenticatable messages while achieving certain privacy goals such as signer ambiguity. The emerging area of vehicular ad-hoc network is a good example application domain with this requirement. The ring signature technique that uses an ad-hoc group of signer identities is a widely used method for generating this type of privacy preserving digital signatures. The identity-based cryptographic techniques do not require certificates. The construction of ring signatures using identity-based cryptography allow for privacy preserving digital signatures to be created in application when certificates are not readily available or desirable such as in vehicle area networks. We propose a new designated verifier identity-based ring signature scheme that is secure against full key exposure attacks even for a small group size. This is a general purpose primitive that can be used in many application domains such as ubiquitous computing where signer ambiguity is required in small groups. We consider the usefulness of identity-based cryptographic primitives in vehicular ad-hoc networks and use a specific example application to illustrate the use of identity-based ring signatures as a tool to create privacy preserving authenticatable messages.

1 Introduction

In many applications it is necessary to create messages that can be proven to be authentic so that forged messages that appear to be valid can be detected. A digital signature, which securely and provably binds an identity to a message, is a convenient and efficient technique to publicly prove the authenticity of a message to a verifier with its properties of *soundness* (verification of valid signatures succeed), *completeness* (verification of invalid signatures fail), and *unforgeability* (only the entity with knowledge of the secret signing key can create valid signatures). The signer and the verifier do not need to have any prior agreement or follow a setup protocol for this standard technique to work.

However, for applications in which privacy is an issue for the signer and in instances when she would wants to prove the authenticity of a message to a verifier without disclosing her true identity, additional work is needed. In this scenario, use of straightforward digital signatures requires a setup phase in which the signer obtains a verifiable pseudonym from a trusted third party. This scheme has the disadvantages of a setup phase and requirement of verifiers to accept

pseudonyms as valid identifiers. Also the privacy of signers is dependent on the trusted third party maintaining the mapping of actual identity to pseudonym secret.

Another solution for signing messages while preserving privacy is to use group signatures introduced by Chaum and van Heijst [1] in which a public key for verification of signatures is generated for a group of signers in such a way while any member of the group can create a valid signature, a verifier is unable to extract the identity of the specific signer. The group signature schemes use a group manager for establishing the group membership, generation of the group public key, and the revocation of membership have the properties of *signer ambiguity* (the signer identity of a signature cannot be determined without the group manager secret key), *signature unlinkability* (signatures cannot be identified as being from the same signer), and *frame-freeness* (a valid signature cannot be created for a member of the group by other members of the group even in collusion with the group manager). The group signature schemes also require a setup phase and the privacy of signers is dependent on the group manager.

The ring signature concept introduced by Rivest, Shamir, and Tauman [2] improves the privacy preserving capability of group signatures by removing the need for a group manager and allowing a signer to create an ad-hoc group membership even without the knowledge of the other members whose identities and public keys she has used. While the ring signature scheme is an excellent primitive for use in applications with the competing requirements of message authenticity and signer privacy, we are interested in some of the emerging application areas in which the use of a standard ring signature scheme provide weak security guarantees for privacy of the signer. We specifically consider applications where the ad-hoc group that a signer can use to create her signature (1) has a small membership and (2) has members who would disclose their private keys in a collusion attack.

In section 2, we sketch an example application from the emerging area of vehicular ad-hoc networks (VANET) to motivate the problem discussed in this paper and also explain the usefulness of ID-based variant of ring signatures to design a solution. A review of the ID-based ring signature scheme used as the building block to create a signature scheme with privacy enhancing properties is given in section 3 and its security properties and vulnerabilities are discussed in section 4. The proposed modifications to the ID-based ring signature scheme is explained in section 5 and a proof of the security properties of this scheme provided in section 6 through a proof-by-equivalence technique. The paper is concluded in section 7 with some comments on the application of the proposed solution.

2 An Application Example

The emerging area of VANET is intended to combine the advance control, communication, navigation and processing systems available in modern vehicles with wireless ad-hoc networks to build intelligent applications for traffic manage-

ment (through cooperative and real-time reporting on road accidents, traffic congestions, vehicle density in roads, road repair work, etc), accident avoidance (through warnings on rapid deceleration, blind spots, incoming vehicles, etc), dynamic navigation (through electronic road-side infrastructure providing vehicle speed and routing information directly to vehicle control systems), city parking space management, etc.

We are interested in the class of VANET applications in which a vehicle want to transmit an authenticatable message in a privacy preserving manner. For example, a vehicle driver that wish to inform the authorities about other vehicles present at a scene of an accident may not directly transmit a signed message to the authorities for fear of reprisals from other vehicle drivers. The authorities may not accept a completely anonymous message that cannot be authenticated as it could be an attempt to mislead an investigation by providing false data.

A useful cryptographic tool in this scenario is the ring signature primitive that allows a signer to create an ad-hoc group of signers and digitally sign a message that provides both unforgeability and ambiguity for signer identity. In the above example, the vehicle reporting on the accident can use the public keys of other vehicles present in the scene of the incident to create a message digitally signed with a ring signature. Due to the properties of a ring signature, while the authorities can correctly authenticate the message, the public knowledge of the message and its corresponding signature does not reveal which specific vehicle in the group created the message. An ID-based ring signature scheme is especially suitable for this VANET application as the signature can be created by simply using the unique vehicle license plate numbers as the identifiers and the signer does not need to obtain public key certificates and verify their authenticity as in standard signature schemes. The vehicle license plate number, which is the standard visual identifier for all on road vehicles, is unique for the country in which the vehicle is registered and an infrastructure already exists for proper management of these identifiers.

3 An Efficient ID-based Ring Signature Scheme

The concept of ring signatures was first introduced by Rivest, Shamir and Tauman [2] and its realization in the ID-based cryptographic setting was first given by Zhang and Kim [3]. The concept of ID-based cryptography was introduced by Shamir [4] as a solution to the difficulty and complexity of public key certificate management in conventional public key cryptography but it should be noted that this scheme has its own limitations due to the introduction of a trusted key-escrow for secret key generation and use of secure channels for secret key distribution. However, many cryptographic techniques that use ID-based concept have been developed for a wide spectrum of applications.

For the development of a modified ID-based ring signature scheme with properties specifically suited for application environments such as the road accident

notification VANET application, we use as a building block an efficient ID-based ring signature scheme proposed recently by Chow, Yiu and Hui [5].

System setup To setup an ID-based (ring) signature scheme, the trusted key generation center, KGC, will select two cryptographic hash functions $H(\cdot)$ and $H_0(\cdot)$ such that $H : \{0,1\}^* \rightarrow \mathbf{G}_1$ and $H_0 : \{0,1\}^* \rightarrow \mathbf{Z}_q^*$, where $\mathbf{G}_1$ is an additive cyclic group of prime order q for some large prime q. The KGC randomly chooses a secret value $x \in_R \mathbf{Z}_q^*$ and securely store it as the master secret key and compute the corresponding public key as $P_{pub} = xP$ where P is a generator of $\mathbf{G}_1$. For a $\mathbf{G}_2$, which is a multiplicative cyclic group of prime order q for the same large prime q, the KGC defines a bilinear pairing $\hat{e} : \mathbf{G}_1 \times \mathbf{G}_1 \rightarrow \mathbf{G}_2$ and publish the system-wide parameters $\langle q, \mathbf{G}_1, \mathbf{G}_2, H(\cdot), H_0(\cdot), \hat{e}(\cdot,\cdot), P, P_{pub}\rangle$.

The bilinear pairing $\hat{e}$ satisfies the properties of *bilinearity* ($\forall P, Q, R \in \mathbf{G}_1$, $\hat{e}(P+Q, R) = \hat{e}(P,R)\hat{e}(Q,R)$ and $\hat{e}(P, Q+R) = \hat{e}(P,Q)\hat{e}(P,R)$), *non-degeneracy* ($\exists P, Q \in \mathbf{G}_1$ such that $\hat{e}(P,Q) \neq 1$), and *computability* ($\hat{e}(P,Q) \forall P, Q \in \mathbf{G}_1$ can be computed efficiently). It is assumed that the Bilinear Diffie-Hellman (BDH) problem [6] in $\langle \mathbf{G}_1, \mathbf{G}_2, \hat{e}\rangle$ of given a tuple $\langle P, aP, bP, cP\rangle$ for some $a, b, c \in \mathbf{Z}_q^*$ then the computing of $\hat{e}(P,P)^{abc} \in \mathbf{G}_2$ is computationally intractable to be true.

Key generation Any entity with identity $ID \in \{0,1\}^*$ can generate its own public key Q_{ID} by simply computing $Q_{ID} = H(ID) \in \mathbf{G}_1$. To obtain the corresponding secret key, the entity must submit it's identity to the KGC, which sets the secret key S_{ID} of ID as $S_{ID} = xQ_{ID}$ and securely transmit this value back to the owner. For the ID-based (ring) signature scheme, the secret signing key is S_{ID} and the public signature verification key is Q_{ID}.

Signing The set L of identities of n users is $L = \{ID_1, ID_2, \ldots, ID_n\}$ and the actual signer is indexed as s. The public key Q_{ID_s} of the signer is $Q_{ID_s} = H(ID_s) \in \mathbf{G}_1$. The signing algorithm for a message m by signer ID_s is as follows:

1. Choose $U_i \in_R \mathbf{G}_1$ and compute $h_i = H_0(m \| L \| U_i) \forall_i \in \{1, \ldots, n\} \backslash \{s\}$.
2. Choose $r'_s \in \mathbf{Z}_q^*$ and compute $U_s = r'_s Q_{ID_s} - \sum_{i \neq s} \{U_i + h_i Q_{ID_i}\}$.
3. Compute $h_s = H_0(m \| L \| U_s)$ and $V = (h_s + r'_s) S_{ID_s}$.
4. Output the signature on m as $\sigma = \{\bigcup_{i=1}^{n} \{U_i\}, V\}$ and L.

Verification The verification of an ID-based ring signature by an entity that receives the tuple (m, L, σ) is as follows:

1. Compute $h_i = H_0(m \| L \| U_i) \forall_i \in \{1, \ldots, n\}$.

2. Check the equality
   $\hat{e}(P_{pub}, \sum_{i=1}^{n}(U_i + h_i Q_{ID_i})) = \hat{e}(P, V)$ and
   if the output of the test is true then accept the signature as correctly verified.
   Otherwise a value of false is output.
   The equality for signature verification is satisfied as follows:

$$
\begin{aligned}
& \hat{e}(P_{pub}, \sum_{i=1}^{n}(U_i + h_i Q_{ID_i})) \\
&= \hat{e}(P_{pub}, \sum_{i \neq s}(U_i + h_i Q_{ID_i}) + (U_s + h_s Q_{ID_s})) \\
&= \hat{e}(P_{pub}, (-U_s + r'_s Q_{ID_s}) + (U_s + h_s Q_{ID_s})) \\
&= \hat{e}(P_{pub}, r'_s Q_{ID_s} + h_s Q_{ID_s}) \\
&= \hat{e}(P_{pub}, (r'_s + h_s) Q_{ID_s}) \\
&= \hat{e}(xP, (r'_s + h_s) Q_{ID_s}) \\
&= \hat{e}(P, (r'_s + h_s) x Q_{ID_s}) \\
&= \hat{e}(P, (r'_s + h_s) S_{ID_s}) \\
&= \hat{e}(P, V)
\end{aligned}
$$

4 Security Analysis of the ID-based Ring Signature Scheme

The above signature scheme by Chow, Yiu and Hui [5] has proven security in terms of (1) existential unforgeability and (2) signer ambiguity. However, in certain application environments, the standard definitions of security for which the proofs are provided is insufficient. For example, in the road accident notification VANET application described earlier, the number of vehicles available for obtaining identifiers to spontaneously create the ID-based ring signature will be limited to a small number. Even more significantly, most of these vehicles in the vicinity may be involved in the accident itself. Therefore, a situation could arise in which owners of other vehicles whose identifiers are in the ring signature may collude to learn the identity of the owner of the vehicle that created the authenticatable message.

The systematic extension of the basic security notions used in ring signature schemes to much stronger security definitions has been done by Bender, Katz, and Morselli [7]. While their definitions for standard ring signature schemes directly apply to the ID-based ring signatures, the construction of signature schemes satisfying the stronger security definitions have been constructed only for the standard ring signatures using public key certificates. In the stronger security definitions given in [7], there are two extended definitions for signer ambiguity as:

1. Ambiguity with respect to adversarially-chosen keys and

2. Ambiguity against full key exposure

While the public keys in standard signature schemes which are random bit strings that can be selected so as to allow for a hidden channel (say, by fixing some of the bits a-priori), for application environments in which the public keys are derived from contextually meaningful data such as the visible vehicle registration numbers for the road accident notification VANET application and the fact the ring is created in a true ad-hoc manner makes an adversarially chosen key an attack unlikely. However, we are specifically interested in the full key exposure attack as there exists an incentive for vehicle owners to collude and the fact the ring size is likely to be small make such an attack practical.

Consider the full key exposure attack for the ID-based ring signature scheme by Chow, Yiu and Hui [5] described earlier where the owner with the vehicle identifier ID_j where $j \in \{1, \ldots, n\} \backslash \{s\}$ discloses his secret key S_{ID_j} and try to convince other members of the ring that he did not create the message m. For this proof, the vehicle owner will use his secret key S_{ID_j} and the publicly available message m, the signature $\sigma = \{\bigcup_{i=1}^{n}\{U_i\}, V\}$, and the set of identities L of the ring members. He will compute the following:

$$
\begin{aligned}
h_i &= H_0(m \| L \| U_i) \forall_i \in \{1, \ldots, j, \ldots, n\} \\
T_1 &= U_j + \sum_{i \neq j} \{U_i + h_i Q_{ID_i}\},\ T_1 \in \mathbf{G}_1 \\
T_2 &= V - h_j S_{ID_j},\ T_2 \in \mathbf{G}_1
\end{aligned}
$$

If $\hat{e}(S_{ID_j}, T_1) \neq \hat{e}(T_2, Q_{ID_j})$, then the owner of the vehicle with identifier ID_j can convince other members of the ring that he did not in fact create the message m with signature σ.

While the bilinear mapping $\hat{e}(\cdot, \cdot)$ creates a mapping which is non-bijective and therefore it is not possible to prove that a particular member from the set L has generated the signature, it is possible to exclude members by individually testing using the above inequality. Therefore, it is necessary to strengthen the ID-based ring signature scheme against full key exposure attack to prevent anonymity violation in an application setting such as the road accident notification VANET application.

5 Solutions for Full Key Exposure Attacks on Signer Identity Ambiguity

One possible solution for the full key exposure attack is to use the identity of an authority (for example, the police department) as the public key of an ID-based encryption scheme and encrypt the signature σ (and possibly the message m also) before transmitting on to the ad-hoc network. This solution is possible in application settings such as the road accident notification VANET application in which the messages transmitted by vehicles are meant for use by specific authorities. The advantage of this scheme is that the signer identity ambiguity is

preserved. However, this solution may present application-context difficulties in implementation if the nodes in the ad-hoc network have policies against forwarding messages that they cannot fully process.

Another solution that does not involve ID-based encryption and therefore free of the above described limitation is to generate the signature as a designated verifier type signature. For this purpose, the signer must select a verifier and use that entity's public signature verification key, which is the identity of that verifier, in the computation of the signature. Let us assume the designated verifier to be an authority such as the police department with identity ID_v.

In the modified ID-based ring signature scheme with designated verification, we propose to change the computation of the signature σ on the message m by signer ID_s as follows.

1. Choose $U_i \in_R \mathbf{G}_1$ and compute
   $h_i = H_0(m\|L\|U_i) \forall_i \in \{1, \ldots, n\} \backslash \{s\}$.
2. Choose $r'_s \in \mathbf{Z}_q^*$ and compute
   $U_s = r'_s Q_{ID_s} - \sum_{i \neq s} \{U_i + h_i Q_{ID_i}\}$,
   $W_s = \hat{e}(r'_s Q_{ID_v}, S_{ID_s})$, and
   $W = r'_s Q_{ID_s}$.
3. Compute $h_s = H_0(m\|L\|U_s\|W_s)$ and
   $V = (h_s + r'_s) S_{ID_s}$.
4. Output the signature on m as
   $\sigma = \{\bigcup_{i=1}^{n} \{U_i\}, V, W\}$ and L
   (the set L now includes the designated verifier ID_v also).

Although the size of a ring signature has now increased by $|W|$, the increase is constant and independent of the group size. In the signature verification step, the designated verifier has to compute the h_i value repeatedly with each time only one of the h_i values computed as

$$h_i = H_0(m\|L\|U_i\|\hat{e}(S_{ID_v}, W)).$$

If the verification equality is satisfied for one of the identifiers ID_i, $i \in \{1, \ldots, n\}$, then the message has been correctly signed by the i^{th} member of the ordered set L and the verification step must return a value of true. The bilinearity property of the mapping ensures that

$$\begin{aligned} & \hat{e}(r'_s Q_{ID_v}, S_{ID_s}) \\ = \; & \hat{e}(r'_s Q_{ID_v}, xQ_{ID_s}) \\ = \; & \hat{e}(xQ_{ID_v}, r'_s Q_{ID_s}) \\ = \; & \hat{e}(S_{ID_v}, r'_s Q_{ID_s}) \\ = \; & \hat{e}(S_{ID_v}, W) \end{aligned}$$

If the signature does not correctly satisfy the verification equality for any value of $i \in \{1, \ldots, n\}$, then the verification step must return a value of false. The disadvantage of this scheme is that the signer identity ambiguity property is

lost with respect to the designated verifier although he still cannot generate a transferable proof of the signer identity.

For this modified scheme, if an attacker with identifier ID_j wish to mount a full key disclosure attack, he has to compute the h_j value using the signature related data available publicly to him. While he can simply calculate the h_i values for other members in the set L as $h_i = H_0(m\|L\|U_i)$ using the known U_i values, he has to compute his own h_j value as $h_j = H_0(m\|L\|U_j\|W_j)$ where only the m, L, and U_j values are known. The attacker ID_j needs to compute the W_j value as $W_j = \hat{e}(r'_s Q_{ID_v}, S_{ID_j})$, but does not know the random value r'_s used by the signer. The value $W = r'_s Q_{ID_s}$ is not helpful to the attacker as a bilinear mapping of W with the public key of the designated verifier results in only $\hat{e}(Q_{ID_v}, W) = \hat{e}(Q_{ID_v}, r'_s Q_{ID_s}) = \hat{e}(r'_s Q_{ID_v}, Q_{ID_s})$.

6 Relation to a Generic Ring Signature Scheme Definition and Proof of Security

To prove the security of the proposed ring signature scheme with a designated verifier in the group membership, we use a proof by equivalence approach. Herranz and Sáez [8, 9] have defined a generic ring signature scheme and have proved its security by extending the *forking lemmas* of Pointcheval and Stern [10]. These new *ring forking lemmas* were used by Chow, Yiu and Hui to prove the security of their efficient ring signature scheme [5] used as a building block for the modified scheme described in section 5.

We first show the equivalence of the modified ID-based ring signature scheme to the *generic* ring signature definition by Herranz and Sáez [8, 9]. Let a group of members L of size n be denoted as $L = \{ID_1, \ldots, ID_n\}$. Let $H : \{0,1\}^* \rightarrow \{0,1\}^k$ be a cryptographic hash function where k is a security parameter. For a message m, a *generic* ring signature scheme will generate a signature σ of the form $\{L, m, R_1, \ldots, R_n, h_1, \ldots, h_n, \omega\}$ where for $i \in \{1, \ldots, n\}$, the component values of σ must satisfy following conditions:

1. Each R_i is distinct and will not appear in a σ with a probability greater than $2/2^k$,
2. Each h_i is computed as $h_i = H(L, m, R_i)$ and
3. The value ω is dependent on all of $\bigcup\{R_i\}$, $\bigcup\{h_i\}$, and m.

Condition 1 The signature σ on a message m by a group of L signers of the proposed ring signature scheme with a designated verifier is of the form $\{L, m, U_1, \ldots, U_n, V, W\}$. Each $U_i \in_R \mathbf{G}_1$ is chosen randomly and distinct for each σ by the signer except for the value U_s which is computed. However, the value U_s is computed with a random input value $r' \in \mathbf{Z}_q^*$. The security parameter k for the ring signature scheme is the size of the prime q, which defines the additive cyclic group $\mathbf{G}_1$ with prime order q. Therefore, if the signer ensures that the U_s value is also distinct from other randomly chosen $U_i \in \{1, \ldots, n\}/s$, then the U_i values correspond to R_i values of the generic scheme and the proposed signature scheme satisfy condition 1 for the generic signature scheme.

Condition 2 In the proposed signature scheme, the individual h_i values are not transmitted but recomputed by the signature verifier as $h_i = H_0(m\|L\|U_i)\forall_i \in \{1,\ldots,n\}$. The computation of all the h_i values by the signer is similar to the generic scheme and therefore satisfy condition 2 for the generic signature scheme.

Condition 3 The value ω of the generic signature scheme corresponds to the value V in the proposed signature scheme which is computed with h_s. The value h_s in turn is computed with m and U_s as input and U_s is dependent on all the other h_i and U_i values for $i \in \{1,\ldots,n\}/s$. Therefore, the proposed signature scheme satisfy condition 3 for the generic signature scheme.

Finally, we have to determine the effect of the additional value W in the proposed signature scheme in proving the equivalence of the generic scheme to the proposed scheme. The value W is computed with the use of random value r' and is not used as input to the computation of components of the signature σ that corresponds to the generic signature. In the proposed signature scheme it appears as simply an additional random value used to further randomize the input to the computation of the h_s value by the signature verifier. Therefore, we can state that the generic ring signature scheme and the proposed modified ID-based ring signature scheme with a designated verifier are equivalent in construction.

7 Conclusion

References

1. D. Chaum and E. van Heijst, *Group signatures*, EUROCRYPT'91, LNCS, vol 547, pages 257-265, Springer, 1991.
2. R. L. Rivest, A. Shamir, and Y. Tauman, *How to leak a secret*, 7th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2001), LNCS, vol 2248,pages 552-565, Springer, 2001.
3. F. Zhang and K. Kim, *ID-based blind signature and ring signature from pairings*, 8th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2002), LNCS, vol 2501, pages 533-547, Springer, 2002.
4. A. Shamir, *Identity-based cryptosystems and signature schemes*, Advances in Cryptology (CRYPTO 1984), LNCS, vol 196, pages 47-53, Springer, 1985.
5. S. S. M. Chow, S.-M. Yiu, and L. C. K. Hui, *Efficient identity based ring signature*, Third International Conference in Applied Cryptography and Network Security (ACNS 2005), LNCS, vol 3531, pages 499-512, Springer, 2005.
6. D. Boneh and M. Franklin, *Identity based encryption from the Weil pairing*, SIAM Journal of Computing, 32(3):586-615, 2003.
7. A. Bender, J. Katz, and R. Morselli, *Ring signatures: Stronger definitions, and constructions without random oracles*, To appear in Third Theory of Cryptography Conference (TCC 2006), LNCS, Springer, 2006.
8. J. Herranz and G. Sáez, *Forking lemmas for ring signature schemes*, 4th International Conference on Cryptology in India (Indocrypt 2003), LNCS, vol 2904, pages 266-279, Springer, 2003.

9. J. Herranz and G. Sáez, *New identity-based ring signature schemes*, 6th International Conference on Information and Communications Security (ICICS 2004), LNCS, vol 3269, pages 27-39, Springer, 2004.
10. D. Pointcheval and J. Stern, *Security arguments for digital signatures and blind signatures*, Journal of Cryptology, 13(3):361-396, 2000.