ANONYMOUS MESSAGE AUTHENTICATION
Universally Composable Definition and Construction

Kazuki Yoneyama
The University of Electro-Communications, 1-5-1, Chofugaoka, Chofu-shi, Tokyo 182-8585, Japan

Keywords: Anonymity, anonymous message authentication, universal composability, ring signature, group-certification authority.

Abstract: Recently, various casual communication tools which are run by a certain group (e.g., social network service, blog and Wiki) are popularized. In such services, a member may want to inform some information to other group members without exposing his identity. For this perpose, message authentication schemes which guarantee anonymity of senders seem to be suitable. In this paper, we introduce a new anonymous message authentication scheme using ring signature with a special certification authority, called group-certification authority. Our scheme does not need any group manager to preserve the anonymity of the group member by the property of ring signature. Therefore, our scheme is suitable to casual services where a strict operation is not required by a system manager. Furthermore, we evaluate the security of our scheme in the universal composability framework.

1 INTRODUCTION

Motivation. In our daily life, open blog services are widely used. Blog is short for weblog, chronological publication of comments and thoughts on the web. Usually, blog is operated by a certain group, and members freely insert comments or contents. Then, we consider the anonymity problem of group members. That is, when each member of the group edits the blog with a message which contains the target part of edit and contents, the blog server can verify whether the editor belongs to the group, but it should not be able to distinguish a member from other members. This property is reasonable for such services because a member may want to inform some information to group members without exposing his identity.

For this purpose, authentication schemes which guarantee anonymity of senders seem to be suitable. There are some previous papers (Schechter et al., 1999; Boneh and Franklin, 1999; Nguyen and Safavi-Naini, 2005; Nguyen, 2006) which study anonymous authentication schemes. These schemes aim for the authentication of the *membership* of users in some group. However, for casual services like open blogs, it is enough to authenticate the *message* of the sender. So, we focus on the message authentication scheme which guarantees anonymity of the sender.

Contribution. We introduce a special type message authentication scheme which guarantees anonymity: a sender belonging to a group sends an authenticated message to a recipient. Then, the recipient verifies that this message is sent by one of the group members, but the recipient cannot distinguish the sender from other group members. We call this scheme *anonymous* message authentication scheme, obtained from *ring signature* schemes. Ring signature-based anonymous message authentication schemes have no property of revoking members. However, in the case of a small system blog within a very limited group (e.g., laboratory) where the joining and revoking of the members are very rare, ring signature is preferable to group signature, because we do not need any group manager in ring signature to preserve the anonymity of the group members, in contrast to group signatures. In an unauthenticated communication model, it is impossible to construct the anonymous message authentication scheme by only using ring signature because we cannot confirm whether verification keys which are gone public are true keys of members. Thus, we need to bind messages and signatures to "physical entities" directly. We make the minimal set-up assumption that parties have access to a "certification authority (CA)" who registers party identities together with verification keys. Since a verifier in ring signature

Yoneyama K. (2008).
ANONYMOUS MESSAGE AUTHENTICATION - Universally Composable Definition and Construction.
In *Proceedings of the International Conference on Security and Cryptography*, pages 351-354
DOI: 10.5220/0001916503510354

schemes verifies signatures by using the list of verification keys for the group from CA, our scheme assumes that parties have access to "group CA (gCA)" who records the list of verification keys for the group.

Furthermore, we evaluate the security of our scheme with *universal composability* (UC) framework which was introduced in (Canetti, 2001). The advantage to traditional frameworks is that UC provides strong secure composability (i.e., the security of a primitive which has UC security in a stand-alone manner will always be preserved even when it is executed concurrently with other unbounded number of UC secure primitives in an adversarially controlled manner).

To formulate our scheme and these settings in UC framework, we first formulate a new ideal anonymous message authentication functionality $\mathcal{F}_{\mathrm{aAUTH}}$ as an extension of the ideal message authentication functionality $\mathcal{F}_{\mathrm{AUTH}}$ in (Canetti, 2004), and assume a ring signature scheme and a group-certification authority which are represented by an ideal ring signature functionality $\mathcal{F}_{\mathrm{rSIG}}$ in (Yoneyama and Ohta, 2007) and a new ideal group-certification authority functionality $\mathcal{F}_{\mathrm{gCA}}$. Next, we show that our anonymous message authentication scheme realizes $\mathcal{F}_{\mathrm{aAUTH}}$ given ideal access to $\mathcal{F}_{\mathrm{rSIG}}$ and $\mathcal{F}_{\mathrm{gCA}}$ (i.e., $(\mathcal{F}_{\mathrm{rSIG}}, \mathcal{F}_{\mathrm{gCA}})$-hybrid model).

2 PRELIMINARIES

In this section, we will present the intuitive framework of ring signature schemes, group-certification authority and our anonymous message authentication scheme. For the formal UC definition, readers refer to (Canetti, 2001).

Ring Signature. Ring signature schemes permit any party to generate a signing key and a verification key. A signer chooses group members from parties who generate keys and makes public their verification keys without the group manager. Let M_{all} be the set of parties who generate their keys, and L_{all} be the list of their verification keys. Furthermore, let M be a subset of M_{all} with n elements of M, and L be the list of verification keys of the group members in M. Also, a signature of a message is generated by a signer of the group M. Though any party can verify the signature using L as a verifier, he cannot identify the signer in M.

Group-Certification Authority. In general, a rudimentary certification authority guarantees binding between a single party's identity with previously registered value. However, our scheme requires guaranteeing binding between a group's identity with the list of the group's verification keys. Therefore, we suppose that there is a group-certification authority gCA which guarantees the connection between a group M and the list of the group's verification keys L.

Anonymous Message Authentication. Our anonymous message authentication scheme is based on ring signature schemes with gCA. Ring signature is used for binding a sender's message m with the group M to which the sender belongs. Furthermore, by using gCA, the recipient can obtain the list of verification keys L which are generated by the group members. Therefore, our scheme guarantees the following three properties:

- **Group Authenticity** the recipient is able to verify that the message m is certainly sent by a member of the group M because a party who does not belong to M cannot generate a valid signature from the property of ring signature.
- **Anonymity of Sender** the recipient cannot identify the sender from other members of the group M because signature verification in ring signature only needs a set of a message, a signature and a list of verification keys as inputs.
- **No trusted Third Party** our scheme does not need the group manager who manages group, e.g., joining and revoking members, because ring signature also does not need the group manager.

3 FORMULATING NEW FUNCTIONALITIES

In this section, we will define a new ideal functionality $\mathcal{F}_{\mathrm{aAUTH}}$ which represents anonymous message authentication schemes and a new group-certification authority functionality $\mathcal{F}_{\mathrm{gCA}}$ based on the ideal message authentication functionality $\mathcal{F}_{\mathrm{AUTH}}$ and the ideal certification authority functionality $\mathcal{F}_{\mathrm{CA}}$ in (Canetti, 2004) respectively.

3.1 Anonymous Message Authentication Functionality $\mathcal{F}_{\mathrm{aAUTH}}$

The essential difference between $\mathcal{F}_{\mathrm{aAUTH}}$ and $\mathcal{F}_{\mathrm{AUTH}}$ is output to a recipient in the Receiving Message phase. When each party behaves correctly, $\mathcal{F}_{\mathrm{aAUTH}}$ provides the name of the group to which the sender belongs instead of the name of an entity to the recipient. As $\mathcal{F}_{\mathrm{AUTH}}$, $\mathcal{F}_{\mathrm{aAUTH}}$ does not ensure the revocation property of recorded data because this is able to

Functionality $\mathcal{F}_{\text{aAUTH}}$

Sending Message: On input (“Send”, sid, P_j, m, M) from party P_i, verify that $P_i \in M$. If not, ignore the input. Else, send (“Sent”, sid, M, P_j, m) to the adversary.

Receiving Message: On input (“Send”,$sid, P_j{}', m'$) from the adversary, verify that P_i is uncorrupted. If not, send (“Sent”,sid, M, m') to party $P_j{}'$. Else, send (“Sent”,sid, M, m) to party P_j.

Figure 1: Anonymous message authentication functionality $\mathcal{F}_{\text{aAUTH}}$.

Functionality $\mathcal{F}_{\text{gCA}}$

Resister Key: On first input (“Register”, sid, v_i) from party P_i, forward (“Registered”, sid, v_i) to the adversary. On input “OK” from the adversary, verify that this is the first request from P_i. If not, ignore the input. Else, record $M_{\text{all}} \leftarrow M_{\text{all}} \cup \{P_i\}$ and $L_{\text{all}} \leftarrow L_{\text{all}} \cup \{v_i\}$.

Retrieve Key: On input (“Retrieve”,sid, M) from party P_j, forward (“Retrieve”,sid, P_j, M) to the adversary. On input “OK” from the adversary, verify that $M \subseteq M_{\text{all}}$. If not, output (“Retrieve”, $sid, \perp$). Else, output (“Retrieve”, sid, L).

Figure 2: Group-certification authority functionality $\mathcal{F}_{\text{gCA}}$.

be considered as an optional property. Figure 1 shows the functionality $\mathcal{F}_{\text{aAUTH}}$.

Here, we show several notable points of formulation of $\mathcal{F}_{\text{aAUTH}}$.

Guaranteeing Anonymity of Sender. When a sender P_i is uncorrupted and belongs to the group M, $\mathcal{F}_{\text{aAUTH}}$ sends (“Sent”,sid, M, m) to party P_j. Then, though P_j recognizes that P_i belongs to the group M, P_j cannot distinguish P_i from other members of M. Therefore, $\mathcal{F}_{\text{aAUTH}}$ guarantees anonymity of the sender.

Group Authenticity. When a sender P_i is uncorrupted and does not belong to the group M, $\mathcal{F}_{\text{aAUTH}}$ ignores the input of P_i. This formulation means that an invalid sender, i.e., non-member of the group M, cannot succeed to be authenticated. Therefore, $\mathcal{F}_{\text{aAUTH}}$ guarantees the property of rejecting such an invalid sender.

3.2 Group-Certification Authority Functionality $\mathcal{F}_{\text{gCA}}$

Next, We define group-certification authority functionality $\mathcal{F}_{\text{gCA}}$. $\mathcal{F}_{\text{gCA}}$ is obtained from an extension of $\mathcal{F}_{\text{CA}}$ in (Canetti, 2004). To adapt to the setting of anonymous message authentication scheme, $\mathcal{F}_{\text{gCA}}$ outputs a list of verification keys instead of a verification key directly. $\mathcal{F}_{\text{gCA}}$ accepts only first registered values, and does not allow for modification or “revocation”. Such more advanced features are of course useful, but are not necessary for our basic use. We stress that $\mathcal{F}_{\text{gCA}}$ does not perform any checks on the registered value; it simply acts as a public bulletin board. (In particular, no “proof of possession of signing key” is required.) Figure 2 shows the functionality $\mathcal{F}_{\text{gCA}}$.

4 REALIZING $\mathcal{F}_{\text{aAUTH}}$ GIVEN RING SIGNATURE WITH GCA

In this section, we present our anonymous message authentication scheme, called RAMA, given a UC secure ring signature scheme. Also, we assume that parties can access to gCA in our scheme. This assumption is considered as an ideal access to $\mathcal{F}_{\text{rSIG}}$ (Yoneyama and Ohta, 2007) and $\mathcal{F}_{\text{gCA}}$ in the UC framework. Then, we claim that RAMA securely realizes $\mathcal{F}_{\text{aAUTH}}$ in the $(\mathcal{F}_{\text{rSIG}}, \mathcal{F}_{\text{gCA}})$-hybrid model.

4.1 Ring Signature-based Anonymous Message Authentication Protocol RAMA

Here, we show our scheme, called RAMA. RAMA stands for “Ring signature-based anonymous message authentication”. Therefore, in the basic definition, this protocol is based on ring signature schemes with gCA, and, in the UC definition, that realizes $\mathcal{F}_{\text{aAUTH}}$ in the $(\mathcal{F}_{\text{rSIG}}, \mathcal{F}_{\text{gCA}})$-hybrid model. Figure 3 shows the protocol RAMA.

The unforgeability property of the ring signature guarantees the group authenticity property of RAMA because an invalid sender which is not a member of the group cannot forge a signature which is accepted by recipients. Also, the anonymity property of the ring signature guarantees the anonymity of sender

Protocol RAMA

For all $P' \in M$, in the first activation, P' sends (“KeyGen”, sid_{rSIG}) to $\mathcal{F}_{\mathrm{rSIG}}$, and obtains (“Verification Algorithms”, $sid_{rSIG}, \mathbf{RV}'$) from $\mathcal{F}_{\mathrm{rSIG}}$. P' sets $v' = \mathbf{RV}'$sends (“Register”, sid_{gCA}, v') to $\mathcal{F}_{\mathrm{gCA}}$.

Sending Message. When party P_i is activated with input (“Send”, sid, P_j, m, M), party P_i does:

1. P_i checks $P_i \in M$. If not, then P_i halts. Else, sets $m' = (m, P_j)$.
2. P_i sends (“Retrieve”, sid_{gCA}, M) to $\mathcal{F}_{\mathrm{gCA}}$, and obtains (“Retrieve”, sid_{gCA}, L). Also, P_i sends (“Sign”, sid_{rSIG}, m', L) to $\mathcal{F}_{\mathrm{rSIG}}$, and obtains (“Signature”, $sid_{rSIG}, m', L, \sigma$) from $\mathcal{F}_{\mathrm{rSIG}}$. Finally, P_i sends (sid, M, m, σ) to party P_j.

Receiving Message. When party P_j is activated with input (sid, M, m, σ), party P_j does:

1. P_j sets $m' = (m, P_j)$.
2. P_j verifies that a pair (M, L) is recorded. If not, P_j sends (“Retrieve”, sid_{gCA}, M) to $\mathcal{F}_{\mathrm{gCA}}$, and obtains (“Retrieve”, sid_{gCA}, L). Then, if $L = \perp$, P_j derives (“Verified”, $sid_{rSIG}, m', 0$), i.e., rejects the signature, outputs nothing. Else, P_j records a pair (M, L).
3. P_j sends (“Verify”, $sid_{rSIG}, m', \sigma, L$) to $\mathcal{F}_{\mathrm{rSIG}}$, and obtains (“Verified”, sid_{rSIG}, m', f) from $\mathcal{F}_{\mathrm{rSIG}}$. If $f = 1$, P_j outputs (“Sent”, sid, M, m) and halts. Else, P_j outputs nothing.

Figure 3: Ring signature-based anonymous message authentication protocol RAMA.

property of RAMA because a recipient cannot distinguish the sender with other members of the group while the recipient is able to authenticate that the message is certainly sent by a member of the group.

Theorem 4.1 *Protocol* RAMA *securely realizes* $\mathcal{F}_{\mathrm{aAUTH}}$ *in the* $(\mathcal{F}_{\mathrm{rSIG}}, \mathcal{F}_{\mathrm{gCA}})$*-hybrid model.*

[**Proof Idea.**] Let $\mathcal{A}$ be an adversary in the $(\mathcal{F}_{\mathrm{rSIG}}, \mathcal{F}_{\mathrm{gCA}})$-hybrid model. The proof outline is that for any $\mathcal{A}$ we can construct a simulator $\mathcal{S}$ such that any environment $\mathcal{Z}$ cannot successfully distinguish the interaction with $\mathcal{A}$ and parties running RAMA in the $(\mathcal{F}_{\mathrm{rSIG}}, \mathcal{F}_{\mathrm{gCA}})$-hybrid model from the interaction with $\mathcal{S}$ and parties for $\mathcal{F}_{\mathrm{aAUTH}}$ in the ideal model. Simulator $\mathcal{S}$ runs simulated copy of $\mathcal{A}$ and the interface for $\mathcal{A}$. Then, $\mathcal{S}$ forwards all instructions from $\mathcal{Z}$ to $\mathcal{A}$ and back. The detail of the proof will be shown in the full paper.

5 PRACTICAL APPLICATION

Here, we consider casual applications, more specifically, open blog services, Wiki and social network services. Especially, we pick up a blog that is promoted by a small group (e.g., a laboratory) and allows members to freely insert comments or contents. In this setting, the case of no group manager is handy to promote for such a small system than the case of a group manager because the change of permission is not frequent. Therefore, our scheme is quite suitable for such services. Because the UC security guarantees strongly composable security under concurrent execution environments among any other protocols, the security of our scheme provides elimination of loads to prove security of these applications.

REFERENCES

Boneh, D. and Franklin, M. K. (1999). Anonymous Authentication with Subset Queries. In *ACM Conference on Computer and Communications Security 1999*, pages 113–119.

Canetti, R. (2001). Universally Composable Security: A New Paradigm for Cryptographic Protocols. In *FOCS 2001*, pages 136–145.

Canetti, R. (2004). Universally Composable Signatures, Certification and Authentication. In *CSFW 2004*, pages 219–233.

Nguyen, L. (2006). Efficient Dynamic *k*-Times Anonymous Authentication. In *VIETCRYPT 2006*, pages 81–98.

Nguyen, L. and Safavi-Naini, R. (2005). Dynamic *k*-Times Anonymous Authentication. In *ACNS 2005*, pages 318–333.

Schechter, S., Parnell, T., and Hartemink, A. (1999). Anonymous Authentication of Membership in Dynamic Groups. In *Financial Cryptography 1999*, pages 184–195.

Yoneyama, K. and Ohta, K. (2007). Ring Signatures: Universally Composable Definitions and Constructions. In *ASIACCS 2007*, pages 374–376.