ECS 227 Project Presentation Writeup

Foundations of Group Signatures

Shizhuo Yu

March 12, 2012

Objective

This paper illustrated the essential and fundamental primitive of group signature, by providing strong and formal definitions for the core requirements of anonymity and traceability. Then the authors showed that this superior definitions implied the existing informal requirements in literature, so the primitive of group signature can be unified and simplified. At last, this paper designed a construction which meets the definition based on a general assumptions of trapdoor permutation existing.

Formal definition

The definition of group signature is introduced by Chaum and Van Heyst. It is a method for allowing a member of a group to sign a message anonymously on behalf of the group. There is a single signature-verification group public key *gpk* associate each group, and each member i can produce a secret key $gsk[i]$ to signing the message relative to *gpk*. There is a group manager for each group who has a secret key *gmsk* on which it can, given a signature σ, extract the member who create the σ, while other members can not do this. So, based on this, there are many informal basic requirements for group signature, including anonymity, traceability, unforgeability, exculpability, coalition resistance, no framing, unlinkability, etc. However, this paper formulated these requirements and defined the stronger versions of the core requirements called full-anonymity and full-traceability, from which all informal requirements can be implied.

- Full-anonymity: The author adopt an indistinguishability based formalization. Given a message and a pair of group member identities, it returned a target signature under one of the two identities. The adversary only have negligible advantage to determine which of the two identities the target signature was produced.
- Full-traceability: It is a stronger form than original traceability, it combines collusion-resistance. A group of colluding group members who pool their secret keys can not create the valid signature, which the algorithm can not catch as belonging to some member of the colluding group.

The paper shows all existing requirements are implied by full-anonymity and full-traceability, which provides a clear advantage, only check two security properties make it easy to give formal proofs under group signature.

Algorithms

In order to using these two superior requirements, the authors use two experiment $Exp^{anon-b}_{\mathcal{GS},\mathcal{A}}(k,n)$ and $Exp^{trace}_{\mathcal{GS},\mathcal{A}}(k,n)$, respectively, to define full-anonymity and full-traceability of group signature. Here, A is the adversary, $b \in \{0,1\}$, $\mathcal{GS}$ is the group signature scheme

$$\mathcal{GS} = \{GKg, GSig, GVf, Open\}$$

consists of four polynomial-time algorithm.

- GKg is the randomized group key generation algorithm, take the input $1^k, 1^n$, returns all the keys need to be used in this group signature scheme, including $(gpk, gmsk, gsk)$.
- $GSig$ is the randomized group signing algorithm, using a secret signing key $gsk[i]$ and a message m to create a group signature.
- GVf is group signature verification algorithm, under a group public key gpk, given a message m and a signature σ, return whether σ is a valid signature of m.
- $Open$ is a deterministic opening algorithm, given a group manager secret key $gmsk$, a message m, and a signature σ of m to return the identity of the signer.

In order to make the scheme correct, it should satisfy

$$GVf(gpk, m, GSig(gsk[i], m)) = 1 \ and \ Open(gmsk, m, GSig(gsk[i], m)) = 1$$

That means the true signatures are always valid, and the opening algorithm correctly recover the identity of the signer from a true signature.

According to the authors, the group signature scheme is fully-anonymous if for any polynomial time adversary A, the advantage

$$Adv^{anon}_{\mathcal{GS},\mathcal{A}}(k,n) = Pr[Exp^{anon-1}_{\mathcal{GS},\mathcal{A}}(k,n) = 1] - Pr[Exp^{anon-0}_{\mathcal{GS},\mathcal{A}}(k,n) = 1]$$

is negligible.

Also, the group signature scheme is fully-traceable of for any polynomial time adversary A, the advantage

$$Adv^{trace}_{GS,A}(k,n) = Pr[Exp^{trace}_{GS,A}(k,n) = 1]$$

is negligible.

Construction

Once defined the four algorithm in group signature scheme, the author start to show how to construct these algorithms one-by-one, beginning to describing the three primitives.

First is "Digital signature scheme" $\mathcal{DS} = K_s, Sig, Vf$, as specified, by algorithms for key generation, signing, and verifying. The authors uses a digital signature scheme that satisfies the standard notion of unforgeability under chosen message attack. $\mathcal{DS}$ is secure against forgeries under chosen message attack if the function $Adv^{unforg-cma}_{\mathcal{DS},A}(\cdot)$ is negligible for any poly-time adversary A. Because the digital signature schemes and unforgeable under chosen message attack exist assuming one-way permutation exists. Thus, it can assume the existence of a family of trapdoor permutations instead.

Then the paper defines a public-key encryption scheme $\mathcal{AE} = (K_e, Enc, Dec)$, by algorithms for key generation, encryption and decryption. The authors make the construction utilize an encryption scheme that satisfy the standard notion of IND-CCA. That is to say, if the encryption scheme $\mathcal{AE}$ us said to be IND-CCA secure, it can be used in the construction of the algorithms.

Finally, a proof system called "Simulation-Sound Non-interactive Zero Knowledge(NIZK)" is used. Here, the author fix a NP relation ρ over domain Dom, and design a pair of polynomial time algorithms (P, V), P is randomized and V is deterministic. If there exist a polynomial p that satisfy the completeness and soundness conditions, then (P, V) form a simulation-sound NIZK proof system.

Based on three primitives above, this paper construct all algorithms. The authors fixed group signature schemes $\mathcal{DS} = (K_s, Sig, Vf)$, public-key encryption scheme $\mathcal{AE} = (K_e, Enc, Dec)$, NP-relation ρ over domain Dom, and NIZK proof system (P, V), the paper conclude the theorem: If there exists a family of trapdoor permutations, then there exist a compact group signature scheme that is fully-anonymous and fully-traceable. This theorem consists of two separate lemmas which are proven in details in this paper, regarding full-anonymity and full-traceability, respectively.

Conclusion

In this paper, the author showed the intuition on foundation of group signatures, by given formal definitions, and simplified informal requirements, to design a construction that fulfill the fully-anonymity and fully-traceability. They first discussed two experiments regarding to these two superior requirements. In order to keep the correctness and compactness, they constructed each of the algorithms with some fundamental primitives. Finally they proved that based on those schemes and a series of definitions, the group signature can reach their strong requirements that are full-anonymity and full-traceability. At the end of the paper, the author forecasted their extension work on dynamic group signatures.