Report on Ring Signatures

-by Shivam Agarwal CSE 2020123

Introduction

Ring Signatures were first introduced in 2001 by Rivest, Shamir and Tauman in their paper “How to Leak a Secret”. Ring Signatures allows users to remain anonymous within a group, i.e, any individual within the group can sign his message as a member of the group and anyone else can check whether that message was signed by a member of that group but they cant tell which member of the group actually signed it. This ability to ensure credibility/verification of identity as a group member while staying anonymous is very important as this shows that the message is not sent by a malicious person/third party. Unlike in the case of Group Signatures, Ring Signatures don't have anyone like a group leader that can deanonymize the signer. They can be generated arbitrarily by anyone using the public keys of the group members without their knowledge.

Similar to one used in the original paper, let's consider an example of how ring signatures can be used in cases of whistleblowers.Say, a whistleblower wants to send some information to a news agency, but he cannot do it openly as it might lead to him losing his job, threats or court cases for leaking confidential information. So he uses Tor which allows him to send the information anonymously, but now the news agency cannot verify the source of this information and might assume that the information came from a malicious party who wanted bad press for that organization, so they might decide to not follow up with it. This shows that along with anonymity, a method to show credibility is also very important for the user. In this case the whistleblower can use the public keys of a large number of his coworkers to sign the message (you can think of it as a cheque with the joint signature of all the group members), and then send it to the news agency. Now the news agency knows that this information came from a member of the group, so the information has credibility but they don't know exactly from whom it came from, maintaining the whistleblower’s anonymity.

Implementation

Assumptions :

- Every member of the group is an honest member.
- Every member has a valid RSA public key available that is known by everyone

Procedure for generating the ring signature:

1. Generate the key : Compute a symmetric key k by performing the hash of the message m

   $$k = H(m)$$

2. Pick a random glue value or v : The signer picks a random glue value called ‘v’ uniformly from $\{0, 1\}^b$

3. Pick random X_i’s : The signer picks X_i’s for all the members of the group other than himself uniformly at random from $\{0, 1\}^b$.

4. Compute Y_i’s : Compute the Y_i’s for all the chosen X_i’s using the function g such that

   $$Y_i = g_i(X_i)$$

   where

   $$g_i(m) = \{ q_i n_i + pow(r_i, e, n) , \text{if } (q_i + 1)n_i <= 2^b$$
   $$\{ m , \text{else}$$

5. Compute Y_s : Use the combination function $C_{k,v}(Y_1, Y_2, \dots , Y_r)$ and equate it to the glue value(v). This gives us a unique value for Y_s (Y for the signer).

   where, $C_{k,v}(Y_1, Y_2, \dots , Y_r) = E_k(Y_r \oplus E_k(Y_{r-1} \oplus E_k(\dots \oplus E_k(Y_1 \oplus v) \dots)))$
   where, Ek is a symmetric encryption function with key k

6. Compute X_s : Calculate the value of X_s using the inverse of gs.

   $$X_s = g_s^{-1}(Y_s)$$

7. Output Signature : $(P_1, P_2, \dots , P_r, v, X_1, X_2, \dots , X_r)$

Procedure for verifying the ring signature:

1. Generate the key : Compute a symmetric key k by performing the hash of the message m

   $$k = H(m)$$

2. Compute Y_i’s : Compute the Y_i’s for all the X_i’s using the function g such that

$$Y_i = g_i(X_i)$$

3. Verify the ring equation : Check whether the combination function
$$C_{k,v}(Y_1, Y_2, \dots, Y_r) = v$$

   If the above equation is satisfied, then the given signature is a valid ring signature.

Practical Applications

We have considered an example earlier where a whistleblower might want to use ring signatures to hide his identity, now we will look at some other areas where we can use ring signatures.

E-voting : We can use ring signatures for e-voting as it allows us to hide which user has voted for a particular party.

Veto Usage: If a proposal is given to the members of a committee to pass, with several members having the power to veto, then it is better to be done using ring signatures as this allows that no action will be taken against the person who vetoed.

Ring signatures can also be used as a form of secret ballot to pass a proposal in a meeting as in this case you need a minimum number of votes (you can specify the number you need) to create a signature while it also does not reveal any information to other members.

Limitations

- Ring Signatures can be inefficient for a large group of people as for computing each signature, we need to iterate over all the group members. And for cases such as e-voting, we would need to generate n number of signatures, making the computation $O(n^2)$.
- As there is no individual who can deanonymize the signer, the signer might use this for nefarious purposes as he can generate ring signatures without the knowledge of other members of the group.
- No security guarantee is given if there is a malicious member in the group, or if some public keys are generated with malicious intent.

Source : R. L. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In ASIACRYPT 2001, pages 552–565. Springer-Verlag, 2001