Project: GeoSecret

Submitters: Alex Livshiz, Hila Bahri, Eliran Moyal

Abstract

Our project is a location-based chat, where a user Alice can enter the group in her region and send anonymous messages. She signs her messages with a ring signature, so that:

- Each other user in the group can verify that the message was sent from inside the group
- There is no evidence that Alice was the one who sent the message. The author of the message is completely anonymous.

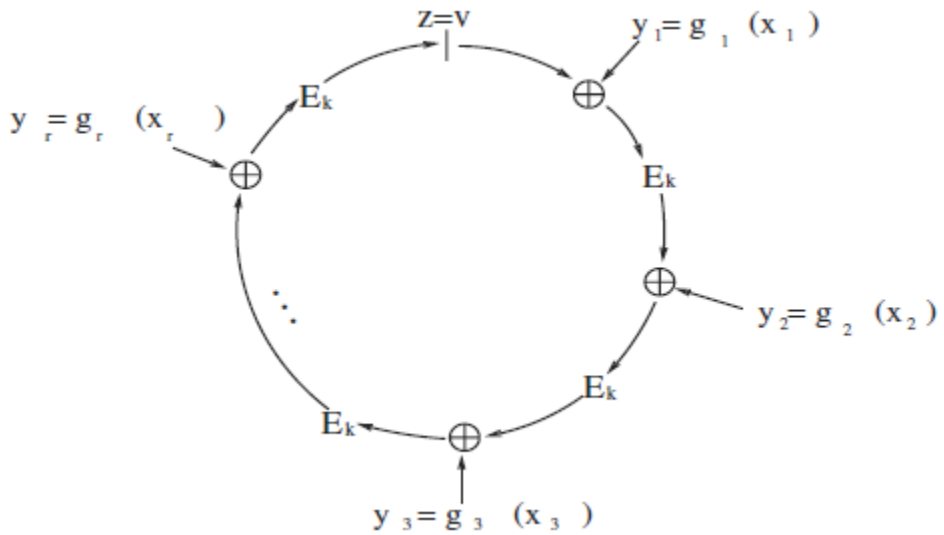
Ring Signatures

As written by Rivest, Shamir, and Tauman, the ring signature makes it possible to specify a set of possible signers without revealing which member actually produced the signature. Unlike group signatures, ring signatures have no group managers, no setup procedures, no revocation procedures, and no coordination.

In our project, the ring signatures are created using RSA functions.

The ring signature is well explained in our presentation and in the original paper, but we write a short explanation to how it works.

Let's take a look at the following figure:



In short, the g functions are RSA-based and are essentially trap door functions. The Ek functions are symmetric encryptions where k (the key) is a hash of the original message. All the x values (except for the x in the index of the member who sends the message) and v are randomly chosen. Let's say that we

hold the private key of g3. Then we can solve the equation z = v, to get the appropriate y3 which causes the ring to "close". Note that the only parameter in the equation is y3, since all the others are known. Since we have the private key, we can find the relevant x3.

Application Flow

- Alice enters the main page and registers using facebook authentication.
- Alice proceeds to the next page and chooses to which group she wants to register.
- Alice registers to a group
    - Alice's client generates a private and public key
    - The public key is saved on the server and is public to each one of the group.
    - The private key is encrypted with a password that Alice chooses and the encrypted private key is stored on the server
    - In the future, Alice can request her encrypted private key and only she will know how to open it
    - From this point on, Bob, who is already in the group, will know that Alice is a part of the group (thanks to her facebook information that the server saves)
- Alice now has her private key, and all of the other participants in the ring have her public key.
- Alice continues to the chat page. At this point her identity is completely unknown. In theory, Alice could use a VPN and browse to the chat page with a completely different IP.
- Notice that if Alice registers to a group, and then leave the site, next time, she can just choose the chat from an existing chats list, without the registration part.
- Alice can now send a message to the ring and sign it with a ring signature. Since everyone in the ring know all the public keys, they can make sure that indeed the signature is valid. But, no one knows that Alice sent the message.

Security Assumptions

In order for the chat to be safe and for Alice to be truly anonymous, a few security assumptions are made regarding Eve:

- Eve cannot access and perform operations on Alice's computer. Since the private key is saved on the client, which is a web browser, if Eve has access to the computer, she can simply see what Alice types – and that loses all the point of the anonymity.
- Even if Eve is in theory capable of breaking the symmetric encryption using in the process of generating the ring, or if Eve is capable of breaking the encrypted private key stored on the server, it still won't be enough to frame Alice and to prove that she sent the message. This is due to the face that the ring calculation uses permutations in each step, so there is no way to know which private key was used to close the ring.