Ring Signature for Kids

A clear explanation of anonymous authentication with Ring Signature

***Abstract*—Digital signatures were an important advent for authentication in the virtual world. Without it, it would be very difficult to have the necessary trust in the digital world to the point that large infrastructures and paradigms emerge, such as: blockchain, edge computing, among other technologies and architectures of decentralized data.**

***Index Terms*—Public-Key, criptography, Ring Signature**

I. Introduction

Ring signatures can ensure anonymity in Internet authentication. This enables operations where the data must be separated from the creators and be reliable at the same time.

The ring signatures were formalized by Ronald Rivest et al. [1]. This document has been prepared with the aim of clarifying the concepts of the ring signature in a simple language, trying to reach the necessary depth of the subject to understand it in its essence.

II. Public-Key criptography

Let's first remember the concept of Public-key and Private-key cryptography. Imagine that Levi wants Eren to communicate securely with him, through any channel. One way to accomplish this is for Levi to tell Eren to transform his message into some other message according to a transformation rule X. If the rule is: make the power of two of the number (imagine the message a single number), then Eren's "4" message will become "16". Levi, in turn, when reading "16" knows he should do the reverse process and make the square root of "16", that is "4" and finally get the original content that Eren sent. However, the rule X said will be public knowledge, not only Eren will know. So does that mean anyone can do like Levi and get Eren's "4"? The answer is no. In real cases, the X rule produces such a complex transformation in the message that anyone who tries to do the inverse of X to get the original message will not get the time to live. Levi will be the only one to obtain the original content, as it will have a kind of trapdoor, a "shortcut" to revert rule X, like "the number is pair". In this analogy, rule X is the public key, while Levi's "shortcut" is the private key.

Given the explanation, an "individual" digital signature uses the same idea, but in reverse. Now it's Levi who wants to convince Eren that the message Eren received is from Levi. Let's assume Levi wants to send number "4" to Eren. Since rule X and "shortcut" are inverse operations of each other, if Levi adds a "signature" being the number "2" (square root of 4 which is the inverse of rule X), Eren can use this value to check if the message is really from Levi. Eren just applies the X rule (power of two) to Levi's signature and checks if he gets the same value as the message, which in this case is "4". As "2" raised to "2" is "4", so this is proof that it is Levi the sender. This is because only someone with the "shortcut" could do such a "magic", otherwise the operation would be very complex.

III. Ring signature

In the case of a ring signature, we will use the same concept as used in Public-Key criptography. The difference now is that Levi will want to prove to Eren that the message Eren receives will be from a place that Levi is a member, but in such a way that Eren can't tell who exactly sent the message. Let's imagine that Levi's soccer team is the place. Following the same reasoning, we could make a signature using the "shortcuts" of all the players on the team and then Eren will use the X rule of each player to do the reverse process. But there is a problem here, the "shortcuts" of the players are private to each of them, and not all players on the team get along well enough to share them. The only thing that is public are each player's X rules. And even then, how would each player's shortcuts combine to produce a signature capable of being reversed? The process is not so intuitive after all.

The trick here will be the following. Levi will choose a random number for each team member, except for himself (which will not be random). In addition, he will choose any initial Y value. The set formed by the numbers assigned to each team member, by the Y value and by the public keys (X rules) of each team member, will be the signature that Levi will make. Right, but how will that guarantee our objective? The secret here is how Levi will calculate your non-random number, which will be the big relevant factor for everything. Levi will choose rule X from some team member, and apply it to that same member's number. If the member Armin has the number 6 and the rule "add 4", we will have the value 10. Then Levi will take the initial value Y defined (which we consider as "5") and apply a rule that we will call "rule of the ring". The ring rule will be "add by Y" to the given element, and therefore we will have 10 + 5 = 15. What Levi will do now is the same process for the second team member, but using the 15 instead of 5 as Y, when applying the ring rule. And so on, for each team member, using the ring rule applied to each member's result iteratively.

If I may, before explaining where we are at, imagine one more account. Imagine that you want to take the result of all the previous operations and apply the ring function once more, in such a way that the result is the initial value Y (which was 5). As the ring operation adds the result of the previous

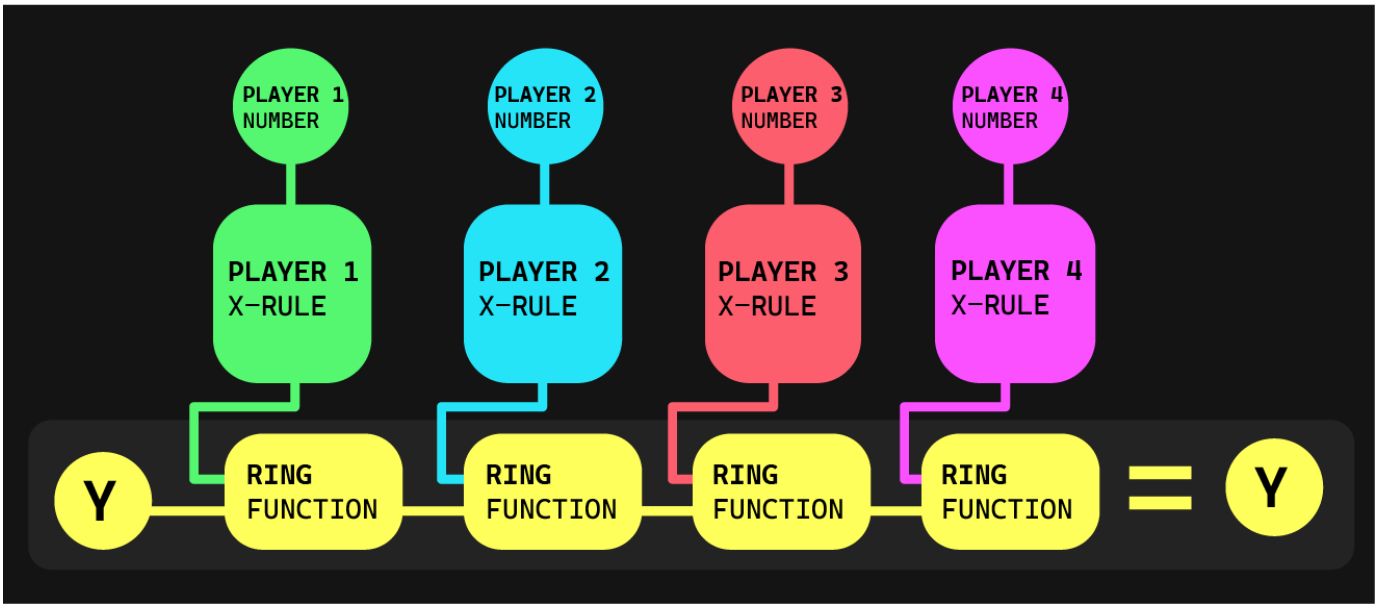

Fig. 1. Visual Ring Signature Scheme

operations to a given element, through a quick equation equating its result to the initial Y, it is easily discovered the necessary element for the operation to be carried out. This discovered element will be applied to Levi's Private Key, the shortcut that only he knows. The number you get will be Levi's long-awaited number. It is the number that, if Levi applies his Public Key and then is used in the ring function in the last iteration, then we get the initial value of Y.

This is impressive. Take a minute to think. Imagine that you have access to the public keys of all members of Levi's team, along with the numbers of each member of Levi's team (including Levi's), and the initial value Y. If we apply the described ring function, it is expected that the result is the very Y value that will initiate the interactions. But for that to happen, it was necessary that in the last iteration, Levi's public key had been applied to Levi's number, and only then was the expected result found. Any number other than Levi's would not work. But think about it, Levi's number choice was made using his private key, which only he has. Anyone who had access to the public keys of the players on Levi's team would not be able to obtain the same result, since to produce Levi's number it is necessary to have Levi's private key, otherwise the Inverse key operation would have to be performed (that was described before and is not exequible).

What is notable here is that, given the public keys of the participants of a given group, together with an initial value Y and numbers for each participant, being a signature, if the verifier uses the ring function and the result Y is obtained, it means that the signature sent was necessarily built by someone who has a private key corresponding to one of the participants' public keys. Note that it is not possible to say who, since in the verifier's view he only has random numbers in his hands. But Levi knows that one of those numbers was chosen minisculely. And this way, Levi can prove that a member of the team signed that message, while nobody will be able to prove who sent it.

References

[1] Rivest, Ronald L. and Shamir, Adi and Tauman, Yael, "How to Leak a Secret",2001