Guió Presentació sobre Secret Sharing Schemes

Introducció:

Introducció dels membres del grup, que farem la presentació sobre secret sharing schemes.

Secret sharing refers to methods for distributing a secret among a number of participants. Each participant will be given a share of the secret, which can only be reconstructed when a certain minimum number of shares are combined. Individual shares are no use on their own.

We will talk about Shamir's Secret Sharing, formulated by Adi Shamir, which uses a type of sharing scheme called (t, n)-threshold. In this type of scheme, there are n total shares, and a minimum of t are needed to rebuild the secret. Any subset of n of size t will be able to rebuild the secret. To be considered secure, a sharing scheme must distribute the shares so that anyone with fewer than t shares has no more information than someone with 0 shares. We will now see a comparison between secure and insecure Shamir's Secret Sharing.

Shamir's Secret Sharing (Canvi d'escena i de persona):

Shamir's Secret Sharing is one of the first secret sharing schemes in cryptography, based on polynomial interpolation over finite fields.

Polynomial interpolation consists in defining a polynomial of the lowest degree possible that passes through all points of a dataset. As a simple example, the polynomial f(x)=x+1 would interpolate a dataset with (-1,0), (1,2), (3,4), etc…

The function and the points appear on the screen as are said by the speaker. (Dibuixats amb geogebra)

We know that to unlock the secret, a minimum number of shares must be combined. Shamir's secret sharing achieves perfect secrecy because an attacker that has discovered a number of shares lower than the threshold has not learned anything about the secret.

Shamir's Secret Sharing is based on the Lagrange Interpolation Problem, specifically that k points are enough to define a

polynomial of degree k - 1 (2 points are enough to define a line, 3 points are enough to define a parabola, …)

Diagrams representing 2 points and a line, 3 points and a parabola. (Dibuix GeoGebra)

This way, we can define our secret as an element of a finite field, and then construct a polynomial with our secret as the constant element and k - 1 other random elements.

Formula appears on screen.

Every participant is given a different point in this polynomial. With k different points, the original polynomial can be rebuilt using interpolation and the original secret can be found.

Now we will see an example that does not use finite fields, and we'll discuss why it doesn't provide complete secrecy. Then, we will see how finite fields fix this problem.

First we must choose our secret S, the number of total shares n and how many shares are needed to unlock the secret, k. We obtain k - 1 random numbers, and we build a polynomial of k - 1 degree using these numbers, and S as the constant.

As every parameter is said, it appears on screen, and finally the formula appears. The numbers are S = 1789, n = 6, k = 3, a1 = 1643, a2 = 805. Formula is f(x) = 1789 + 1643x + 805x^2

Now we can give each participant their points, starting at 1 because f(0) = S.

Points appear on screen, (1,4237), (2,8295), (3, 13963), (4, 21241), (5, 30129), (6, 40627).

The original polynomial and thus the secret can be reconstructed using any subset of three points of the shares, using Lagrange Basis Interpolation.

Lagrange basis interpolation formula appears on screen. As the speaker talks, the two parts of the formula get highlighted

This formula calculates the scaled basis polynomials of each point (polynomials that pass through the point and are 0 where the x is of another point) and then sums them to obtain the interpolation polynomial. The constant in the polynomial is the secret S.

In this case, we only need 3 points to rebuild the secret. We calculate the scaled basis polynomials of each point and then we sum them. The result is the original function, and we can recall that the secret was the free term, which means that S = 1789 and we are done.

Calculations appear on screen while the speaker explains them.

This example does not provide perfect secrecy, and we will see why. Let's assume a spy has obtained these two shares. In theory, since they don't have 3 shares, they shouldn't be able to learn anything about the secret, but they can, using this procedure which combines their known shares and the public information:

As the speaker explains, the formulas appear on screen.

The attacker first fills the function with the shares they know. Then, they subtract one from the other to obtain a third formula, which can be rearranged to equal a term to the others. In this case, the others are just a2 and a free term.

Now, because the attacker knows that a1 and a2 are natural numbers, they can change a2 for a natural number starting from 0 until a1 is negative, to find all possible a1 and a2 pairs.

Now, the spy replaces a1 in the first formula by the third formula, to obtain the secret based only on a2. The spy can now change a2 by the range it found, to find all the possible values of the secret.

Now the attacker only has to guess between a small list of numbers instead of all the natural numbers.

This is solved using finite fields, because this attack exploits the fact that the points must lie on a smooth curve. If instead we represent our polynomial over a finite field instead of the natural numbers, we see that it becomes very disorganized.

A polynomial over a finite field appears on screen (descargat).

To cover our secret, we just need a small change. We need a prime p larger than S and all a values, and now our points will be (x, f(x) mod p) instead of (x, f(x)).

Prime p = 1913 appears on screen, points go from the ones before to (1,411), (2,643), (3, 572), (4, 198), (5, 1434), (6, 454).

Now the spy cannot learn any information with less than k shares because equalizing a parameter of the function to the others must also take into account the prime number, which causes that for a natural value of a parameter, there are infinite values of the other, not just one.

Properties of Shamir's secret sharing (Canvi d'escena i persona)

Shamir's secret sharing has some useful properties:

Screen shows "Secure" and a padlock.

It is conditionally secure, because an attacker would need to check for every number from 0 to p to find the secret using brute force.

Screen shows “Minimal” and a diagram showing bits(f(x)) >= bits(Share).

It is minimal, because the size of each share does not exceed the size of the original data.

Screen shows “Extensible” and … (7, 1084), (8, 1411), (9,1435).

It is extensible because new shares can be added without affecting the other pieces.

Screen shows “Dynamic” and the formula f(x) with the same S but changing a1, a2

It is dynamic, because security can be enhanced by changing the factors of the polynomial without changing the secret and rebuilding the shares.

Screen shows “Flexible” and a diagram with a top person with 3 shares but 3 bottom persons with 1 share each.

It is flexible, because in situations where hierarchy is important, each participant can receive more or less shares according to their importance, for example a more important person can get the secret by themselves, while the less important ones need to collaborate.

Screen shows “Non verifiable” and (x, f(x)?).

It is not verifiable however, because there is no way to verify that a share is correct, and that a participant is not submitting a fake share.

Improvised conclusion.