Introduction the ones used in real life are

Introduction Secret Sharing Schemes were independently introduced by two mathematicians – Adi Shamir and George Blakley in 1979. The scheme proposed by the former one bases on Lagrange interpolation and modular arithmetic, whereas that of the latter one bases on planes. Secret sharing schemes have a gamut of application in real-life. They are used whenever the piece of information required to access the secret is strongly prevented from getting unauthorized entities. Most common applications are in military and banking – an industry in which I want to develop my professional career. Though in this paper quite small prime numbers are used in examples, the ones used in real life are vastly bigger. The aim of this work is to describe the Shamir's Secret Sharing Scheme.

The goal of Shamir's Secret Sharing Scheme is to divide secret into pieces, called shares, in such a way that: 1. Knowledge of any or more shares makes easily computable. It means that the complete secret can be reconstructed from any combination of t pieces of data. 2. Knowledge of any or fewer shares leaves completely undetermined. Possible values for seem as likely as with knowledge of 0 pieces of information. In other words, secret cannot be reconstructed with fewer than pieces.

This is called threshold scheme. In a case when every piece of the original secret is required to reconstruct the secret. The main idea behind this scheme is that at least 2 points are required to define a line, at least 3 points to define a parabola, at least 4 points to define a curve of degree 3 and so on. In general, it takes points to define a polynomial of degree The polynomial is retrieved with the use of Lagrange interpolation.

As the scheme's main goal is to provide security, all the computations are conducted in a finite field. Otherwise, unauthorized person would be able to narrow the set of possible secrets down with trial and error. Use of modular arithmetic allows full security of the secret. Bearing in mind the significance of modular arithmetic and Lagrange interpolation, the work starts with explanation of these concepts and leads to the main topic: Shamir's Secret Sharing Scheme. My interest in this issue was prompted by this year's rise of Bitcoin's value on international markets. As I am an active trader, I wanted to get to know the technical aspect of cryptocurrencies. The world of cryptography intrigued me and I started to dig deeper.

One day, I stumbled across secret sharing. The simplicity and efficiency of the scheme proposed by Shamir astonished me. During my summer internship in one of the biggest Polish banks – ING Bank – I had an opportunity to talk to an IT Specialist.

I asked him about the use of this scheme in real life and his answer was that it and its generalizations are widely used, not only in that particular organization. It proved to me that the topic of Shamir's Secret Sharing Scheme is worth further investigation. Modular arithmeticWithout the use of modular arithmetic, it would be possible to retrieve the polynomial without the knowledge of all the required points – security of encrypted information would be vulnerable. Moreover, use of a modular arithmetic, allows computers to conduct computations faster. In a later part of this work this concept will be applied to Shamir's Secret Sharing Scheme.

NotationIf is an integer number greater than 0 then " x mod m" indicates remainder of division of " x" over " m". Example1.   12 mod 7 = 52.   3682 mod 64 = 34 Let's consider a set of .

In this set operation of addition can be defined in a following way: The operation of addition can be expanded to a table. Let's consider one in a set 0 1 2 3 4 5 6 0 0 1 2 3 4 5 6 1 1 2 3 4 5 6 0 2 2 3 4 5 6 0 1 3 3 4 5 6 0 1 2 4 4 5 6 0 1 2 3 5 5 6 0 1 2 3 4 6 6 0 1 2 3 4 5   Definition1 Identity element of addition in a set is such element , that   One can easily deduce that the identity element of addition in a set is 0. Definition Additive inverse element to the element in a set is such element that   Additive inverse element to is denoted by . Let's notice that every element in a set has an additive inverse element. Moreover, if is an additive inverse element to , then is an additive inverse element to Example: Consider set . Then: Let's JW1 consider a set .

In this set one can define multiplication in a following manner: Example: Let's consider a set . For this set one can construct a table of multiplication as follows: 0 1 2 3 4 5 6 0 0 0 0 0 0 0 0 1 0 1 2 3 4 5 6 2 0 2 4 6 1 3 5 3 0 3 6 2 5 1 4 4 0 4 1 5 2 6 3 5 0 5 3 1 6 4 2 6 0 6 5 4 3 2 1   Definition Identity element of multiplication in a set is such element , that   It is not hard to notice that identity element of multiplication in a set is 1. DefinitionMultiplication inverse element to element in a set is such element that Multiplication inverse element to is denoted by . ExampleLet's consider a set . Then: Theorem. Element in set has a multiplication inverse element if is coprime with . It means that GCD () = 1.

What results from this theorem is that when is a prime number, then in a set every element different from 0 has a multiplication inverse element. Moreover, if is an inverse element to , then is an inverse element to Multiplication inverse elements are crucial for Shamir’s Secret Sharing Scheme. Concept of multiplication inverse elements allows to avoid such situation in which one cannot compute the polynomial from Lagrange interpolation in a modular arithmetic. It is because multiplication inverse element is determined unambiguously. On the other hand, if one wouldn’t apply the theory of identity elements when using Lagrange interpolation, they would not only obtain wrong result, but most probably would not be able to even conduct computations. It is because operation of division does not exist in modular arithmetic and instead is substituted with multiplication by multiplication inverse element. Such situation is shown below: Suppose .

Let’s divide this polynomial by a factor of 3. It is because and Order of operations in modular arithmetic follows “ PEMDAS” rule. Lagrange InterpolationLet’s consider points on a plane: . These points are called “ nodes.

” Lagrange Interpolation’s aim is to find such polynomial of the degree at most that for all As one can see, it squares with the main idea of Shamir’s Secret Sharing Scheme. Coefficients of and computations can be within or Lagrange polynomial can be represented with the use of pi notation. This symbol represents a multiplication of a bunch of terms. For instance: Theorem3. Polynomial described above is always well-defined and is given by the following formula: Where Lagrange Interpolation can be conducted in sets where is a prime number.

Furthermore, it has to be prime, because we want all the elements different from 0 to have an multiplication inverse element. Let’s use concepts of modular arithmetic and Lagrange interpolation in practice. ExampleLet’s consider and the following nodes: .

One can construct a Langrange polynomial of order at most 3 from them as follows: In order to check my computations, I created an excel formula. The outcome gave the coordinates of nodes, which proved the Lagrange interpolation to work properly. Shamir’s Secret Sharing Scheme Let be a finite set of participants. The value of , a secret, is chosen by a special participant, called “ dealer”.

The dealer is denoted by and it is assumed that   When wants to share the secret S with the participants in , he gives each participant a piece of information called a “ share”. The shares should be distributed secretly, so that no participant knows the share given to another participant. SchemeThe scheme is divided into preliminary phase and actual execution. The data generated during the first one is publicly known.

It consists of the following: 1.   determines a finite set , where is a prime number and 2.   chooses pairwise, non-zero elements of denoted by (those are called identifiers), (For gives the value to   3.   choses a threshold t, where After this is done, main phase takes place.

The information created during this stage is not publicly known. Assume wants to share a 4.   secretly chooses elements of which are denoted .

5. For , computes , where 6. For , sends the share to accordingly. It is important to mention that shares are sent by a safe channel. It is to increase security and privacy, which is a main concern of cryptography.

Later, a subset of participants will gather their shares in order to calculate the secret . If then they will be able to find the value of with the shares they collectively own. Otherwise secret is impossible to find. They will use Lagrange interpolation in order to retrieve the secret.

Assume that the secret is 15. Let's construct an example following the order of operations of scheme presented above. 1.

D determines a finite set 2. D choses 5 identifiers and gives them to participants respectively. 3.

D chooses a threshold . The preliminary phase is done. Now the main phase begins. 4. D chooses 2 elements His polynomial is therefore 5. D computes .

For this purpose, I created an excel formula displayed below. The results are as follows: 6. D sends shares to participants accordingly.

Later a required subset of participants gathers and using Lagrange interpolation they try to retrieve the polynomial. The following calculations are conducted in online. As it can be seen, free coefficient, 15, is equal to the secret It means that the scheme worked properly and the required value was found.

It is worth noticing that, as we are looking for a secret which is a free coefficient, one could compute . Such operation would ease the computations. In real life, however, numbers used in the scheme are of much bigger magnitude. It is due to security issues: in case of usage of small set, e. g.

mod 17, one could try all the possible (here 17) items and they would finally " guess" a proper one. Use of big sets eliminates this threat. ConclusionsShamir's Secret Sharing Scheme is quite an easy tool to divide a secret. During the work on this paper I was fascinated with Shamir's simplistic approach to a complex issue of sharing a secret.

What delighted me the most was the way in which mathematics can be used to solve serious, real-life problems. It realized me that I prefer concepts of applied mathematics, instead of the ones used in pure mathematics. Moreover, the modular arithmetic seemed to me very funny way to exercise some computational skills and I enjoyed working with it a lot. Lagrange interpolation was an unknown for me way to retrieve a polynomial. I haven't heard about it before, but now, as I got to know it better, I see many applications, even in some tasks from the IB syllabus. BibliographyGraham,

R., Knuth, D.

, Patashnik, O. (2017). Concrete mathematics. Upper Saddle River, NJ u. a.

: Addison-Wesley. Kincaid, D. and Cheney, E. (2009). Numerical analysis. Providence: American Mathematical Society.

Stinson, D. (2006). Cryptography: Theory and Practice.

3rd ed. Boca Raton, Fla.: Chapman 1 Graham, R., Knuth, D., Patashnik, O. (2017).

Concrete mathematics. Upper Saddle River, NJ u. a.

: Addison-Wesley2 Graham, R., Knuth, D., Patashnik, O. (2017).

Concrete mathematics. Upper Saddle River, NJ u. a.: Addison-Wesley. 3 Kincaid, D. and Cheney, E. (2009).

Numerical analysis. Providence: American Mathematical Society4 Stinson, D. (2006). Cryptography: Theory and Practice.

3rd ed. Boca Raton, Fla.: Chapman and Hall/CRC. JW1Zrobi? co? z tymi letsami