38. Сутність та якими властивостями володіє протокол з застосуванням порогової схеми Аді Шаміра?

Побудова відомої порогової схеми Аді Шаміра базується на поліноміальній інтерполяції і на тому факті, що одномірний поліном $f(x)$ степені $k-1$ над полем Галуа унікально задається по k точках. Поліноми можуть бути задані над p-ічним розширеним полем. При цьому коефіцієнти a_i полінома $f(x)=a_0+a_1x+a_2x^2+...+a_{k-1}x^{k-1}$ задаються над полем $GF(p)$ як елементи поля Z_p. Основними параметрами такої схеми є числа (k,n), де k – мінімальне число частин секрету, з використанням яких може бути відновлений загальний секрет, а n – загальне число часток секрету, причому, $1 \le k \le n$.

Коефіцієнти a_i визначаються чи задаються числом n часток секрету. Потім випадковим чином формується загальний секрет S, що має бути розділений на частки секрету S_i, $i=\overline{1,n}$. Пропонована схема має бути такою, щоб будь-які k об'єктів чи суб'єктів, об'єднавши свої k приватних секретів могли однозначно відновити загальний секрет S. При цьому всі частки секрету S_i є конфіденційними, і протягом їхнього життєвого циклу мають бути забезпечені цілісність, дійсність, конфіденційність і приступність.
При виконанні наведених вище вимог і умов порогова схема поділу секрету А. Шаміра реалізується в такий спосіб:

1.Формується велике просте число P, що реально більше припустимого $P_П$, тобто $P > P_П$.

2.Формується випадковим чином загальний секрет S, що є елементом поля $GF(p)$, тобто ціле S задовольняє умову: $1 < S < p$.

3. Випадково формується $k-1$ коефіцієнтів полінома $f(x)$ – $a_1, a_2, \ldots, a_{k-1}$, що оголошуються конфіденційними.

4. Як a_0 приймається значення загального секрету S, тобто $a_0 = S$.

5. Довірена сторона розділяє загальний секрет, обчисливши частки секрету $S_i = f(i)$, де i – числовий ідентифікатор або номер кожного з об'єктів чи суб'єктів, причому, $1 \le i \le p-1$. Розподіл секрету може полягати в присвоєнні кожному з об'єктів чи суб'єктів унікального випадкового ідентифікатора.

6.Усі частки секрету S_i транспортуються і установлюються чи вкладаються кожному з об'єктів чи суб'єктів із забезпеченням конфіденційності, дійсності, цілісності, приступності і спостережливості.

Основними властивостями порогової схеми Аді-Шаміра є такі:

1.Бездоганність. При знанні будь-яких $k-1$ і менших часток секрету S_i всі значення загального секрету S залишаються рівно імовірними і теоретично можуть вибиратися з інтервалу $0 \le S \le p-1$.

2.Відсутність недоведених допущень. На відміну від ймовірнісно-стійких схем схема А. Шаміра не базується ні на яких недоведених допущеннях (наприклад, складності вирішення таких задач як факторизація модуля, перебування дискретного логарифма і т.д.).

3.Розширювання з появою нових користувачів. Ця властивість полягає в тому, що нові частини секрету можуть бути обчислені і розподілені без впливу на вже існуючі частини.

4.Ідеальність, під якою розуміється той факт, що всі частини загального секрету і сам загальний секрет мають однаковий розмір і можуть приймати значення над полем $GF(p)$ з рівною імовірністю.

Особливістю граничної схеми розподілу секрету є те, що вона вимагає виконання модульних операцій над великим полем $GF(p)$, складність яких має поліноміальний характер. Крім того довірений пристрій повинний мати можливість контролювати цілісність і дійсність частин секрету перед виробленням загального секрету.