Модифікація схеми Шаміра для поділу секретної інформації

Іван Савка

Кафедра інформаційних технологій
ДВНЗ "Прикарпатський національний університет імені Василя Стефаника"
м.Івано-Франківськ, Україна

***Abstract*—Пропонується модифікація (2, n)-порогової схеми Шаміра, яка ґрунтується на лінійній комбінації показникових функцій.**

Keywords—криптографія, схема Шаміра, поділ секрету.

I. Вступ

«Поділ секрету» (англ. Secret sharing) – це термін в криптографії, під яким розуміють будь-який спосіб поділу секрету серед групи учасників, кожному з яких дістається своя частина (дивись мал. 1). Криптографічні протоколи поділу секрету застосовуються для розподіленого зберігання інформації. Прикладом такої інформації можуть бути секретні ключі або паролі користувачів.

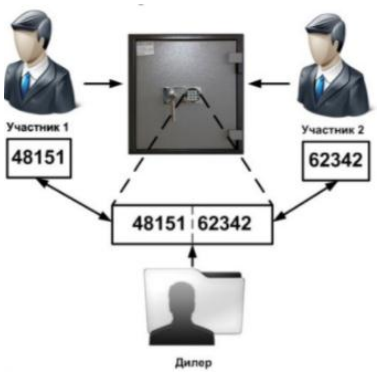

Рис. 1. Схема розподілу секрету між двома учасниками

Задача поділу секрету полягає у передачі деякої таємної інформації S у вигляді набору рівноцінних фрагментів $S_1, S_2, \dots S_n$ (часток секрету), які розподіляються між n учасниками. Якщо секрет S можна відновити із будь-якої підсистеми $\{S_{i_1}, S_{i_2}, \dots S_{i_k}\} \subset \{S_1, S_2, \dots S_n\}$, що містить k часток секрету, але не можна відновити з будь-якої меншої кількості таких часток, то така схема поділу секрету називається (k, n)-пороговою. При $k = n$ отримаємо схему розбиття секрету.

Добре відомим є алгоритм (схема) Шаміра поділу секретного повідомлення. Цей алгоритм ґрунтується на концепції поліноміальної інтерполяції, що задання k різних точок дозволяє однозначно відтворити многочлен $(k-1)$-степеня [1].

II. Виклад основного матеріалу

У алгоритмі Шаміра спочатку дилер (посередник) вибирає велике просте число p таке, що $p > S, p \gg n$, і многочлен

$$f(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_1x + a_0, \qquad a_0, a_1, \dots, a_{k-1} \in \mathbb{Z}_p, \tag{1}$$

де вважається, що вільний член є секретом, тобто $a_0 = S$, а решта коефіцієнтів випадково обираються дилером. Далі дилер формує частки секрету

$$S_j = (x_j, y_j), \quad j = 1,2, \dots n, \tag{2}$$

де $y_j := f(x_j) \bmod p$, причому $x_1, \dots, x_n$ вибираються як попарно різні елементи із скінченного поля $\mathbb{Z}_p$, «забуває» про секрет S і рандомні коефіцієнти $a_1, \dots, a_{k-1}$, після чого розподіляє ці частки між n учасниками. Відновити секрет S можуть тільки k або більше учасників, використовуючи відновлення многочлена $f(x)$ за інтерполяційною формулою Лагранжа [2, с.180] по заданій системі точок $\{S_{i_1}, S_{i_2}, \dots S_{i_k}\}$ цього многочлена і обчислення секрету як $S = f(0)$. Всі обчислення відбувається в полі класів лишків $\mathbb{Z}_p$, операцію ділення у формулі Лагранжа слід розуміти як операцію обернення знаменника за модулем p.

У роботі розглядається (2, n)-порогова схема поділу секрету із заміною у цьому випадку інтерполяційної прямої (1) при $k=2$ на показникову функцію

$$f(x) = ca^x + S, \tag{3}$$

де S є секретом, число c вибирається дилером випадково, число a заздалегідь обране і відоме всім сторонам, причому $a \in \{2,3,..,p-1\}$. Формування часток секрету формується аналогічно до (2) за умови, що $x_1, \dots, x_n$ попарно задовольняють умови

$$a^{x_i - x_j} \neq 1 \pmod p, \quad i \neq j, \ i,j \in \{1,2, \dots, n\}.$$

Відновлення коефіцієнтів у (3) можна виконати через розв'язання системи рівнянь стосовно невідомих c і S

$$\begin{cases} ca^{x_i} + S = y_i, \\ ca^{x_j} + S = y_j, \end{cases} \tag{4}$$

у полі $\mathbb{Z}_p$ для двох учасників з номерами $i,j \in \{1,2, \dots, n\}$, оскільки визначник цієї системи не перетворюється у нуль. Тоді отримуємо секрет як $S = (y_j a^{x_i} - y_i a^{x_j})(a^{x_i} - a^{x_j})^{-1}$.

III. Висновки

Запропоновано заміну прямої на функцію (3) при інтерполяції у (2, n)-пороговій схемі Шаміра. Цікавим є узагальнення інтерполяції на випадок (k, n)-порогової схеми. Але тут виникають деякі проблеми із розв'язанням системи лінійних рівнянь у скінченному полі $\mathbb{Z}_p$.

Література

[1] Shamir A. How to share a secret / A. Shamir // Comm. of the ACM. – 1979. – Vol. 22. – P. 612–613.

[2] Вербіцький О. В. Вступ до криптології. – Львів: Видавництво НТЛ., 2008. – 248 с.

[3] Шнайер Б. Прикладная криптография. 2-е издание. Протоколы, алгоритмы и исходные тексты на языке С. – М.: " Диалектика ", 2001. – 610 с.'