Схема розподілу секретних ключів криптосистеми Голдвассер-Голдріха-Халеві

Артемій Ліхачов

Національний університет «Києво-Могилянська академія», Київ

Київ, 23 травня 2024

- Shamir A. *How to share a secret* — Communications of the Association for Computing Machinery. — 1995. — V. 22, № 11. — p. 612–613.
- Binu V.P., Sreekumar A. *Simple and Efficient Secret Sharing Schemes for Sharing Data and Image* — International Journal of Computer Science and Information Technologies — Vol. 6(1), p. 404-409 — 2015.
- Ravi P., Howe J., Chattopadhyay A., Bhasin S. *Lattice-Based Key Sharing Schemes: A Survey* — ACM Computing Surveys, Volume 54, Issue 1 — Article №9, p. 1-39 — 2021.

Решітка

Нехай $v_1, \ldots, v_n \in \mathbb{R}^m$ є множиною лінійно незалежних векторів. Решіткою L породженою $v_1, \ldots, v_n$ називається множина всіх лінійних комбінацій $v_1, \ldots, v_n$ з цілими коефіцієнтами, тобто

$$L = \{a_1 v_1 + a_2 v_2 + \ldots + a_n v_n | a_1, a_2, \ldots, a_n \in \mathbb{Z}\}$$

Приклад хорошого та поганого базисів

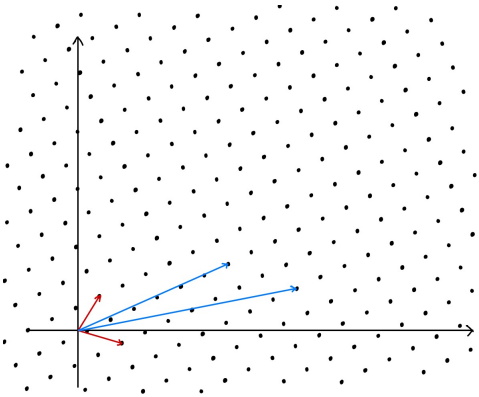

Рис.: Двовимірна решітка із різними базисними векторами

Задача пошуку найближчого вектора (CVP)

- знайти такий вектор $y \in L$, щоб

$$\|x - y\| \leq \|x - z\|$$

для всіх $z \in L$.

- CVP_γ: знайти такий y, щоб

$$\|x - y\| \leq \gamma \cdot \|x - z\|$$

для всіх $z \in L$ та малої константи γ.

Графічний приклад знаходження CVP

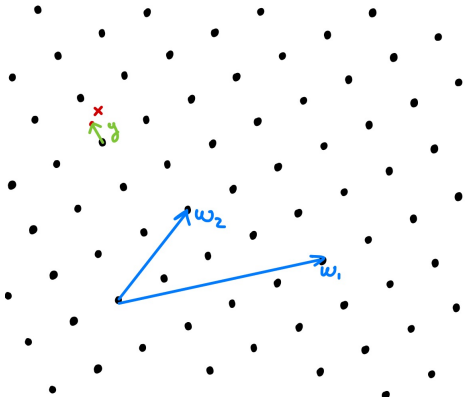

Рис.: Двовимірна решітка із базисними векторами ω_1, ω_2, точкою x, яка не належить решітці та найкоротшим вектором y до неї

Схема розподілення секрету

Схема розподілення секрету є фундаментальним криптографічним примітивом що допускає розподілення секрету між множиною учасників, при цьому відновлення секрету можливе тільки при авторизації всіх або певної частини учасників (порогу учасників).
Також необхідною умовою схеми розподілення секрету є неможливість окремих учасників, або груп учасників, кількість яких менша за поріг, відновити секрет.

Порогова схема розподілення секрету

Визначимо t-порогову схему як $(t, n, \varepsilon_c, \varepsilon_s)$-схему розподілення секрету.

В нашій роботі запропоновано n-порогову схему розподілу секрету для n учасників, що базується на криптосистемі Голдвассер-Голдріха-Халеві.

Схема розподілення секрету на GGH

- Нехай маємо наступні три базисні вектора, що формують решітку L:

$$v_1, v_2, v_3.$$

  Матриця V, яку формують ці вектори, є приватним ключом.
- Генеруємо матрицю U, у якої $det(U) = \pm 1$.
- Знаходимо "поганий" базис $W = UV$, який є публічним ключом.

Схема розподілення секрету на GGH

- Маємо секрет S та малий вектор збурення r. Шифруємо секрет:

$$S_{enc} = SW + r$$

Схема розподілення секрету на GGH

Кожнен із трьох учасників схеми отримує свою пару (v_i, S_{enc}):

- перший учасник отримує (v_1, S_{enc});
- другий учасник отримує (v_2, S_{enc});
- третій учасник отримує (v_3, S_{enc}).

Схема розподілення секрету на GGH

Для відновлення секрету, застосуємо алгоритм Бабаї. Ми шукатимемо найближчий вектор решітки із базисними векторами V до S_{enc}. Запишемо S_{enc} у вигляді

$$S_{enc} = t_1 v_1 + t_2 v_2 + t_3 v_3,$$

розв'язуючи це рівняння отримуємо: $t_1 = a_1, t_2 = a_2, t_3 = a_3$.

Схема розподілення секрету на GGH

- Далі обчислюємо

$$y = a_1 v_1 + a_2 v_2 + a_3 v_3$$

  та отримуємо y, який буде найближчим вектором до S_{enc}.
- Щоб відновити секрет S, треба обчислити yW^{-1}.

У роботі сформулювано та доведено наступну теорему:

Theorem

Схема розподілу секретних ключів криптосистеми Голдвассер-Голдріха-Халеві є коректною та статистично конфіденційною.

Висновки

У кваліфікаційній роботі побудовано схему розподілення секрету, що базується на криптосистемі Голдвассер-Голдріха-Халеві (GGH). Запропонована схема є коректною та статистично конфіденційною. Розглянуто приклад для трьох учасників . Дана робота є логічним продовженням курсової роботи та має потенціал для подальших досліджень - а саме (t, n)-порогова схема.

Література

- Smart N. P. *Cryptography Made Simple*. — Springer International Publishing Switzerland, 2016.— 481 p.
- Hoffstein J., Pipher J., Silverman J.H. *An Introduction to Mathematical Cryptography*. — Springer Science+Business Media, LLC, 2008.— 523 p.
- Shamir A. *How to share a secret* — Communications of the Association for Computing Machinery. — 1995. — V. 22, № 11. — p. 612–613.

Література

- Binu V.P., Sreekumar A. *Simple and Efficient Secret Sharing Schemes for Sharing Data and Image* — International Journal of Computer Science and Information Technologies — Vol. 6(1), p. 404-409 — 2015.
- Ravi P., Howe J., Chattopadhyay A., Bhasin S. *-Lattice-Based Key Sharing Schemes: A Survey* — ACM Computing Surveys, Volume 54, Issue 1 — Article №9, p. 1-39 — 2021.
- Alford W.R., Granville A., Pomerance C. *There are infinitely many Carmichael numbers* — Ann. of Math.(2), — 139(3):703-722, — 1994.

Література

- Babai L., *On Lovász' lattice reduction and the nearest lattice point problem* — Combinatorica, 6:1-13, — 10.1007/BF02579403 — 1986.
- Goldreich O., Goldwasser S., Halevi S. *Public-key cryptosystems from lattice reduction problems* — Proceedings of 17th Annual International Cryptology Conference, — Santa Barbara, California, USA. — pp. 112-131, — 1997.
- Nguyen P. *Cryptoanalysis of the Goldreich–Goldwasser–Halevi Cryptosystem from Crypto'97* — Advances in Cryptology, — 1999.

Література

- Srinvasan A., Vasudevan P. N. *Leakage Resilient Secret Sharing and Applications* — Advances in Cryptology, — CRYPTO 2019, pp. 480-509 — 2019.