ВИКОРИСТАННЯ ПРЕДСТАВЛЕНЬ ПО МНОЖИННИМ ОСНОВАМ В ЕЛІПТИЧНІЙ КРИПТОГРАФІЇ

Кузнецов О.В., Гапіченко А.М., Мельникова О.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Системи захисту інформації зазвичай мають функціонувати в режимі реального часу. При застосуванні криптографічних алгоритмів, які використовують перетворення в групах точок еліптичних кривих (ЕК), найбільший час витрачається на операції еліптичного скалярного множення (однократного або одночасного двократного). Тому важливим питанням є зменшення обчислювальної складності саме цих операцій. Одним із підходів до зменшення обчислювальної складності криптографічних алгоритмів, які використовують багаторозрядні значення, є застосування нестандартних форм їх представлення. **Метою доповіді є** аналіз методів еліптичного скалярного множення з використанням представлень багаторозрядних значень по множинним основам (зокрема, по подвійним). Більш детально розглянуто метод представлення по подвійним основам із використанням направленого ациклічного графу.

Направлений (орієнтований) ациклічний граф (DAG) — випадок орієнтованого графу, в якому відсутні орієнтовані цикли. Тобто відсутні шляхи, що починаються і закінчуються в одній і тій самій вершині. В роботі [1] було запропоновано метод, заснований на DAG, для представлення чисел по подвійним основам. Основною метою цього методу є пошук ланцюга, оптимального за вагою. Ідея методу на основі DAG полягає в тому, щоб створити таблицю зі стовпцями й рядками, які містять значення основ.

Однією з переваг є нижча оцінка обчислювальної складності у порівнянні з іншими методами представлення чисел, а саме $O = (\log n)^{2.5+o(1)}$, де n — ціле додатне число. Наприклад, алгоритм представлення запропонований у [2], має обчислювальну складність $O = (\log n)^{4+o(1)}$. Для стандартного алгоритму [3], вказано обчислювальну складність $O = (\log n)^{5+o(1)}$.

Проведений аналіз показав, що методи формування представлень багаторозрядних чисел по подвійним основам, у яких використовуються графи, є перспективним напрямком, але для отримання практичних реалізацій потребують значного обсягу додаткових експериментальних досліджень.

Список літератури

1.Bernstein D. Double-base scalar multiplication revisited / D. Bernstein, C. Chuengsatiansup, T. Lange. // Cryptology ePrint Archive. — 2017. — № 37.

2.Alex Capunay, Nicolas Th´eriault / Computing optimal 2-3 chains for pairings, Latincrypt. —2015. — pp. 225 - 244.

3.Dimitrov V. S. The Double-Base Number System And Its Application to Elliptic Curve Cryptography / V. S. Dimitrov, L. Imbert, P. K. Mishra. // Mathematics of Computation. — 2008. — № 262. — pp. 1075 - 1104.