АНАЛОГ ШИФРСХЕМЫ ЭЛЬ-ГАМАЛЯ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Матвеев Н. С., Орлов Д. В., Скиба И. Г.
Центр информатизации и инновационных разработок,
Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
E-mail: {n.matveev, i.skiba}@bsuir.by

В работе рассматривается построение криптографической схемы, аналогичной шифрсхеме Эль-Гамаля, на основе эллиптических кривых. Приведены процедуры шифрования и расшифрования сообщений. Описаны особенности применения эллиптических кривых в сравнении с классической схемой, основанной на дискретном логарифмировании в мультипликативной группе.

Введение

Шифрсхема Эль-Гамаля является одной из базовых криптографических схем с открытым ключом. Ее классическая версия основана на задаче дискретного логарифмирования в мультипликативной группе по модулю большого простого числа. При этом для обеспечения криптостойкости требуется использование длинных ключей, что приводит к увеличению вычислительных затрат.

Одним из направлений развития является использование эллиптических кривых, для которых также формулируется задача дискретного логарифмирования. Сложность этой задачи позволяет построить аналогичные по структуре криптографические схемы, но с меньшими параметрами. В данной работе рассматривается алгоритм Эль-Гамаля на эллиптических кривых, описываются его основные этапы и особенности применения.

I. Классическая шифрсхема Эль-Гамаля

Шифрсистема Эль-Гамаля была предложена в 1985 г. и является фактически одним из вариантов метода выработки открытых ключей Диффи-Хеллмана. Криптографическая стойкость данной системы основана на сложности проблемы логарифмирования в мультипликативной группе конечного простого поля.

Задаётся простое число p и примитивный элемент g в мультипликативной группе Z_p^*.

Числа $x \in \{1, \ldots, p-2\}$ и $y = g^x \bmod p$ выступают в качестве открытого и закрытого ключей соответственно.

Пусть сообщение $m \in Z_p^*$. Для шифрования выбирается случайное число $k \in \{1, \ldots, p-2\}$. Вычисляются:

$$c_1 = g^k \bmod p,$$

$$c_2 = m \cdot y^k \bmod p.$$

Шифротекст имеет вид пары (c_1, c_2).

Получатель, обладающий закрытым ключом x, вычисляет:

$$m = c_2 \cdot (c_1^x)^{-1} \bmod p,$$

где $(c_1^x)^{-1}$ обозначает мультипликативный обратный элемент по модулю p.

Для проверки корректности схемы подставим выражения для c_1 и c_2:

$$c_2 \cdot (c_1^x)^{-1} \equiv (m \cdot y^k) \cdot (g^{kx})^{-1} \pmod p.$$

Так как $y = g^x$, то

$$m \cdot g^{kx} \cdot (g^{kx})^{-1} \equiv m \pmod p.$$

Следовательно, исходное сообщение m корректно восстанавливается [1].

II. Основная идея

Классическая схема Эль-Гамаля строится на задаче дискретного логарифмирования в мультипликативной группе Z_p^*. Адаптация заключается в замене этой группы на аддитивную группу точек эллиптической кривой $E(F_p)$.

В обоих случаях принцип работы сохраняется:

- выбор секретного ключа x и вычисление открытого ключа как g^x (в Z_p^*) или xP (в $E(F_p)$);
- использование случайного параметра k для шифрования;
- возможность восстановления исходного сообщения благодаря симметрии операций.

III. Параметры системы

Параметрами схемы на эллиптических кривых являются [2]:

- простое число p — модуль эллиптической кривой;
- эллиптическая кривая $E(F_p)$;
- целое число $m \neq p$ — порядок группы точек эллиптической кривой $E(F_p)$;
- простое число q — порядок циклической подгруппы группы точек эллиптической кривой $E(F_p)$, для которого выполнены следующие условия:

$$m = nq,\ n \in Z,\ n \geq 1.$$

- точка $P \neq O$ эллиптической кривой $E(F_p)$ с координатами (x_p, y_p), удовлетворяющая равенству $qP = O$.

Каждый пользователь схемы цифровой подписи должен обладать личными ключами:

- закрытым ключом – (d, q), удовлетворяющим неравенству $0 < d < q$;
- открытым ключом – (P, q, Q), где точка эллиптической кривой Q с координатами (x_q, y_q), удовлетворяет равенству $dP = Q$.

IV. Шифрование

Для точки $R \in F$ через $X(R)$ обозначим её x-координату.

Процесс шифрования можно описать следующим образом:

- генерируется случайный $k \in \{1, \ldots, n-1\}$;
- вычисляется $C_1 = kP$;
- вычисляется общий секрет $S = kQ$. Берётся $u = X(S)$;
- шифротекст: $C_2 = M + u \pmod q$;
- отправляется пара (C_1, C_2).

Здесь C_1 играет роль аналога $g^k \bmod q$, а C_2 — аналога $m \cdot y^k \bmod p$ из классической схемы.

V. Расшифрование

Для расшифровки сообщения:

- получатель вычисляет

$$S' = dC_1 = d(kP) = k(dP) = kQ;$$

- берёт $u' = X(S')$ и восстанавливает

$$M = C_2 - u' \pmod q.$$

Здесь операция вычитания точек соответствует делению в классической схеме, где сообщение восстанавливалось как $m = c_2 \cdot (c_1^x)^{-1} \bmod p$.

VI. Корректность

Подставим определения:

$$C_2 - u' \bmod q = (M + X(k(Q)) - X(d(kP)) \bmod q.$$

Так как $Q = dP$, имеем:

$$M + X(k(dP)) - X(d(kP)) \bmod q = M.$$

VII. Применение

Ключевое преимущество предложенной адаптации схемы Эль-Гамаля на эллиптических кривых заключается в том, что при сопоставимом уровне криптостойкости алгоритм требует существенно меньших размеров ключей по сравнению с классическими реализациями на основе дискретного логарифмирования в мультипликативной группе простого модуля или на основе RSA [3].

Уменьшенная длина ключей открывает ряд прикладных возможностей:

1. Устройства с ограниченными ресурсами (IoT, смарт-сенсоры). Сокращённый объём ключевых материалов облегчает хранение и управление миллионами ключей в распределённых системах.
2. Мобильные приложения и тонкие клиенты. Компактные ключи упрощают резервирование и синхронизацию ключевых данных в ограниченных пользовательских хранилищах и облачных бэкапах.
3. Протоколы с ограничением размера сообщений. Встроенные системы, блокчейн-транзакции и другие протоколы с жёсткими лимитами на размер сообщений выигрывают за счёт уменьшения длины открытых ключей и подписей [4].
4. Хранение ключей в облаке. При массовом хранении и репликации ключей меньшие размеры существенно экономят место и снижают эксплуатационные расходы.

Таким образом, уменьшение длины ключей обеспечивает не только более компактное хранение и передачу данных, но и расширяет применимость асимметричных схем в условиях, где ранее использование криптографии было затруднено из-за ограничений по объёму данных.

Заключение

Представленная схема шифрования является вариантом адаптации алгоритма Эль-Гамаля на эллиптических кривых.

Ключевая особенность данной схемы заключается в том, что её безопасность опирается на задачу дискретного логарифмирования на эллиптических кривых, которая в настоящее время считается более трудной по сравнению с классическим дискретным логарифмированием. Это позволяет достигать сопоставимой стойкости при меньших размерах ключей.

Практическая значимость метода определяется именно сокращением длины ключей, что упрощает хранение, распространение и использование криптографических данных в прикладных системах, где критичны ограничения по размеру ключей и сообщений.

1. Paar, C. Understanding Cryptography: From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms / C. Paar, J. Pelzl, T. Güneysu. – Cham : Springer, 2024. – 543 p.
2. Государственный стандарт Российской Федерации. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи / – М. : Стандартинформ, 2012. – 36 с.
3. National Institute of Standards and Technology. Recommendation for Key Management, Part 1. / – Gaithersburg, MD : NIST, 2020. – 142 p.
4. Jiang, S. Key-and-Signature Compact Multi-Signatures for Blockchain: A Compiler with Realizations / S. Jiang, D. Alhadidi, H. F. Khojir. // Cryptology ePrint Archive, Paper 2023/061. – 2023. – 35 p.