УДК 004.94 Вестник УрФО № 3(53) / 2024, с. 26–31

Воробьев А. П., Кротова Е. Л., Воробьева Е. Ю. DOI: 10.14529/secur240303

ИСПОЛЬЗОВАНИЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ ДЛЯ ОБМЕНА КЛЮЧАМИ В IOT

Статья посвящена основам криптографии на эллиптических кривых, проведен анализ преимущества использования ECDLP алгоритмов для IoT устройств. Был исследован алгоритм обмена ключами ECDH, применимый для IoT. При использовании кривой Curve25519 построен метод обмена ключами X25519. Данный алгоритм обеспечивает 128-битный уровень защиты, что соответствует уровню симметричного шифрования AES-128, который может использоваться после обмена ключами.

Ключевые слова: *криптография, эллиптические кривые, обмен ключами в IoT устройствах.*

Vorobev A. P., Krotova E. L., Vorobeva E. Yu.

USING ELLIPTIC CURVES FOR KEY EXCHANGE IN IOT

The article is devoted to the basics of elliptic curve cryptography and analyzes the advantages of using ECDLP algorithms for IoT devices. The ECDH key exchange algorithm applicable to IoT was investigated. Using Curve25519, the X25519 key exchange method has been built. This algorithm provides a 128-bit security level, which corresponds to the AES-128 symmetric encryption level that can be used after key exchange.

Keywords: *cryptography, elliptic curves, key exchange in IoT devices.*

Интернет вещей (IoT) – это концепция сети, в которой физические объекты обмениваются данными через Интернет, без необходимости прямого вмешательства человека. IoT представляет собой систему взаимодействия между физическими устройствами, работающими с помощью встроенных датчиков и программного обеспечения для обмена данными через интернет. Использование IoT предполагается в различных отраслях, начиная от носимых устройств и умного дома, до промышленного оборудования в рамках концепции умного предприятия.

Согласно анализу IoT Analytics, к 2027 году число подключений к Интернету вещей, вероятно, превысит 29 миллиардов [1]. Однако, одним из основных недостатков IoT является проблема безопасности подключения. Подключенные устройства IoT могут стать объектом взлома, и злоумышленники могут получить доступ к чувствительным данным или даже контролировать эти устройства. Поэтому с ростом количества устройств Интернета вещей вопрос эффективной защиты становится ключевым в развитии этой технологии: безопасность играет важную роль в разработке, установке и эксплуатации сетей IoT.

В данном контексте необходимо обратить внимание на применение современных методов криптографии для обеспечения безопасности передачи данных в IoT сетях.

Причины применения криптографии для Iot устройств на эллиптических кривых

Устройства IoT имеют ограниченные функциональные возможности, которые характеризуются меньшим объемом памяти и вычислительной мощности, чем обычные устройства [2]. Криптография на эллиптических кривых может стать лучшим решением для таких устройств, так как алгоритмы на эллиптических кривых имеют существенно меньшую длину ключа при равной стойкости [3]. Алгоритмы, основанные на проблеме дискретного логарифмирования (DLP – Discrete Logarithm Problem), имеют больший ключ, чем алгоритмы с проблемой дискретного логарифмирования на эллиптических кривых (ECDLP – Elliptic Curve Discrete Logarithm Problem). Например, 2028 бит для алгоритма Диффи-Хеллмана и 256 бит для Диффи-Хеллмана на эллиптических кривых.

При увеличении вычислительных мощностей растет и вероятность взлома алгоритмов, что влечет за собой необходимость увеличивать длину ключа для обеспечения достаточного уровня защиты. Например, до 1 октября 2015 года 1024-разрядные ключи RSA были разрешены для использования, сейчас настоятельно рекомендуется использовать 2048-разрядные ключи RSA [4].

Также при увеличении уровня защиты длина ключей DLP алгоритмов и ECDLP алгоритмов увеличивается непропорционально. Например, при увеличении ключа DH в два раза (с 1024 до 2048 бит) аналогичный алгоритм на эллиптических кривых ECDH увеличивает длину в 1,4 раза (с 160 до 224 бит). Сравнение алгоритмов по длине ключа приведено в таблице 1 [5].

Таким образом, при дальнейшем использовании и увеличении уровня защиты ECDLP алгоритмы будут эффективнее использовать память устройства. Данное свойство может быть крайне полезно для IoT устройств.

Протоколы с использованием эллиптических кривых

Пусть задано конечное простое поле F_p, характеристика которого $p > 3$. Пусть кривая E, заданная уравнением

$$E : y^2 \equiv x^3 + ax + b \pmod{p}, \qquad (1)$$

определена над полем F_p и точка $P \in E(F_p), P \neq O$. Здесь O – точка на бесконечности (нейтральный, нулевой элемент) [6].

При этом кривая (1) является несингулярной, т. е. ее дискриминант

$$\Delta(E) = 4a^3 + 27b^2 \neq 0 \pmod{p}.$$

n-кратным точки P назовем композицию (сумму):

$$[n]P = \underbrace{P + P + \ldots + P}_{n \text{ раз}}.$$

Наименьшее натуральное число n такое, что $[n]P = O$, называется порядком P в группе $E(F_p)$. Количество точек кривой E будем обозначать N.

Таблица 1.

Сравнение алгоритмов по длине ключа.

Уровень защиты	Алгоритм симметричного шифрования	DSA, DH (L – открытый ключ, N – закрытый ключ), бит	RSA (k – длина ключа), бит	ECDSA, EdDSA, ECDH (f – длина ключа), бит
≤ 80	2TDEA	L = 1024 N = 160	k = 1024	f = 160-223
112	3TDEA	L = 2048 N = 224	k = 2048	f = 224-255
128	AES-128	L = 3072 N = 256	k = 3072	f = 256-383
192	AES-192	L = 7680 N = 384	k = 7680	f = 384-511
256	AES-256	L = 15360 N = 512	k = 15360	f = 512+

Для задания эллиптической кривой согласно национальному стандарту РФ (ГОСТ Р 34.10-2012) необходимо определить следующие параметры [7]:

p – простое число, модуль эллиптической кривой $(p>3)$, задающее размер конечного поля;

a, b – коэффициенты уравнения (1);

P – порождающая точка, или генератор точек кривой, точка большого порядка q. При $1 \le m \le q-1$ последовательность $\{[m]P\}$ задает все различные точки кривой, $[q]P = O$;

q – порядок точки P или порядок подгрупп; $2^{254} < q < 2^{256}$ или $2^{508} < q < 2^{512}$;

$h = \frac{N}{q}$ – кофактор кривой (подгруппы) [8].

Алгоритм ECDSA

Алгоритм цифровой подписи на эллиптической кривой – это криптографически защищенная схема цифровой подписи, основанная на криптографии с эллиптической кривой (ECC). Алгоритм подтверждения цифровой подписи ECDSA (Elliptic Curve Digital Signature Algorithm) основан на умножении точек эллиптической кривой.

Ключи и подписи ECDSA короче, чем в RSA, для того же уровня безопасности. 256-разрядная подпись ECDSA обладает такой же степенью защиты, как и 3072-разрядная подпись RSA [9].

Алгоритм ECDH

Протокол Диффи-Хеллмана на эллиптических кривых – ECDH (Elliptic curve Diffie–Hellman) – криптографический протокол, позволяющий двум сторонам, имеющим пары ключей, получить общий секретный ключ, используя незащищённый от прослушивания канал связи [10].

Алгоритм Диффи Хеллмана на эллиптических кривых (ECDH) отличается от общего алгоритма Диффи Хеллмана (DH) тем, что он основан на задаче дискретного логарифмирования эллиптической кривой (ECDLP) вместо задачи дискретного логарифмирования (DLP). Это означает, что мы можем обойтись ключами меньшей длина, чем при использовании DH.

Опишем общий алгоритм ECDH:

– Выбор эллиптической кривой $E(a,b)$ и базовой точки P (генератора кривой).

– Пользователь **A** выбирает свой секретный ключ K_A ($K_A \in [2, n-1]$), определяет открытый ключ $Q_A = K_A \cdot P$ и отправляет пользователю **B** свой открытый ключ Q_A.

– Пользователь **B** получает ключ открытый Q_A, выбирает секретный ключ K_B, определяет свой открытый ключ $Q_B = K_B \cdot P$ и отправляет пользователю **A** свой открытый ключ Q_B.

– Пользователь **A** вычисляет общий секретный ключ $X_K = K_A \cdot Q_B = K_A \cdot K_B \cdot P$.

– Пользователь **B** вычисляет общий секретный ключ $X_K = K_B \cdot Q_A = K_B \cdot K_A \cdot P$.

При использовании алгоритма ECDH обеим сторонам необходимо выбрать общую эллиптическую кривую $E(a,b)$. Q_A и Q_B являются открытыми ключами IoT-устройства и сервера соответственно, K_A и K_B являются закрытыми ключами. Устройство IoT и сервер умножают базовую точку P на свои закрытые ключи. В результате получаются точки на эллиптической кривой – открытые ключи.

Общий секретный ключ – это координата x результирующей точки, которую они получают после умножения своих соответствующих закрытых ключей на открытый ключ друг друга [11].

Выбор эллиптической кривой для ECDH

После обмена ключами полученный общий секретный ключ можно использовать для алгоритма симметричного шифрования. В качестве такого алгоритма можно использовать, например, AES-128 (Advanced Encryption Standard с 128-битным секретным ключом). Степень защиты алгоритма обмена ключами (ECDH) не должна уступать степени защиты используемого алгоритма традиционного шифрования (AES-128).

Для обеспечения сопоставимого уровня защиты AES-128 можно использовать алгоритм Диффи-Хеллмана на эллиптических кривых с диной ключа 256-283 бит.

Будем использовать эллиптическую кривую Curve25519, с помощью которой генерируются 256 битные ключи. Кривая имеет параметры [12]:

p = 0x7fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffed

a = 0x76d06

b = 0x01

P = (0x09, 0x20ae19a1b8a086b4e01edd2c7748d14c923d4d7e6d7c61b229e9c5a27eced3d9)

n = 0x1000000000000000000000000000000014def9dea2f79cd65812631a5cf5d3ed

h = 8

Метод обмена ключами при помощи выполнения операций над эллиптической кривой Curve25519 носит название X25519. Сам алгоритм обмена ключами аналогичен ECDH [13]:

– Пользователь **А** генерирует a - 32-битное случайное число, вычисляет K_A = X25519(a, 9) и передает пользователю **Б**, где 9 – это x-координата базовой точки.

– **Б** генерирует b - 32-битное случайное число, вычисляет = X25519(b, 9) и передает **А**.

– Используя сгенерированные значения и полученные входные данные, **А** вычисляет X25519(a, K_B), а **Б** вычисляет X25519(b, K_A).

– Теперь оба пользователя могут использовать

K = X25519(a, X25519(b, 9)) = X25519(b, X25519(a, 9)) в качестве общего секрета.

Пример использования X25519:

Секретный ключ **А**:

a = 0x77076d0a7318a57d3c16c17251b26645df4c2f87ebc0992ab177fba51db92c2a

Открытый ключ **А**:

K_A = 0x8520f0098930a754748b7ddcb43ef75a0dbf3a0d26381af4eba4a98eaa9b4e6a

Секретный ключ **Б**:

b = 0x5dab087e624a8a4b79e17f8b83800ee66f3bb1292618b6fd1c2f8b27ff88e0eb

Открытый ключ **Б**:

K_B = de9edb7d7b7dc1b4d35b61c2ece435373f8343c85b78674dadfc7e146f882b4f

Секретный ключ, полученный обеими сторонами после обмена:

K = 4a5d9d5ba4ce2de1728e3bf480350f25e07e21c947d19e3376f09b3c1e161742

В результате обмена оба пользователя получили общий секретный ключ K.

Заключение

Поскольку асимметричная криптография основана на сложности решения задачи дискретного логарифма, то криптосистемы с открытым ключом безопасны благодаря тому, что вызывает сложность разложение составного числа на простые множители. При использовании алгоритмов на эллиптических кривых предполагается, что не существует субэкспоненциальных алгоритмов для решения задачи дискретного логарифмирования в группах их точек. При этом сложность задачи определяется порядком группы точек эллиптической кривой. И, следовательно, для достижения того же уровня безопасности, как и в RSA необходимы группы меньших порядков, что неизбежно приводит к уменьшению затрат на хранение и передачу информации. В данной работе были рассмотрены основы криптографии на эллиптических кривых, преимущества использования ECDLP алгоритмов для IoT устройств. Был кратко рассмотрен алгоритм цифровой подписи ECDSA и более глубоко был изучен алгоритм обмена ключами ECDH, для которого выбрана кривая Curve25519 и метод обмена ключами X25519. Данный алгоритм обеспечивает 128-битный уровень защиты, что соответствует уровню симметричного шифрования AES-128, который может использоваться после обмена ключами. Основное преимущество криптографии на эллиптических кривых – это малый размер ключа по сравнению с другими схемами асимметричного шифрования. Это свойство особенно важно при реализации криптографических протоколов в условиях ограниченности ресурсов памяти и производительности, например, при программировании смарт-карт. Но также понятно, что при постоянно улучшающейся производительности компьютеров данные шифры становиться более уязвимыми при малой длине ключа. А при увеличении длины ключа схемы, основанные на эллиптических кривых, приобретают еще большее преимущество над другими схемами.

Литература

1. State of IoT 2023: Number of connected IoT devices. [Электронный ресурс]: https://iot-analytics.com/number-connected-iot-devices/

2. Калхиташвили Д. Ш. Операционные системы интернета вещей: возможности, проблемы и решения / Д. Ш. Калхиташвили — Москва: РАНХиГС, 2023. — 5 с.

3. Рябко, Б. Я. Криптографические методы защиты информации: учеб. пособие / Б. Я. Рябко, А. Н. Фионов. — 2-е изд., стер. — М.: Горячая линия – Телеком, 2012. — 229 с.

4. NIST Special Publication 800-57 Part 3 Revision 1. Recommendation for Key Management. Part 3: Application-Specific Key Management Guidance. / NIST – 2015 – P. 52.

5. NIST Special Publication 800-57 Part 1 Revision 5 Recommendation for Key Management: Part 1 – General. / NIST – 2020 – P. 54 – 55.

6. Жданов, О. Н. Применение эллиптических кривых в криптографии: учеб. пособие / О. Н. Жданов, Т. А. Чалкин. — Красноярск: СибГАУ, 2011 - 65 с.

7. Национальный стандарт Российской Федерации. Криптографическая защита информации. [Электронный ресурс]: https://www.altell.ru/legislation/standards/gost-34.10-2012.pdf

8. Chandrasekhara, K.R. Elliptic Curve based authenticated session Key establishment protocol for High Security Applications in Constrained Network environment / K.R. Chandrasekhara, M.P. Pillai1 and Sebastian, 2010. [Электронный ресурс]: http://www.arxiv.org/pdf/1202.1895

9. ECDSA: Elliptic Curve Signatures. [Электронный ресурс]: https://cryptobook.nakov.com/digital-signatures/ecdsa-sign-verify-messages (дата обращения: 12.04.2024)

10. Fatma Ahmed, Dalia Elkamchouchi. A New Efficient Protocol for Authenticated Key Agreement // International Journal of Computer and Communication Engineering – 2013 – Vol. 2, No. 4. – P. 1 – 3.

11. Rakel Haakegaard, Joanna Lang. The Elliptic Curve Diffie-Hellman (ECDH) / 2015 – P. 1 – 2.

12. Standard curve database. Curve25519. [Электронный ресурс]: https://neuromancer.sk/std/other/Curve25519 (дата обращения: 19.04.2024)

13. RFC 7748. Elliptic Curves for Security. / IRTF – 2016 – P. 14.

References

1. State of IoT 2023: Number of connected IoT devices. [Электронный ресурс]: https://iot-analytics.com/number-connected-iot-devices/

2. Kalhitashvili D. Sh. Operacionnye sistemy interneta veshhej: vozmozhnosti, problemy i reshenija / D. Sh. Kalhitashvili — Moskva: RANHiGS, 2023. — 5 s.

3. Rjabko, B. Ja. Kriptograficheskie metody zashhity informacii: ucheb. posobie / B. Ja. Rjabko, A. N. Fionov. — 2-e izd., ster. — M.: Gorjachaja linija – Telekom, 2012. — 229 s.

4. NIST Special Publication 800-57 Part 3 Revision 1. Recommendation for Key Management. Part 3: Application-Specific Key Management Guidance. / NIST – 2015 – P. 52.

5. NIST Special Publication 800-57 Part 1 Revision 5 Recommendation for Key Management: Part 1 – General. / NIST – 2020 – P. 54 – 55.

6. Zhdanov, O. N. Primenenie jellipticheskih krivyh v kriptografii: ucheb. posobie / O. N. Zhdanov, T. A. Chalkin. — Krasnojarsk: SibGAU, 2011 - 65 s.

7. Nacional'nyj standart Rossijskoj Federacii. Kriptograficheskaja zashhita informacii. [Jelektronnyj resurs]: https://www.altell.ru/legislation/standards/gost-34.10-2012.pdf

8. Chandrasekhara, K.R. Elliptic Curve based authenticated session Key establishment protocol for High Security Applications in Constrained Network environment / K.R. Chandrasekhara, M.P. Pillai1 and Sebastian, 2010. [Электронный ресурс]: http://www.arxiv.org/pdf/1202.1895

9. ECDSA: Elliptic Curve Signatures. [Электронный ресурс]: https://cryptobook.nakov.com/digital-signatures/ecdsa-sign-verify-messages (дата обращения: 12.04.2024)

10. Fatma Ahmed, Dalia Elkamchouchi. A New Efficient Protocol for Authenticated Key Agreement // International Journal of Computer and Communication Engineering – 2013 – Vol. 2, No. 4. – P. 1 – 3.

11. Rakel Haakegaard, Joanna Lang. The Elliptic Curve Diffie-Hellman (ECDH) / 2015 – P. 1 – 2.

12. Standard curve database. Curve25519. [Электронный ресурс]: https://neuromancer.sk/std/other/Curve25519 (дата обращения: 19.04.2024)

13. RFC 7748. Elliptic Curves for Security. / IRTF – 2016 – P. 14.

ВОРОБЬЕВ Артем Павлович, студент, кафедра Технология твердых химических веществ Казанского национального исследовательского технологического университета. 420015, Республика Татарстан, г. Казань, ул. Карла Маркса, 68. E-mail: drsleepwalker@yandex.ru

КРОТОВА Елена Львовна, кандидат физико-математических наук, доцент, кафедра Высшей математики, Пермский национальный исследовательский политехнический университет. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: lenkakrotova@yandex.ru

ВОРОБЬЕВА Елена Юрьевна, старший преподаватель, кафедра Прикладной математики, Пермский национальный исследовательский политехнический университет. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: lena-vorobey@yandex.ru

VOROBEV Artem Pavlovich, student, Department of Solid Chemical Substances Technology, Kazan National Research Technological University. 420015, Republic of Tatarstan, Kazan, Karl Marx St., 68. Email: drsleepwalker@yandex.ru

KROTOVA Elena Lvovna, Candidate of Physical and Mathematical Sciences, Associate Professor, Department of Higher Mathematics, Perm National Research Polytechnic University. 614990, Perm Krai, Perm, Komsomolsky Prospekt, 29. Email: lenkakrotova@yandex.ru

VOROBEVA Elena Yuryevna, Senior Lecturer, Department of Applied Mathematics, Perm National Research Polytechnic University. 614990, Perm Krai, Perm, Komsomolsky Prospekt, 29. Email: lena-vorobey@yandex.ru