Эвристика Фиата — Шамира

В криптографии**эвристика Фиата — Шамира**, или **преобразование Фиата — Шамира**, — это метод создания интерактивной доказательной базы знания и цифровой подписи на её основе. Таким образом, можно публично доказать какой-либо факт (например, знание определённого секретного числа), не раскрывая при этом исходную информацию. Этот метод был разработан Амосом Фиатом и Ади Шамиром (1986).[1] Чтобы этот метод работал, исходное интерактивное доказательство должно быть публичным, то есть случайные монеты проверяющего должны быть общедоступными на протяжении всего протокола доказательства.

Обзор

Изначально эвристика была представлена без доказательства безопасности. Позже Пойнтшеваль и Штерн[2] доказали её безопасность против атак с выбранным сообщением в *модели случайного оракула*, то есть при условии существования случайных оракулов. Этот результат был обобщён на квантово-доступный случайный оракул (QROM) Доном, Фером, Майенцем и Шаффнером,[3] а также Лю и Жандри.[4] В случае отсутствия случайных оракулов эвристика Фиата — Шамира была признана небезопасной Шафи Голдвассером и Яэль Тауман Калаи. [5] Таким образом, эвристика Фиата — Шамира демонстрирует одно из основных применений случайных оракулов. В более общем смысле эвристика Фиата — Шамира может рассматриваться как преобразование интерактивного доказательства знания с использованием публичной монеты в неинтерактивное доказательство знания. Если интерактивное доказательство используется в качестве инструмента идентификации, то неинтерактивную версию можно использовать непосредственно в качестве цифровой подписи, включив сообщение в качестве входных данных для случайного оракула.[6]

Пример

Для понимания алгоритма, описанного ниже, читателям следует ознакомиться с мультипликативными группами $\mathbb{Z}_q^*$, где q — простое число, и теоремой Эйлера о распределении для функции Эйлера о распределении φ.

Вот **интерактивное** доказательство знания дискретного логарифма в $\mathbb{Z}_q^*$, основанное на подписи Шнорра.[7] Открытыми значениями являются $y \in \mathbb{Z}_q^*$ и генератор g группы $\mathbb{Z}_q^*$, а секретным значением — дискретный логарифм y по основанию g.

1. Peggy wants to prove to Victor, the verifier, that she knows x satisfying $y \equiv g^x$ without revealing x.
2. Peggy picks a random $v \in \mathbb{Z}_q^*$, computes $t = g^v$ and sends t to Victor.
3. Victor picks a random $c \in \mathbb{Z}_q^*$ and sends it to Peggy.
4. Peggy computes $r = v - cx \bmod \varphi(q)$ and returns r to Victor.
5. Victor checks whether $t \equiv g^r y^c$. This holds because $g^r y^c \equiv g^{v-cx} g^{xc} \equiv g^v \equiv t$ and $g^{\varphi(q)} \equiv 1$.

Fiat–Shamir heuristic allows to replace the interactive step 3 with a **non-interactive** random oracle access. In practice, we can use a cryptographic hash function instead.[8]

1. Peggy wants to prove that she knows x such that $y \equiv g^x$ without revealing x.
2. Peggy picks a random $v \in \mathbb{Z}_q^*$ and computes $t = g^v$.

3. Peggy computes $c = H(g, y, t)$, where H is a cryptographic hash function.
4. Peggy computes $r = v - cx \bmod \varphi(q)$. The resulting proof is the pair (t, r).
5. Anyone can use this proof to calculate c and check whether $t \equiv g^r y^c$.

If the hash value used below does not depend on the (public) value of y, the security of the scheme is weakened, as a malicious prover can then select a certain value t so that the product cx is known.[9]

Extension of this method

As long as a fixed random generator can be constructed with the data known to both parties, then any interactive protocol can be transformed into a non-interactive one.

See also

- Forking lemma
- Random oracle model
- Non-interactive zero-knowledge proof
- an application in anonymous veto network

References

1. Fiat, Amos; Shamir, Adi (1987). "How to Prove Yourself: Practical Solutions to Identification and Signature Problems". *Advances in Cryptology — CRYPTO' 86*. Lecture Notes in Computer Science. Vol. 263. Springer Berlin Heidelberg. pp. 186–194. doi:10.1007/3-540-47721-7_12 (https://doi.org/10.1007%2F3-540-47721-7_12). ISBN 978-3-540-18047-0.
2. Pointcheval, David; Stern, Jacques (1996). "Security Proofs for Signature Schemes". *Advances in Cryptology — EUROCRYPT '96*. Lecture Notes in Computer Science. Vol. 1070. Springer Berlin Heidelberg. pp. 387–398. doi:10.1007/3-540-68339-9_33 (https://doi.org/10.1007%2F3-540-68339-9_33). ISBN 978-3-540-61186-8.
3. Don, Jelle; Fehr, Serge; Majenz, Christian; Schaffner, Christian (2019). "Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model". *Advances in Cryptology – CRYPTO 2019*. Lecture Notes in Computer Science. Vol. 11693. Springer Cham. pp. 356–383. arXiv:1902.07556 (https://arxiv.org/abs/1902.07556). Bibcode:2019arXiv190207556D (https://ui.adsabs.harvard.edu/abs/2019arXiv190207556D). doi:10.1007/978-3-030-26951-7_13 (https://doi.org/10.1007%2F978-3-030-26951-7_13). ISBN 978-3-030-26950-0. S2CID 67769879 (https://api.semanticscholar.org/CorpusID:67769879).
4. Liu, Qipeng; Zhandry, Mark (2019). "Revisiting Post-quantum Fiat-Shamir". *Advances in Cryptology – CRYPTO 2019*. Lecture Notes in Computer Science. Vol. 11693. Springer Cham. pp. 326–355. doi:10.1007/978-3-030-26951-7_12 (https://doi.org/10.1007%2F978-3-030-26951-7_12). ISBN 978-3-030-26950-0. S2CID 75135227 (https://api.semanticscholar.org/CorpusID:75135227).
5. Goldwasser, S.; Kalai, Y. T. (October 2003). "On the (In)security of the Fiat-Shamir paradigm". *44th Annual IEEE Symposium on Foundations of Computer Science, 2003. Proceedings*. pp. 102–113. doi:10.1109/SFCS.2003.1238185 (https://doi.org/10.1109%2FSFCS.2003.1238185). ISBN 0-7695-2040-5. S2CID 295289 (https://api.semanticscholar.org/CorpusID:295289).
6. "Inserting electronic signature to Word document" (https://signmydocument.com/blog/how-to-insert-esignature-to-word). Retrieved 2025-02-16.
7. Camenisch, Jan; Stadler, Markus (1997). "Proof Systems for General Statements about Discrete Logarithms" (https://web.archive.org/web/20170706132221/ftp://ftp.inf.ethz.ch/pub/crypto/publications/CamSta97b.pdf) (PDF). *Dept. Of Computer Science, ETH Zurich*. Archived from the original (ftp://ftp.inf.ethz.ch/pub/crypto/publications/CamSta97b.pdf) (PDF) on 2017-07-06.
8. Bellare, Mihir; Rogaway, Phillip (1995), *Random Oracles are Practical: A Paradigm for Designing Efficient Protocols*, ACM Press, pp. 62–73, CiteSeerX 10.1.1.50.3345 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.50.3345)

9. Bernhard, David; Pereira, Olivier; Warinschi, Bogdan. "How not to Prove Yourself: Pitfalls of the Fiat-Shamir Heuristic and Applications to Helios" (http://www.uclouvain.be/crypto/services/download/publications.pdf.87e67d05ee05000b.6d61696e2e706466.pdf) (PDF). In Wang, Xiaoyun; Sako, Kazue (eds.). *Advances in Cryptology – ASIACRYPT 2012*. pp. 626–643.|https://eprint.iacr.org/2016/771.pdf

---