Реферат: Цифровая подпись

Дисциплина: Математические основы защиты информации и информационной безопасности
Автор: Фатеева Елизавета Артёмовна, группа НПИмд-01-24
Преподаватель: Кулябов Дмитрий Сергеевич
Дата: 5 ноября 2025 г.

Введение

В условиях стремительного развития информационных технологий и повсеместного распространения электронного документооборота, вопрос обеспечения целостности, подлинности и неотказуемости данных становится особенно актуальным. Цифровая подпись (ЦП) — один из ключевых криптографических инструментов, позволяющих гарантировать подлинность электронных сообщений и документов, подтверждать авторство и обеспечивать невозможность отказа от подписи. Актуальность темы обусловлена как научно-техническим прогрессом в области криптографии, так и растущими требованиями к защите информации со стороны государственных и коммерческих структур.

Цель настоящего реферата — рассмотреть математические основы цифровой подписи, проанализировать наиболее распространённые алгоритмы её реализации и оценить применение в реальных информационных системах.

Задачи реферата:

1. Дать определение цифровой подписи и отличить её от электронной подписи.
2. Рассмотреть математические концепции, лежащие в основе алгоритмов цифровой подписи (RSA, DSA, ECDSA).
3. Проанализировать применение цифровой подписи в современных системах.
4. Выявить преимущества и ограничения цифровой подписи как средства защиты информации.

Теоретические основы цифровой подписи

Цифровая подпись — это криптографическая метка, создаваемая с использованием закрытого ключа отправителя и проверяемая с помощью соответствующего открытого ключа. Согласно определению, принятому в стандартах ISO/IEC 9796 и RFC 5751, цифровая подпись обеспечивает следующие свойства:

- **Подлинность** — получатель может убедиться, что сообщение подписано конкретным лицом.
- **Целостность** — любое изменение сообщения делает подпись недействительной.
- **Неотказуемость** — подписанное сообщение не может быть отречено автором.

Отличие цифровой подписи от **электронной подписи (ЭП)** важно понимать в правовом контексте. Электронная подпись — более широкое понятие, включающее в себя любые данные в электронной форме, присоединённые к другим электронным данным для определения лица, подписавшего их. В России, согласно Федеральному закону №63-ФЗ «Об электронной подписи», выделяют:

- **Простую электронную подпись** (ПЭП) — данные для идентификации подписавшего (например, логин и пароль);
- **Усиленную неквалифицированную электронную подпись** (УНЭП);
- **Усиленную квалифицированную электронную подпись** (УКЭП), которая *всегда реализуется с использованием цифровой подписи*, соответствующей требованиям признанного стандарта.

Таким образом, цифровая подпись является математической основой для усиленных видов электронной подписи.

Процесс цифровой подписи состоит из двух этапов:

1. **Подписание**: отправитель вычисляет хеш-функцию от сообщения $ H(m) $, а затем шифрует его с помощью своего закрытого ключа: $ \sigma = S_{sk}(H(m)) $.
2. **Проверка**: получатель вычисляет хеш от полученного сообщения, расшифровывает подпись с помощью открытого ключа отправителя и сравнивает результаты: $ H(m) \stackrel{?}{=} V_{pk}(\sigma) $.

Математические основы

RSA

Алгоритм RSA, предложенный в 1977 году Ривестом, Шамиром и Адлеманом, основан на сложности факторизации больших целых чисел. Для генерации ключей выбираются два больших простых числа $ p $ и $ q $, вычисляется $ n = pq $ и функция Эйлера $ \phi(n) = (p-1)(q-1) $. Затем выбирается открытый показатель $ e $, взаимно простой с $ \phi(n) $, и вычисляется закрытый ключ $ d $ как мультипликативная инверсия:
$$
ed \equiv 1 \pmod{\phi(n)}.
$$

Подпись сообщения $ m $ вычисляется как:
$$
\sigma = H(m)^d \bmod n,
$$
а проверка — как:
$$
H(m) \stackrel{?}{=} \sigma^e \bmod n.
$$

Безопасность RSA зависит от вычислительной сложности задачи факторизации $ n $.

DSA (Digital Signature Algorithm)

DSA был разработан NIST в 1991 году и стандартизирован в FIPS 186. Основан на проблеме дискретного логарифмирования в конечных полях. Алгоритм использует параметры:

- простое число $ p $ (длиной 1024–3072 бит),
- простое число $ q $, делящее $ p - 1 $ (160–256 бит),
- генератор $ g = h^{(p-1)/q} \bmod p $, где $ h \in [2, p - 2] $.

Закрытый ключ — случайное число $ x \in [1, q - 1] $, открытый ключ: $ y = g^x \bmod p $.

Подпись состоит из пары $ (r, s) $:
$$
r = (g^k \bmod p) \bmod q, \quad s = k^{-1}(H(m) + xr) \bmod q,
$$
где $ k $ — случайное число.

Проверка:
$$
w = s^{-1} \bmod q, \quad u_1 = H(m)w \bmod q, \quad u_2 = rw \bmod q, \\
v = (g^{u_1} y^{u_2} \bmod p) \bmod q, \quad v \stackrel{?}{=} r.
$$

ECDSA (Elliptic Curve Digital Signature Algorithm)

ECDSA — аналог DSA, но основанный на эллиптических кривых. Безопасность обеспечивается сложностью решения задачи дискретного логарифмирования на эллиптической кривой (ECDLP).

Используется эллиптическая кривая над конечным полем $ \mathbb{F}_p $, задаваемая уравнением:
$$
y^2 = x^3 + ax + b \quad (\text{при } 4a^3 + 27b^2 \ne 0).
$$

Базовая точка $ G $ порядка $ n $ определяет подгруппу. Закрытый ключ — целое число $ d \in [1, n - 1] $, открытый ключ — точка $ Q = dG $.

Подпись:

1. Выбирается случайное $ k \in [1, n - 1] $.
2. Вычисляется $ (x_1, y_1) = kG $.
3. $ r = x_1 \bmod n $, если $ r = 0 $ — повтор.
4. $ s = k^{-1}(H(m) + dr) \bmod n $, если $ s = 0 $ — повтор.

Проверка:

1. $ w = s^{-1} \bmod n $,
2. $ u_1 = H(m)w \bmod n $, $ u_2 = rw \bmod n $,
3. $ (x_1, y_1) = u_1G + u_2Q $,
4. Подпись верна, если $ r \equiv x_1 \bmod n $.

ECDSA обеспечивает ту же степень безопасности, что и RSA и DSA, но при значительно меньших размерах ключей (например, 256-битный ключ ECDSA эквивалентен 3072-битному RSA).

Применение цифровой подписи в реальных системах

TLS/SSL

В протоколах TLS/SSL цифровая подпись используется для аутентификации сервера (и, при необходимости, клиента). Сервер представляет сертификат, подписанный доверенным центром сертификации (CA). Подпись в сертификате (обычно RSA или ECDSA) подтверждает достоверность открытого ключа сервера. Также при установлении сессии сервер подписывает параметры обмена ключами (например, в рамках ECDHE), что предотвращает атаки типа «человек посередине».

Электронный документооборот

В России цифровая подпись лежит в основе УКЭП, используемой в системах межведомственного взаимодействия (например, на портале госуслуг), бухгалтерского обмена (СБИС, Контур), а также в судебной практике (Федеральный закон №63-ФЗ). В качестве алгоритмов подписи часто применяются отечественные стандарты ГОСТ Р 34.10–2012, основанные на эллиптических кривых над простым полем или полем характеристики 2.

Криптовалюты

В блокчейн-системах (например, Bitcoin) ECDSA применяется для подписи транзакций. Владелец кошелька использует свой закрытый ключ для подписи, подтверждая право на расходование средств. Сеть проверяет подпись с помощью открытого ключа, включённого в транзакцию. При этом квантовая устойчивость таких систем пока не обеспечена, что стимулирует исследования в области постквантовой криптографии.

Преимущества и ограничения

Преимущества:

- Обеспечение подлинности, целостности и неотказуемости.
- Прозрачная верификация любым обладателем открытого ключа.
- Возможность интеграции в распределённые системы.
- Поддержка стандартами (PKI, X.509, CMS).

Ограничения:

- Зависимость от безопасности закрытого ключа: если он скомпрометирован, подпись может быть подделана.
- Отсутствие встроенной защиты от повтора (replay attacks) — требует дополнительных механизмов (например, временных меток или nonce).
- Вычислительная сложность, особенно для RSA с длинными ключами.
- Уязвимость к квантовым атакам (алгоритм Шора позволяет эффективно решать задачи факторизации и дискретного логарифмирования).
- Необходимость доверенной инфраструктуры (PKI), что усложняет развёртывание.

Заключение

Цифровая подпись является фундаментальным инструментом обеспечения информационной безопасности в современных цифровых системах. Её математические основы — модульная арифметика, дискретное логарифмирование и теория эллиптических кривых — обеспечивают высокий уровень криптостойкости при корректной реализации. Несмотря на существующие ограничения, цифровая подпись остаётся неотъемлемой частью инфраструктуры безопасности в интернете, государственном управлении и финансовых технологиях. Перспективы развития связаны с переходом на постквантовые алгоритмы (например, на основе решёток или хеш-функций), стандартизация которых уже ведётся в рамках NIST и других организаций.

Список использованных источников

1. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.
   https://cacr.uwaterloo.ca/hac/

2. National Institute of Standards and Technology (NIST). (2013). *Digital Signature Standard (DSS)*. FIPS PUB 186-4.
   https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

3. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
   http://publication.pravo.gov.ru/Document/View/0001201104060032

4. ГОСТ Р 34.10–2012. *Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи*.
   https://docs.cntd.ru/document/1200099133

5. Barker, E., & Dang, Q. (2015). *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*. NIST Special Publication 800-56A Rev. 3.
   https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf

6. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2), 120–126.
   https://doi.org/10.1145/359340.359342

7. Johnson, D., Menezes, A., & Vanstone, S. (2001). The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security*, 1, 36–63.
   https://doi.org/10.1007/s102070100002