Федеральное государственное автономное образовательное учреждение высшего образования
Национальный исследовательский ядерный университет «МИФИ»

Кафедра «Криптология и кибербезопасность»

Основы блокчейн-технологий

Запечников Сергей Владимирович,
д.т.н., профессор

14 октября 2025 г.

Тема 2.
Криптография в блокчейн-технологиях

Криптология, криптография и криптоанализ

Криптология – наука о методах создания и анализа систем безопасной связи.

Криптография – раздел криптологии, изучающей создание (синтез) систем безопасной связи:

- ✓ **симметричная (криптография с секретным ключом, одноключевая, классическая);**
- ✓ **асимметричная (криптография с открытым ключом, двухключевая).**

Криптоанализ – раздел криптологии, изучающий методы нарушения безопасности связи (методы «взлома» систем криптографической защиты).

IACR – Международная ассоциация криптологических исследований [www.iacr.org]

Архив электронных публикаций IACR [eprint.iacr.org]

Основные аспекты информационной безопасности

Секретность (конфиденциальность)

– гарантии того, что содержание документа не станет известно лицам, которым документ не предназначен

Целостность

– гарантии того, что документ не был изменён в процессе движения от создателя к получателю

Подлинность

– гарантии того, что документ действительно был создан именно лицом, которое указано в качестве его автора

Целостность + **Подлинность** = **Аутентичность**

Неотказуемость

– гарантии невозможности отказаться от факта создания документа (ознакомления с документом)

Разграничение доступа

Анонимность

Др. аспекты безопасности

Классификация криптографических алгоритмов

♦ **Бесключевые:**

✓ **Хэш-функции – обеспечивают целостность данных.**

♦ **Симметричные (одноключевые, с секретным ключом):**

✓ **Симметричные шифры – обеспечивают конфиденциальность;**

✓ **Коды аутентификации сообщений – обеспечивают целостность и аутентичность.**

♦ **Асимметричные (двухключевые, с открытым ключом):**

✓ **Схема открытого распределения ключей – позволяет выработать общий ключ, пользуясь только открытыми каналами связи;**

✓ **Схемы открытого шифрования – обеспечивают конфиденциальность;**

✓ **Цифровая подпись – обеспечивает подлинность (аутентичность) данных.**

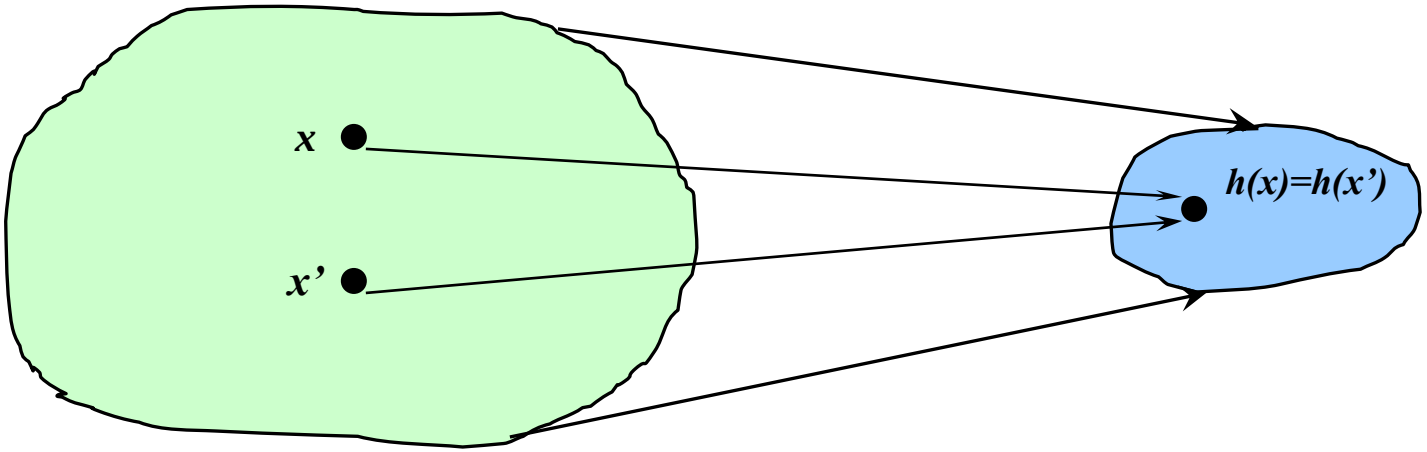
♦ **Любая достаточно сложная криптосистема включает в себя как симметричные, так и асимметричные алгоритмы.**

♦ **Асимметричные алгоритмы преобладают – симметричные используются, когда не удовлетворяет скорость.**

Криптографические хэш-функции

Хэш-функция (функция хэширования) – функция вида $y = h(x)$, обладающая специальными свойствами:

- ✓ **функция преобразует вход x любой длины в выход фиксированной длины — хэш-код (message digest), который согласован со входом на цифровую подпись;**
- ✓ **функция является однонаправленной, т.е. найти $y = h(x)$ — легко (это можно сделать за полиномиальное время), а $h^{-1}(y)$ — вычислительно невозможно;**
- ✓ **вычислительно невозможно найти такую пару чисел x и x', таких что $x \neq x'$, но $h(x) = h(x')$ — если такая ситуация случается, то она называется коллизией.**



Стандарты по криптографическим хэш-функциям

- **SHA – Secure Hash Algorithm:**

✓ Семейство хэш-функций с разными длинами хэш-кодов: 160, 256, 384, 512 бит;

✓ Длина хэш-кода (message digest) – 160, 224, 256 или 512 битов.

- **ГОСТ 34.11-2018.** Информационная технология. Криптографическая защита информации. Функция хеширования:

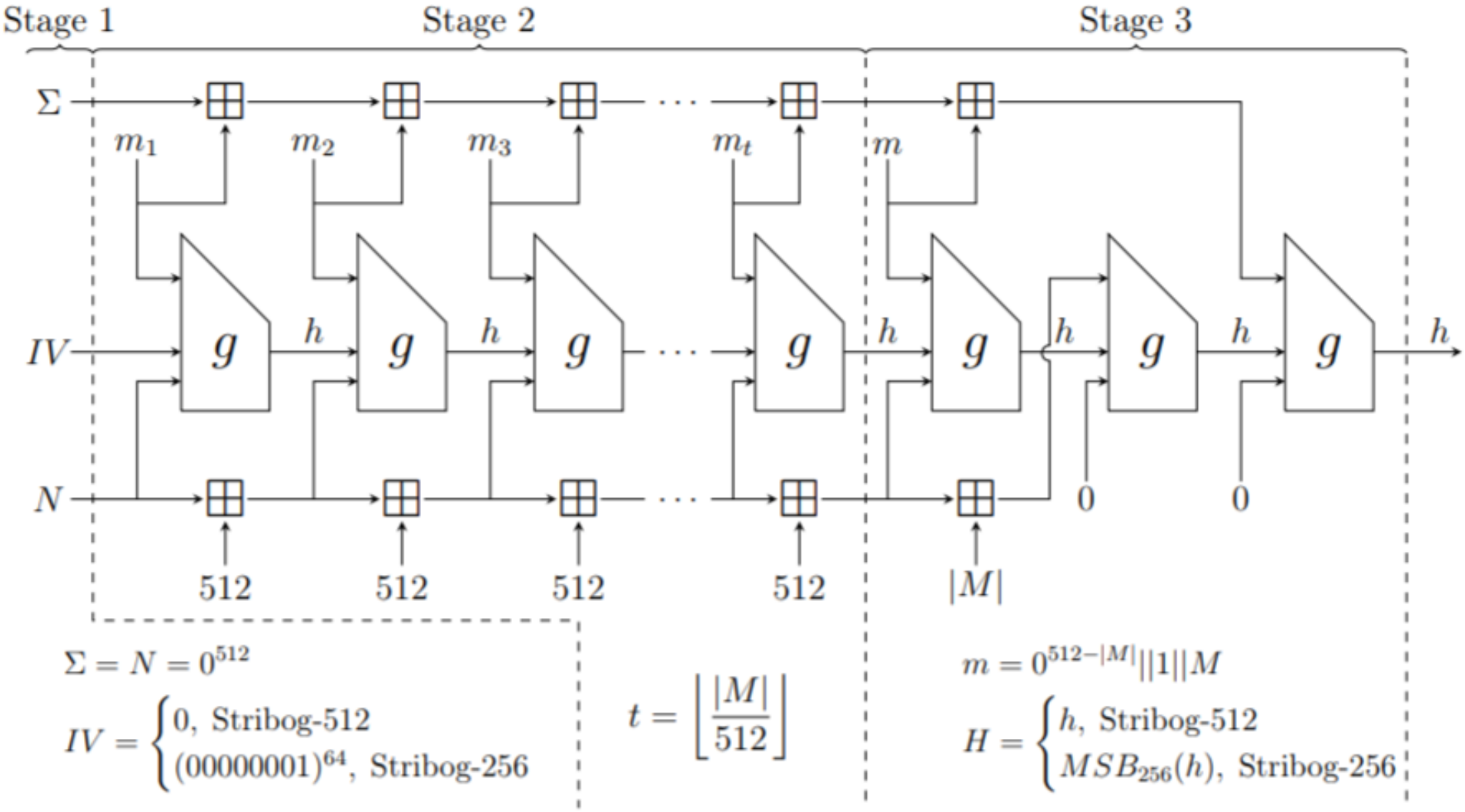
✓ Две функции хэширования «Стрибог» с длинами хэш-кодов 256 и 512 бит.

Другие криптографические хэш-функции: MD4, MD5, RIPEMD-160, MDC-2, MDC-4, Whirlpool, …

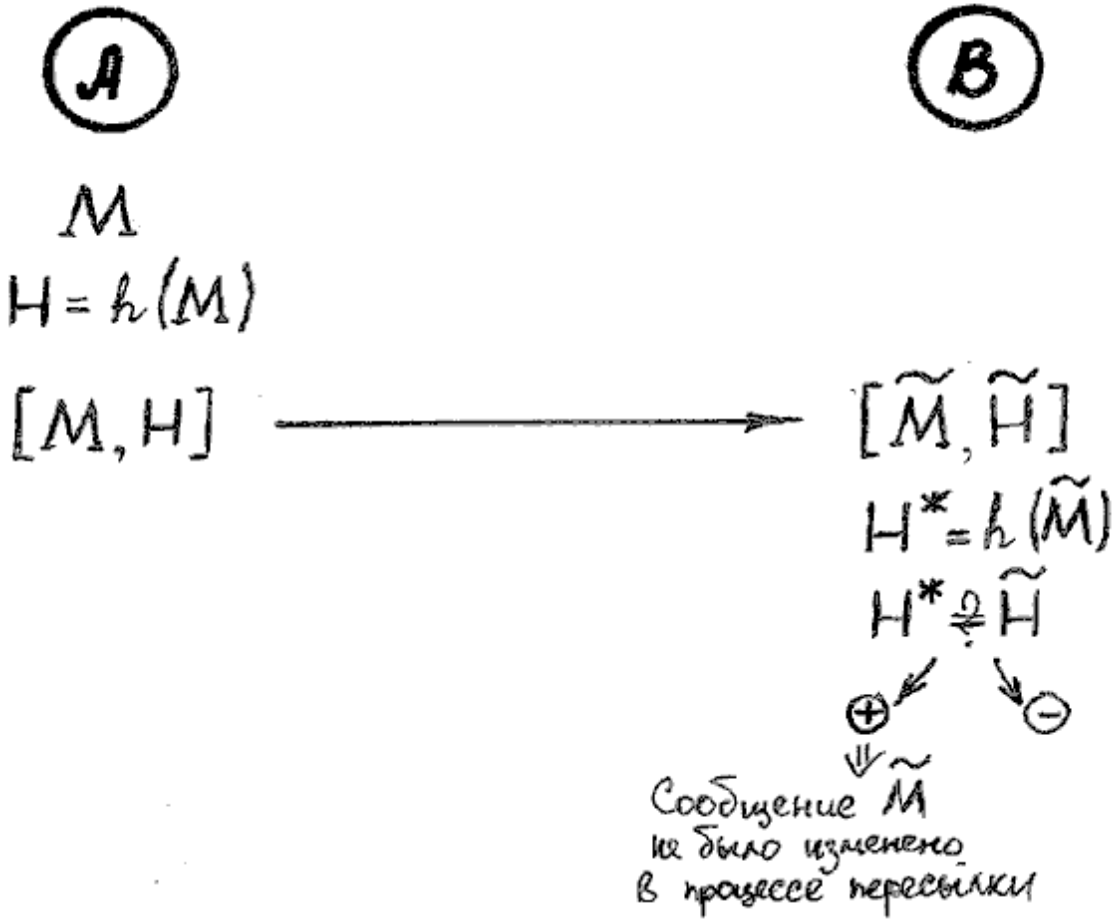
Алгоритм «Стрибог»

1. Обработка сообщения происходит итерационно, блоками фиксированной длины:

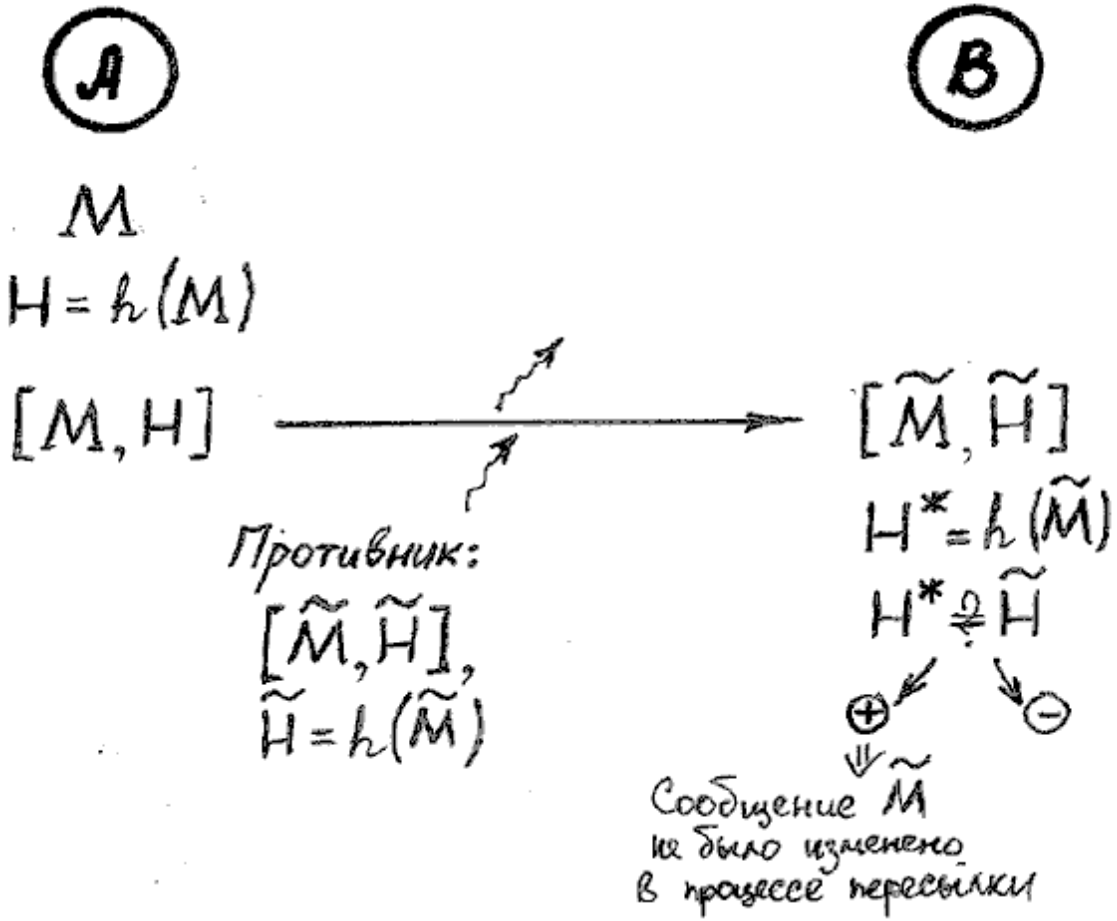
2. На каждом шаге применяется так называемая шаговая функция хэширования:



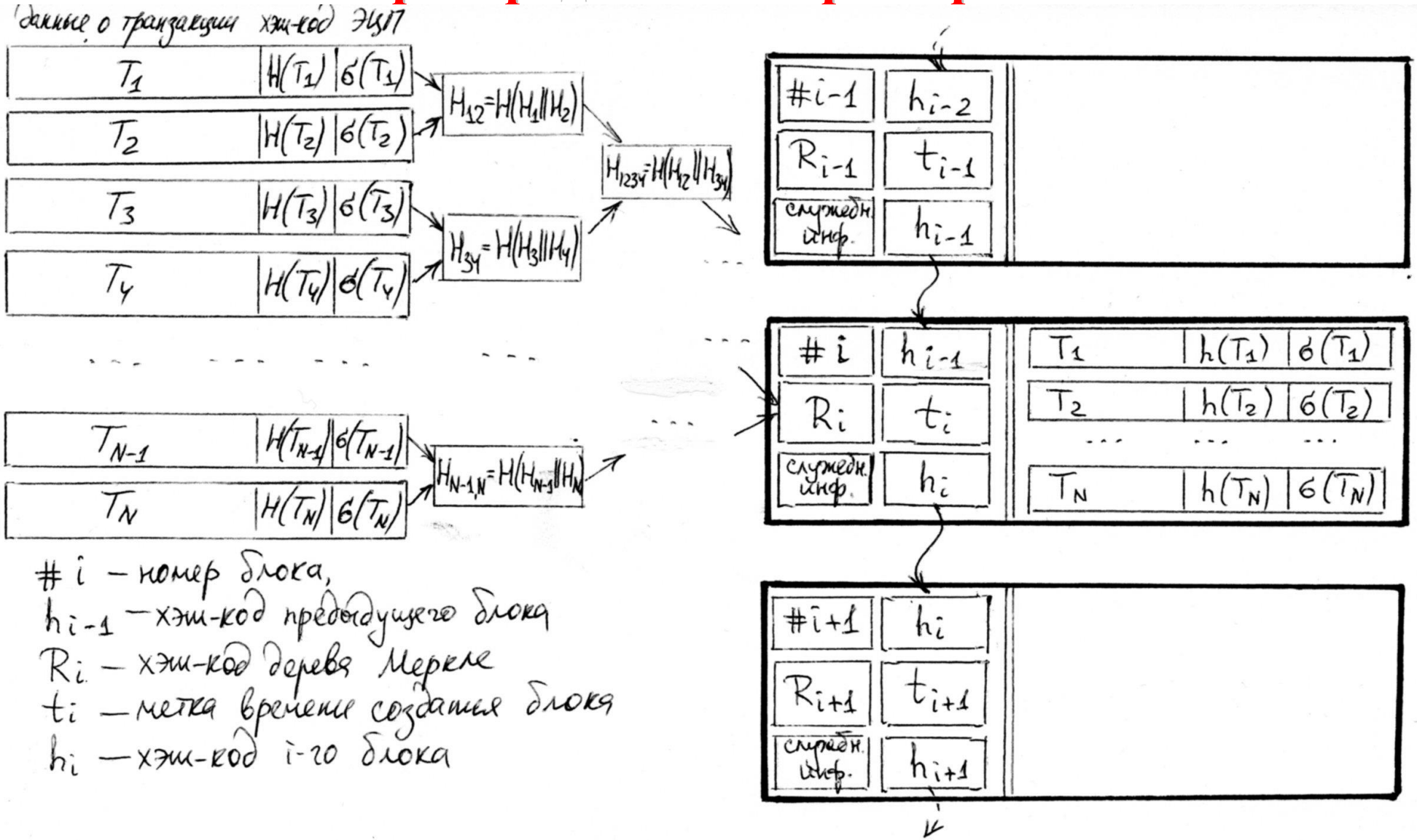
Применение хэш-функции для проверки целостности документа (1/2)



Применение хэш-функции для проверки целостности документа (2/2)

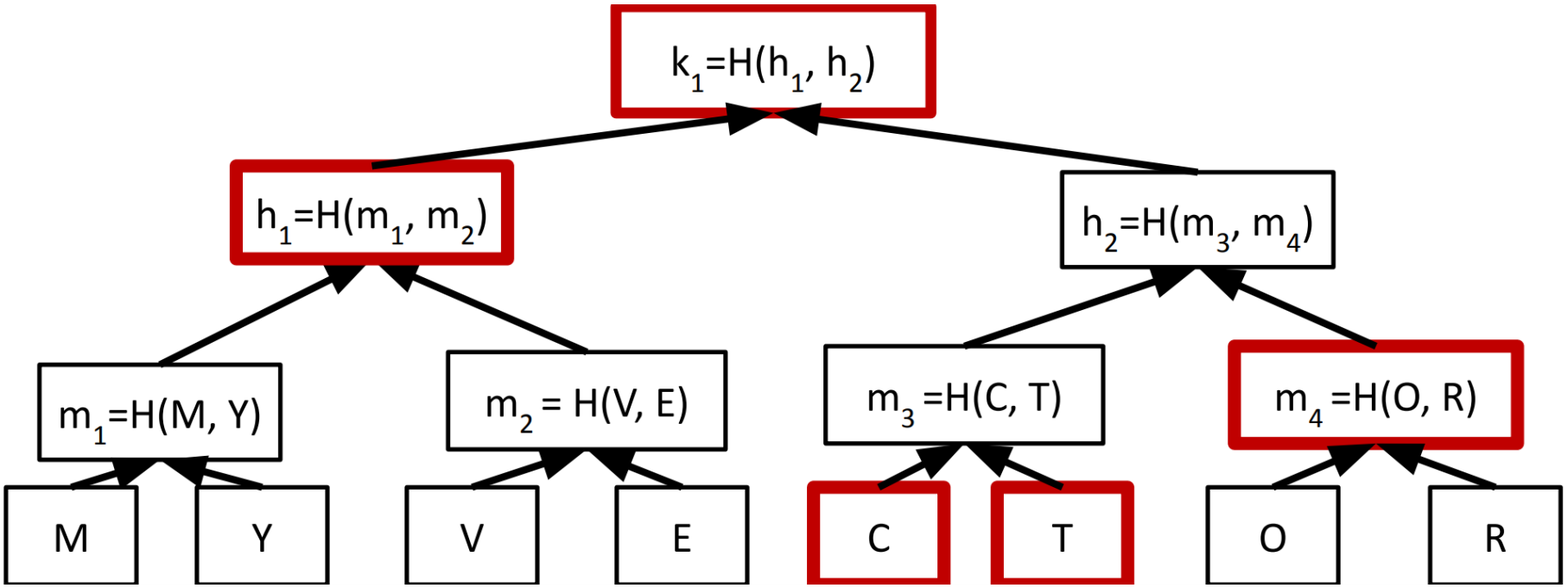


Применение хэш-функций для связывания блоков распределенного реестра



#i – номер блока,
h_{i-1} – хэш-код предыдущего блока
R_i – хэш-код дерева Меркле
t_i – метка времени создания блока
h_i – хэш-код i-го блока

Дерево Меркле



- Commitment to vector is root hash.
- To open an entry of the committed vector (leaf of the tree):
  - Send sibling hashes of all nodes on root-to-leaf path.
  - V checks these are consistent with the root hash.
  - "Opening proof" size is O(log n) hash values.
- Binding: once the root hash is sent, the committer is bound to a fixed vector.
  - Opening any leaf to two different values requires finding a hash collision (assumed to be intractable).

Однонаправленные функции с секретом

Обычную однонаправленную функцию невозможно использовать для целей шифрования, т.к. преобразование шифра должно быть обратимо.

Определение: **Однонаправленная функция с секретом (с потайной дверью) - функция вида $y = f_z(x)$, которая:**

- **если z — *известно*, является обычной функцией, легко вычислимой в обе стороны, т.е.:**
  - **(1) вычислить $y = f_z(x)$ — легко;**
  - **(2) вычислить $x = f_z^{-1}(y)$ — легко;**
- **если z — *неизвестно*, является однонаправленной функцией, т.е.:**
  - **(3) вычислить $y = f_{(z)}(x)$ – легко;**
  - **(4) по заданному y получить $f_{(z)}^{-1}(y)$ – вычислительно невозможно.**

Схема электронной цифровой подписи (1/4)

(Подписывающий) **(Проверяющий)**

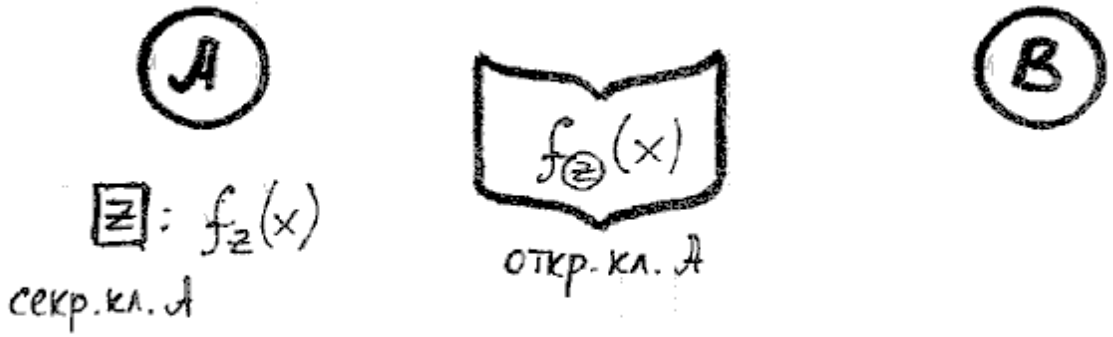


Схема электронной цифровой подписи (2/4)

(Подписывающий) **(Проверяющий)**

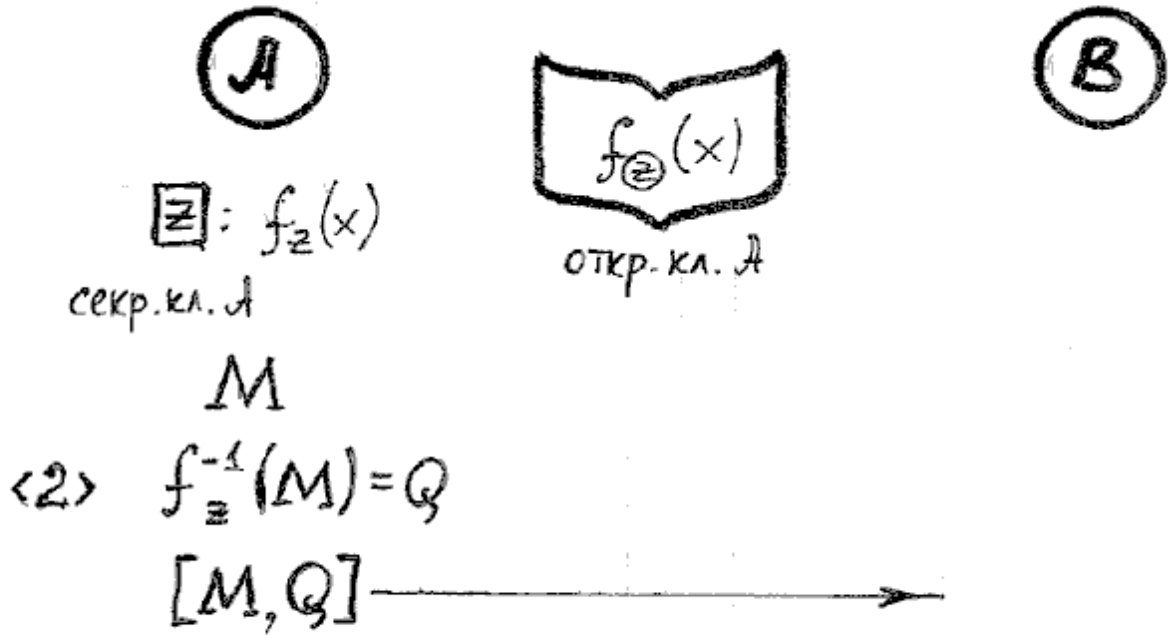


Схема электронной цифровой подписи (3/4)

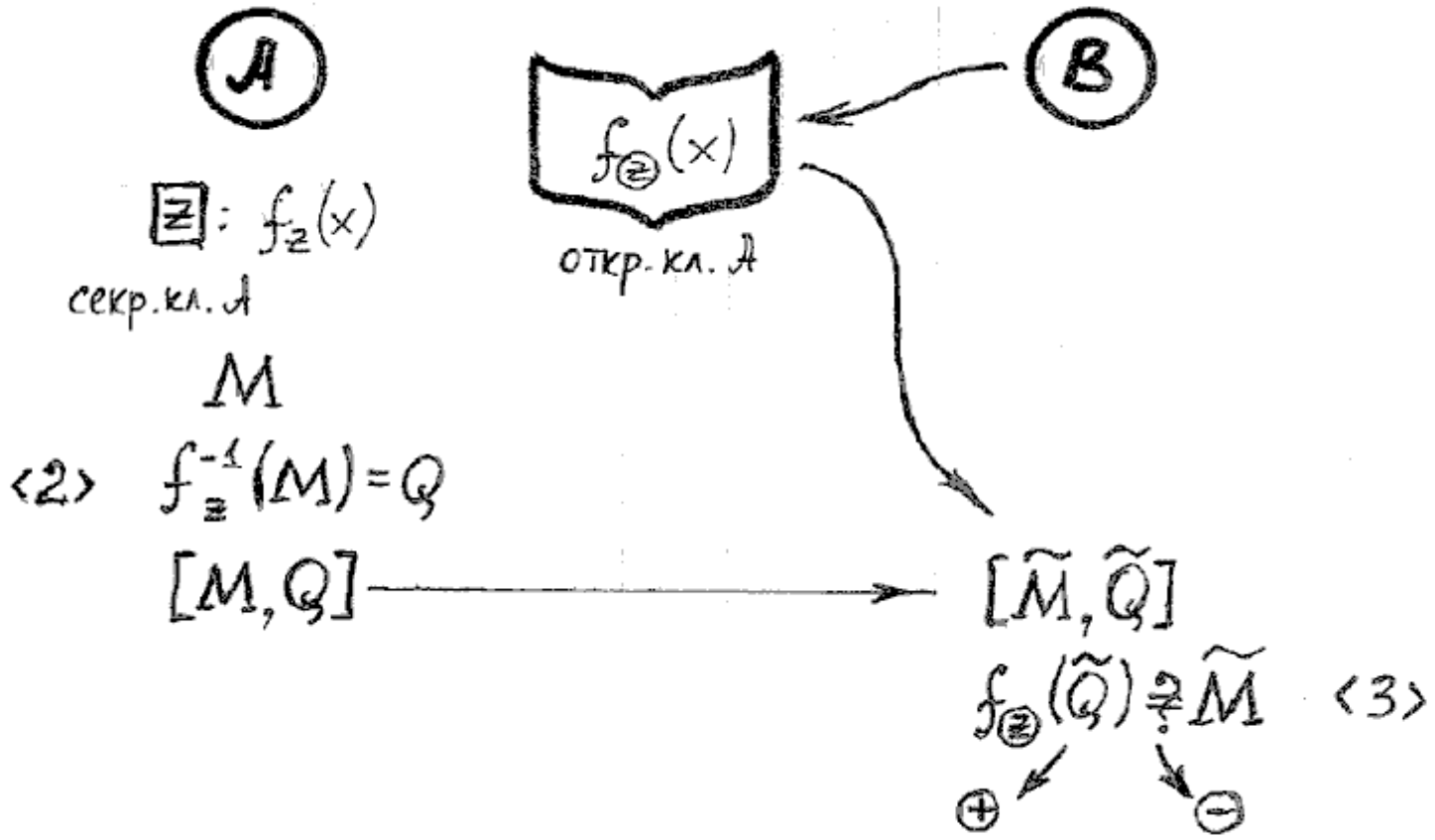


Схема электронной цифровой подписи (4/4)

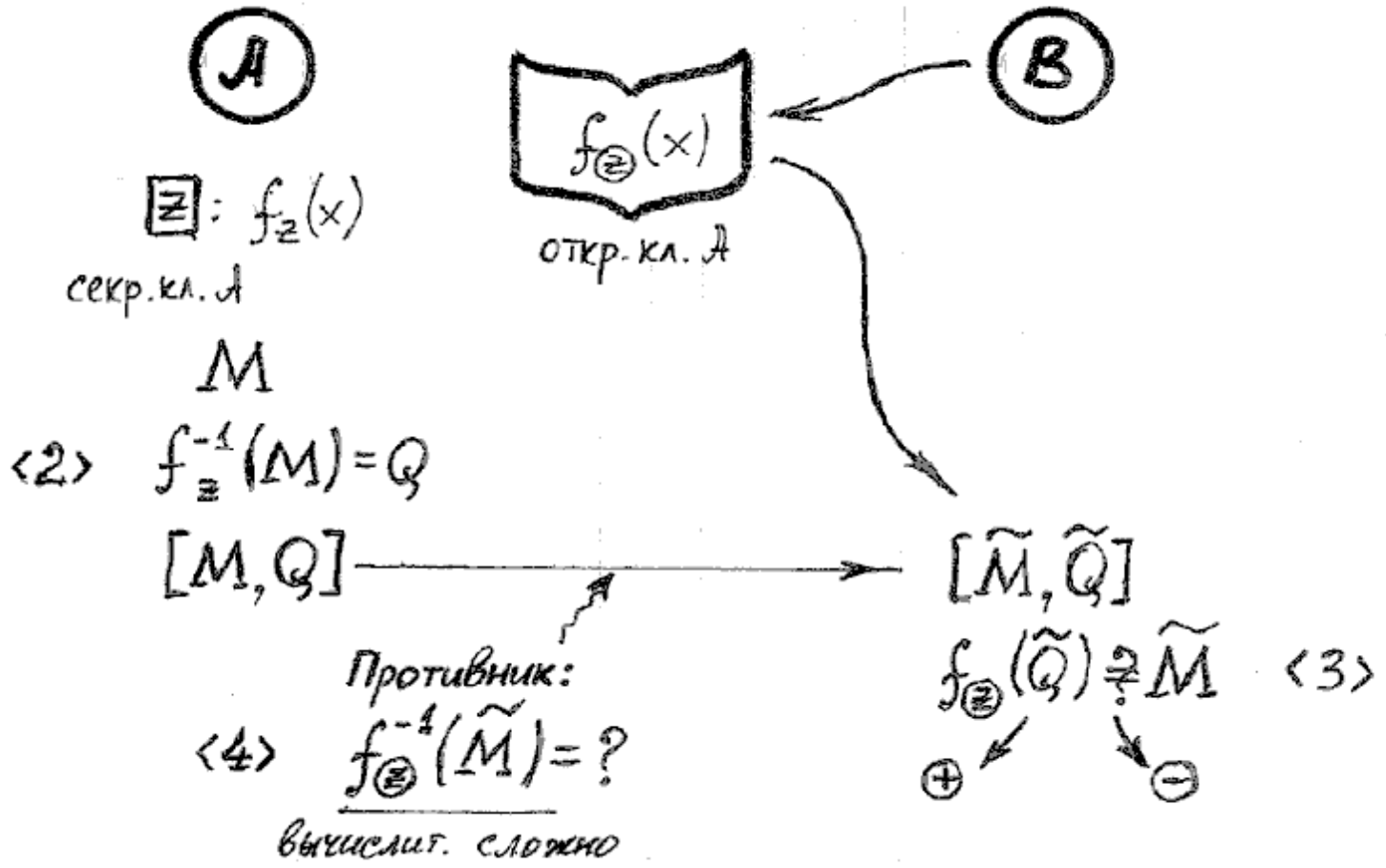
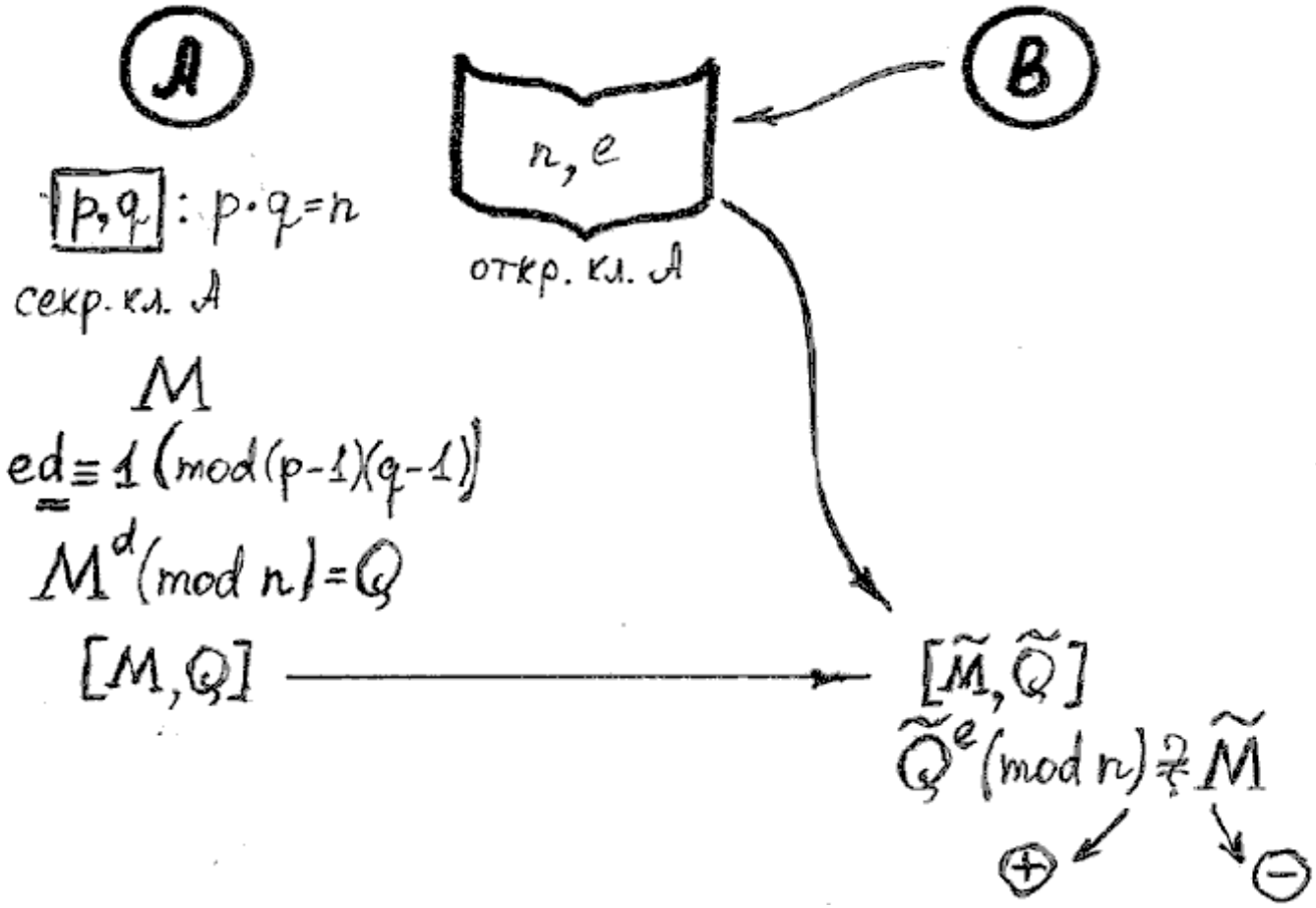


Схема электронной цифровой подписи RSA

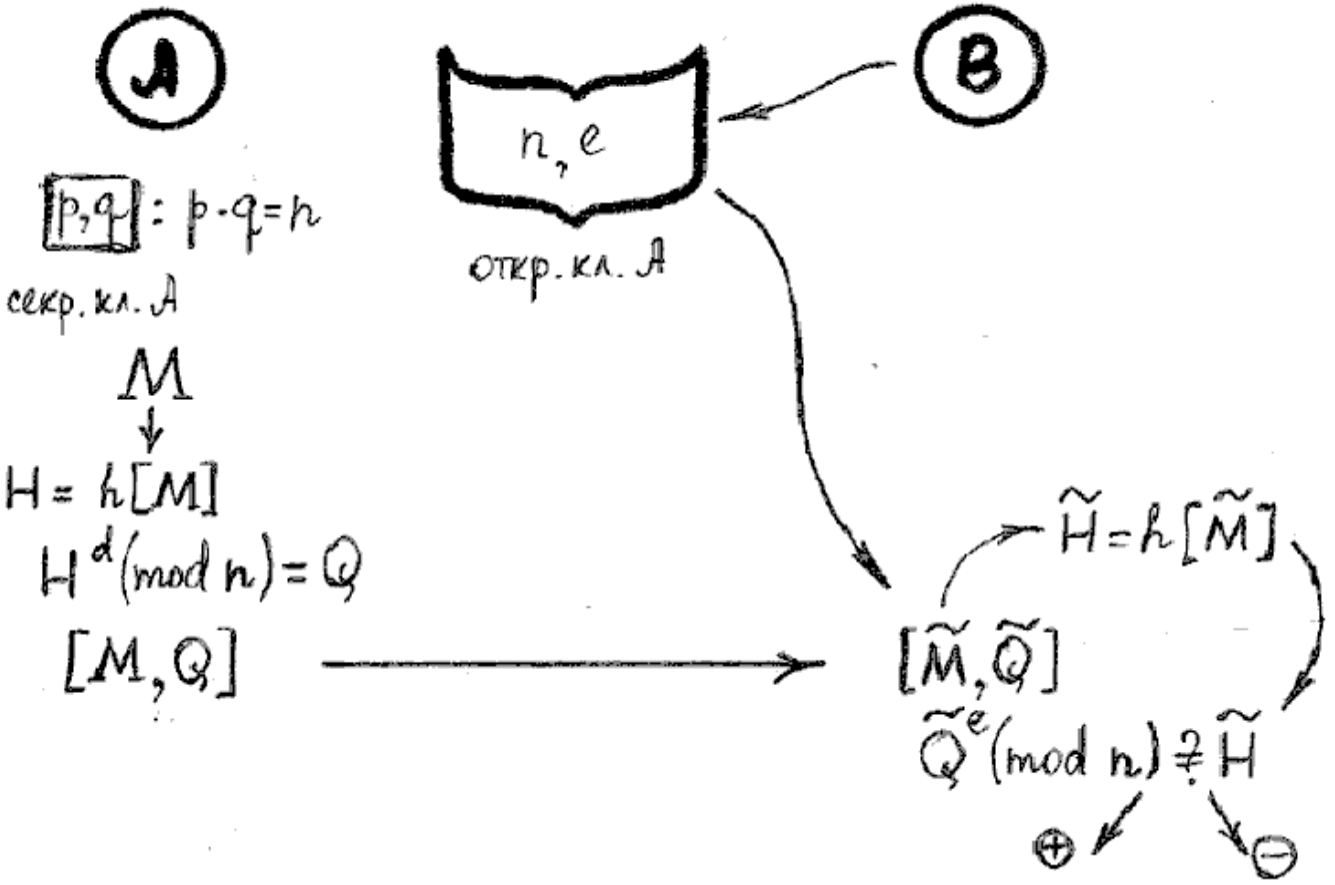
(Подписывающий) **(Проверяющий)**



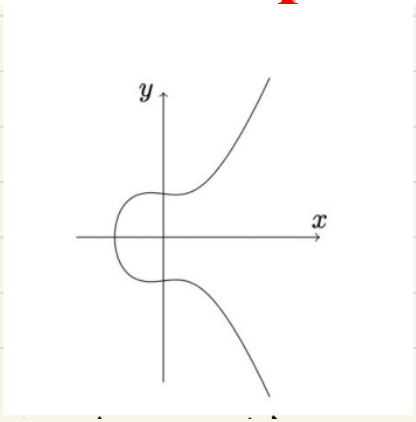
Стандарты электронной цифровой подписи

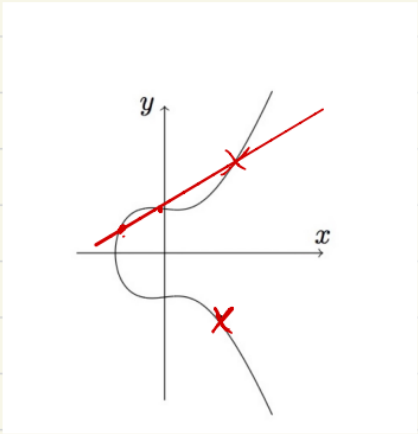
- **EC-DSA – Digital Signature Standard:**
  - ✓ на базе математического аппарата эллиптических кривых;
  - ✓ длина подписываемого сообщения зависит от применяемого алгоритма подписи, минимальная длина |M| = 160 битов;
  - ✓ длина подписи зависит от применяемого алгоритма, минимальная длина |Q| = 320 битов.
- **ГОСТ 34.10-2018.** Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи:
  - ✓ на базе математического аппарата эллиптических кривых;
  - ✓ |Q| = 512 или 1024 бит.

Совместное применение электронной цифровой подписи и хэш-функции (на примере RSA)



Эллиптические кривые (над полем рациональных чисел)





This is called an Elliptic Curve and generally has the form

$$y^2 = x^3 + Ax + B \quad \text{s.t. } 4a^3+27b^2 \neq 0$$

And these are the starting point for the groups we use in crypto today.

1) if (x,y) is on curve, so is $(x,-y)$

2) Chord method: given 2 points on curve, drawing a line through them gives a third point on the curve

3) tangent method: given 1 point on curve, its tangent line crosses 1 other point on the curve.

So we can get new points on curve by drawing lines through known points and by flipping?

Do the points on the curve form a group with the "draw line + flip" operation?

Определение эллиптической кривой над конечным полем (в форме Вейерштрасса)

Definition 15.1. *Let $p > 3$ be a prime. An **elliptic curve** E defined over $\mathbb{F}_p$ is an equation*

$$y^2 = x^3 + ax + b, \tag{15.3}$$

where $a, b \in \mathbb{F}_p$ satisfy $4a^3 + 27b^2 \neq 0$. We write $E/\mathbb{F}_p$ to denote the fact that E is defined over $\mathbb{F}_p$.

The condition $4a^3 + 27b^2 \neq 0$ ensures that the equation $x^3 + ax + b = 0$ does not have a double root. This is needed to avoid certain degeneracies.

The set of points on the curve. Let $E/\mathbb{F}_p$ be an elliptic curve, and let $e \geq 1$. We say that a point (x_1, y_1), where $x_1, y_1 \in \mathbb{F}_{p^e}$, is a point **on the curve** E if (x_1, y_1) satisfies the curve equation (15.3). When $e = 1$ the point (x_1, y_1) is defined over the base field $\mathbb{F}_p$. When $e > 1$ the point is defined over an extension of $\mathbb{F}_p$.

The curve includes an additional "special" point $\mathcal{O}$ called **the point at infinity**. Its purpose will become clear in a minute. We write $E(\mathbb{F}_{p^e})$ to denote the set of all points on the curve E that are defined over $\mathbb{F}_{p^e}$, including the point $\mathcal{O}$.

For example, consider the curve $E: \ y^2 = x^3 + 1$ defined over $\mathbb{F}_{11}$. Then

$$E(\mathbb{F}_{11}) = \Big\{\mathcal{O}, \ \ (-1, 0), \ \ (0, \pm 1), \ \ (2, \pm 3), \ \ (5, \pm 4), \ \ (7, \pm 5), \ \ (9, \pm 2)\Big\} \tag{15.4}$$

This curve has 12 points in $\mathbb{F}_{11}$ and we write $|E(\mathbb{F}_{11})| = 12$.

Схема цифровой подписи ECDSA (1/3)

Алгоритм генерации ключей:

Suppose Alice wants to send a signed message to Bob. Initially, they must agree on the curve parameters (CURVE, G, n). In addition to the field and equation of the curve, we need G, a base point of prime order on the curve; n is the multiplicative order of the point G.

Parameter	
CURVE	the elliptic curve field and equation used
G	elliptic curve base point, a point on the curve that generates a subgroup of large prime order n
n	integer order of *G*, means that $n \times G = O$, where O is the identity element.
d_A	the private key (randomly selected)
Q_A	the public key $d_A \times G$ (calculated by elliptic curve)
m	the message to send

Alice creates a key pair, consisting of a private key integer d_A, randomly selected in the interval $[1, n-1]$; and a public key curve point $Q_A = d_A \times G$. We use $\times$ to denote elliptic curve point multiplication by a scalar.

Схема цифровой подписи ECDSA (2/3)

Алгоритм генерации подписи:

For Alice to sign a message m, she follows these steps:

1. Calculate $e = \mathrm{HASH}(m)$. (Here HASH is a cryptographic hash function, such as SHA-2, with the output converted to an integer.)
2. Let z be the L_n leftmost bits of e, where L_n is the bit length of the group order n. (Note that z can be *greater* than n but not *longer*.[2])
3. Select a **cryptographically secure random** integer k from $[1, n-1]$.
4. Calculate the curve point $(x_1, y_1) = k \times G$.
5. Calculate $r = x_1 \mod n$. If $r = 0$, go back to step 3.
6. Calculate $s = k^{-1}(z + rd_A) \mod n$. If $s = 0$, go back to step 3.
7. The signature is the pair (r, s). (And $(r, -s \mod n)$ is also a valid signature.)

Схема цифровой подписи ECDSA (3/3)

Алгоритм проверки подписи:

For Bob to authenticate Alice's signature r, s on a message m, he must have a copy of her public-key curve point Q_A. Bob can verify Q_A is a valid curve point as follows:

1. Check that Q_A is not equal to the identity element O, and its coordinates are otherwise valid.
2. Check that Q_A lies on the curve.
3. Check that $n \times Q_A = O$.

After that, Bob follows these steps:

1. Verify that r and s are integers in $[1, n-1]$. If not, the signature is invalid.
2. Calculate $e = \mathrm{HASH}(m)$, where HASH is the same function used in the signature generation.
3. Let z be the L_n leftmost bits of e.
4. Calculate $u_1 = zs^{-1} \mod n$ and $u_2 = rs^{-1} \mod n$.
5. Calculate the curve point $(x_1, y_1) = u_1 \times G + u_2 \times Q_A$. If $(x_1, y_1) = O$ then the signature is invalid.
6. The signature is valid if $r \equiv x_1 \pmod n$, invalid otherwise.

Инфраструктура криптосистем

До сих пор мы предполагали, что криптографические ключи даются нам готовыми. На практике это не так.

Правило Керкхоффса: все долговременные элементы криптосистем считаются известными противнику. Безопасность криптосистем обеспечивается безопасностью используемых в ней ключей.

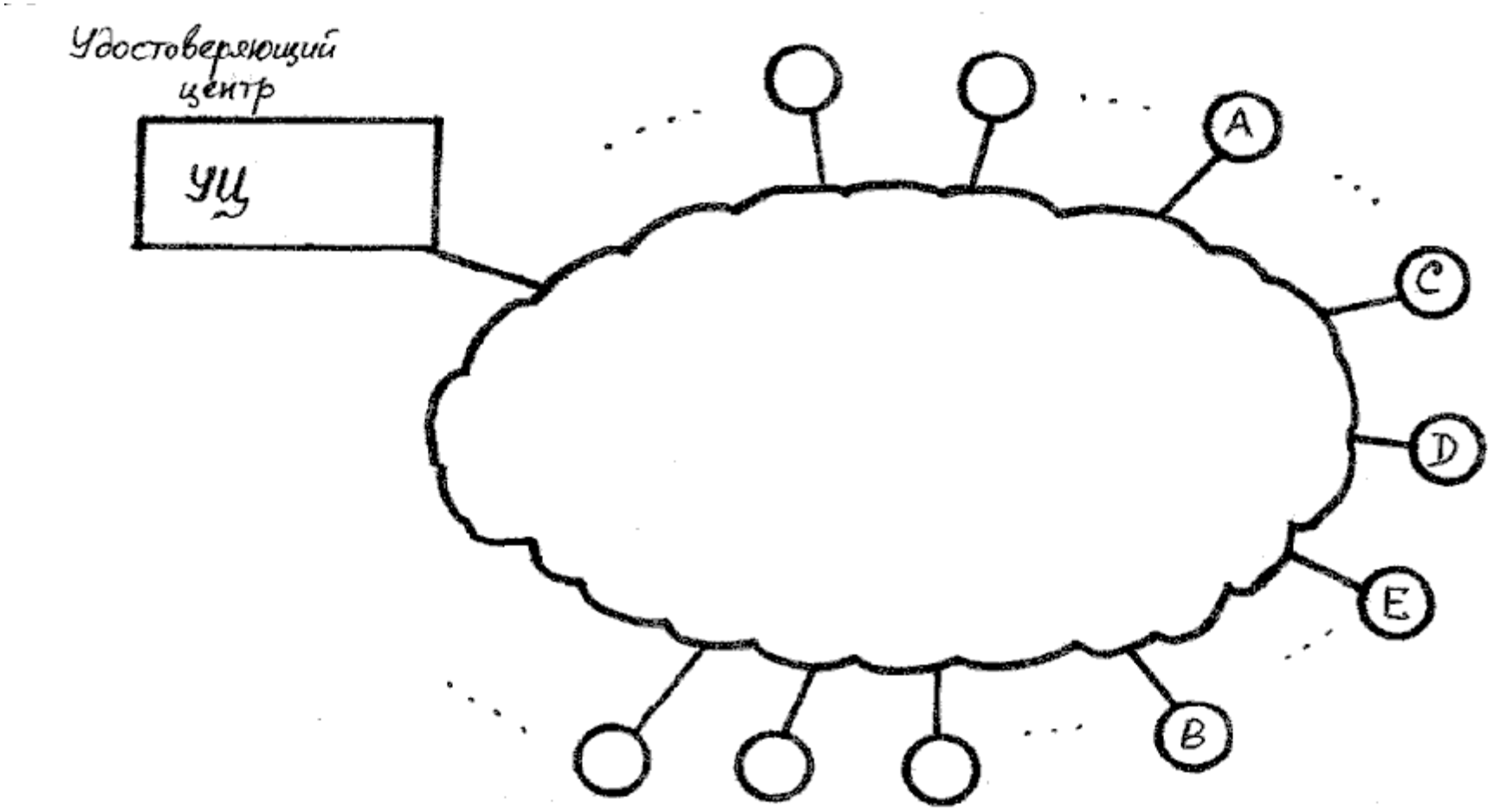
Инфраструктура – составные части общего устройства системы, носящие вспомогательный, подчинённый характер и обеспечивающие нормальную деятельность системы в целом.

Инфраструктура открытых ключей (ИОК) (англ. PKI – Public Key Infrastructure) – универсальная модель организованной поддержки криптографических средств защиты информации в крупномасштабных компьютерных системах в соответствии с принятыми в них политиками безопасности, которая реализует управление криптографическими ключами на всех этапах их жизненного цикла, обеспечивая взаимодействие всех средств защиты.

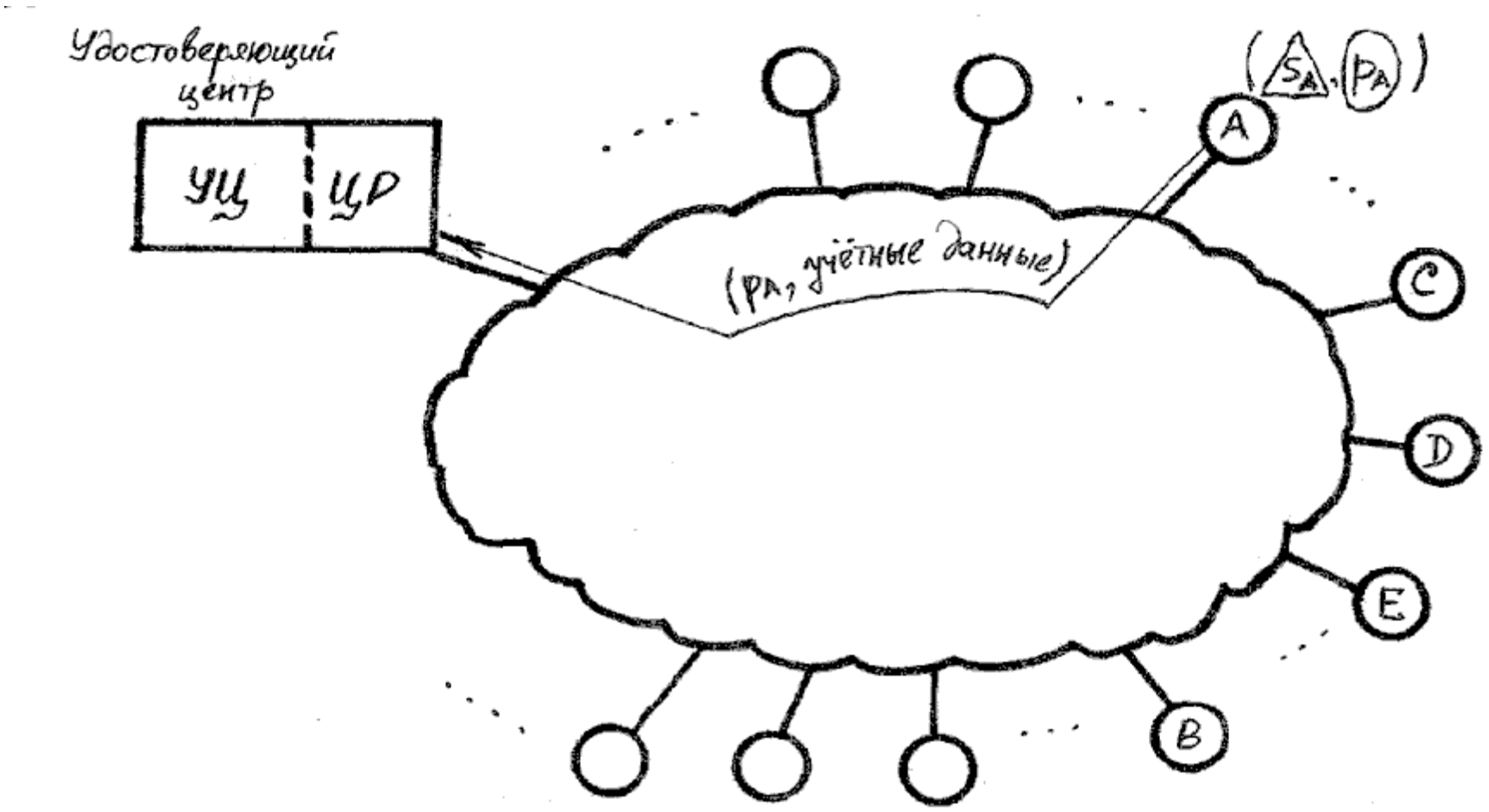
Разрабатываются рядом международных организаций:

- **PKIX (Public Key Infrastructure for X.509)** – модель IETF на базе X.509 – рекомендации Международного телекоммуникационного союза ITU;
- **SPKI (Simple Public Key Infrastructure)** – модель IETF.

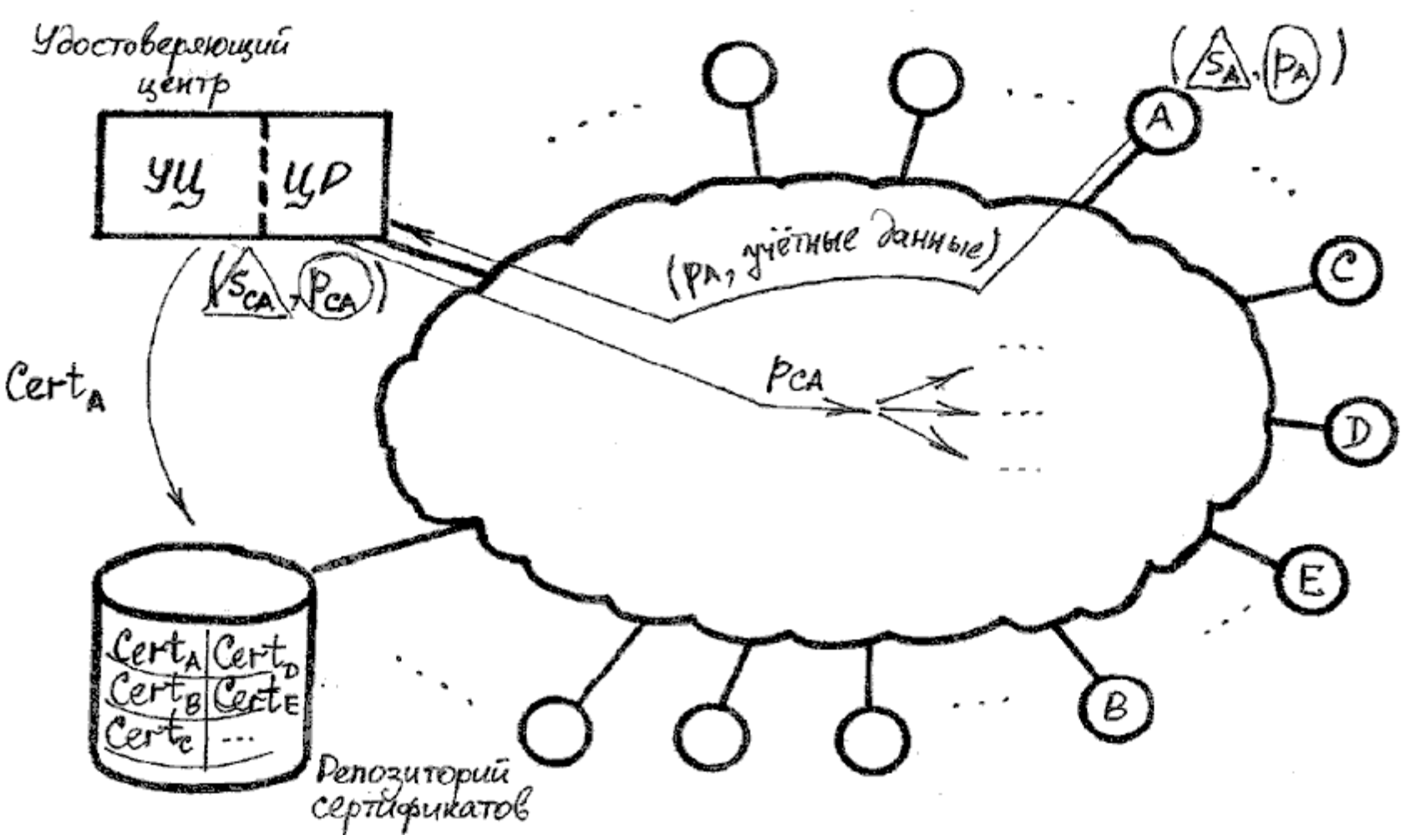
Обобщенная модель ИОК (1/5)



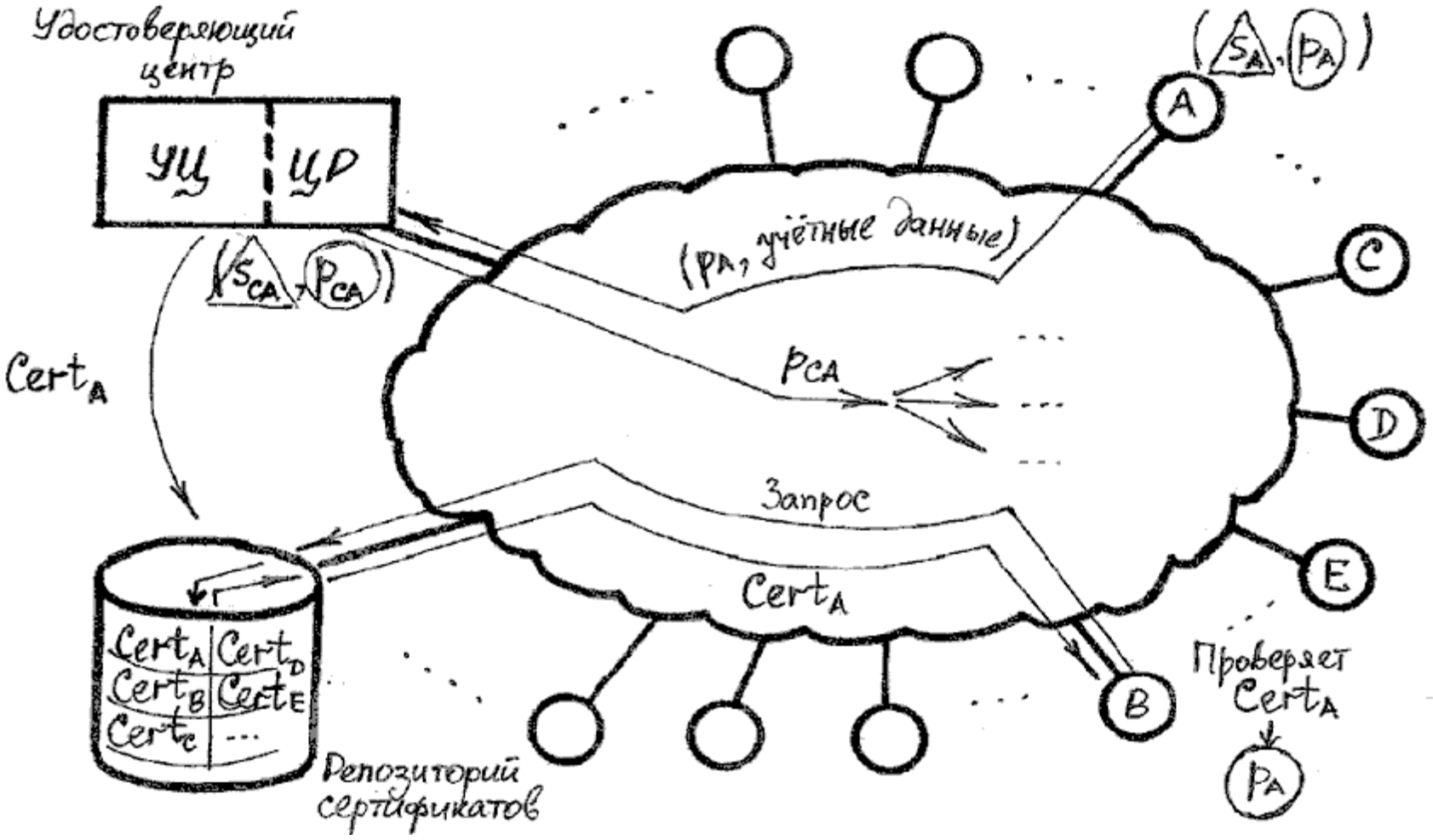
Обобщенная модель ИОК (2/5)



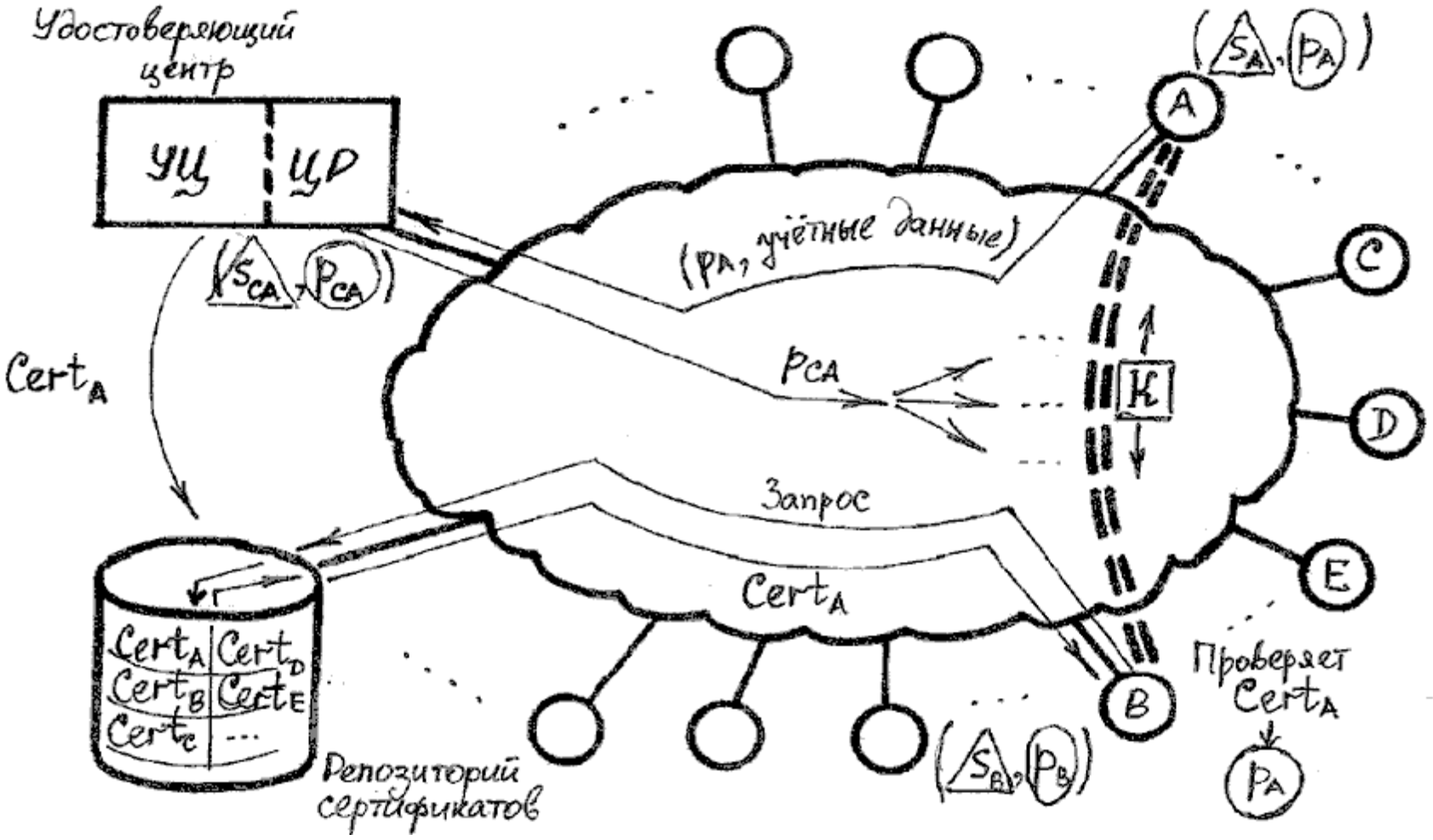
Обобщенная модель ИОК (3/5)



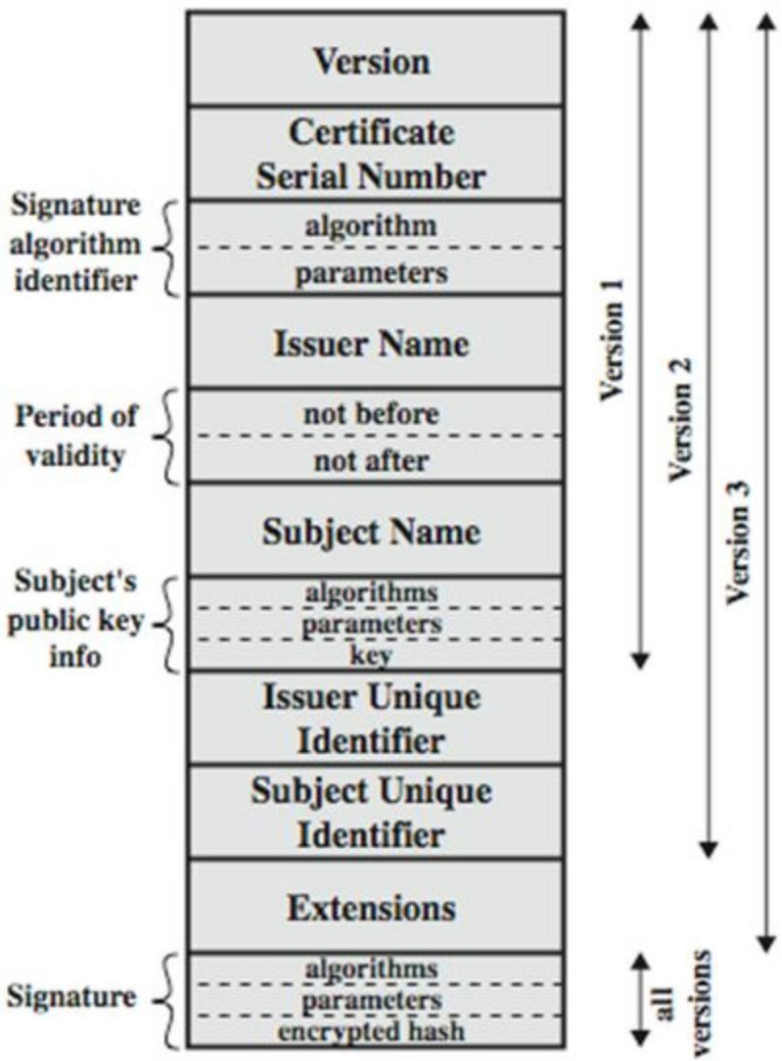
Обобщенная модель ИОК (4/5)



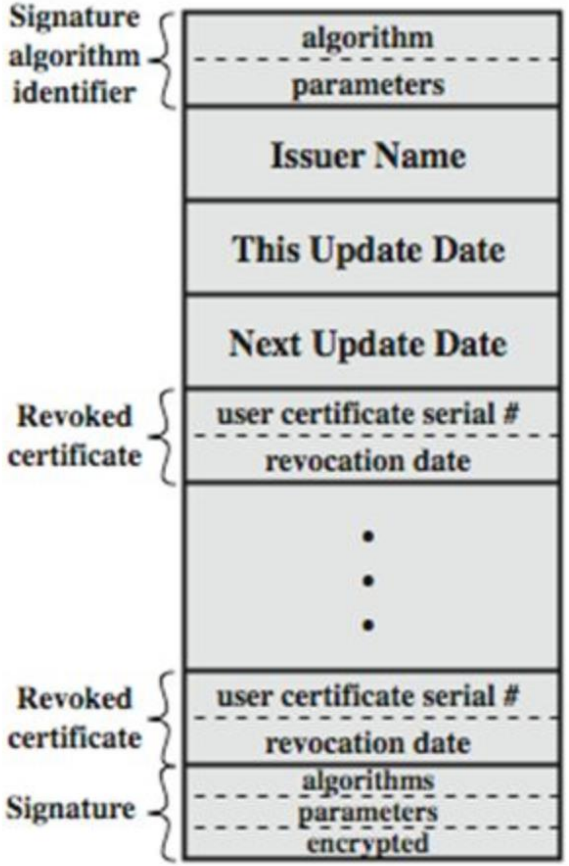
Обобщенная модель ИОК (5/5)



Формат сертификата открытых ключей и списка аннулированных сертификатов (по ITU X.509)



(a) X.509 Certificate



(b) Certificate Revocation List

Спасибо за внимание!

Вопросы?