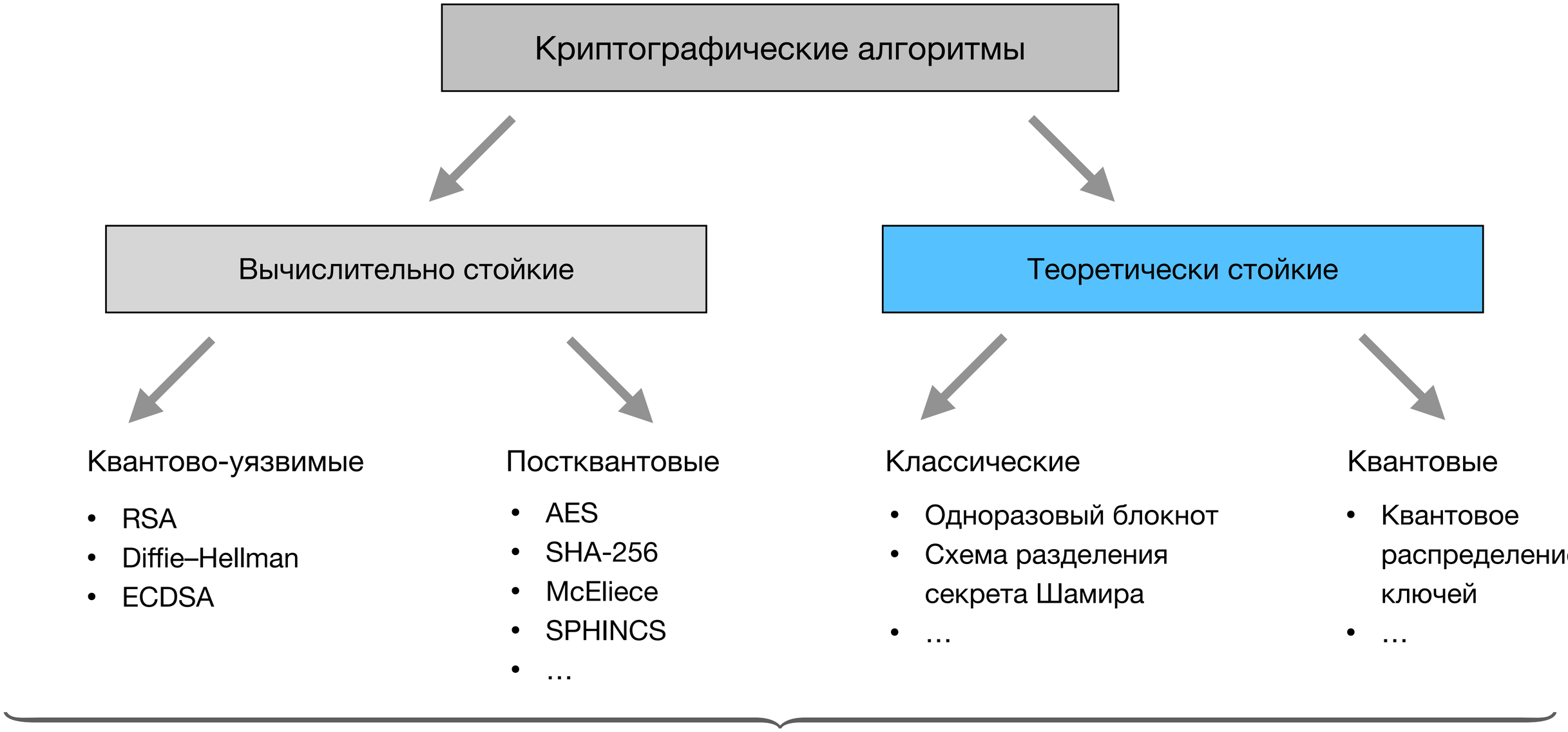
# Теоретически стойкие алгоритмы на основе квантового распределения ключей

**Киктенко Евгений Олегович**

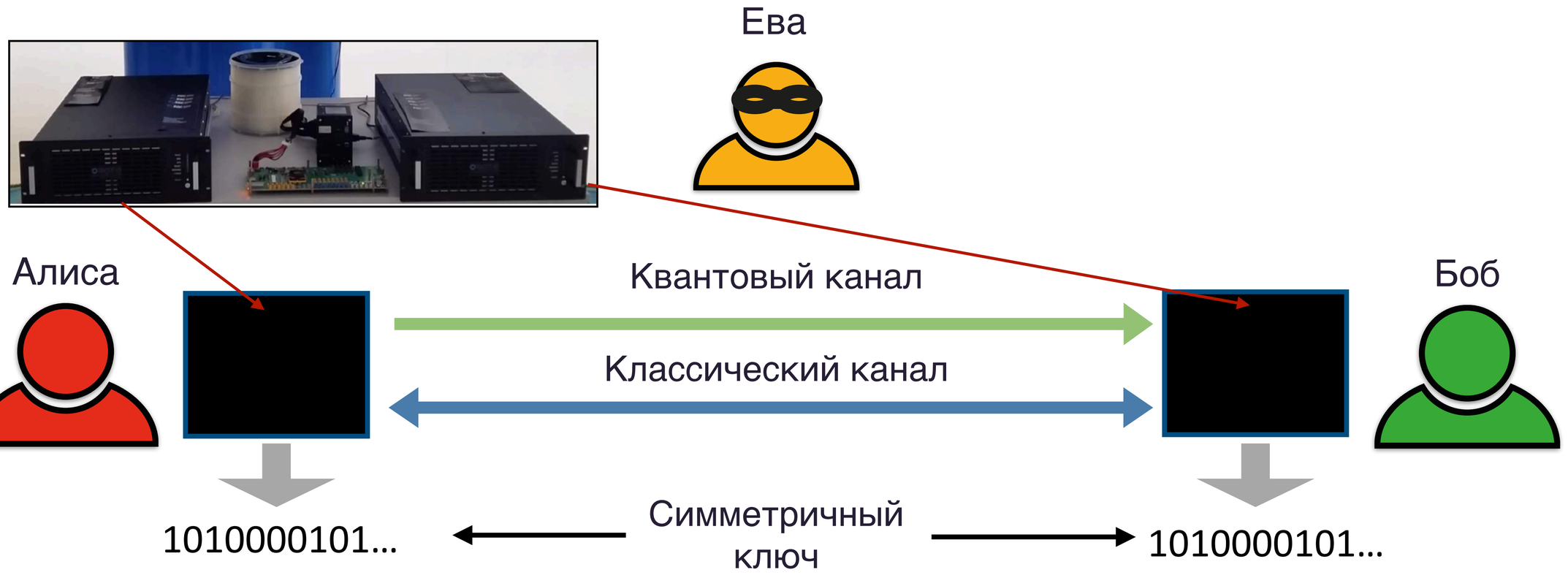
Российский квантовый центр
Математический институт им. В.А. Стеклова РАН

Научный совет РАН «Квантовые технологии»
3 марта 2022 г.

# Подходы к обоснованию защищенности криптографических алгоритмов



# Квантовое распределение ключа (КРК)

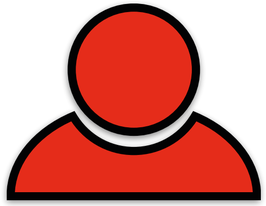



$$\frac{1}{2}\|\rho_{\mathrm{ABE}} - \rho_{\mathrm{AB}}^{\mathrm{perfect}} \otimes \rho_{\mathrm{E}}\|_1 < \varepsilon$$

А.С. Трушечкин "Об операционном смысле и практических аспектах использования параметра стойкости в квантовом распределении ключей" // Квантовая электроника, т. 50, № 5, с. 426–439 (2020)

# Теоретически стойкое симметричное шифрование: одноразовый блокнот

Алиса



$K = (k_0, k_1, k_2, \ldots)$

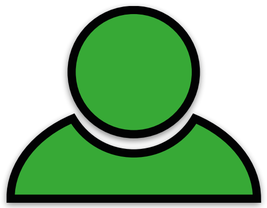
$M = (m_0, m_1, m_2, \ldots)$

$C := M \oplus K \equiv (m_0 \oplus k_0, m_1 \oplus k_1, \ldots)$

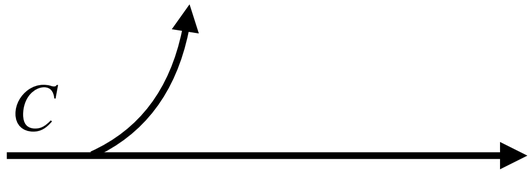
Ева

$\Pr[M \mid C] = \Pr[M]$

Боб



$K = (k_0, k_1, k_2, \ldots)$



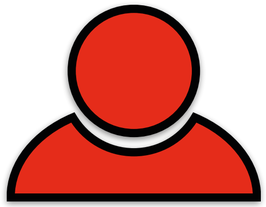

$C \oplus K = M \oplus K \oplus K = M$

Одноразовый блокнот должен быть одноразовым!

$$C_1 = M_1 \oplus K, C_2 = M_2 \oplus K \rightarrow C_1 \oplus C_2 = M_1 \oplus M_2$$

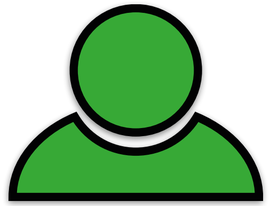
# Защита от подделки сообщения во время передачи: аутентификация с помощью иммитовставки (message authentication codes)

Алиса



Ева

Боб



$k* \in \mathcal{K}$ — симметричный ключ

$\mathcal{F} = \{f_k : \mathcal{M} \to \mathcal{T}\}_{k \in \mathcal{K}}$ — семейство функций

$m \in \mathcal{M}$ — сообщение

$t := f_{k*}(m)$ — иммитовставка («тэг»)

$(m, t)$

$(m', t')$

$k* \in \mathcal{K}$

$\mathcal{F} = \{f_k : \mathcal{M} \to \mathcal{T}\}_{k \in \mathcal{K}}$

**если** $f_{k*}(m') = t'$:
принять сообщение
**иначе:**
заблокировать сообщение

# Требования к семейству функций для теоретически стойкой аутентификации: почти-строго универсальные функции 2-го порядка [almost strongly universal$_2$ (ASU$_2$)]

Семейство функций $\mathscr{F} = \{f_k : \mathscr{M} \to \mathscr{T}\}_{k \in \mathscr{K}}$ называется $\varepsilon$-ASU$_2$, если выполняются следующие условия:

1) для равномерно случайного $k$ и произвольных $m$ и $t$, $\Pr[f_k(m) = t] = |\mathscr{T}|^{-1}$; ← «тэг трудно угадать»

2) для равномерно случайного $k$, произвольных $m_1 \neq m_2$ и произвольных $t_1, t_2$: $\Pr[f_k(m_2) = t_2 \,|\, f_k(m_1) = t_1] \leq \varepsilon$.

↑

«зная тэг для одного сообщения, трудно угадать тэг для другого сообщения»

На текущий момент предложены различные эффективные способы построения $\varepsilon$-ASU$_2$ семейств.

Длина тэга $\approx \log_2(1/\varepsilon)$, длина ключа для вычисления тэга $\sim \log\log|\mathscr{M}|$


M.N. Wegman and J.L. Carter, J. Comp. Syst. Sci. **22**, 265 (1981)

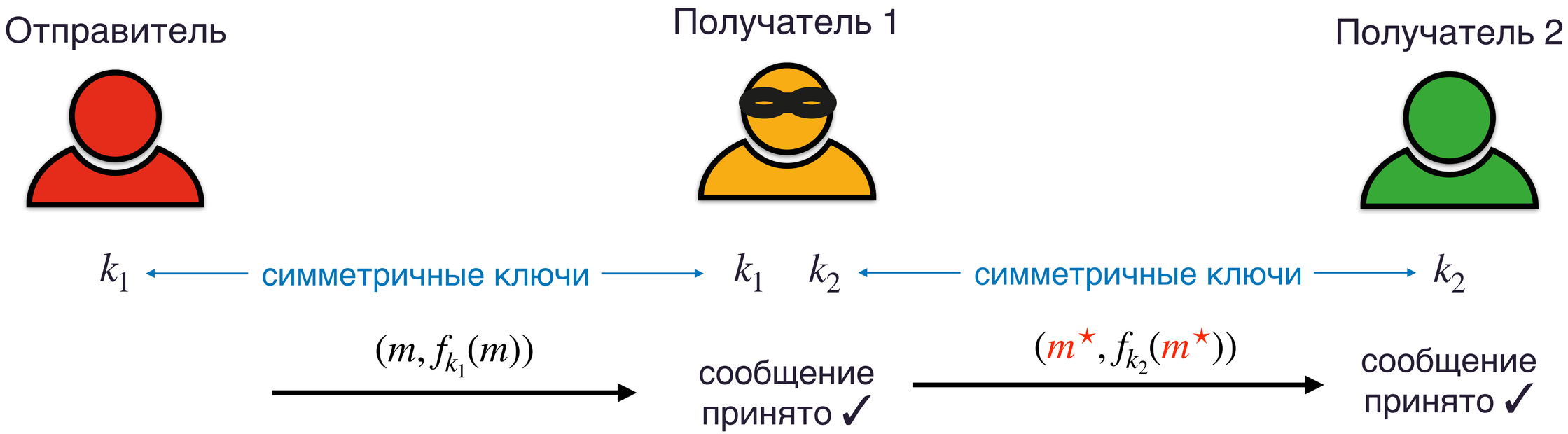
J. Bierbrauer, T. Johansson, G. Kabatianskii, B. Smeets Advances in Cryptology — CRYPTO' 93. Lecture Notes in Computer Science, **773** (1994)

G.A. Kabatianskii, B. Smeets and T. Johansson, in IEEE Transactions on Information Theory, **42** (2), 566-578 (1996)

C. Portmann, IEEE Trans. Inf. Theory **60**, 4383 (2014)

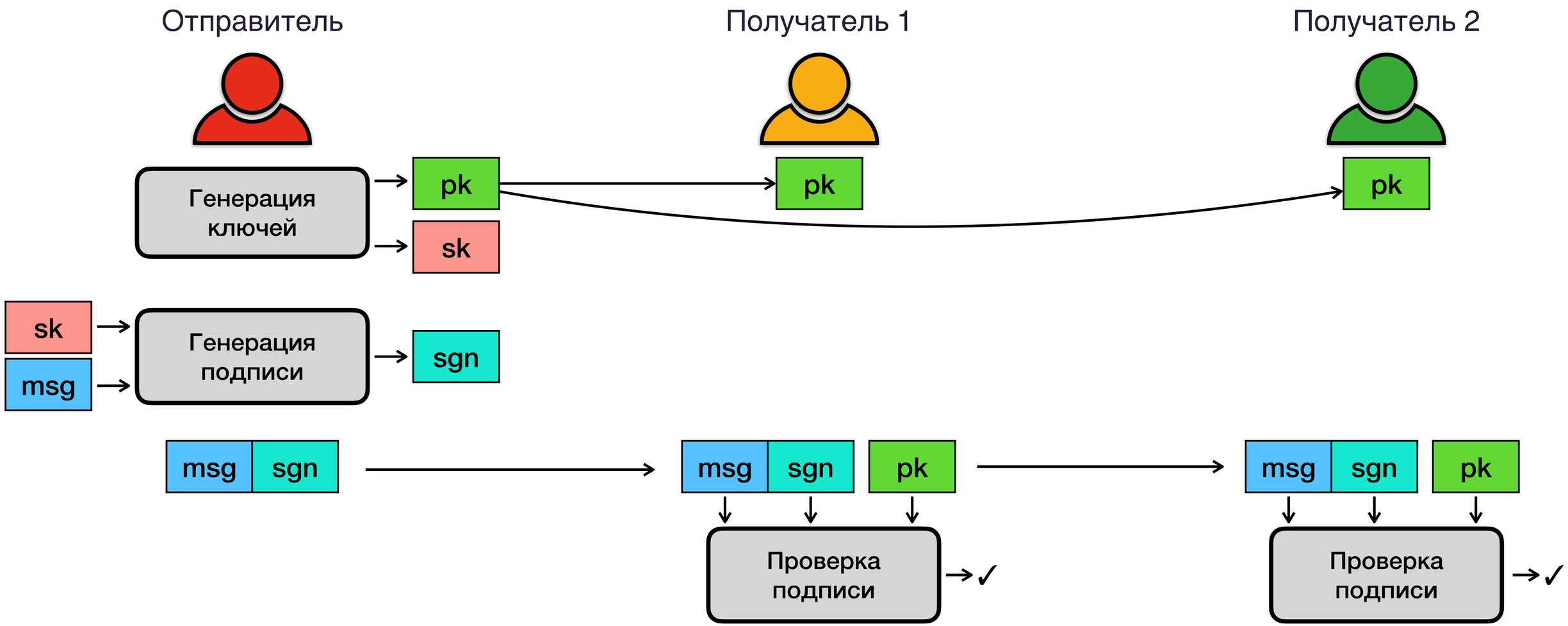

…

# Иммитовставка не обеспечивает возможности защищенной переадресации




Для обеспечения возможности защищенной переадресации необходим иной криптографический примитив!

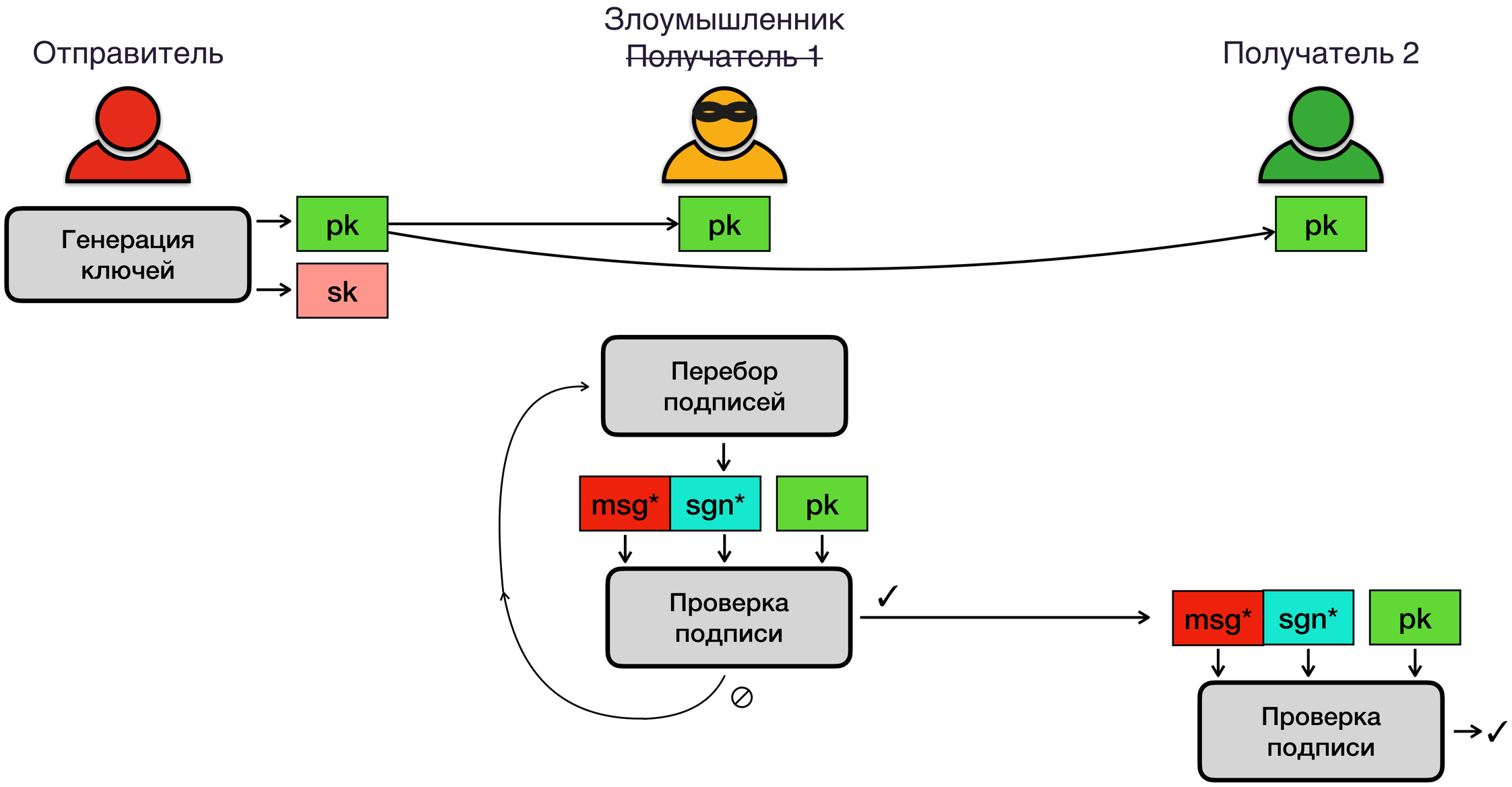
# Электронная цифровая подпись (ЭЦП)




ЭЦП защищает от двух угроз: (i) подделки сообщения отправителя (forging), (ii) отказа от авторства (repudiation)

Все предложенные ЭЦП являются вычислительно стойкими

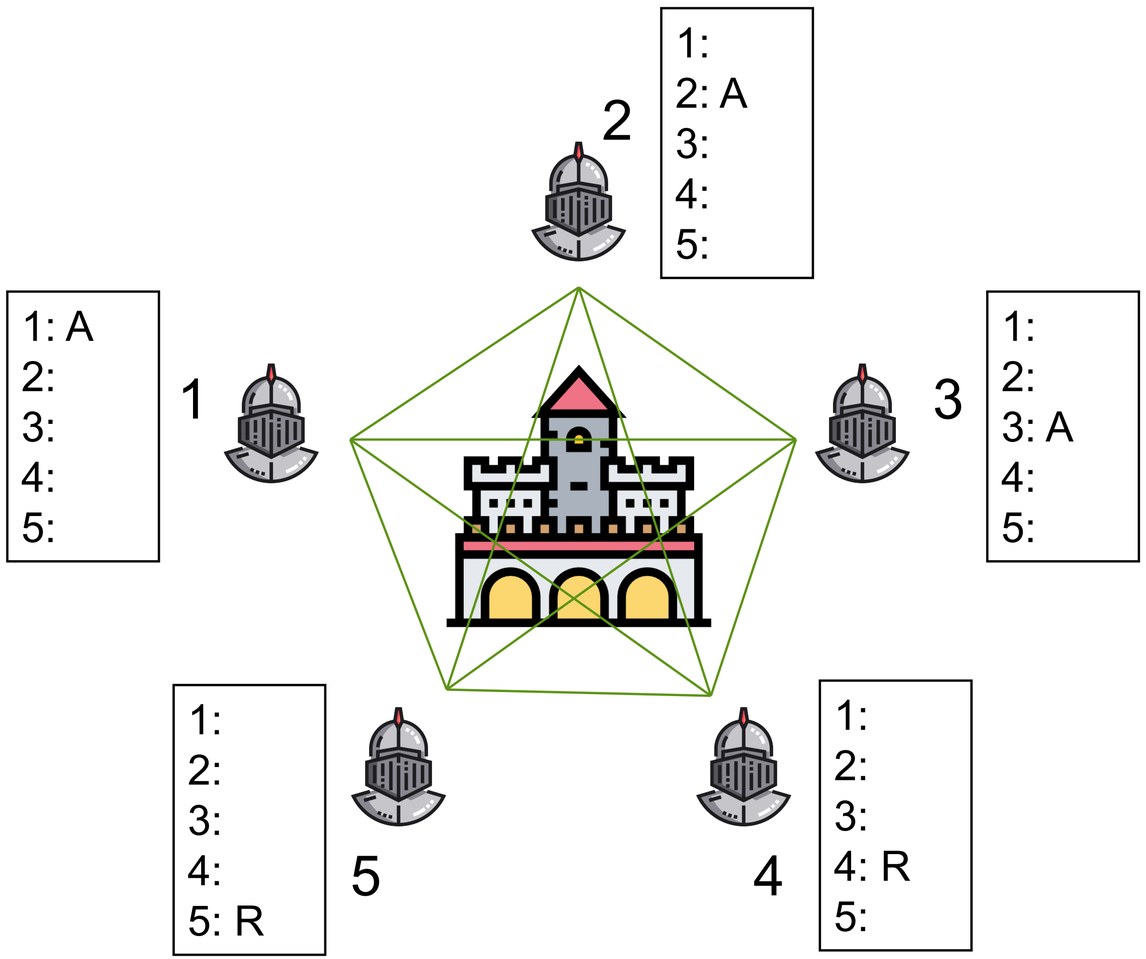
# Построение теоретически стойкой ЭЦП невозможно

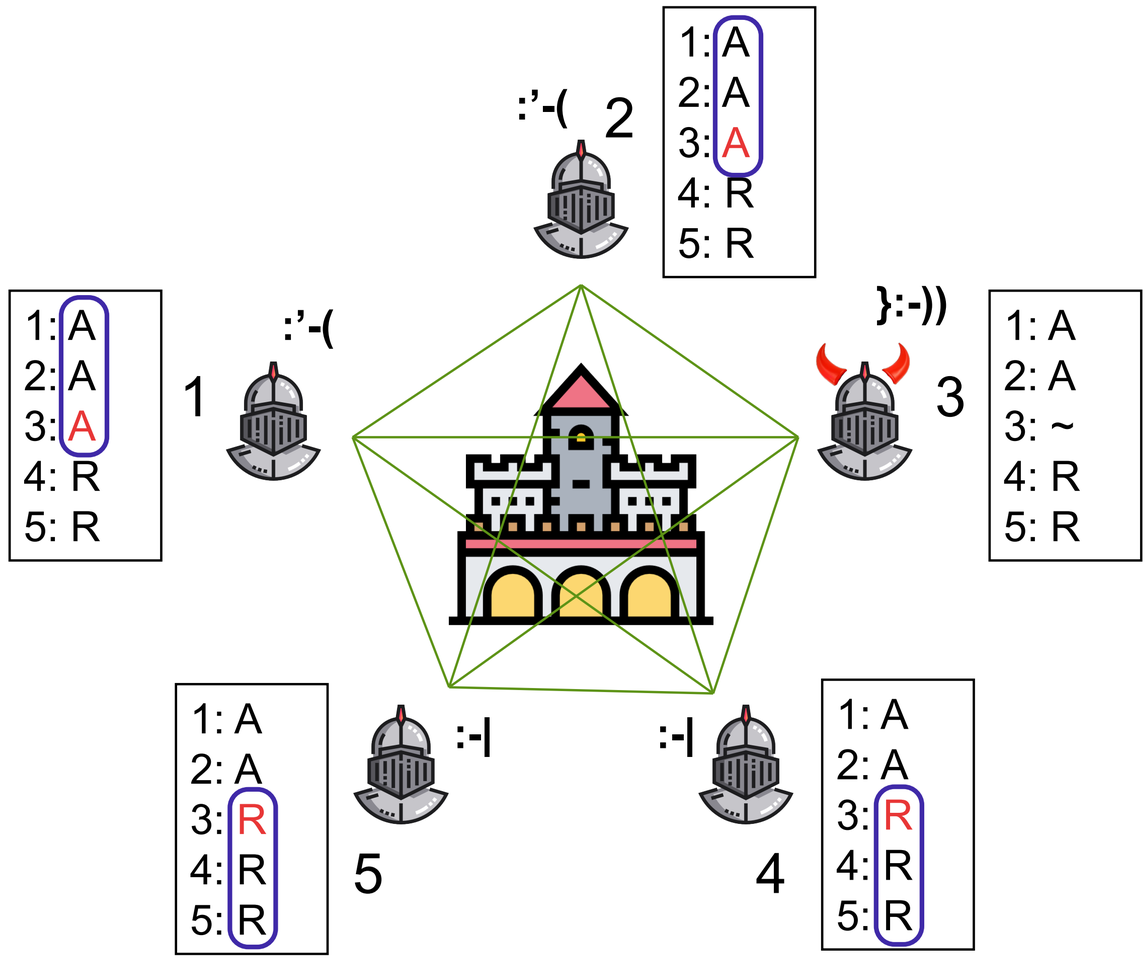


# Возможные теоретически стойкие алгоритмы на основе КРК

1. Квантово-защищенный распределенный реестр
2. Квантовая подпись на основе сетей КРК

# Задача византийских генералов

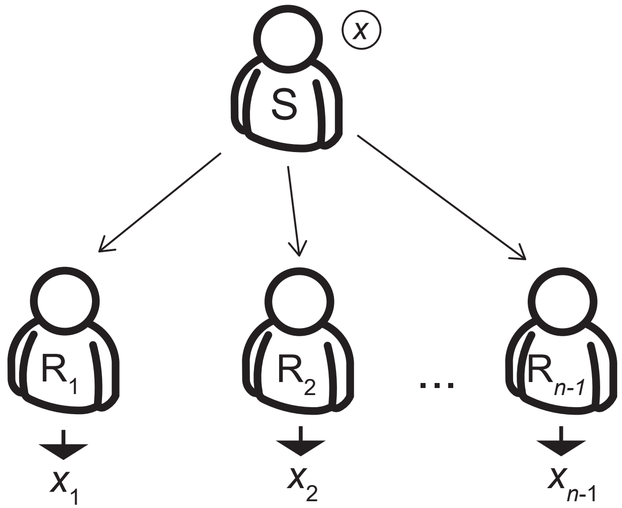


# Задача византийских генералов: строгая формулировка

Протоколом широковещания (broadcast protocol) называют протокол, реализуемый $n$ участниками: отправителем $\mathrm{S}$ и получателями $\mathrm{R}_1, \ldots, \mathrm{R}_{n-1}$, в котором отправитель $\mathrm{S}$ изначально владеет некоторым значением $x$, а каждый из получателей $\mathrm{R}_i$ завершает протокол со значением $x_i$, удовлетворяющим следующим условиям:

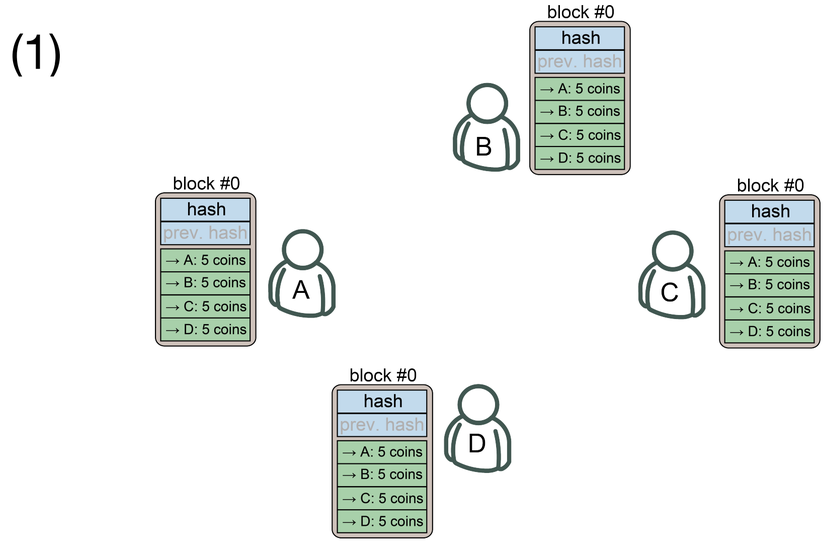
1) все честные получатели получают одинаковые значения: $x_i = \bar{x}$;
2) если отправитель честный, то $x_i = x$.

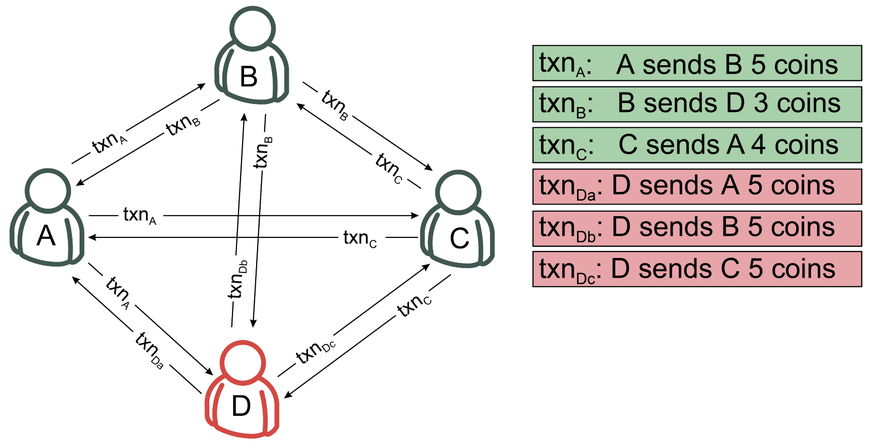


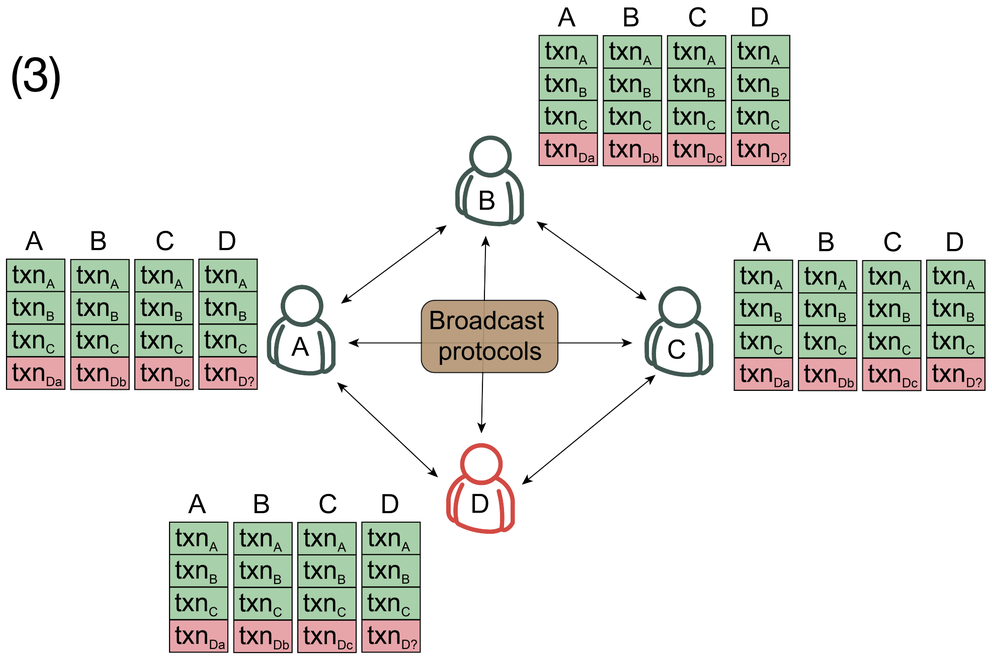

Предложен теоретически стойкий алгоритм широковещания на основе попарно аутентифицированных каналов для случая $\#\mathrm{dishonest} < n/3$, требующий $\#\mathrm{dishonest} + 1$ раундов коммуникации.

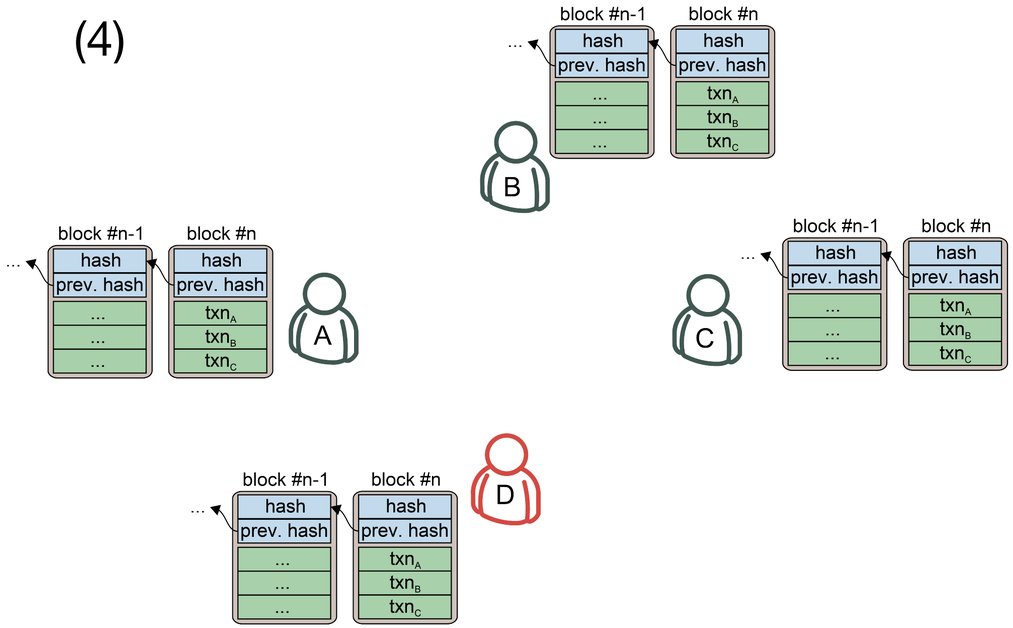
L. Lamport, R. Shostak, M. Pease, ACM Transactions on Programming Languages and Systems, 4 (3): 382–401 (1982).

# Квантово-защищенный распределенный реестр: схема протокола



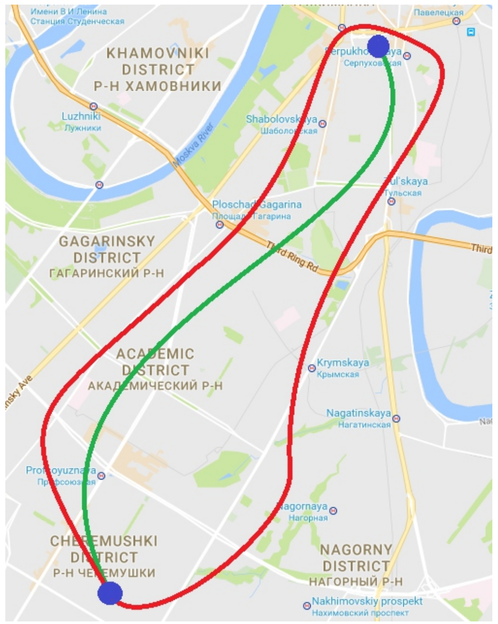




EOK, N.O. Pozhar, M.N. Anufriev, A.S. Trushechkin, R.R. Yunusov, Y.V. Kurochkin, A.I. Lvovsky, A.K. Fedorov, Quantum Sci. Technol. **3**, 035004 (2018)

# Квантово-защищенный распределенный реестр: некоторые детали технической реализации

| | |
|---|---|
| Number of nodes in the network | $n = 4$ |
| Upper bound on the number of faulty nodes | $m = 1$ |
| Number of rounds in the broadcast protocol | 2 |
| Duration of broadcast protocol | $< 10$ sec |
| Time between block generation events | 5 min |
| Authentication hash length | 40 bit |
| Quantum key consumption in the initial broadcast of a transaction | 40 bit |
| Quantum key consumption in the broadcast protocol | 80 bit |
| Average quantum key consumption required for a transaction rate of 10 per minute | $< 7$ bit/s |




EOK, N.O. Pozhar, M.N. Anufriev, A.S. Trushechkin, R.R. Yunusov, Y.V. Kurochkin, A.I. Lvovsky, A.K. Fedorov, Quantum Sci. Technol. **3**, 035004 (2018)

# Возможные теоретически стойкие алгоритмы на основе КРК

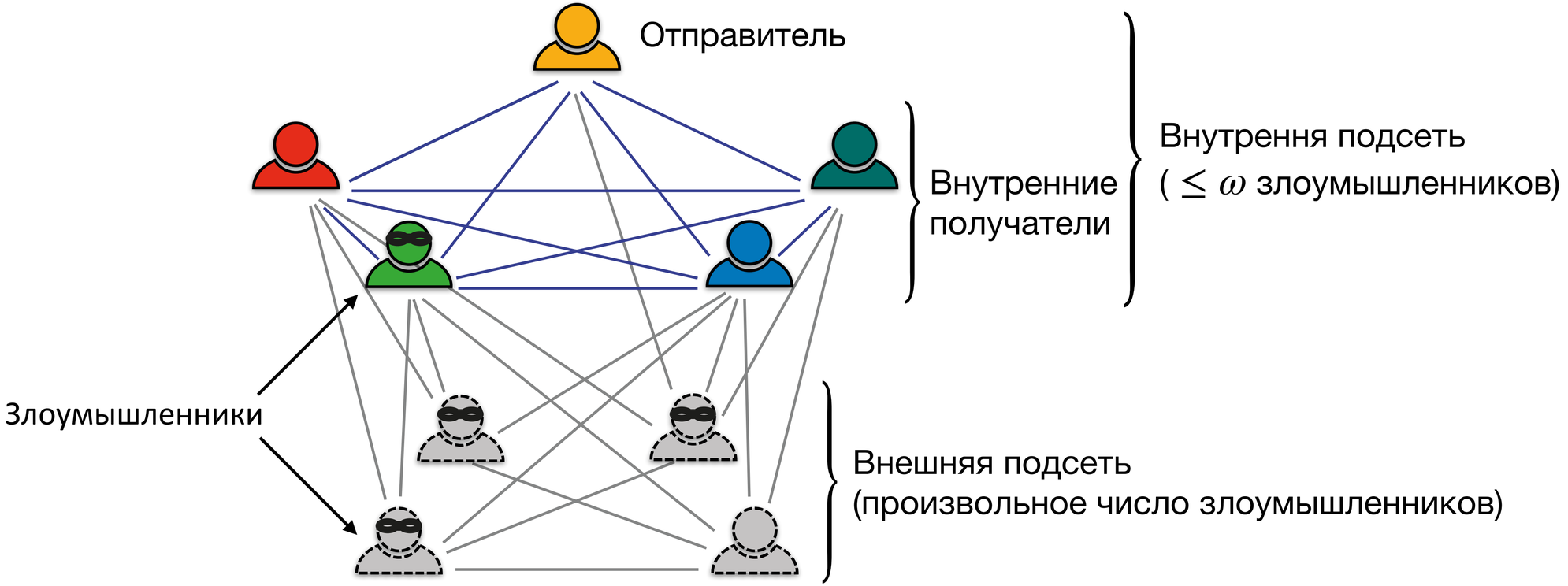
1. Квантово-защищенный распределенный реестр
2. Алгоритм подписи на основе сетей КРК

# Основные подходы к формированию теоретически стойкой «ЭЦП»

1. Добавление доверенного арбитра
2. Использование индивидуальных (классических или квантовых) «верифицирующих» ключей

| Классические теоретически стойкие подписи | Квантовые подписи, требующие квантовую память | Квантовые подписи, не требующие квантовую память | Подписи на основе сетей КРК |
|---|---|---|---|
| • D. Chaum and S. Roijakkers, In: CRYPTO ’90. LNCS, Springer-Verlag 206–214 (1991).<br>• B. Pfitzmann and M. Waidner, IBM (1996).<br>• G. Hanaoka, J. Shikata, Y. Zheng, and H. Imai, In: ASIACRYPT 2000. Springer 130–142 (2000).<br>• G. Hanaoka, J. Shikata, Y. Zheng, IEICE transactions on fundamentals of electronics, communications and computer sciences 87(1), 120–130 (2004).<br>• J. Shikata, G. Hanaoka, Y. Zheng, H. Imai, In: EUROCRYPT 2002, Springer 434–449 (2002).<br>• C.M. Swanson, D.R. Stinson, In: Information Theoretic Security. LNCS, Springer 100–116 (2011).<br>• R. Amiri and E. Andersson, Entropy 17(8) 5635–5659 (2015).<br>• Amiri, A. Abidin, P. Wallden, and E. Andersson, Lect. Notes Comp. Sci. 10892, 143 (2018).<br>• … | • D. Gottesman and I. Chuang, Quantum digital signatures, arXiv:quant-ph/0105032v2 (2001).<br>• X. Lu and D.-G. Feng, arXiv:quantph/0403046v2 (2004).<br>• P.J. Clarke, R.J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G.S. Buller, Nat. Commun. 3, 1174 (2012).<br>• … | • E. Andersson, M. Curty, and I. Jex, Phys. Rev. A 74, 022304 (2006).<br>• V. Dunjko, P. Wallden, and E. Andersson, Phys. Rev. Lett. 112, 040502 (2014).<br>• H.-L. Yin, Y. Fu, and Z.-B. Chen, Phys. Rev. A 93, 032316 (2016).<br>• R. Amiri, Petros Wallden, Adrian Kent, and Erika Andersson, Phys. Rev. Lett. 112, 040502 (2016).<br>• P. Wallden, V. Dunjko, A. Kent, and E. Andersson, Phys. Rev. A 91, 042304 (2015).<br>• R. Amiri and E. Andersson, Entropy 17(8) 5635–5659 (2015).<br>• R.J. Collins, R.J. Donaldson, V. Dunjko, P. Wallden, P.J. Clarke, E. Andersson, J. Jeffers, and G.S. Buller, Phys. Rev. Lett. 113, 040502 (2014).<br>• … | • P. Wallden, V. Dunjko, A. Kent, and E. Andersson, Phys. Rev. A 91, 042304 (2015).<br>• G. L. Roberts, M. Lucamarini, Z. L. Yuan, J. F. Dynes, L. C. Comandar, A. W. Sharpe, A. J. Shields, M. Curty, I. V. Puthoor, and E. Andersson, Nat. Commun. 8, 1098 (2017).<br>• EOK, A.S. Zelenetsky, A.K. Fedorov, Phys. Rev. A 105, 012408 (2022). |

# Схема подписи на основе сетей КРК: общая схема



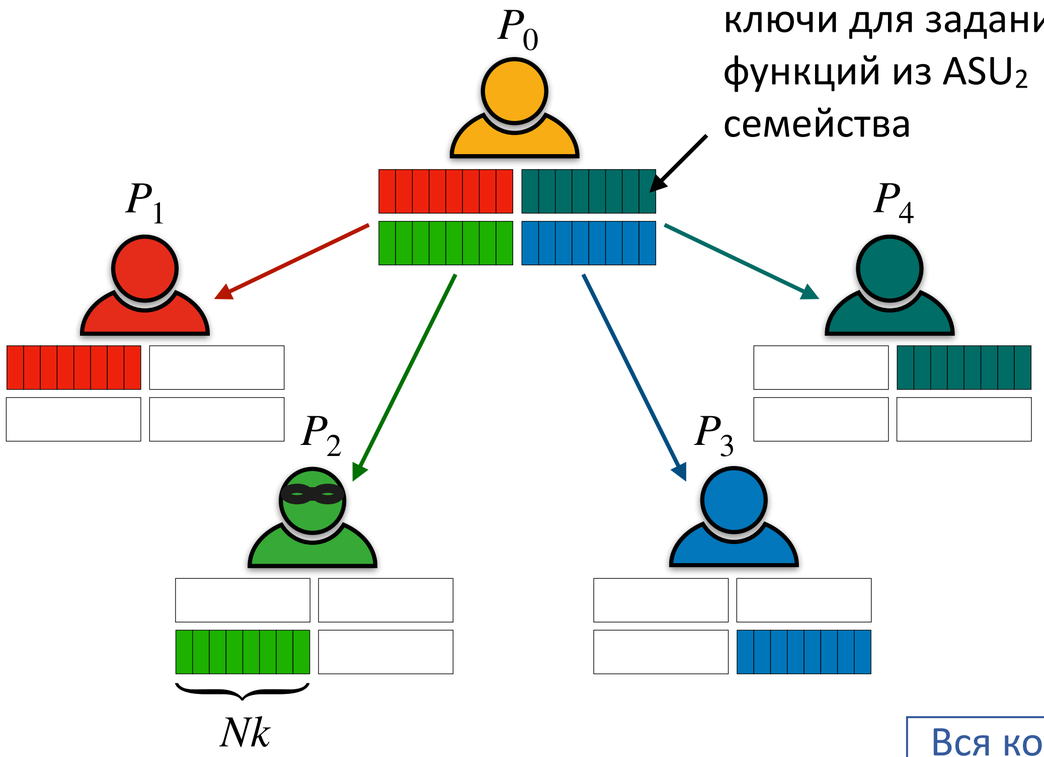

Общие принципы:

- Отправитель и каждый из внутренних получателей владеют индивидуальными секретными ключами (ключ подписывающего узла позволяет генерировать подпись, ключи получателей — верифицировать подпись).
- Узлы внутренний подсети связаны друг с другом попарными КРК каналами.
- Каждый из узлов внешней подсети должен быть связан не менее с $2\omega + 1$ внутренними получателями.
- Работа схемы основана на использовании ASU2
- Схема защищает от подделки (forgery) и отказа от авторства (repudiation).

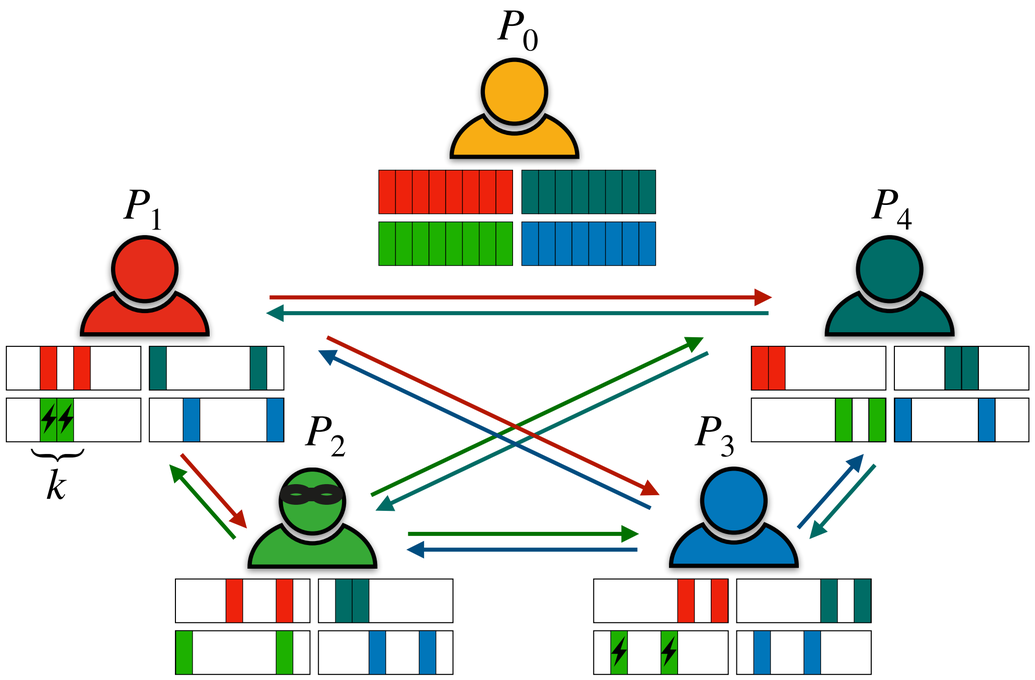
EOK, A.S. Zelenetsky, A.K. Fedorov, Phys. Rev. A 105, 012408 (2022).

# Схема подписи на основе сетей КРК: начальное распределение ключей

Шаг 1




Шаг 2



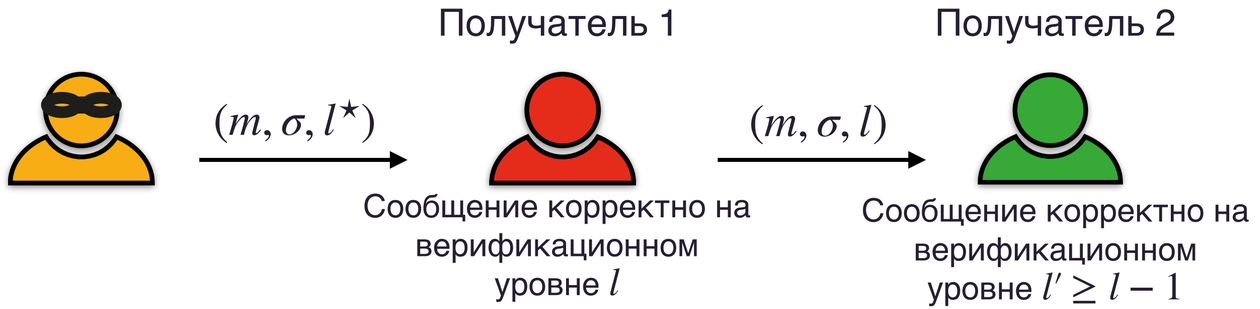

Вся коммуникация шифруется одноразовым блокнотом

Подпись для сообщения — $N^2k$ аутентификационных тэгов для этого сообщения

EOK, A.S. Zelenetsky, A.K. Fedorov, Phys. Rev. A 105, 012408 (2022).

# Схема подписи на основе сетей КРК: верификация подписей

## Верификационные уровни

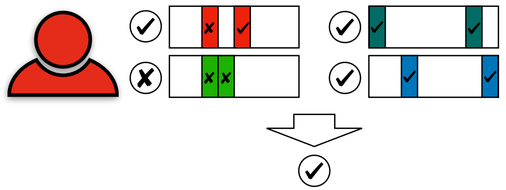



## Верификация внутренним получателем $P_i$

Шаг 1. Для каждого $j$ вычисляется

$$T^m_{i,j,l} = \begin{cases} 1 & \text{if } \sum_{r \in R_{j\to i}} \delta_{\neq}(f_{\kappa_r}(m), t_r) < s_l k, \\ 0 & \text{otherwise,} \end{cases}$$

где $s_l = \left(1 - l/l_{\max}\right) s_0, s_0 \in (0, 1 - 2^{1-b})$.

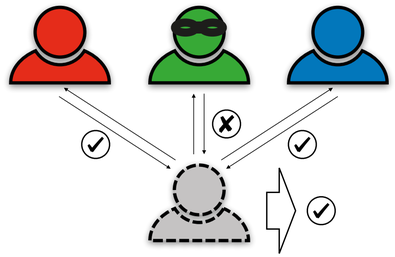


Шаг 2. Если $\sum_{j=1}^{N} T^m_{i,j,l} > \omega + l\omega$ тогда $(m, \sigma)$принимается на верификационном уровне $l$ (максимальное из всех возможных).

## Верификация внешним получателем $E_i$

Шаг 1. Запрашиваются $2\omega + 1$ внтренних получателей для проверки подписи.

Шаг 2. Если подписи принимается как минимум $\omega + 1$ внутренними получателями — подпись принимается, иначе— овтергается



EOK, A.S. Zelenetsky, A.K. Fedorov, Phys. Rev. A 105, 012408 (2022).

# Схема подписи на основе сетей КРК: анализ секретности

Ограничение на количество злоумышленников во внутренней подсети: $\omega < N/(2 + l_{\max})$.

Вероятность взлома: $\Pr[\text{Forgery}] < N^2(\omega + M(\omega + M))e^{-2k(1-s_0-2^{1-b})^2}$.

Вероятность отказа от авторства: $\Pr[\text{Repudiation}] \leq 2N^2(N-1)e^{-k(s_0/l_{\max})^2/2}$.

$N$ — количество получателей во внутренней подсети

$M$ — количество получателей во внешней подсети

$l_{\max}$ — максимальный верификационный уровень

$b$ — длина аутентификационного тэга

$k, s_0$ — внутренние параметры схемы

EOK, A.S. Zelenetsky, A.K. Fedorov, Phys. Rev. A 105, 012408 (2022).

# Схема подписи на основе сетей КРК: потребление симметричных ключей

$L_{\mathrm{sr}}$ — длина требуемого ключа между подписывающим узлом и внутренним получателем

$L_{\mathrm{rr}}$ — длина требуемого ключа между внутренними получателями

| Input parameters | | | | | | Results of optimization for $b = b_{\mathrm{opt}}$ | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $N$ | $M$ | $\omega$ | $l_{\max}$ | $a$ | $\varepsilon_{\mathrm{tot}}$ | $k$ | $b$ | $s_0$ | $L_{\mathrm{sr}}$ | $L_{\mathrm{rr}}$ | sig_len |
| 4 | 0 | 1 | 1 | 8 Mbits | $10^{-10}$ | 125 | 7 | 0.658 | 37.6 kbits | 21.5 kbits | 151 kbits |
| 4 | 10 | 1 | 1 | 8 Mbits | $10^{-10}$ | 136 | 6 | 0.630 | 39.3 kbits | 22.8 kbits | 157 kbits |
| 10 | 10 | 1 | 7 | 8 Mbits | $10^{-10}$ | 2947 | 9 | 0.996 | 2.33 Mbits | 587 kbits | 23.3 Mbits |
| 10 | 10 | 3 | 1 | 8 Mbits | $10^{-10}$ | 147 | 6 | 0.632 | 106 kbits | 25.3 kbits | 1062 kbits |
| 10 | 10 | 2 | 2 | 8 Mbits | $10^{-10}$ | 403 | 6 | 0.766 | 291 kbits | 70.8 kbits | 2.84 Mbits |
| 10 | 10 | 2 | 2 | 32 Mbits | $10^{-10}$ | 403 | 6 | 0.766 | 307 kbits | 74.0 kbits | 3.00 Mbits |
| 10 | 10 | 2 | 2 | 8 Mbits | $10^{-12}$ | 475 | 6 | 0.758 | 343 kbits | 83.5 kbits | 3.35 Mbits |
| 10 | 100 | 2 | 2 | 8 Mbits | $10^{-10}$ | 414 | 6 | 0.756 | 299.2 kbits | 72.8 kbits | 2.92 Mbits |

EOK, A.S. Zelenetsky, A.K. Fedorov, Phys. Rev. A 105, 012408 (2022).

# Заключение

Теоретически стойкие алгоритмы обеспечивают защиту информации без предположении о вычислительных возможностях потенциального злоумышленники (= «высший уровень защищенности»)

Квантовое распределение ключей, являясь по сути теоретически стойким алгоритмом, открывает возможности реализации более сложных теоретически стойких алгоритмов. В частности, возможно построение квантово-защищенных распределенных реестров и теоретически стойких подписей.

Существующий прогресс в области сетей КРК уже достаточен для реализации указанных алгоритмов.

# Спасибо за внимание!

Разработка алгоритма подписи в сетях КРК выполнена при поддержке Министерства науки и высшего образования РФ (грант № 075-15-2020-788)