Перенос секретных ключей в квантовой сети с доверенными промежуточными узлами и шифрованием блочным шифром

С.Н.Молотков
Академия Криптографии Российской Федерации
ЦКТ МГУ имени М.В.Ломоносова
ВМК МГУ имени М.В.Ломоносова
Кафедра Суперкомпьютеров и квантовой информатики

Обсуждаемые вопросы

Рассматривается вопрос о переносе независимого ключа через доверенные узлы квантовой сети, между которыми имеются ключи, полученные в результате квантового распределения ключей.

Квантовые ключи используются для шифрования переносимого ключа. Шифрование переносимого ключа возможно как блочным шифром, так и одноразовым блокнотом.

Показано, что трудоемкость (сложность перебора) по поиску продвигаемого по сети ключа зависит от неидеальности внешнего ключа и квантовых ключей, а также от неидеальности -- средней вероятности коллизий блочного шифра.

В случае шифрования переносимого ключа одноразовым блокнотом трудоемкость зависит только от неидеальности переносимого ключа и ключей шифрования.

Связь квантового критерия секретности ключей с классическими переборными (сложностными) критериями

Секретность ключей в квантовой криптографии выражается в терминах близости квантового состояния подслушивателя после распределения ключей к идеальному квантовому состоянию, которое некоррелировано с ключом легитимных пользователей.

Метрикой близости двух квантовых состояний является следовая метрика.

В классической криптографии секретность ключей понимается в терминах, например, сложности перебора ключей при наличии побочной информации.

Для секретных ключей, используемых в различных алгоритмах шифрования предъявляются требования, которые формулируются совершенно в других терминах. Шенноном был введен критерий практической секретности криптосистемы, который понимается как

''The average amount of work to determine the key for a cryptogram....''.

Данный критерий не был формализован, поэтому в зависимости от ситуации возможны различные критерии средней работы (трудоемкости) по определению ключа.

Идеальный секретный ключ

$$K \to \{0,1\}^n \qquad K_E \to \{0,1\}^n$$

$$P(K = k) = \frac{1}{2^n}$$

$$P(K = k \mid K_E = k_E) = \frac{1}{2^n}$$

$$D(\rho_{XE}, \rho_U \otimes \rho_E) = \|\rho_{XE} - \rho_U \otimes \rho_E\|_1 < \varepsilon.$$

Вероятность различения двух ситуаций – квантовых состояний –

идеальной $\rho_U \otimes \rho_E$

и реальной ρ_{XE}

$$\Pr_{succes} = \frac{1}{2} + \frac{1}{2} D(\rho, \sigma)$$

$$D(\rho_{XE}, \rho_U \otimes \rho_E) = \|\rho_{XE} - \rho_U \otimes \rho_E\|_1 < \varepsilon.$$

$$D(\rho_{XE}, \rho_U \otimes \rho_E) = ||\rho_{XE} - \rho_U \otimes \rho_E||_1 < \varepsilon.$$

$$D(\rho_{XE}, \rho_U \otimes \rho_E) = \max_{\{0 \le \Lambda \le I_{XE}\}} \mathrm{Tr}_{XE}\{\Lambda(\rho_{XE} - \rho_U \otimes \rho_E)\}$$

$$x \in X = \{0,1\}^n$$

Средняя вероятность угадывания по ключам

$$\Pr_{key\ guess} = \sum_{x \in X} P_{XY}(x,x) \le \frac{1}{N} + D(\rho_{XE}, \rho_U \otimes \rho_E) < \frac{1}{N} + \varepsilon$$

Трудоемкость тотального перебора – ключ определяется с вероятностью единица

$$G(X) = \sum_{i=1}^{N} i \cdot P_X(x_i)$$

$$\frac{N+1}{2} - N||P_X - P_U||_1 \leq G(X) \leq \frac{N+1}{2} - \frac{N}{2}||P_X - P_U||_1$$

$$G(X) \geq \frac{N+1}{2} - N||\rho_{XE} - \rho_U \otimes \rho_E||_1 > \frac{N(1-2\varepsilon)+1}{2}$$

$$G(X|Y) \geq \frac{N+1}{2} - N||\rho_{XE} - \rho_U \otimes \rho_E||_1 > \frac{N(1-2\varepsilon)+1}{2}$$

Трудоемкость частичного перебора при наличии побочной информации о ключе при заданной вероятности успеха

$$Q(X|Y,\pi_0) = \min_{\{M:\pi(M)\geq\pi_0\}} G(X|Y,M) \geq \left(1-\frac{2\varepsilon}{\pi_0}\right)\left(\frac{N(1-8\varepsilon)+1}{2}\right)$$

Пример

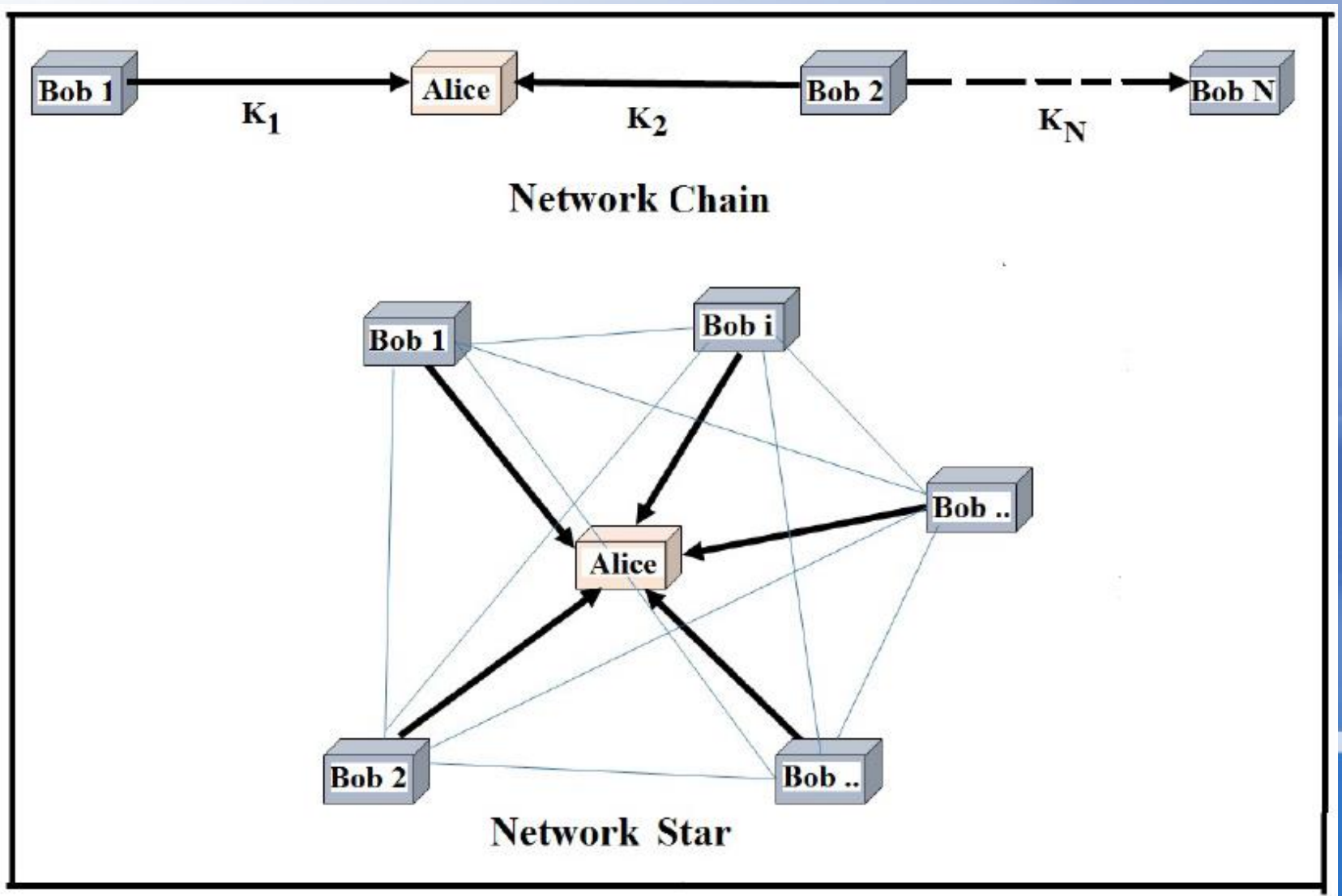
На данные оценки можно взглянуть под другим углом. Пусть криптосистема производит сообщения длиной 256 бит каждую секунду, каждое сообщение шифруется в режиме одноразового блокнота ε--секретным ключом длиной 256 бит.

За 100 лет система произведет 10^9 сообщений. Пусть имеется идеальный критерий читаемости дешифрованного сообщения.
Для каждого сообщения осуществляется частичный перебор по M первым наиболее вероятным ключам. Тогда через примерно через 100 лет возможно будет дешифровано (прочитано) одно сообщение.

Среднее число сообщений до первого дешифрованного

$$\approx \frac{1}{\varepsilon} \approx 10^{10}$$

Согласование секретных ключей в сетях с квантовым распределением ключей с доверенными узлами



Согласование идеальных ключей

КЛИЕНТ 1 **СЕРВЕР** **КЛИЕНТ 2**

$$k = k_1 \oplus k_2$$

0100101100 **0100101100** **0110111000**

0110111000

$$k_2 \rightarrow k_1 = k_2 \oplus k$$

Сервер разглашает через открытый канал позиции, где биты не совпадают

В итоге для средней сложности Q_{U,π_0} поиска ключа находим

$$Q_{U,\pi_0} \geq \left(1 - \frac{2\delta_1}{\pi_0}\right)\left(\frac{|\mathcal{K}|(1-8\delta_1)+1}{2}\right),$$

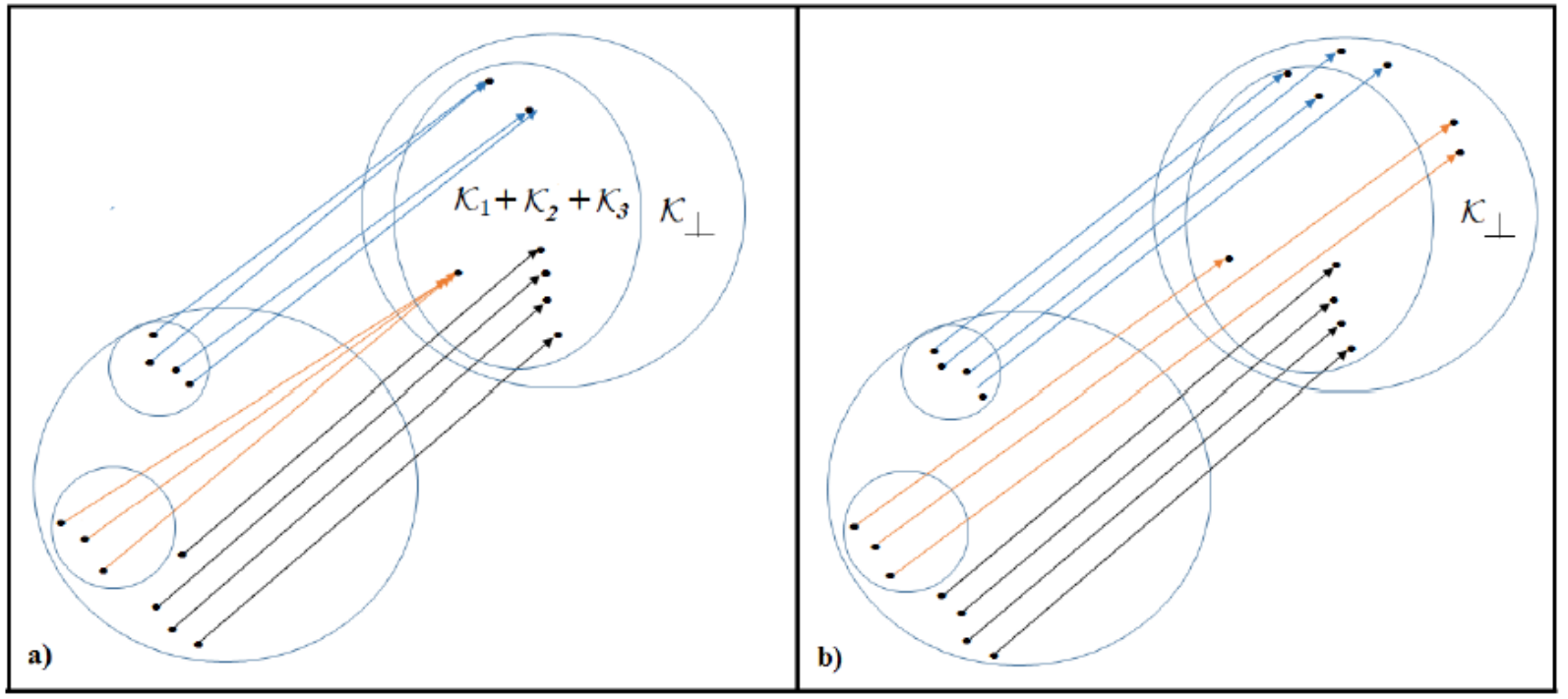
$$\delta_1 \leq \frac{1}{2}||\rho^{cip}_{K_1 KEC_1} - \rho^{OTP}_{U_{K_1} U_K EC_1}||_1,$$

Оценка следового расстояния блочного шифра до одноразового блокнота

$$\frac{1}{2}||\rho^{cip}_{U_{K_1}U_K C_1} - \rho^{OTP}_{U_{K_1}U_K C_1}||_1 =$$

$$= \frac{1}{2}\frac{1}{|\mathcal{K}|}\frac{1}{|\mathcal{K}|}\sum_k\sum_{k_1}\mathrm{Tr}_{C_1}\{|\ |c_1(k_1,k)\rangle_{C_1C_1}\langle c_1(k_1,k)| - |c_{OTP}(k_1,k)\rangle_{C_1C_1}\langle c_{OTP}(k_1,k)|\ |\} =$$

$$= \frac{1}{|\mathcal{K}|}\frac{1}{|\mathcal{K}|}\sum_k\sum_{k_1}\sqrt{1 - |_{C_1}\langle c_1(k_1,k)|c_{OTP}(k_1,k)\rangle_{C_1}|^2}.$$



При каждом k определим множества:

$\mathcal{K}_\perp(k)$ – множество значений шифр-текстов при данном сообщении k, которые отсутствуют – не достигаются ни при одном ключе k_1.

$\mathcal{K}_1(k)$ – множество значений шифр-текстов при данном сообщении k, которые имеют место только при одном ключе k_1.

$\mathcal{K}_2(k)$ – множество значений шифр-текстов при данном сообщении k, которые имеют место при двух ключах k_{1_1} и k_{1_2}.

...

$\mathcal{K}_L(k)$ – множество значений шифр-текстов при данном сообщении k, которые имеют место при L ключах k_{1_1}, k_{1_2}, ..., k_{1_L}, $L \leq |\mathcal{K}|$.

При шифровании одноразовым блокнотом для каждого открытого текста (k) и каждого ключа ключа (k_1) имеется только одно значение шифр-текста – все множество шифр-текстов накрывается однократно (рис.1). На рис.1 для иллюстрации показаны множества без коллизий и только множества парных и тройных коллизий.

Множество $\mathcal{K}_\perp$, это множество шифр-текстов, которые отсутствуют при шифровании блочным шифром.

$$\frac{1}{2}\frac{1}{|\mathcal{K}|}\sum_{k_1}\mathrm{Tr}_{C_1}\{|\ |c_1(k_1,k)\rangle_{C_1C_1}\langle c_1(k_1,k)| - |c_{OTP}(k_1,k)\rangle_{C_1C_1}\langle c_{OTP}(k_1,k)|\ |\} =$$

$$= \frac{1}{|\mathcal{K}|}\sum_{k_1}\sqrt{1-|_{C_1}\langle c_1(k_1,k)|c_{OTP}(k_1,k)\rangle_{C_1}|^2}.$$

$$= \frac{1}{|\mathcal{K}|}|\mathcal{K}_\perp(k)| = \frac{1}{|\mathcal{K}|}\sum_{i=2}^{L}(i-1)|\mathcal{K}_i(k)| = \frac{|\mathcal{K}_{coll}(k)|}{|\mathcal{K}|} =$$

Из рассуждений выше следует, что число ненулевых слагаемых совпадает с размером множества $|\mathcal{K}_{\perp}(k)|$, это та часть множества шифр-текстов, которые отсутствуют при шифровании блочным шифром. Из рассуждений выше также следует, что

$$|\mathcal{K}_{\perp}(k)| = \sum_{i=2}^{L}(i-1)|\mathcal{K}_i(k)|,$$

здесь $|\mathcal{K}_i(k)|$ размер множества i-ых коллизий при данном сообщении k.

Далее, имеем

$$\frac{1}{2}||\rho^{cip}_{U_K U_{K_1} C_1} - \rho^{OTP}_{U_K U_{K_1} C_1}||_1 = \frac{1}{|\mathcal{K}|}\sum_k \frac{|\mathcal{K}_{coll}(k)|}{|\mathcal{K}|} = \overline{|\mathcal{K}_{coll}|}.$$

В итоге для средней сложности Q_{U,π_0} поиска ключа находим

$$Q_{U,\pi_0} \geq \left(1 - \frac{2\delta_1}{\pi_0}\right)\left(\frac{|\mathcal{K}|(1-8\delta_1)+1}{2}\right),$$

СПАСИБО ЗА ВНИМАНИЕ.