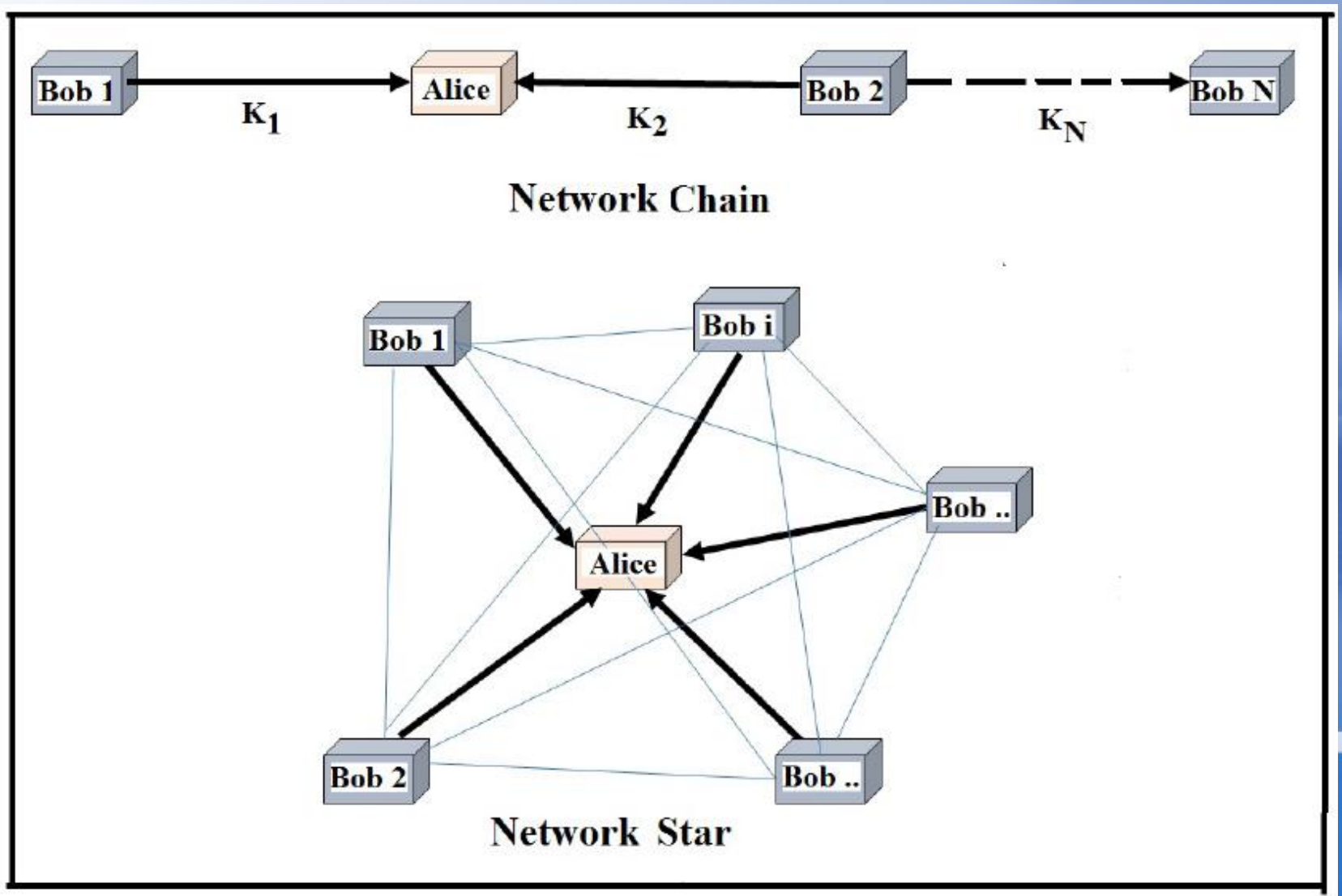
Согласование/проталкивание секретных ключей через доверенные узлы

С.Н.Молотков
Академия криптографии РФ
ЦКТ МГУ имени М.В.Ломоносова

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



Идеальный секретный ключ

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

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

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

Согласование идеальных секретных ключей (одноразовый блокнот)

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

Проталкивание идеальных ключей (одноразовый блокнот)

КЛИЕНТ 1	СЕРВЕР	КЛИЕНТ 2
k_1=0100101100	k_1=0100101100 k_2=0110111000	k_2=0110111000

внешний ключ
k=1111100000

$k \oplus k_1 \Rightarrow$ $k=k \oplus k_1 \oplus k_1$ $k \oplus k_2 \Rightarrow$ $k=k \oplus k_2 \oplus k_2$

Как быть, если ключи неидеальны?

Станут ли ключи более неидеальными?

Если “да”, то насколько?

Что будет, если использовать блочный шифр вместо одноразового блокнота?

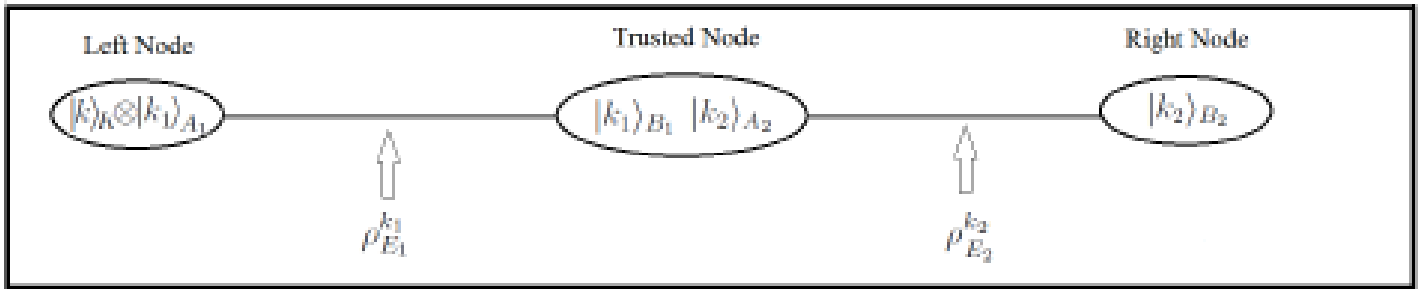
Как изменится трудоемкость поиска истинного согласованного/проталкиваемого ключа?

Критерий секретности ключей в квантовой криптографии. Что известно про ключи?

$$\rho_{k_1 E_1} = \sum_{k_1 \in \{0,1\}^n} P_{K_1}(k_1) |k_1\rangle_{11}\langle k_1| \otimes \rho_{E_1}^{k_1}$$

$$|k_1\rangle_{11}\langle k_1| = (|k_1\rangle_{A_1} \otimes |k_1\rangle_{B_1})({}_{A_1}\langle k_1| \otimes {}_{B_1}\langle k_1|)$$

$$\rho_{E_1} = \mathrm{Tr}_{K_1}\{\rho_{K_1 E_1}\} = \sum_{k_1 \in \{0,1\}^n} P_{K_1}(k_1)\rho_{E_1}^{k_1},$$



Критерий секретности ключей в квантовой криптографии

$$\rho_{U_1} \otimes \rho_{E_1}, \quad \rho_{U_1} = \sum_{k_1 \in \{0,1\}^n} P_U(k_1) |k_1\rangle_{11}\langle k_1|, \quad P_U(k_1) = \frac{1}{2^n}$$

$$\left|\left|\rho_{K_1 E_1} - \rho_{U_1} \otimes \rho_{E_1}\right|\right|_1 < \varepsilon_1$$

$$\left|\left|\rho_{K_2 E_2} - \rho_{U_2} \otimes \rho_{E_2}\right|\right|_1 < \varepsilon_2,$$

$$\left|\left|\rho_K - \rho_{U_K}\right|\right|_1 < \varepsilon_K,$$

$$\rho_{U_K} = \frac{1}{2^n} \sum_{k \in \{0,1\}^n} |k\rangle_{KK}\langle k|, \quad \rho_K = \sum_{k \in \{0,1\}^n} P_K(k) |k\rangle_{KK}\langle k|.$$

В классическом случае следовое расстояние есть расстояние Колмогорова между двумя распределениями вероятностей

$$||\rho_K - \rho_{U_K}||_1 = \mathrm{Tr}_K\{|\rho_K - \rho_{U_K}|\} =$$

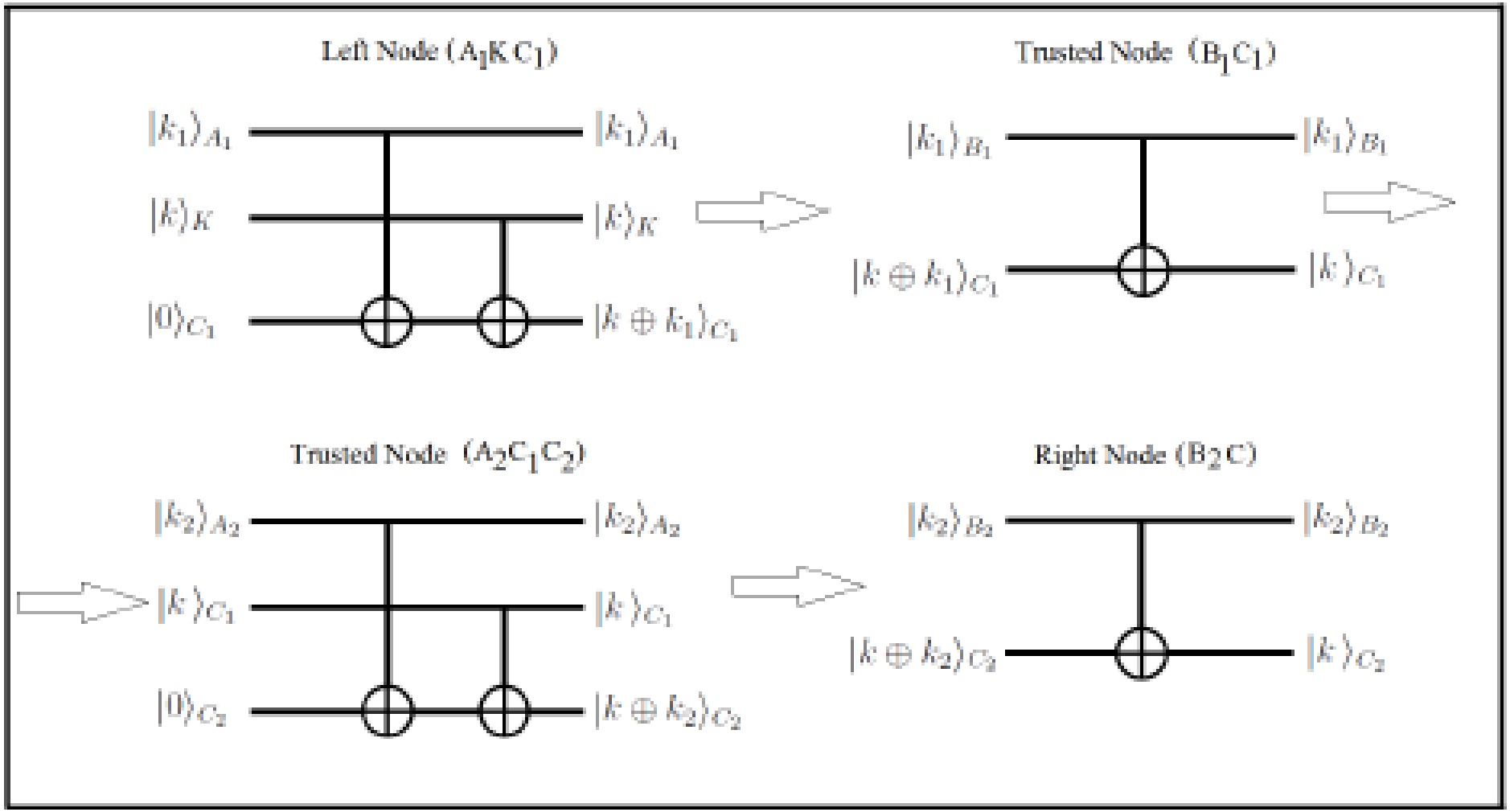
$$= ||P_K - P_{U_K}||_1 = \sum_{k\in\{0,1\}^n} |P_K(k) - P_{U_K}(k)| = \sum_{k\in\{0,1\}^n} |P_K(k) - \frac{1}{N}| < \varepsilon_K$$

Состояния для реальной и идеальной ситуаций до проталкивания

$$\rho_K \otimes \rho_{K_1E_1} \otimes \rho_{K_2E_2} \otimes |0\rangle_{C_1C_1}\langle 0| \otimes |0\rangle_{C_2C_2}\langle 0|$$

$$\rho_{U_K} \otimes (\rho_{U_1} \otimes \rho_{E_1}) \otimes (\rho_{U_2} \otimes \rho_{E_2}) \otimes |0\rangle_{C_1C_1}\langle 0| \otimes |0\rangle_{C_2C_2}\langle 0|$$

Проталкиванием внешнего ключа (одноразовый блокнот)



$$U_{CNOT}(A_1K : C_1)\left(|k\rangle_K \otimes (|k_1\rangle_{A_1} \otimes |k_1\rangle_{B_1}) \otimes |0\rangle_{C_1}\right) =$$

$$= |k\rangle_K \otimes |k_1\rangle_{A_1} \otimes |k_1\rangle_{B_1} \otimes |k \oplus k_1\rangle_{C_1}.$$

$$U_{CNOT}(B_1 : C_1)\left(|k\rangle_K \otimes (|k_1\rangle_{A_1} \otimes |k_1\rangle_{B_1}) \otimes |k \oplus k_1\rangle_{C_1}\right) =$$

$$|k\rangle_K \otimes |k_1\rangle_{A_1} \otimes |k\rangle_{B_1} \otimes |k\rangle_{C_1}.$$

$$U_{CNOT}(A_2C_1 : C_2)\left(|k\rangle_K \otimes (|k_2\rangle_{A_2} \otimes |k_2\rangle_{B_2} \otimes |k\rangle_{C_1}) \otimes |0\rangle_{C_2}\right) =$$

$$= |k\rangle_K \otimes (|k_2\rangle_{A_2} \otimes |k_2\rangle_{B_2} \otimes |k\rangle_{C_1}) \otimes |k \oplus k_2\rangle_{C_2}.$$

$$U_{CNOT}(B_2 : C_2)\left(|k\rangle_K \otimes (|k_2\rangle_{A_2} \otimes |k_2\rangle_{B_2}) \otimes |k \oplus k_2\rangle_{C_2}\right) =$$

$$= |k\rangle_K \otimes (|k_2\rangle_{A_2} \otimes |k_2\rangle_{B_2}) \otimes |k\rangle_{C_2}.$$

Расстояние между квантовыми состояниями реальной и идеальной ситуациями после проталкивания (одноразовый блокнот)

$$||U_{CNOT}(B_2 : C_2)U_{CNOT}(A_2C_1 : C_2)U_{CNOT}(C_1 : B_1)U_{CNOT}(A_1K : C_1)$$

$$((\rho_K \otimes \rho_{K_1E_1} \otimes \rho_{K_2E_2} - \rho_{U_K} \otimes (\rho_{U_1} \otimes \rho_{E_1}) \otimes (\rho_{U_2} \otimes \rho_{E_2})) \otimes |0\rangle_{C_1C_1}\langle 0| \otimes |0\rangle_{C_2C_2}\langle 0|)$$

$$U^+_{CNOT}(A_1K : C_1)U^+_{CNOT}(C_1 : B_1)U^+_{CNOT}(A_2C_1 : C_2)U^+_{CNOT}(B_2 : C_2)||_1 =$$

$$= ||\,(\rho_K \otimes \rho_{K_1E_1} \otimes \rho_{K_2E_2} - \rho_{U_K} \otimes (\rho_{U_1} \otimes \rho_{E_1}) \otimes (\rho_{U_2} \otimes \rho_{E_2}))\,||_1 \leq$$

$$\leq ||\,(\rho_K - \rho_{U_K}) \otimes \rho_{K_1E_1} \otimes \rho_{K_2E_2}||_1 +$$

$$+||\,(\rho_{K_1E_1} - \rho_{U_1} \otimes \rho_{E_1}) \otimes \rho_{U_K} \otimes \rho_{K_2E_2}||_1 + ||\,(\rho_{K_2E_2} - \rho_{U_2} \otimes \rho_{E_2}) \otimes \rho_{U_1} \otimes \rho_{U_K} \otimes \rho_{E_1}||_1 =$$

$$= ||\rho_K - \rho_{U_K}||_1 + ||\rho_{K_1E_1} - \rho_{U_1} \otimes \rho_{E_1}||_1 + ||\rho_{K_2E_2} - \rho_{U_2} \otimes \rho_{E_2}||_1 <$$

$$< \varepsilon_K + \varepsilon_1 + \varepsilon_2.$$

Вероятность успешного различения двух ситуаций - реальной и идеальной ситуациями после проталкивания (одноразовый блокнот)
(мало полезно для криптографии, ничего не говорит о том как изменится трудоемкость по поиску согласованного/протолкнутого ключа).
Нужно перейти от квантовых состояний к распределениям вероятностей

$$\Pr_{OK} = \frac{1}{2}\left(1 + \frac{1}{2}\|\rho_K \otimes \rho_{K_1E_1} \otimes \rho_{K_2E_2} - \rho_{U_K} \otimes (\rho_{U_1} \otimes \rho_{E_1}) \otimes (\rho_{U_2} \otimes \rho_{E_2})\|_1\right) \leq$$

$$\leq \frac{1}{2}\left(1 + \frac{1}{2}(\varepsilon_K + \varepsilon_1 + \varepsilon_2)\right).$$

Связь следового расстояния для квантовых состояний и классических распределений вероятностей

$$\rho_{KK_1K_2E_1E_2C_1C_2} =$$

$$= \sum_{k\in\{0,1\}^n} \sum_{k_{p_1}\in\{0,1\}^n} \sum_{k_{p_2}\in\{0,1\}^n} P_K(k)P_{K_1}(k\oplus k_{p_1})P_{K_2}(k\oplus k_{p_2})|k\rangle_{KK}\langle k|\otimes$$

$$\otimes \left(|k\rangle_{K_1K_1}\langle k| \otimes \rho_{E_1}^{k\oplus k_{p_1}}\right) \otimes \left(|k\rangle_{K_2K_2}\langle k| \otimes \rho_{E_2}^{k\oplus k_{p_2}}\right) \otimes \left(|k_{p_1}\rangle_{C_1C_1}\langle k_{p_1}|\right) \otimes \left(|k_{p_2}\rangle_{C_2C_2}\langle k_{p_2}|\right).$$

Построим измерение, которое дает распределение вероятностей. Измерение задается разложением единицы в пространстве $KE_1E_2C_1C_2$,

$$I_{KK_1K_2E_1E_2C_1C_2} = \sum_{k\in\{0,1\}^n} \sum_{k_{p_1}\in\{0,1\}^n} \sum_{k_{p_2}\in\{0,1\}^n} \sum_{y\in\{0,1\}^{2n}} \mathcal{F}_{KK_1K_2E_1E_2C_1C_2} =$$

$$= \sum_{k\in\{0,1\}^n} \sum_{k_{p_1}\in\{0,1\}^n} \sum_{k_{p_2}\in\{0,1\}^n} \sum_{y\in\{0,1\}^{2n}} (|k\rangle_{KK}\langle k|) \otimes (|k\rangle_{K_1K_1}\langle k|) \otimes (|k\rangle_{K_2K_2}\langle k|) \otimes$$

$$\otimes (|k_{p_1}\rangle_{C_1C_1}\langle k_{p_1}|) \otimes (|k_{p_2}\rangle_{C_2C_2}\langle k_{p_2}|) \otimes \mathcal{M}^y_{E_1E_2}.$$

Вероятность есть

$$P_{KK_1K_2YC_1C_2}(k, y, k_{p_1}, k_{p_2}) = \mathrm{Tr}_{KK_1K_2YC_1C_2}\left\{\rho_{KK_1K_2E_1E_2C_1C_2}\, \mathcal{F}_{KK_1K_2E_1E_2C_1C_2}\right\} =$$

$$= P_K(k)P_{K_1}(k\oplus k_{p_1})P_{K_2}(k\oplus k_{p_2})\mathrm{Tr}_{E_1E_2}\left\{\left(\rho_{E_1}^{k\oplus k_{p_1}} \otimes \rho_{E_2}^{k\oplus k_{p_2}}\right)\mathcal{M}^y_{E_1E_2}\right\}.$$

Сделаем комментарии по поводу обозначений. Функция распределения вероятностей $P_{KK_1K_2YC_1C_2}(k, y, k_{p_1}, k_{p_2})$ после измерений является функцией четырех случайных величин (k, y, k_{p_1}, k_{p_2}), где введены обозначения, привязывающие случайные величины к соответствующим множествам $y \in Y = \{0,1\}^{2n}$, $k_{p_1} \in C_1 = \{0,1\}^n$, $k_{p_2} \in C_2 = \{0,1\}^n$, последнее обозначение $k \in KK_1K_2 = \{0,1\}^n$ символизирует и напоминает тот факт, что внешний ключ k шифруется на ключах k_1, k_2 на двух сегментах.

После проталкивания ключа распределение вероятностей после измерения над матрицей плотности, отвечающей идеальной ситуации, имеет вид

$$P_{U_KU_1U_2YC_1C_2}(k, y, k_{p_1}, k_{p_2}) = \mathrm{Tr}_{KK_1K_2YC_1C_2}\left\{\rho_{U_KU_{K_1}U_{K_2}E_1E_2C_1C_2}\,\mathcal{F}_{KK_1K_2E_1E_2C_1C_2}\right\} =$$

$$= \frac{1}{N^2}\mathrm{Tr}_{E_1E_2}\{\mathcal{M}^y_{E_1E_2}(\rho_{E_1}\otimes\rho_{E_2})\} = \frac{1}{N^2}P_Y(y).$$

$$\sum_{k\in\{0,1\}^n}\sum_{y\in\{0,1\}^{2n}}\sum_{k_{p_1}\in\{0,1\}^n}\sum_{k_{p_2}\in\{0,1\}^n}|P_{KK_1K_2YC_1C_2}(k,y,k_{p_1},k_{p_2})-\frac{1}{N^3}P_Y(y)|=$$

$$=\sum_{k\in\{0,1\}^n}\sum_{y\in\{0,1\}^{2n}}\sum_{k_{p_1}\in\{0,1\}^n}\sum_{k_{p_2}\in\{0,1\}^n}|\mathrm{Tr}\{\mathcal{F}_{k,y,k_{p_1},k_{p_2}}(\rho_{KK_1K_2E_1E_2C_1C_2}-\rho_{U_KU_{K_1}U_{K_2}E_1E_2C_1C_2})\}|\leq$$

$$\leq\sum_{k\in\{0,1\}^n}\sum_{y\in\{0,1\}^{2n}}\sum_{k_{p_1}\in\{0,1\}^n}\sum_{k_{p_2}\in\{0,1\}^n}\mathrm{Tr}\{\mathcal{F}_{k,y,k_{p_1},k_{p_2}}|(\rho_{KK_1K_2E_1E_2C_1C_2}-\rho_{U_KU_{K_1}U_{K_2}E_1E_2C_1C_2})|\}=$$

$$=\mathrm{Tr}\{\left(\sum_{k\in\{0,1\}^n}\sum_{y\in\{0,1\}^{2n}}\sum_{k_{p_1}\in\{0,1\}^n}\sum_{k_{p_2}\in\{0,1\}^n}\mathcal{F}_{k,y,k_{p_1},k_{p_2}}\right)|(\rho_{KK_1K_2E_1E_2C_1C_2}-\rho_{U_KU_{K_1}U_{K_2}E_1E_2C_1C_2})|\}=$$

$$=\mathrm{Tr}\{I_{KK_1K_2E_1E_2C_1C_2}|(\rho_{KK_1K_2E_1E_2C_1C_2}-\rho_{U_KU_{K_1}U_{K_2}E_1E_2C_1C_2})|\}=$$

$$=||(\rho_{KK_1K_2E_1E_2C_1C_2}-\rho_{U_KU_{K_1}U_{K_2}E_1E_2C_1C_2})||_1=$$

$$=||\left(\rho_K\otimes\rho_{K_1E_1}\otimes\rho_{K_2E_2}-\rho_{U_K}\otimes\left(\rho_{U_1}\otimes\rho_{E_1}\right)\otimes\left(\rho_{U_2}\otimes\rho_{E_2}\right)\right)||_1<$$

$$<\varepsilon_K+\varepsilon_1+\varepsilon_2.$$

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.

В квантовой криптографии побочной информацией для подслушивателя является вся совокупность информации о ключах, полученная как из квантового, так и классического каналов.

Тот факт, что математический аппарат при доказательстве секретности ключей в классической и квантовой криптографии существенно отличается, приводит к недопониманию и эмоциональным дискуссиям. Поэтому необходимо уметь отвечать на вопрос как связаны между собой различные критерии криптостойкости.

Показана прямая связь между критерием секретности в квантовой криптографии, основанном на следовом расстоянии, определяющим различимость квантовых состояний, и критерием, использующим трудоемкость по определению ключа при наличии побочной информации, в классической криптографии.

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.

Пусть упорядочение условных вероятностей *при заданных* (y_i, k_{p_1}, k_{p_2}) есть

$$P_{KK_1K_2|YC_1C_2}(k_{1(y_i,k_{p_1},k_{p_2})})|y_i,k_{p_1},k_{p_2}) \geq P_{KK_1K_2|YC_1C_2}(k_{2(y_i,k_{p_1},k_{p_2})})|y_i,k_{p_1},k_{p_2}) \ldots \geq$$

$$\geq P_{KK_1K_2|YC_1C_2}(k_{M(y_i,k_{p_1},k_{p_2})})|y_i,k_{p_1},k_{p_2}).$$

было показано, что трудоемкость $(G(K|YC_1C_2,M))$ частичного перебора с заданной вероятностью успеха (π_0) при наличии побочной информации (y,k_{p_1},k_{p_2}) имеет вид

$$Q(K|YC_1C_2,\pi_0) = \min_{\{M:\pi(M)\geq\pi_0\}} G(K|YC_1C_2,M) \geq \left(1-\frac{2\delta}{\pi_0}\right)\left(\frac{N(1-8\delta)+1}{2}\right),$$

где величина δ имеет вид

$$\delta = \sum_{m=1}^{N} |p(m) - \frac{1}{N}|,$$

введено обозначение

$$p(m) = \sum_{k_{p_1}\in\{0,1\}^n}\sum_{k_{p_2}\in\{0,1\}^n}\sum_{y\in\{0,1\}^{2n}} P_{YC_1C_2}(y,k_{p_1},k_{p_2})P_{KK_1K_2|YC_1C_2}(k(m)|y,k_{p_1},k_{p_2}) =$$

$$= \sum_{k_{p_1}\in\{0,1\}^n}\sum_{k_{p_2}\in\{0,1\}^n}\sum_{y\in\{0,1\}^{2n}} P_{KK_1K_2YC_1C_2}(k(m),y,k_{p_1},k_{p_2}),$$

данная вероятность зависит только от номера шага опробования m.

$$\delta = \sum_{m=1}^{N} |p(m) - \frac{1}{N}| =$$

$$= \sum_{m=1}^{N} \Bigg| \sum_{k_{p1} \in \{0,1\}^n} \sum_{k_{p2} \in \{0,1\}^n} \sum_{y \in \{0,1\}^{2n}} \Big(P_{Y C_1 C_2}(y, k_{p_1}, k_{p_2}) P_{K K_1 K_1 | Y C_1 C_2}(k(m) | y, k_{p_1}, k_{p_2}) -$$

$$- \frac{1}{N} P_{Y C_1 C_2}(y, k_{p_1}, k_{p_2}) \Big) \Bigg| =$$

$$= \sum_{m=1}^{N} \Bigg| \sum_{k_{p1} \in \{0,1\}^n} \sum_{k_{p2} \in \{0,1\}^n} \sum_{y \in \{0,1\}^{2n}} \Big(\Big(P_{K K_1 K_1 Y C_1 C_2}(k(m), y, k_{p_1}, k_{p_2}) - \frac{1}{N^3} P_Y(y) \Big) -$$

$$- \frac{1}{N} \Big(P_{Y C_1 C_2}(y, k_{p_1}, k_{p_2}) - \frac{1}{N^2} P_Y(y) \Big) \Big) \Bigg| \leq$$

$$\leq \sum_{m=1}^{N} \sum_{k_{p1} \in \{0,1\}^n} \sum_{k_{p2} \in \{0,1\}^n} \sum_{y \in \{0,1\}^{2n}} \Big| P_{K K_1 K_1 Y C_1 C_2}(k(m), y, k_{p_1}, k_{p_2}) - \frac{1}{N^3} P_Y(y) \Big| =$$

$$= \sum_{k \in \{0,1\}^n} \sum_{k_{p1} \in \{0,1\}^n} \sum_{k_{p2} \in \{0,1\}^n} \sum_{y \in \{0,1\}^{2n}} \Big| P_{K K_1 K_1 Y C_1 C_2}(k_1, y, k_{p_1}, k_{p_2}) - \frac{1}{N^3} P_Y(y) \Big| <$$

$$< \varepsilon_K + \varepsilon_1 + \varepsilon_2.$$

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

$$Q(K|YC_1C_2,\pi_0) = \min_{\{M:\pi(M)\geq\pi_0\}} G(K|YC_1C_2,M) \geq$$

$$\geq \left(1-\frac{2\delta}{\pi_0}\right)\left(\frac{N(1-8\delta)+1}{2}\right)$$

$$\delta < \varepsilon_K + \varepsilon_1 + \varepsilon_2.$$

СПАСИБО ЗА ВНИМАНИЕ.