Practical secrecy of a key under individual attack in quantum cryptography

I.M. Arbekov

Practical secrecy

Let $\kappa \in \{1,\dots,\mathrm{N}\}$ be the random key, $z \in Z$ - random observation, $P(m,z)$ - the joint probability distribution,

$$P\left(i_1(z)\middle|z\right) \geq \dots \geq P\left(i_M(z)\middle|z\right) \geq \dots \geq P\left(i_N(z)\middle|z\right)$$

- the ordered posterior probability distribution of keys,

$\left(i_1(z),\dots,i_N(z)\right)$ - a some permutation of $\{1,\dots,N\}$

Truncated algorithm U : M keys are being tested in the order

$$\left(i_1(z),i_2(z),\dots,i_M(z)\right) = K_z(M)$$

Practical secrecy of a key

Probability of *success:* $\pi_U^*(M) = P(\kappa \in K_z(M)) = \sum_{m=1}^{M} p_m^*,$

$p_m^* = \sum_{z \in Z} P(i_m(z)|z)P(z).$ Restriction: $\pi_U^*(M) \geq \pi_0$

The average amount of work to determine the *encryption* key

$$\overline{R}_U^*(M) = \frac{S_U^* \cdot T}{\pi_U^*(M) \cdot T} = \frac{\left(1-\pi_U^*(M)\right)M + \pi_U^*(M)\sum_{m=1}^{M} m \frac{p_m^*}{\pi_U^*(M)}}{\pi_U^*(M)} =$$

$$= \frac{1-\pi_U^*(M)}{\pi_U^*(M)}M + \sum_{m=1}^{M} m \frac{p_m^*}{\pi_U^*(M)},$$

$\frac{1-\pi_U^*(M)}{\pi_U^*(M)}$ - the expectation of *steps* before the first *success*,

$\sum_{m=1}^{M} m \frac{p_m^*}{\pi_U^*(M)}$ - the expectation of number of keys tested on condition $\kappa \in K_z(M)$

Practical secrecy of a key

The *practical secrecy* of a key: $Q^* = \min\limits_{M:\pi_U^*(M)\geq\pi_0} \bar{R}_U^*(M) \leq \frac{N+1}{2}$

The *total variation distance:*

$$d = \frac{1}{2}\sum_{m,z}\left|P(m,z) - \frac{1}{N}P(z)\right| = \sum_{z\in Z}P(z)\left(\frac{1}{2}\sum_{m=1}^{N}\left|P(m|z) - \frac{1}{N}\right|\right)$$

We have proved the inequality (CTCrypt 2016)

$$Q^* \geq \left(1 - \frac{2d}{\pi_0}\right)\left(\frac{N(1-8d)+1}{2}\right)$$

It is interesting to include the point $M = 0$ in the set of keys to be tested. This is the case when *keys are not tested* for some observations.

Practical secrecy of a key

Let $D \subseteq Z$ be some region of observations, $P(\eta \in D) = P(D)$. The algorithm U is that we wait until an event $z \in D$ occurs, then we arrange the keys and use the *exhaustive* key search algorithm.

Probability of *success* $P(D)$, the *practical secrecy* of a key

$$q^* = \min_{D:P(D)\geq\pi_0} \bar{R}_U^*(D), \qquad \bar{R}_U^*(D) = \sum_{z\in D} \frac{P(z)}{P(D)} \left(\sum_{m=1}^{N} mP\left(i_m(z)\middle|z\right) \right)$$

$$q^* \geq \left(1 - \frac{4d}{\pi_0}\right) \frac{N+1}{2}$$

In general (*the advertised result*)

$$Q^* = \min_{M,D:\ \pi_U^*(M,D)\geq\pi_0} \bar{R}_U^*(M,D) \geq \left(1 - \frac{2d}{\pi_0}\right) \left(\frac{N\left(1 - 8d/\pi_0\right) + 1}{2} \right)$$

Individual attack in quantum cryptography

1. QKD protocol BB84:

$$R-basis: w\in\{0,1\}\Rightarrow|\varphi\rangle\in\{|0\rangle,|1\rangle\},$$

$$D-basis: w\in\{0,1\}\Rightarrow|\varphi\rangle\in\left\{\frac{|0\rangle+|1\rangle}{\sqrt{2}},\frac{|1\rangle-|0\rangle}{\sqrt{2}}\right\}$$

2. Individual attack :

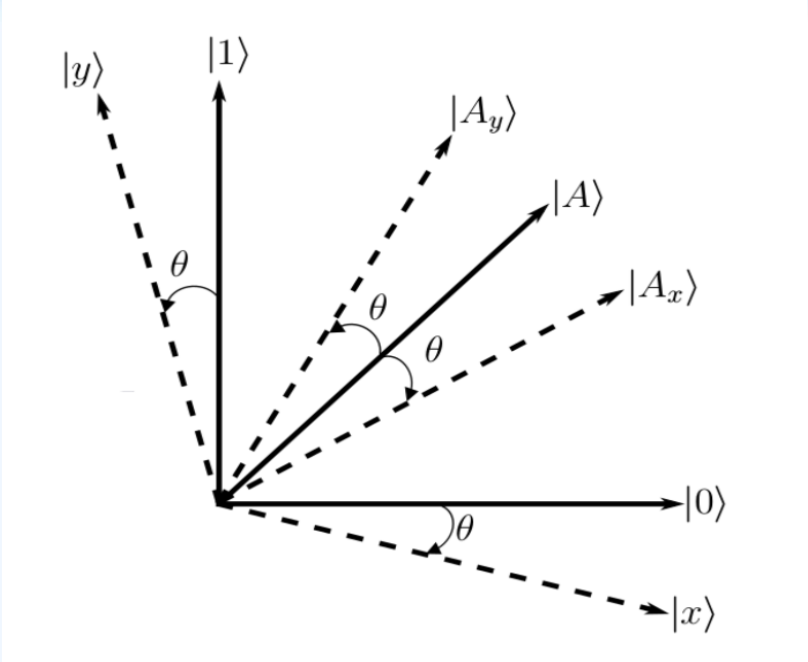
$$W^A=\left(w_1^A,\dots,w_L^A\right),\qquad W^B=\left(w_1^B,\dots,w_L^B\right)$$

$W^E=\left(w_1^E,\dots,w_L^E\right)$ - bit strings of Alice, Bob and Eve.

Probability of error:

$$p_{AB}=P\left(w_i^A\neq w_i^B\right),\qquad p_{AE}=P\left(w_i^A\neq w_i^E\right)$$

Individual attack in quantum cryptography



Mechanism of individual attack ($R-basis$), $|A\rangle$ - Eve's ancilla (quantum memory)

$$p_{AE}=\frac{1}{2}-\frac{1}{2}\sqrt{1-\left(\langle A_x|A_y\rangle\right)^2}=\frac{1}{2}-\frac{1}{2}\sqrt{1-\cos^2(2\theta)},$$

$$p_{AB}=\frac{1}{2}-\frac{1}{2}\sqrt{1-\left(\langle x|y\rangle\right)^2}=\frac{1}{2}-\frac{1}{2}\sqrt{1-\sin^2(2\theta)},$$

$$p_{AE}=\frac{1}{2}-\frac{1}{2}\sqrt{p_{AB}(1-p_{AB})}$$

Individual attack in quantum cryptography

3. Reconciliation procedure:

block partitioning, parity checking in blocks, deleting part of the bits,

$W \in \{0,1\}^S$ - common bit string ,

$S = L - s,$ s - the number of bits to be deleted.

4. Privacy amplification:

$W \in \{0,1\}^S \xrightarrow{g(W)} \kappa \in \{0,1\}^n$ - final key, g – random function.

$G = \left\{ g : \{0,1\}^S \to \{0,1\}^n \right\}$ - *2-universal* set of functions:

$W_1 \neq W_2,$ $P\Big(g\big(W_1\big) = g\big(W_2\big)\Big) \leq 2^{-n}$

Individual attack in quantum cryptography

An example:

$g \in GF\left(2^S\right)$, $W \in \{0,1\}^S$ is interpreted as an element $GF\left(2^S\right)$,

then $\kappa \in \{0,1\}^n$ - the first *n* bits of $g \cdot W \in GF\left(2^S\right)$.

Before amplification:

$P\left(W / W^E\right)$, $W \in \{0,1\}^S$ - posterior distribution,

$$R\left(\mathbf{W} / W^E\right) = -\log_2\left(\sum_W \left[P\left(W / W^E\right)\right]^2\right)$$ - conditional Renyi entropy,

$$\overline{R}\left(\mathbf{W} / \mathbf{W}^E\right) = -\log_2 \mathbf{E}_{W^E}\left(\sum_W \left[P\left(W / W^E\right)\right]^2\right)$$

- average conditional Renyi entropy

Individual attack in quantum cryptography

After amplification:

Generalized Leftover Hash/Privacy Amplification Lemma

$$\frac{1}{2}\sum_{W,g,W^E}\left|P\left(g(W),\left(g,W^E\right)\right)-2^{-n}P\left(g,W^E\right)\right|\le$$

$$\le\frac{1}{2}\sqrt{\exp_2\left\{-\bar{R}\left(\mathbf{W}/\mathbf{W}^E\right)+n\right\}},$$

$g\left(W\right)=m\in\left\{1,\dots,N\right\}, N=2^n$ - key set,

$\left(g,W^E\right)=z\in Z$ - observations

Individual attack in quantum cryptography

$$d = \frac{1}{2}\sum_{m,z}\left|P(m,z) - \frac{1}{N}P(z)\right| \le \frac{1}{2}\sqrt{\exp_2\left\{-\bar{R}\left(\mathbf{W} / \mathbf{W}^E\right) + n\right\}}$$

We have:

$$\bar{R}\left(\mathbf{W} / \mathbf{W}^E\right) \ge \bar{R}\left(\mathbf{W}^A / \mathbf{W}^E\right) - s$$

$$W^E = W^A \oplus \tau,\ \tau = \left(\tau_1, .., \tau_L\right) - i.i.d,\ P\left(\tau_i = 1\right) = p_{AE},$$ then

$$\bar{R}\left(\mathbf{W}^A / \mathbf{W}^E\right) = -\log_2 \sum_{\tau \in \{0,1\}^L} P^2(\tau) = -L\log\left(p_{AE}^2 + \left(1 - p_{AE}\right)^2\right),$$

$$d \le \frac{1}{2}\sqrt{\exp_2\left(L\log\left(p_{AE}^2 + \left(1 - p_{AE}\right)^2\right) + s + n\right)}$$

Individual attack in quantum cryptography

Example:

$$n = 256, \quad p_{AB} = 5\%, \quad p_{AE} = \frac{1}{2} - \sqrt{p_{AB}\left(1 - p_{AB}\right)} = 0.282, \quad L = 1500,$$

$$s \approx L/2 = 750, \quad S \approx 750, \quad d < 10^{-15},$$

$$Q^* \geq \left(1 - \frac{2d}{\pi_0}\right)\frac{N\left(1 - 8d/\pi_0\right) + 1}{2} \approx \frac{N+1}{2}$$

The end