Elementary quantum cryptography

Igor Arbekov

JSC «InfoTeCS», LLC «SFB Lab»

CTCrypt 2020

September 17, 2020

igor.arbekov@sfblaboratory.ru

The Purpose of Quantum Cryptography

... is to *provide* Alice and Bob with a *secret* keys.

The Purpose of Quantum Cryptography

... is to *provide* Alice and Bob with a *secret* keys.

1. Transmission:
   – bit as quantum state transfers through an optical QC

The Purpose of Quantum Cryptography

... is to *provide* Alice and Bob with a *secret* keys.

1. Transmission:

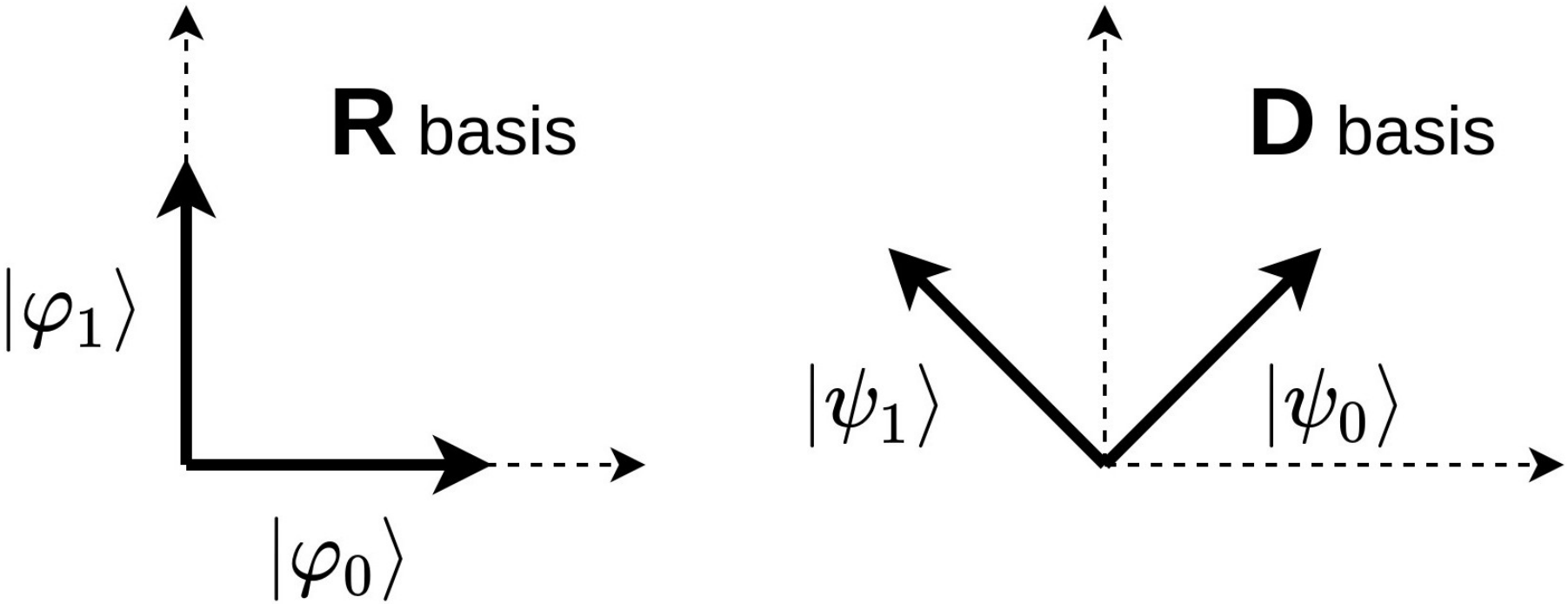
   – bit as quantum state transfers through an optical QC

2. Security:

   – the «**no cloning theorem**» $\Rightarrow$ physically impossible to make a perfect copy of an unknown quantum state

   – the **Heisenberg uncertainty principle** $\Rightarrow$ by measuring an unknown quantum-mechanical state, it is physically changed

BB84


R basis
$|\varphi_1\rangle$
$|\varphi_0\rangle$
D basis
$|\psi_1\rangle$
$|\psi_0\rangle$

BB84

Alice, **R** – basis, $0 \to |\varphi_0\rangle\,, 1 \to |\varphi_1\rangle$,

Bob, **R** – basis,

$$|\varphi_0\rangle \to \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \begin{matrix} \textit{Bob bit} \\ \textit{prob} \end{matrix} \quad ,|\varphi_1\rangle \to \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$$

Alice, **D** – basis, $0 \to |\psi_0\rangle\,, 1 \to |\psi_1\rangle$,

Bob, **R** – basis,

$$|\psi_0\rangle \sim \begin{pmatrix} 0 & 1 \\ 1/2 & 1/2 \end{pmatrix} \quad \begin{matrix} \textit{bit} \\ \textit{prob} \end{matrix} \quad ,|\psi_1\rangle \sim \begin{pmatrix} 0 & 1 \\ 1/2 & 1/2 \end{pmatrix}$$

Alice and Bob save bits with matching bases

Intercept-resend strategy

N. Gisin et al.

Quantum cryptography

Reviews of modern physics, v. 74, 2002

Alice – Bob, $Q = 25\%$ (Quantum Bit Error Rate – QBER)

Alice – Eve, $Q_E = 25\%$

Intercept-resend strategy

Alice – Bob, $Q = 25\%$ (Quantum Bit Error Rate – QBER)

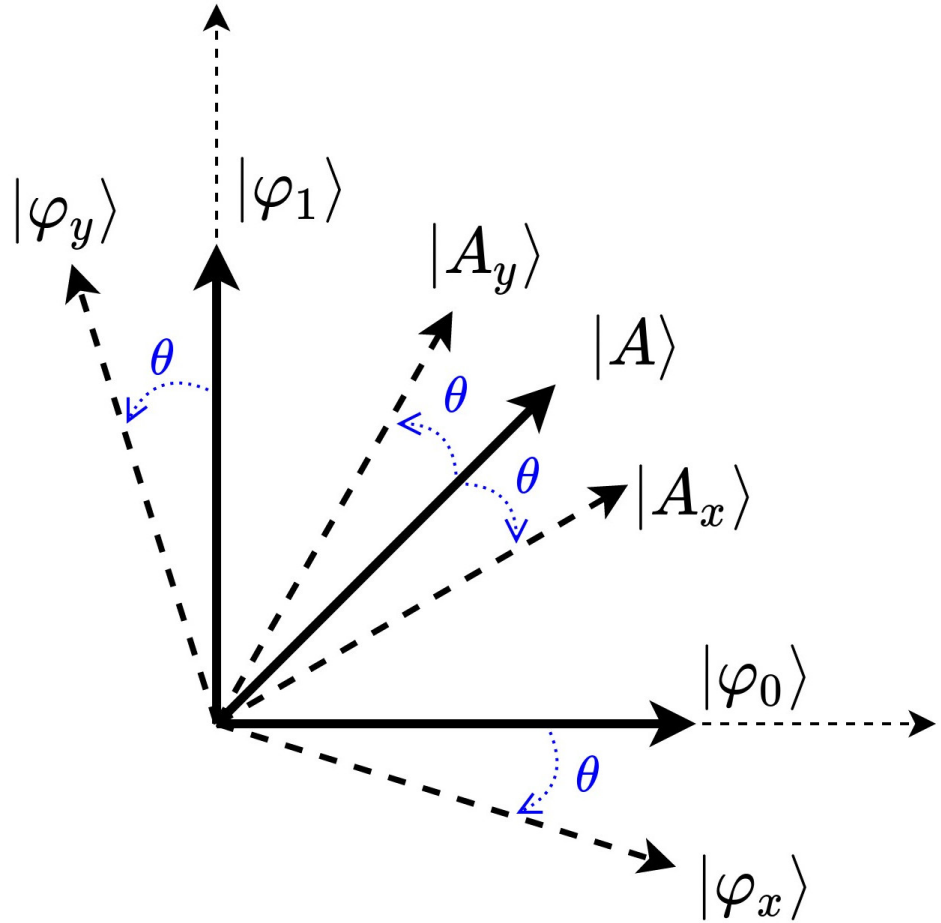
Alice – Eve, $Q_E = 25\%$

M. Christandl, R. Renner, A. Ekert, 2004: *«Quantum key distribution provides perfect security because, unlike its classical counterpart, it relies on the laws of physics».*

Individual attack

$Q \approx 5\%$ due to imperfection of a *real* QC.

ETSI GS QKD 005 V1.1.1 (2010-12). **Individual attack**



Individual attack

Bob:

$$|\varphi_y\rangle \sim \begin{pmatrix} 0 & 1 \\ p_y^{(0)} & p_y^{(1)} \end{pmatrix}, |\varphi_x\rangle \sim \begin{pmatrix} 0 & 1 \\ p_x^{(0)} & p_x^{(1)} \end{pmatrix}, \; Q = \frac{1}{2} - \frac{1}{2}\cos(2\theta)$$

Eve:

$$|A_y\rangle \sim \begin{pmatrix} 0 & 1 \\ q_y^{(0)} & q_y^{(1)} \end{pmatrix}, |A_x\rangle \sim \begin{pmatrix} 0 & 1 \\ q_x^{(0)} & q_x^{(1)} \end{pmatrix}, \; Q_E = \frac{1}{2} - \frac{1}{2}\sin(2\theta)$$

$$Q_E = \frac{1}{2} - \sqrt{Q(1-Q)}, Q = 5\%, Q_E \approx 28.2\%$$

Individual attack

Binary symmetric channels.

Alice: $x = (x_1, \ldots, x_L)$,

Bob: $y = (y_1, \ldots, y_L), y_i = x_i \oplus \tau_i, \Pr(\tau_i = 1) = Q$,

Eve: $u = (u_1, \ldots, u_L), u_i = x_i \oplus \tau_i^E, \Pr(\tau_i^E = 1) = Q^E$.

Alice-Bob: Error Correction (Reconciliation)

Alice sends

$$b = (b_1, \ldots, b_C) = xH, C < L,$$

over the public channel.

H – some special matrix (LDPC - correcting code).

Bob computes $b' = yH$, changes y_i-bits so that $b' = b$.

Errors corrected.

Alice-Bob: Error Correction (Reconciliation)

What is the C value?

Let $x \in \{0,1\}^L$ – entry, $(y, b) \in \{0,1\}^{L+C}$ – output,

$y_i = x_i \oplus \tau_i$, Q, $b = xH \in \{0,1\}^C$.

$\mathbb{C} = \max_{P_X(x)} \left(H(\boldsymbol{y}, \boldsymbol{b}) - H(\boldsymbol{y}, \boldsymbol{b} \,|\boldsymbol{x})\right)$ – capacity.

$$H(\boldsymbol{y}, \boldsymbol{b}) \leq H(\boldsymbol{y}) + H(\boldsymbol{b}) \leq L + C.$$

$$H(\boldsymbol{y}, \boldsymbol{b} \,|\boldsymbol{x}) = H(\boldsymbol{y} \,|\boldsymbol{x}) = H(\boldsymbol{\tau}) = L \cdot h(Q)$$

If $2^L \leq 2^{\mathbb{C}}$ or (requirement) $L < L + C - L \cdot h(Q)$,

then $Q_{\text{decod}} \to 0$, hence $C \geq L \cdot h(Q)$.

LDPC

$C = L \cdot f \cdot h(Q)$, $f \approx 1.1 \div 1.2$

Hash functions. Privacy Amplification

Hash function

$$g(x) = k$$

$$g : \{0,1\}^L \to \{0,1\}^n, L > n$$

Two-universal family of hash functions

$$g \in G, P_G(g) = \frac{1}{|G|},\ x_1, x_2 \in \{0,1\}^L, x_1 \neq x_2$$

$$\Pr(\boldsymbol{g}(x_1) = \boldsymbol{g}(x_2)) = \sum_{a \in \{0,1\}^n} \Pr(\boldsymbol{g}(x_1) = a,\ \boldsymbol{g}(x_2) = a) = 2^{-n}.$$

Example:

$x = (x_1, \ldots, x_L) \in \{0,1\}^L : x \leftrightarrow w \in GF\left(2^L\right)$,

$g * w = w' \in GF\left(2^L\right) \leftrightarrow x' = (x'_1, ..., x'_n, ..., x'_L) \to (x'_1, ..., x'_n) \in \{0,1\}^n$

Entropy secrecy criterion

Bennett C., Brassard G., Crepeau C.

Generalized Privacy Amplification

IEEE Trans. Inf. Th. 1995

Probability space

$$g \in G, P_G(g) = 1/|G|$$

$$x \in \{0,1\}^L, P_X(x) = 2^{-L}$$

$$v = \left(u = x \oplus \tau^E, b = xH\right) \in V$$

$$P_V(v), P_{X|V}(x|v), k = g(x)$$

Entropy secrecy criterion

Second-order conditional Renyi entropy

$$H(\boldsymbol{k}|\boldsymbol{g},\boldsymbol{v}) =$$

$$= \sum_{v\in V} P_V(v) \sum_{g\in G} P_G(g) \left(- \sum_{a\in\{0,1\}^n} \Pr\left(g(\boldsymbol{x}) = a \,|\, \boldsymbol{v} = v\right) \log \Pr\left(g(\boldsymbol{x}) = a \,|\, \boldsymbol{v} = v\right) \right)$$

$$\geq n - \frac{2^n}{\ln 2} \sum_v P_V(v) \sum_x \left(P_{X|V}(x|v)\right)^2 = n - \frac{2^{n-R(\boldsymbol{x}|\boldsymbol{v})}}{\ln 2}$$

$$R(\boldsymbol{x}|\boldsymbol{v}) = -\log \sum_v P_V(v) \sum_x \left(P_{X|V}(x|v)\right)^2$$

Entropy secrecy criterion

Second-order conditional Renyi entropy

Let $v = u = x \oplus \tau^E$, then

$$R(\boldsymbol{x}|\boldsymbol{u}) = -\log \sum_u P_U(u) \sum_x \left(P_{X|U}(x|u)\right)^2 =$$

$$= -\log \sum_u P_U(u) \sum_m \binom{L}{m} (1-Q_E)^{2m} Q_E^{2(L-m)} =$$

$$= -L \log \left((1-Q_E)^2 + Q_E^2\right) \to \infty$$

But $v = \left(u = x \oplus \tau^E, b = xH\right)$, then ...

- ...how to evaluate $R(\boldsymbol{x}|\boldsymbol{u}, \boldsymbol{b})$?
- Also, is $H(\boldsymbol{k}|\boldsymbol{g}, \boldsymbol{v})$ good as a measure of secrecy?

ε-secrecy of the key

Leftover-Hash Lemma

J. Hastad et al.

A pseudorandom generator from any one-way function

SIAM Journal on Computing, 1999

Y. Dodis et al.

Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data

SIAM Journal on Computing, 2008

ε-secrecy of the key

Leftover-Hash Lemma

Probability space

$$g \in G, P_G(g) = 1/|G|, x \in \{0,1\}^L, P_X(x) = 2^{-L}$$

$$v = \left(u = x \oplus \tau^E, b = xH\right) \in V, P_V(v), P_{X|V}(x|v)$$

$$g(x) = k$$

ε-secrecy of the key

Leftover-Hash Lemma

Lemma 1

Statistical distance

$$SD\left(\left(\boldsymbol{g}\left(\boldsymbol{x}\right),\boldsymbol{v},\boldsymbol{g}\right),\left(\mathcal{O},\boldsymbol{v},\boldsymbol{g}\right)\right)=$$

$$=\frac{1}{2}\sum_{v\in V}\sum_{g\in G}\sum_{a\in\{0,1\}^n}\left|\Pr\left(g\left(\boldsymbol{x}\right)=a,\boldsymbol{v}=v,\boldsymbol{g}=g\right)-2^{-n}P_V\left(v\right)P_G\left(g\right)\right|=$$

$$=\frac{1}{2}\sum_{v\in V}P_V\left(v\right)\sum_{g\in G}P_G\left(g\right)\sum_{a\in\{0,1\}^n}\left|\Pr\left(g\left(\boldsymbol{x}\right)=a\left|\boldsymbol{v}=v\right.\right)-2^{-n}\right|\leq$$

$$\leq\frac{1}{2}\sqrt{\sum_{v}P_V\left(v\right)\sum_{x}\left(P_{X|V}\left(x|v\right)\right)^2 2^n}=$$

$$=\frac{1}{2}\sqrt{2^{-R(\boldsymbol{x}|\boldsymbol{v})+n}}$$

ε-secrecy of the key

Leftover-Hash Lemma

$$z = (g, v) \in Z, v = \left(u = x \oplus \tau^E, b = xH\right) \in V$$

$$k = g(x) \in K, |K| = 2^n = N$$

$$\frac{1}{2} \sum_{z \in Z} \sum_{k=1}^{N} \left| P_{KZ}(k, z) - \frac{1}{N} P_Z(z) \right| =$$

$$= \frac{1}{2} \sum_{z \in Z} P_Z(z) \sum_{k=1}^{N} \left| P_{K|Z}(k|z) - \frac{1}{N} \right| \leq \frac{1}{2} \sqrt{2^{-R(\boldsymbol{x}|\boldsymbol{v})+n}}$$

ε-secrecy of the key

Leftover-Hash Lemma

R. Renner

Security of Quantum Key Distribution

2006

Key k is ε-secure with respect to Z if

$$\frac{1}{2}\sum_{z\in Z}\sum_{k=1}^{N}\left|P_{KZ}(k,z)-\frac{1}{N}P_Z(z)\right|\leq\varepsilon.$$

$$\frac{1}{2}\sum_{z\in Z}\sum_{k=1}^{N}\left|P_{KZ}(k,z)-\frac{1}{N}P_Z(z)\right|\leq\frac{1}{2}\sqrt{2^{-R(\boldsymbol{x}|\boldsymbol{v})+n}}$$

The same problem: $v=\left(u=x\oplus\tau^E, b=xH\right)$.

How to take $\boldsymbol{b = xH}$ into account?

Min-entropy

$$H_{\min}(\boldsymbol{x}|\boldsymbol{v}) = -\log_2 \left(\max_{x,v \in (X,V)} P_{X|V}(x|v) \right), R(\boldsymbol{x}|\boldsymbol{v}) \geq H_{\min}(\boldsymbol{x}|\boldsymbol{v})$$

$$2^{-R(\boldsymbol{x}|\boldsymbol{u},\boldsymbol{b})} = \sum_{u,b} P_{UB}(u,b) \sum_{x} \left(P_{X|UB}(x|u,b) \right)^2 \leq$$

$$\leq \sum_{u,b} \max_{x} P_{XUB}(x,u,b) \leq 2^{C} \sum_{u} \max_{x} P_{XU}(x,u) \leq$$

$$\leq 2^{C} \sum_{u} \max_{x} P_{X|U}(x|u) P_U(u) \leq 2^{-(H_{\min}(\boldsymbol{x}|\boldsymbol{u})-C)}$$

Applying min-entropy

Lemma 2

$$\frac{1}{2}\sum_{z\in Z}\sum_{k=1}^{N}\left|P_{KZ}(k,z)-\frac{1}{N}P_Z(z)\right|\leq\frac{1}{2}\sqrt{2^{-(H_{\min}(\boldsymbol{x}|\boldsymbol{u})-C)+n}}$$

If $u=x\oplus\tau^E$ then

$$H_{\min}(\boldsymbol{x}|\boldsymbol{u})=-\log\max_{\tau}P_T(\tau)=-L\log(1-Q_E)\to\infty$$

$$C=L\cdot f\cdot h(Q),h(x)=-x\log x-(1-x)\log(1-x),f\approx 1.1$$

$$\frac{1}{2}\sum_{z\in Z}\sum_{k=1}^{N}\left|P_{KZ}(k,z)-\frac{1}{N}P_Z(z)\right|\leq\frac{1}{2}\sqrt{2^{-L(-\log(1-Q_E)-f\cdot h(Q))+n}}$$

ε-smooth min-entropy

$$\frac{1}{2}\sum_{z\in Z}\sum_{k=1}^{N}\left|P_{KZ}(k,z)-\frac{1}{N}P_Z(z)\right|$$

$$(\boldsymbol{K},\boldsymbol{Z})=(\boldsymbol{K},\boldsymbol{Z})_{\mathbf{1}}\bigcup(\boldsymbol{K},\boldsymbol{Z})_{\mathbf{2}}$$

$$\Pr\left((k,z)\in(\boldsymbol{K},\boldsymbol{Z})_{\mathbf{1}}\right)=1-\varepsilon$$

$$\frac{1}{2}\sum_{z\in Z}\sum_{k=1}^{N}\left|P_{KZ}(k,z)-\frac{1}{N}P_Z(z)\right|\leq$$

$$\leq\frac{1}{2}\sum_{(k,z)\in\boldsymbol{KZ_1}}\left|P_{KZ}(k,z)-\frac{1}{N}P_Z(z)\right|+\varepsilon$$

ε-smooth min-entropy

R. Renner, S. Wolf

Simple and Tight Bounds for Information Reconciliation and Privacy Amplification – ASIACRYPT 2005

$$H_{\min}^{\varepsilon}(\boldsymbol{x}|\boldsymbol{v}) = \max_{\Omega}\left(-\log\left(\max_{x,v} P_{\Omega X|V}(x|v)\right)\right)$$

$$\Pr\left((x,v):(x,v)\in\Omega\right) \geq 1-\varepsilon$$

$$P_{\Omega X|V}(x|v) = P_{\Omega|XV}(x,v)\,\frac{P_{XV}(x,v)}{P_V(v)}$$

$$P_{\Omega|XV}(x,v) = \begin{cases} 1 & x,v\in\Omega \\ 0 & x,v\notin\Omega \end{cases}$$

ε-smooth min-entropy

Maurer U., Renner R., Wolf S.

Unbreakable keys from random noise

Security with Noisy Data, 2007

Lemma 3

$$\frac{1}{2}\sum_{z\in Z}\sum_{k=1}^{N}\left|P_{KZ}(k,z)-\frac{1}{N}P_Z(z)\right| \leq \frac{1}{2}\sqrt{2^{-\left(H_{min}^{\varepsilon}(\boldsymbol{x}|\boldsymbol{u})-C\right)+n}}+\varepsilon$$

Applying ε-smooth min-entropy

Number of zeros

$$u = x \oplus \tau^E, Q_E$$

$$T(L_0) = \left\{ \tau^E : \text{ number of zeros} \leq L_0 \right\}$$

$$X(u, L_0) = \left\{ x : \ x = u \oplus \tau^E, \ \tau^E \in T(L_0) \right\}$$

$$\Omega = \left\{ (x, u) : \ u \in \{0,1\}^L, x \in X(u, L_0) \right\}$$

$$L_0 = L(1 - Q_E) + \chi_{1-\varepsilon} \sqrt{L Q_E (1 - Q_E)}$$

$$P(\Omega) = 1 - \varepsilon$$

Applying ε-smooth min-entropy

Final inequality

$$H_{\min}^{\epsilon}(\boldsymbol{x}|\boldsymbol{u}) = -\log \max_{(x,u)\in\Omega} P_{X|U}(x|u) =$$

$$= -\log (1-Q_E)^{L_0} Q_E^{L-L_0} = Lh(Q_E) + O\left(\sqrt{L}\right)$$

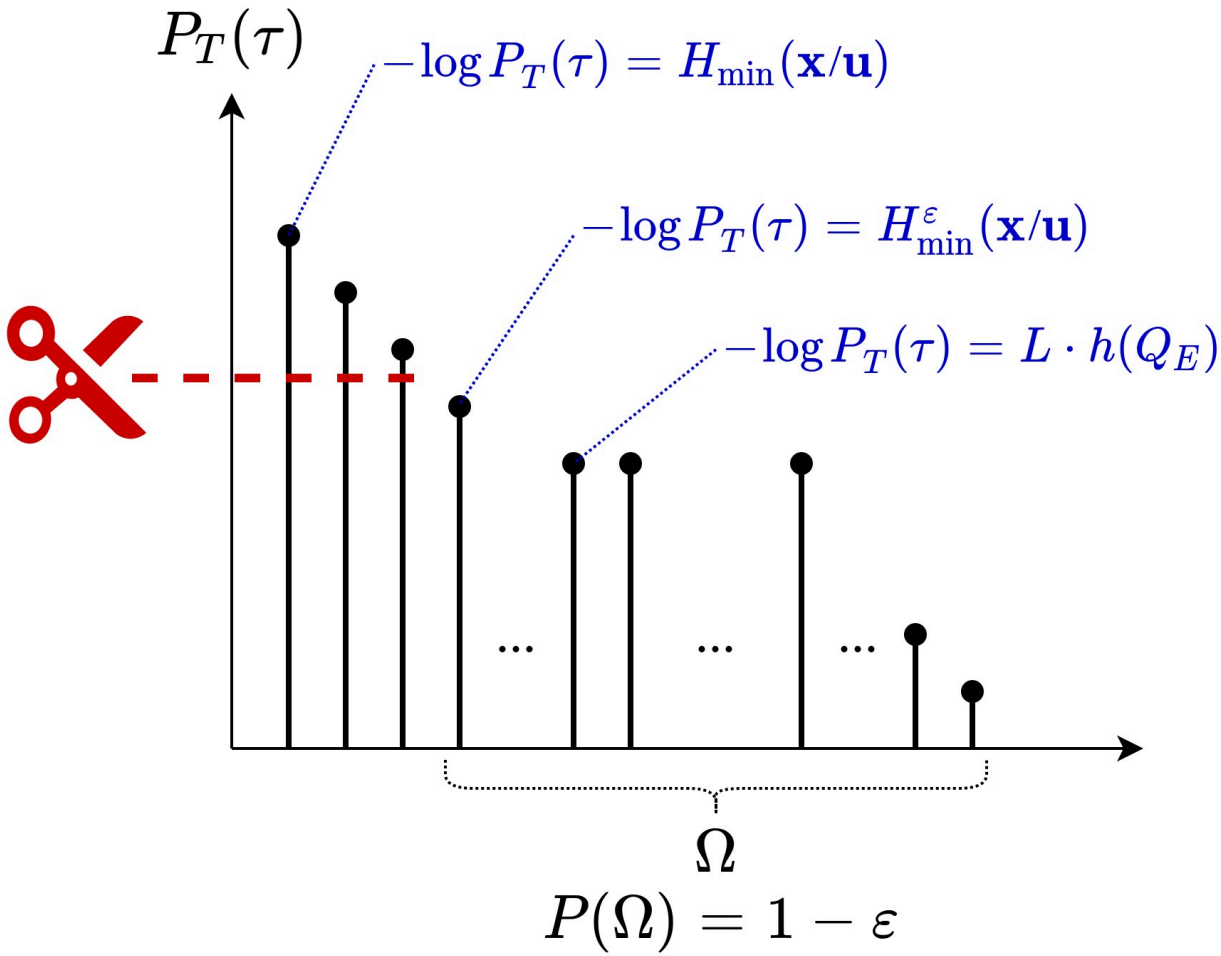
$$\frac{1}{2}\sum_{z\in Z}\sum_{k=1}^{N}\left|P_{KZ}(k,z) - \frac{1}{N}P_Z(z)\right| \leq$$

$$\leq \frac{1}{2}\sqrt{2^{-L(h(Q_E)-f\cdot h(Q)-\delta_L)+n}} + \varepsilon$$

$$\delta_L \approx \frac{1}{\sqrt{L}}$$

Applying ε-smooth min-entropy

Picture



Optimal attack

Quantum and classical leakage

We have

$$\frac{1}{2}\sum_{z\in Z}\sum_{k=1}^{N}\left|P_{KZ}(k,z)-\frac{1}{N}P_Z(z)\right|\leq\frac{1}{2}\sqrt{2^{-L(h(Q_E)-f\cdot h(Q)-\delta_L)+n}}+\varepsilon$$

We can rewrite

$$h(Q_E)-f\cdot h(Q)=1-[1-h(Q_E)]-f\cdot h(Q)$$

$1-h(Q_E)$ – quantum leakeage for Individual attack (per bit)

$f\cdot h(Q)$ – classic leakeage (per bit)

Optimal attack

M. Tomamichel, R. Renner

The Uncertainty Relation for Smooth Entropies – 2012

$$\frac{1}{2}\sum_{z\in Z}\sum_{k=1}^{N}\left|P_{KZ}(k,z)-\frac{1}{N}P_Z(z)\right| \leq \frac{1}{2}\sqrt{2^{-L\left(\frac{H_{\min}^{\varepsilon}(x|E)_q}{L}-f\cdot h(Q)\right)+n}}+\varepsilon$$

Uncertainty Relation

$$\frac{H_{\min}^{\varepsilon}(x|E)_q}{L}+\frac{H_{\max}^{\varepsilon}(x|y)}{L}\approx 1,$$

$$H_{max}^{\varepsilon}(x|y)=\min_{\Omega}\max_{y}\left(\log_2\left|\left\{x: P_{X\Omega|Y}(x|y)>0\right\}\right|\right)$$

$$\Pr(\Omega)\geq 1-\varepsilon$$

$$\frac{H_{\max}^{\varepsilon}(x|y)}{L}\approx h(Q),\ \frac{H_{\min}^{\varepsilon}(x|E)_q}{L}\approx (1-h(Q))$$

Optimal attack

Uncertainty Relation for Smooth Entropies

Quantum leak for **optimal** attack

$$1 - \frac{H_{\min}^{\varepsilon}(\boldsymbol{x}|\boldsymbol{E})_q}{L} \approx h(Q) = 0.286$$

Quantum leak for **individual** attack

$$1 - h(Q_E) = 0.142$$

ε-secrecy and complexity to determine the key

I.M. Arbekov, S.N. Molotkov

Distinguishability of Quantum States and Shannon Complexity in Quantum Cryptography,

Journal of Experimental and Theoretical Physics, 2017

I. M. Arbekov

Lower bounds for the practical secrecy of a key

Mat. Vopr. Kriptogr., № 2, 2017

$$\frac{1}{2}\sum_{z\in Z} P_Z(z)\sum_{k=1}^{N}\left|P_{K|Z}(k|z)-\frac{1}{N}\right|\leq\varepsilon$$

$$k\in\{1,2,...,N\},\ P_{K|Z}(k|z)$$

ε-secrecy and complexity to determine the key

Truncated algorithm U

$$P_{K|Z}\left(k_1\left(z\right)|z\right) \geq P_{K|Z}\left(k_2\left(z\right)|z\right) \geq \ldots \geq P_{K|Z}\left(k_M\left(z\right)|z\right)$$

$$\pi_U\left(M\right) = \sum_{z \in Z} P_Z\left(z\right) \sum_{m=1}^{M} P_{K|Z}\left(k_m\left(z\right)|z\right) = \sum_{m=1}^{M} \overline{p}_m$$

$$S_U\left(M\right) = \left(1 - \sum_{m=1}^{M} \overline{p}_m\right) M + \pi_U\left(M\right) \sum_{m=1}^{M} m \frac{\overline{p}_m}{\pi_U\left(M\right)}$$

$$Q_U\left(M\right) = \frac{S_U\left(M\right) \cdot T}{\pi_U\left(M\right) \cdot T} = \frac{\left(1 - \sum_{m=1}^{M} \overline{p}_m\right) M + \sum_{m=1}^{M} m \overline{p}_m}{\sum_{m=1}^{M} \overline{p}_m}$$

ε-secrecy and complexity to determine the key

$$Q_{\pi_0} = \min_{M:\pi_U(M)\geq\pi_0} Q_U(M) \geq \left(1 - \frac{\varepsilon}{\pi_0}\right) \frac{N(1-4\varepsilon)+1}{2}$$

Thank you for attention!