QKD secrecy for privacy amplification matrices with selective individual attacks

Matteo Canale, Francesco Renna, and Nicola Laurenti
Department of Information Engineering, University of Padua, via G. Gradenigo, 6/b, 35131 Padova, Italy.
E-mail: {canalema, frarenna, nil}@dei.unipd.it

A customary solution for the privacy amplification phase in practical QKD systems is to use randomly generated binary (Toeplitz) matrices [1]. Starting from the reconciled key $\boldsymbol{x} \in \{0,1\}^n$, the final key $\boldsymbol{k} \in \{0,1\}^s$ is thus obtained as $\boldsymbol{k} = \boldsymbol{A}\boldsymbol{x}$, for a given realization of the matrix $\boldsymbol{A} \in \{0,1\}^{s \times n}$. Since both the class of binary matrices and its Toeplitz subclass are universal$_2$, the bound in [2, Corollaries 4-5] holds, and is usually invoked to guarantee the security of the distilled key. However in such (and similar) bounds: 1) the eavesdropper is assumed to have learned exactly (or at most) t bits of information from the reconciled key; and 2) the measure of information leakage $I(\boldsymbol{k};\boldsymbol{z},\boldsymbol{A})$ is taken as average over all possible realizations of $\boldsymbol{A}$.

A. *Secrecy and information leakage with a known linear attack*

For a generic attack in which Eve has observed some t-bit linear function $\boldsymbol{z}$ of the reconciled key x, we can write $\boldsymbol{z} = \boldsymbol{M}\boldsymbol{x}$ with $\boldsymbol{M} \in \{0,1\}^{t \times n}$. Then, once a hashing matrix is chosen $\boldsymbol{A} \in \{0,1\}^{s \times n}$, one wishes to obtain

1) perfect uniformity: $H_{\boldsymbol{A}}(\boldsymbol{k}) = s$
2) perfect secrecy: $I_{\boldsymbol{A},\boldsymbol{M}}(\boldsymbol{k};\boldsymbol{z}) = 0$

where the subscripts $\boldsymbol{A}$ and $\boldsymbol{M}$ in the entropy and mutual information underline that these quantities depend on the two matrices.

Let $\mathcal{N}(\cdot)$ denote the null space of a matrix.

Proposition 1: If $\dim \mathcal{N}(\boldsymbol{M}) - \dim(\mathcal{N}(\boldsymbol{M}) \cap \mathcal{N}(\boldsymbol{A})) = s$ and $\boldsymbol{x}$ is uniform over $\{0,1\}^n$, then $\boldsymbol{k}$ is uniform and perfectly secret.

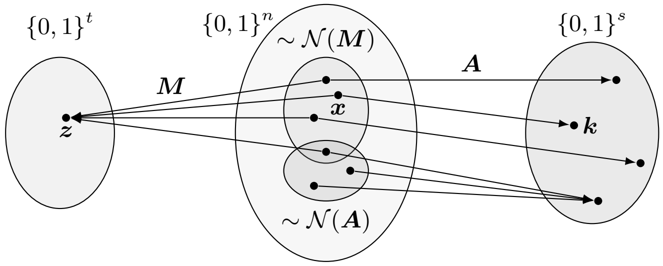

Fig. 1. Illustration of Proposition 1

Proposition 2: The information leaked to Eve about $\boldsymbol{k}$, with the eavesdropper matrix $\boldsymbol{M}$ and privacy amplification matrix $\boldsymbol{A}$ is

$$\begin{aligned} I_{\boldsymbol{A},\boldsymbol{M}}(\boldsymbol{k};\boldsymbol{z}) &= s - (\dim \mathcal{N}(\boldsymbol{M}) - \dim(\mathcal{N}(\boldsymbol{M}) \cap \mathcal{N}(\boldsymbol{A}))) \\ &= s - \operatorname{rank}(\boldsymbol{A}\boldsymbol{N}_{\boldsymbol{M}}) \end{aligned}$$

where $\boldsymbol{N}_{\boldsymbol{M}}$ is any matrix whose columns form a basis for $\mathcal{N}(\boldsymbol{M})$.

B. *Selective individual attacks*

We consider selective individual attacks, in which the eavesdropper learns each transmitted bit with probability q (and learns nothing of it with probability $1-q$), independent of all the others. Examples of such attacks are the *intercept and resend* [3] with probability $2q$, the *photon number splitting* [4], the unambiguous state discrimination [5]. Each realization of such an attack can be modeled as linear with $\boldsymbol{N}_{\boldsymbol{M}} = \boldsymbol{I}_{-\boldsymbol{j}}$, the matrix obtained from the $n \times n$ identity by erasing the columns with indices in $\boldsymbol{j}$, corresponding to the bits observed by Eve.

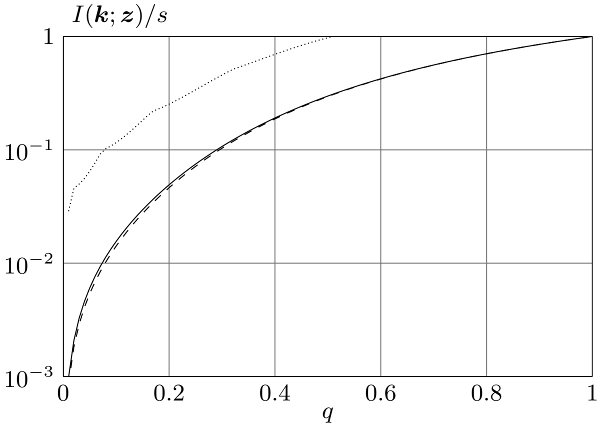

Fig. 2. Average fraction of key information leaked to Eve under a selective individual attack versus the attack rate q, for the classes of binary (solid line) and binary Toeplitz (dashed line) matrices. Here, $n = 12$, $s = 8$. The upper bound in [2, Corollary 4] is also plotted for comparison (dotted line).

C. *Information leakage with a selective individual attack*

Proposition 3: For a given hashing matrix $\boldsymbol{A} \in \{0,1\}^{s \times n}$ the average (over the attack statistics) of the information leaked to Eve in the final key $\boldsymbol{k}$ is given by

$$I_{\boldsymbol{A}}(\boldsymbol{k};\boldsymbol{z}) = \sum_{\boldsymbol{j} \in \mathcal{I}_n} q^{\ell(\boldsymbol{j})}(1-q)^{n-\ell(\boldsymbol{j})} \operatorname{rank}(\boldsymbol{A}_{-\boldsymbol{j}}) \tag{1}$$

where $\mathcal{I}_n$ denotes the set of all possible index vectors and $\ell(\boldsymbol{j})$ is the length of vector $\boldsymbol{j}$.

In principle, since the value of q can be precisely estimated by Alice and Bob prior to privacy amplification, (1) would yield them the expected amount of information leaked. However, it should be pointed out that even for moderate values of n the calculation of all the ranks in (1) becomes impractical.

D. *Numerical results*

In Figure 2 we plot the result of averaging equation (1) over a uniform choice of $\boldsymbol{A}$ in the class of full row rank binary matrices and in its Toeplitz subclass. It can be seen that the result is much lower than the bound in [2].

References

[1] C.-H. Fung *et al.*, *Phys. Rev. A* **81**, 012318 (2010)
[2] C. H. Bennett *et al.*, *IEEE Trans. Inf. Th.*, **41**, 1915 (1995)
[3] B. Huttner *et al.*, *Phys. Rev. A* **51**, 1863 (1995)
[4] N. Lütkenhaus, *Phys. Rev. A* **61**, 052304 (2000)
[5] M. Dušek *et al.*, *Phys. Rev. A* **62**, 022306 (2000)