Privacy Amplification Theorem for Noisy Main Channel

Valeri Korjik[1], Guillermo Morales-Luna[2], and Vladimir B. Balakirsky[3]

[1] Telecommunications,
CINVESTAV-IPN, Guadalajara Campus
Prol. López Mateos Sur No. 590, Guadalajara, Jalisco. Mexico
vkorjik@gdl.cinvestav.mx

[2] Programa de Simulación Molecular, Instituto Mexicano del Petróleo,
on leave of absence from Computer Science Section, CINVESTAV-IPN,
Av. I. P. N. 2508, 07300 Mexico City, Mexico
gmorales@cs.cinvestav.mx

[3] Euler Institute for Discrete Mathematics and its Applications (EIDMA),
P.O.Box 513, 5600 MB Eindhoven, The Netherlands
v.b.balakirsky@ele.tue.nl

Abstract. Secret key agreement protocol between legal parties based on reconciliation and privacy amplification procedure has been considered in [2]. The so called *privacy amplification theorem* is used to estimate the amount of Shannon's information leaking to an illegal party (passive eavesdropper) about the final key. We consider a particular case where one of the legal parties (Alice) sends to another legal party (Bob) a random binary string $\boldsymbol{x}$ through a binary symmetric channel (*BSC*) with bit error probability ε_m while an eavesdropper (Eve) receives this string through an independent *BSC* with bit error probability ε_w. We assume that $\varepsilon_m < \varepsilon_w$ and hence the *main channel* is superior to the *wire-tap channel*. To reconcile the strings between legal parties Alice sends to Bob through noiseless channel the check string $\boldsymbol{y}$ based on some good error correcting code. Since this transmission is completely public Eve can eavesdrop it and therefore this extra information has to be taken into account in an estimation of the information leaking to Eve about the final key. In [3] an inequality has been proved to upper bound the information of Eve in such scenario. The main contribution of the running paper is to improve this inequality and hence to enhance the privacy amplification theorem. We present also bounds for the probability of false reconciliation when the check symbols of the linear code are transmitted through noiseless channel. The presented results can be very useful when considering the non-asymptotic case.
Keywords. Key-sharing, privacy amplification, hashing, Rènyi information, error correcting codes.

1 Introduction

We consider a cryptographic scenario where two honest persons, Alice and Bob, do not share any secret data initially but their goal is the generation of a shared *information-theoretically secure* key. Alice is able to send messages to Bob through a main *BSC* with bit error probability ε_m while *passive eavesdropper* Eve can intercept these messages through the independent wire-tap *BSC* with bit error probability $\varepsilon_w > \varepsilon_m$. At the same time Alice is able to send messages to Bob over another binary *noiseless* but completely *public* channel. (Hence all information transmitted through this channel is known for Eve without errors.)

Such setup seems strange at a single glance but in fact it is a good model of *quantum cryptography* where a noisy *BSC* can be established due to the use of special modulation of photon flow with small intensity while noiseless channel is created by conventional amplitude modulation of photon flow with large intensity.

The *key sharing algorithm* (*KSA*) between Alice and Bob comprises both *reconciliation* and *privacy amplification* procedures and it is the following:

1. Alice generates truly random binary string $\boldsymbol{x}$ of length k and sends it to Bob through noisy main channel.
2. Alice generates *hash function* $h(\ldots)$ chosen truly randomly and sends it to Bob through noiseless public channel.
3. Alice forms the binary string $\boldsymbol{y} = f(\boldsymbol{x})$ of length $r = n - k$ as the sequence of check symbols $\boldsymbol{y}$ to information symbols $\boldsymbol{x}$ using some binary linear systematic error correcting (n, k)-code C with the known function $f(\cdots)$, previously agreed with Bob.
   We believe of course that this code C has good (the best if possible) *error correcting capability* and *constructive error correction algorithm* like *BCH* or *Goppa* codes.
4. Alice sends the check string $\boldsymbol{y}$ to Bob over noiseless public channel. Eve can learn the check string $\boldsymbol{y}$ received also on noiseless channel.
5. Bob receives the string $\boldsymbol{x}$ as noisy version $\boldsymbol{x}'$ and corrects errors on $\boldsymbol{x}'$ using the check string $\boldsymbol{y}$. We believe that after such correction Bob *reconciles* $\boldsymbol{x}$ and $\boldsymbol{x}'$ with high probability.
6. Both Alice and Bob *hash* their strings $\boldsymbol{x}$ and $\boldsymbol{x}'$ (after reconciliation with $\boldsymbol{x}$) to produce the final *shared key* $\tilde{\boldsymbol{z}} = h(\boldsymbol{x})$.

The amount of *Shannon's information* I_0 leaking to Eve under the condition that she knows completely the key sharing protocol given above, the code C, the check string $\boldsymbol{y}$ and the noisy version $\boldsymbol{x}''$ of the string $\boldsymbol{x}$ received through wire-tap *BSC* is given by the so called *Privacy Amplification Theorem* [2]:

$$I_0 \leq \frac{2^{-(k-t_c-\ell_0)}}{\ln 2} \tag{1}$$

where t_c is the Rènyi (or *collision*) information that has Eve from all her knowledge mentioned above, and ℓ_0 is the length of the string after hashing. The collision information t_c is comprised of the collision information t_c' about $\boldsymbol{x}$ contained in $\boldsymbol{x}''$ and the collision information t_c'' contained in the check string $\boldsymbol{y}$. We recall that collision information contained in $\boldsymbol{x}''$ is defined [2] as $t_c' = k - H_c(X)$, where $H_c(X)$ is the *collision entropy*. In the particular case of *BSC* as wire-tap channel with symbol error probability ε_w, the collision entropy can be calculated as

$$H_c(X) = -k \log\left(\varepsilon_w^2 + (1 - \varepsilon_w)^2\right) \tag{2}$$

The total collision information t_c is not the sum of those particular collision informations t_c' and t_c''. To estimate an increase $\Delta_c = t_c - t_c'$ of the total collision information given side information $\boldsymbol{y}$, the following probabilistic bound can be used [3]

$$Prob(\Delta_c \leq 2r + 2s) \geq 1 - 2^{-s} \tag{3}$$

for any $s > 0$, where r is the length of the check string $\boldsymbol{y}$. In Section 2 we will improve this inequality and treat the privacy amplification theorem in more general form than in [2]. It is especially important if we are interested in a consideration of non-asymptotic case when the length k of the string $\boldsymbol{x}$ is not too large.

In Section 3 we will present a modified Gallager's bound in the case of a noiseless channel for a transmission of check symbols that is just the case of our cryptographic scenario and discuss the main results.

2 Enhanced privacy amplification theorem

Let $\boldsymbol{x}$ be a binary uniformly distributed k-string transmitted on a communication channel from Alice to Bob during execution of step 1 in the *KSA*.

We propose to perform a hashing procedure $\tilde{\boldsymbol{z}} = h(\boldsymbol{x})$ presented in step 6 of *KSA* in two stages: Firstly, the initial string $\boldsymbol{x}$ is transformed into a shorter string $\boldsymbol{z}$ using a hash function chosen randomly from *universal*$_2$ *class*. It can be done as follows [7]

$$\boldsymbol{z} = \boldsymbol{x}A \tag{4}$$

where A is a truly random $k \times (\ell + r)$-matrix, $k > \ell + r$. Secondly, the string $\boldsymbol{z}$ obtained by eq. (4) is transformed to the final key $\tilde{\boldsymbol{z}}$ of length ℓ after the "puncturing" given by the transformation

$$\tilde{\boldsymbol{z}} = \boldsymbol{z}H_1 \tag{5}$$

where H_1 is a binary $(\ell + r) \times \ell$-matrix containing exactly one 1 in each column and at most one 1 in each row. (In fact this transformation saves some ℓ digits of $\boldsymbol{z}$ and deletes the remaining ones.)

Let us assume that the check string $\boldsymbol{y}$ is produced at step 3 in *KSA* as follows

$$\boldsymbol{y} = \boldsymbol{z}H_2 \tag{6}$$

where H_2 is some binary $(\ell + r) \times r$-matrix. All matrices A, H_1 and H_2 are public.

Theorem 1. *Under the conditions of our cryptographic scenario and the KSA presented above, there exists such a matrix H_1 that the eavesdropper's expected Shannon information I_0, about the final key $\tilde{\boldsymbol{z}}$ shared by legal parties, satisfies the inequality*

$$I_0 \leq \frac{2^{-(k - t'_c - \ell - r)}}{\gamma \cdot \ln 2} \tag{7}$$

where

k is the length of the string $\boldsymbol{x}$ generated by Alice in the first step of the KSA,
t'_c is the Rènyi (or collision) information obtained by Eve about the string $\boldsymbol{x}$ using just the string $\boldsymbol{x}''$ of her knowledge ($\boldsymbol{x}''$ is the version of $\boldsymbol{x}$ received by Eve through a BSC with bit error probability ε_w),

r is the number of check symbols sent from Alice to Bob in order to reconcile their strings and

γ is a coefficient that approaches to 0.42 for any fixed r, as k, ℓ and $k-\ell$ increase.

In order to prove this theorem, we need to prove the following lemma:

Lemma 1. *Let Z,$\tilde{Z}$ and Y be the probability spaces that describe the random strings $\boldsymbol{z}$, $\tilde{\boldsymbol{z}}$ and $\boldsymbol{y}$ respectively and let E be the probability space that models the eavesdropper's information on $\boldsymbol{z}$. Then, the following inequality holds*

$$I(\tilde{Z};E,Y) \leq I(Z;E) \tag{8}$$

whenever

$$\det H \neq 0, \tag{9}$$

where $H = [H_2\, H_1]$.

Proof of the lemma. By very well known information-theoretic relations [1] we have

$$I(\tilde{Z};E,Y) = I(\tilde{Z};Y) + I(\tilde{Z};E|Y) \tag{10}$$

Let us prove first that if eq. (9) were true, then $I(\tilde{Z};Y) = 0$. Consider the joint probability $Prob[\tilde{\boldsymbol{z}}, \boldsymbol{y}] = Prob[\boldsymbol{z}H]$. The condition (9) implies that H is a non-singular $(\ell+r) \times (\ell+r)$-matrix and therefore

$$Prob[\tilde{\boldsymbol{z}}, \boldsymbol{y}] = Prob[\boldsymbol{z} = (\tilde{\boldsymbol{z}}, \boldsymbol{y})H^{-1}] = 2^{-(\ell+r)}$$

for any $\tilde{\boldsymbol{z}}, \boldsymbol{y}$ since $\boldsymbol{z}$ is uniformly distributed over $GF(2)^{\ell+r}$. On the other hand, for any $\boldsymbol{y}$

$$Prob[\boldsymbol{y}] = \sum_{\boldsymbol{z}_1 \in GF(2)^\ell} Prob[\boldsymbol{z} = (\boldsymbol{y}, \tilde{\boldsymbol{z}}_1)H^{-1}] = 2^\ell \cdot 2^{-(\ell+r)} = 2^{-r} \tag{11}$$

In a similar manner we obtain that for any $\tilde{\boldsymbol{z}}$

$$Prob[\tilde{\boldsymbol{z}}] = \sum_{\boldsymbol{z}_2 \in GF(2)^r} Prob[\boldsymbol{z} = (\boldsymbol{z}_2, \tilde{\boldsymbol{z}})H^{-1}] = 2^r \cdot 2^{-(\ell+r)} = 2^{-\ell} \tag{12}$$

Combining (11) and (12) we obtain that $Prob[\tilde{\boldsymbol{z}}, \boldsymbol{y}] = Prob[\boldsymbol{y}] \cdot Prob[\tilde{\boldsymbol{z}}]$ for any $\tilde{\boldsymbol{z}}, \boldsymbol{y}$ and hence $I(\tilde{Z};Y) = 0$. Adding $I(E;Y) \geq 0$ on the right hand side in (10) it results in

$$I(\tilde{Z};E,Y) \leq I(\tilde{Z};E|Y) + I(E;Y) = I(\tilde{Z},Y;E).$$

But $\boldsymbol{z} = (\tilde{\boldsymbol{z}}, \boldsymbol{y})H^{-1}$ and hence $I(\tilde{Z},Y;E) = I(Z;E)$. This completes the lemma's proof. □

Proof of the theorem. With condition (9), the proof of the theorem follows inmediately, with factor $\gamma = 1$, from the lemma if we substitute eq. (1), where t_c means Rènyi information that has Eve about $\boldsymbol{x}$ from her knowledge of $\boldsymbol{x}''$ only, into the right hand side of eq. (8) and take into account that $\ell_0 = \ell + r$. On the other hand, if we assume that rank $H_2 = r$ then there exists a set of r rows of this matrix that are linearly independent. If we choose these rows in the matrix H_1 to be zero rows and put a single 1 in the remaining rows of H_2 we obtain the relation (9). Thus the theorem is proved under the assumption $\operatorname{rank} H_2 = r$.

By (4) and (6)

$$\boldsymbol{y} = \boldsymbol{x}AH_2 = \boldsymbol{x}P \tag{13}$$

where

$$P = AH_2 \tag{14}$$

Let us assign P as the matrix of the reduced echelon form representation of the generator matrix of some fixed linear binary $(k, k + r)$ code C, i. e. $[I_k P]$ is the generator matrix of C. This code (properly the matrix P) can be chosen by legal parties to be good (with large minimum code distance and having constructive algorithm of error correction).

It is easy to see that if $\operatorname{rank} P = r$, provided $k \geq r$ (that is, P is a full-rank matrix) then it implies that $\operatorname{rank} H_2 = r$ which is necessary to be true in order that the theorem holds. The condition $\operatorname{rank} P = r$ may not be satisfied for any generator matrix G of the linear binary code presented in reduced echelon form as $G = [I_k\, P]$, but it is possible to get such condition after a number of column transpositions of G and a representation of new matrix $\tilde{G}$ in reduced-echelon form $\tilde{G} = [I_k\, \tilde{P}]$ where $\operatorname{rank} \tilde{P} = r$. (Obviously such transformations do not change the minimal code distance of the code C.)

In this manner legal parties can share initially the full rank matrix P corresponding to the "good" code and Bob will be able to correct errors in his string $\boldsymbol{x}'$ after reception of check string $\boldsymbol{y}$.

But it is necessary to know the mathrix H_2 in order to perform the second stage of the hashing defined by eq. (5) satisfying simultaneously condition (9). Hence a solution of matrix equation (14) is required. However, it may fail to exist. A sufficient (but not necessary) condition for its existence is the following

$$\det (A^T \cdot A) \neq 0 \tag{15}$$

where A^T is the transpose of matrix A. Under this assumption, the solution of matrix equation (14) can be obtained as

$$H_2 = (A^T \cdot A)^{-1} A^T P \tag{16}$$

The binary matrix A is a truly random $k \times (\ell + r)$-matrix and consequently (15) is a probabilistic inequality. This probability is

$$\begin{aligned} \mathit{Prob}\left[\det (A^T \cdot A) \neq 0\right] = \mathit{Prob}\left[\operatorname{rank} A = \ell + r\right] \cdot \\ \mathit{Prob}\left[\det (A^T \cdot A) \neq 0 \,\middle|\, \operatorname{rank} A = \ell + r\right] \end{aligned} \tag{17}$$

It is very easy to prove that

$$\mathit{Prob}\left[\operatorname{rank} A = \ell + r\right] = \beta = \prod_{j=1}^{\ell+r} \left(1 - \frac{1}{2^{k-\ell-r+j}}\right) \tag{18}$$

On the other hand, $\alpha = \mathit{Prob}\left[\det (A^T \cdot A) \neq 0 \,\middle|\, \operatorname{rank} A = \ell + r\right]$ is the probability that chosen randomly matrix A^T is just the generator matrix of linear binary *complementary dual code* V (so called *LCD-code*) [4]. It means that the *hull* of the LCD-code V

(defined as its intersection with its dual) has dimension 0. As it has been proven in [6], α approaches to $0.41942244417951075977099\cdots$ for any fixed r, as k and ℓ increase.

Now we have to change slightly the first stage of the hashing presented by (4). If it happens that for random chosen matrix A the condition (15) is satisfied then the next steps of the algorithm can be pursued. Otherwise, Alice should repeat a random choice of matrix A till (15) holds.

It follows from the proof of the basic privacy amplification theorem [2] that such modification of hashing procedure results in an increasing of collision probability by the factor $\frac{1}{\gamma} = \frac{1}{\alpha\beta}$ and thus it increases Shannon's information about $\tilde{\boldsymbol{z}}$ leaking Eve by the same factor. Since β is very close to 1, whenever there is a large difference between k and $\ell + r$ (a rather common situation for this algorithm) we can keep just the factor $\frac{1}{\alpha}$. This completes the proof of the theorem. $\square$

3 Discussion of the main results and concluding remarks

It has been proven in the previous section that for the *KSA* presented in section 1 and specified by formulas (4)-(6) with a slight change of the first stage of hashing when a random generation of matrix A is repeated until condition (15) is met, the upper bound (7) can be used to estimate Shannon's information leaking to eavesdropper about the final key. Practically, we can neglect by factor γ because it is close to $\frac{1}{2}$ and typically the value I_0 should be very small. Moreover we can change the *KSA* and believe that Alice repeats the first step of *KSA* using new randomly generated string $\boldsymbol{x}$ unless she meets the condition (15). Such modification results in the bound (7) with $\gamma = 1$ but the number of the main channel uses increases by $\frac{1}{\gamma}$ (a factor of 2, roughly speaking).

If the main channel is *BSC* with bit error probability ε_m, then asymptotically $k \cdot H(\varepsilon_m)$ check symbols sent through noiseless channel, where $H(\cdots)$ is the entropy function, are sufficient to provide a reconciliation of strings $\boldsymbol{x}$ and $\boldsymbol{x}'$ with high probability. In fact, a transmission of information symbols through *BSC* with symbol error probability ε_m and check symbols through noiseless channel can be considered as a transmission of both groups of symbols over *time sharing channel* with the *capacity*

$$C_{ts} = \frac{k}{k+r} C_m + \frac{r}{k+r} \tag{19}$$

where $C_m = 1 - H(\varepsilon_m)$. Substitution of (19) in Shannon's condition of reliable communication [1] gives $R = \frac{k}{k+r} < C_{ts}$ which implies the condition $r \sim k \cdot H(\varepsilon_m)$. Taking into account that asymptotically [2] $t'_c \sim (1 - H(\varepsilon_m))k$ we get from eq. (7) the condition on key rate $R_k = \frac{\ell}{k}$ to provide an exponential decreasing of information I_0 leaking to eavesdropper, as $k \to +\infty$

$$R_k < H(\varepsilon_w) - H(\varepsilon_m) = C_{ks} \tag{20}$$

where C_{ks} is just the capacity of key sharing scenario under consideration [5]. When $\varepsilon_w > \varepsilon_m$ the key rate is positive and hence this algorithm works. Otherwise it is necessary to use *public discussion* [5] to transform the condition $\varepsilon_w \leq \varepsilon_m$ into the condition $\varepsilon_w > \varepsilon_m$.

But an improvement of the bound for I_0 is important first of all in a *non-asymptotic* case. Then it is necessary to estimate the probability of errors in the string of Bob after the error correction procedure based on the use of r error free check symbols. The way of doing this is a modification of known bounds in the case when a noiseless channel is used to transmit check symbols.

Let $\lambda_k(R|P)$, where $R = \frac{k}{k+r}$ and P is a binary $r \times k$ matrix, denote the probability that the information vector $\boldsymbol{x}$ of length k is incorrectly decoded by Bob based on its corrupted version $\boldsymbol{y}$ and parity $\boldsymbol{x}P^T$ of length r. Let

$$W(\boldsymbol{y}|\boldsymbol{x}) = \varepsilon_m^{d_H(\boldsymbol{x},\boldsymbol{y})}(1-\varepsilon_m)^{k-d_H(\boldsymbol{x},\boldsymbol{y})}$$

where d_H denotes the Hamming distance, and let

$$\mathcal{C}(\boldsymbol{x}, P) = \left\{ \boldsymbol{x}' \in \{0,1\}^k : \boldsymbol{x}P^T = \boldsymbol{x}P^T \right\}$$

be the coset of a linear code consisting of codewords having the same parity as the vector $\boldsymbol{x}$. Then $\lambda_k(R|P)$ can be expressed as

$$\lambda_k(R|P) = 2^{-k} \sum_{\boldsymbol{x}\in\{0,1\}^k} \lambda_k(R|\boldsymbol{x}, P)$$

where

$$\lambda_k(R|\boldsymbol{x}, P) = \sum_{\mathbf{y}\in\{0,1\}^k} W(\boldsymbol{y}|\boldsymbol{x})\chi\{\beta\} \tag{21}$$

$$\beta \equiv [\, \exists \boldsymbol{x}' \in \mathcal{C}(\boldsymbol{x}, P), \boldsymbol{x}' \neq \boldsymbol{x} : d_H(\boldsymbol{x}', \boldsymbol{y}) \leq d_H(\boldsymbol{x}, \boldsymbol{y})\,]$$

and χ stands for the indicator function, i.e., $\chi\{\beta\} = 1$ if the statement β is true and $\chi\{\beta\} = 0$ otherwise.

Proposition 1. *Let $\overline{\lambda_k(R|P)}$ denote the expectation of the probability $\lambda_k(R|P)$ over the ensemble of matrices P of dimension $k \times r$ whose entries are i.i.d. random variables chosen from $\{0,1\}$ with probability $1/2$, i.e.,*

$$\overline{\lambda_k(R|P)} = 2^{-kr} \sum_P \lambda_k(R|P).$$

Then

$$\overline{\lambda_k(R|P)} \leq 2^{-kE(R)} \tag{22}$$

where

$$E(R) = \max_{\rho\in(0,1]} \Big[\, E_0(\rho) - \rho(2R-1)/R) \,\Big] \tag{23}$$

and

$$E_0(\rho) = \rho - (1+\rho)\log\left(\varepsilon_m^{1/(1+\rho)} + (1-\varepsilon_m)^{1/(1+\rho)}\right)$$

is the Gallager function for a BSC with crossover probability ε_m.

Proof. Let us introduce a parameter $\rho > 0$ and let us upper–bound the probability $\lambda_k(R|\boldsymbol{x}, P)$ defined in (21) as

$$\lambda_k(R|\boldsymbol{x}, P) \le \sum_{\boldsymbol{y}\in\{0,1\}^k} W(\boldsymbol{y}|\boldsymbol{x}) \Big[\sum_{\substack{\boldsymbol{x}'\in\mathcal{C}(\boldsymbol{x},P)\\ \boldsymbol{x}'\neq\boldsymbol{x}}} \left(\frac{W(\boldsymbol{y}|\boldsymbol{x}')}{W(\boldsymbol{y}|\boldsymbol{x})}\right)^{1/(1+\rho)} \Big]^{\rho} \tag{24}$$

If $\rho \in (0, 1]$, then

$$\begin{aligned} &2^{-kr}\sum_P \Big[\sum_{\substack{\boldsymbol{x}'\in\mathcal{C}(\boldsymbol{x},P)\\ \boldsymbol{x}'\neq\boldsymbol{x}}} W^{1/(1+\rho)}(\boldsymbol{y}|\boldsymbol{x}') \Big]^{\rho} \\ &\le \Big[2^{-kr}\sum_P \sum_{\substack{\boldsymbol{x}'\in\mathcal{C}(\boldsymbol{x},P)\\ \boldsymbol{x}'\neq\boldsymbol{x}}} W^{1/(1+\rho)}(\boldsymbol{y}|\boldsymbol{x}') \Big]^{\rho} &(25)\\ &= \Big[\sum_{\boldsymbol{x}'\neq\boldsymbol{x}} W^{1/(1+\rho)}(\boldsymbol{y}|\boldsymbol{x}') 2^{-kr}\sum_P \chi\{\, \boldsymbol{x}'\in\mathcal{C}(\boldsymbol{x},P)\,\} \Big]^{\rho} \\ &= \Big[\sum_{\boldsymbol{x}'\neq\boldsymbol{x}} W^{1/(1+\rho)}(\boldsymbol{y}|\boldsymbol{x}') 2^{-r} \Big]^{\rho} &(26)\\ &\le 2^{-\rho r}\left(\varepsilon_m^{1/(1+\rho)} + (1-\varepsilon_m)^{1/(1+\rho)}\right)^{k\rho}. &(27) \end{aligned}$$

Inequality (25) follows from Jensen's inequality and (26) holds because of the linearity:

$$2^{-kr}\sum_P \chi\{\, \boldsymbol{x}'\in\mathcal{C}(\boldsymbol{x},P)\,\} = 2^{-kr}\sum_P \chi\{(\boldsymbol{x}\oplus\boldsymbol{x}')P^T = (0,\ldots,0)\} = 2^{-r}$$

where $(0, \ldots, 0)$ is the vector consisting of r zeroes.

Thus, (24) and (27) imply

$$2^{-kr}\sum_P \lambda_k(R|\boldsymbol{x}, P) \le \min_{\rho\in(0,1]} 2^{-\rho r}\left(\varepsilon_m^{1/(1+\rho)} + (1-\varepsilon_m)^{1/(1+\rho)}\right)^{k(1+\rho)}$$

and (22) follows.

The function $E(R)$ is given in Fig. 1 for a BSC with crossover probability 0.01. Note that this function is always positive if

$$R < \frac{1}{1 - \varepsilon_m \log\varepsilon_m - (1-\varepsilon_m)\log(1-\varepsilon_m)}$$

Note also that if $\rho = 1$, then (22) becomes the union bound :

$$\overline{\lambda_k(R|P)} \le \left(1 + 2\sqrt{\varepsilon_m(1-\varepsilon_m)}\right)^k 2^{k(1-R)}.$$

These approaches can be also used to estimate the probability $\lambda_k(R|P)$ for specific matrices P.

Thus, we have some tools of analysis that allow us to assign the parameters k, r, and ℓ to provide both reliable and secure key sharing between legal parties in the presence of passive eavesdropper.

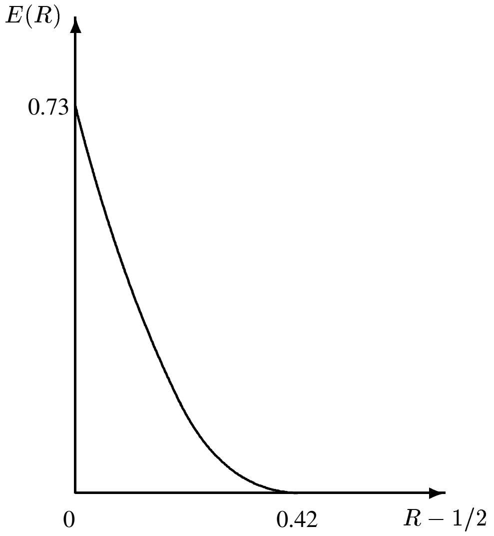

Fig. 1. Exponent $E(R)$ defined in (23) for a BSC with crossover probability 0.01.

References

1. Ash, R.B. "*Information Theory*". Dover, New York, 1990.
2. Bennett, C. H., Brassard, G., Maurer, U. M. "Generalized Privacy Amplification". *IEEE Trans. on IT*, vol. 41, nr. 6, pp. 1915-1923. 1995.
3. Cachin, C., Maurer, U. M. "Linking Information-Reconciliation and Privacy Amplification". *Eurocrypt'94: Advances in cryptology, Lecture Notes in Computer Science*, vol. 950, pp. 267-274. Springer-Verlag. 1995.
4. Massey, J.L. "Linear Codes with Complimentary Duals". *Discrete Math.*, 106/107. 1992.
5. Maurer, G. "Secret Key Agreement by Public Discussion Based on Common Information". *IEEE Trans. on I. T.*, vol. 39, nr. 3, 1998, p. 733-742.
6. Sendrier, N. "On the dimension of the hull". *SIAM Journal on Discrete Mathematics*, vol. 4, nr. 2, pp. 282-293, 1997.
7. Stinson, D.R.. "Universal Hashing and Authentication Codes". *Advances in cryptology, Crypto'91, Lecture Notes in Computer Science*, vol. 576, 1992, pp. 74-85. Springer-Verlag. 1992.