Bit Error Rate and Efficiency Analysis of Wireless Reciprocal Channel Key Generation

Rajesh K. Sharma and Jon W. Wallace*
Jacobs University Bremen, School of Engineering and Science
Campus Ring 1, 28759 Bremen, Germany
E-mail: ra.sharma@jacobs-university.de, wall@ieee.org

Introduction

Physical layer security is a method which exploits the random nature of the physical propagation channel. In reciprocal channel key generation (RCKG), legitimate nodes (Alice and Bob) observe a common time-varying channel to generate keys that are safe from the eavesdropper (Eve), in contrast to more complicated physical layer approaches that transmit random information through the channel and distill common randomness at Alice and Bob unobservable by Eve [1]. In [2] a simple method based on phase quantization for scalar channels is presented. In [3] and [4], expressions for the available key bits and those safe from an eavesdropper are derived for MIMO systems with correlated complex Gaussian statistics, and two simple channel quantization (CQ) methods are presented. This paper extends the results of [4] by computing exact bit error rate (BER) probability of two CQ methods under Gray code mapping and by giving an improved definition of key generation efficiency that includes overhead due to practical error protection.

Analysis of Key Generation Methods

In [4], two channel quantization methods have been presented where Alice and Bob divide the space of observable channels into M rectangular quantization sectors (QSs) with equal probability such that the number of one-sided one-dimensional quantization intervals (QIs) is $M' = \sqrt{M}/2$. In channel quantization with guardband (CQG), specified guardband g between sectors is considered. In channel quantization alternating (CQA), alternate interleaved maps are used instead of guardband. Here we briefly present the analytical expressions to evaluate the BER and efficiency of the methods. For the reciprocal channel h_a with variance σ_a^2, the channel observed by Alice and Bob is $\hat{h}_a = h_a + \varepsilon_1$ and $\hat{h}_{a'} = h_a + \varepsilon_2$, where ε_1 and ε_2 are estimation errors at Alice and Bob, with variances σ_1^2 and σ_2^2, respectively.

To compute the efficiency and error probability of CQ methods, we consider the random real scalars $Y = \mathrm{Re}\{\hat{h}_{a'}\}$ and $Z = \mathrm{Re}\{\hat{h}_a\}$ with variances $\sigma_y^2 = (\sigma_a^2 + \sigma_1^2)/2$ and $\sigma_z^2 = (\sigma_a^2 + \sigma_2^2)/2$, respectively, and the analysis for the imaginary parts is identical. The observation probabilities of interest are

$$P_{yz}(\mathcal{Y}, \mathcal{Z}) = \Pr\{Y \in \mathcal{Y},\ Z \in \mathcal{Z}\}, \quad P_y(\mathcal{Y}) = \Pr\{Y \in \mathcal{Y}\}, \quad P_z(\mathcal{Z}) = \Pr\{Z \in \mathcal{Z}\}, \tag{1}$$

where $\mathcal{Y}$ and $\mathcal{Z}$ are intervals taken from the QI sets $\mathcal{Y} \in \{\mathcal{Y}_n\}$ and $\mathcal{Z} \in \{\mathcal{Z}_n\}$, for Alice and Bob, respectively.

Considering the real zero-mean Gaussian random variables X, ϵ_1, and ϵ_2, with variances σ_x^2, σ_1^2, and σ_2^2, corresponding to h_a, ε_1 and ε_2, channel estimates for the two nodes are now given by $Y = X + \epsilon_1$ and $Z = X + \epsilon_2$, respectively. The marginal probability of observing Y on the interval $\mathcal{Y} = [y_1, y_2]$ is obtained by integrating the PDF $p(y) = 1/(\sqrt{2\pi}\sigma_y)\exp[-y/(2\sigma_y^2)]$, where $\sigma_{\{y,z\}}^2 = \sigma_x^2 + \sigma_{\{1,2\}}^2$, or

$$P_y(\mathcal{Y}) = \Pr\{Y \in \mathcal{Y}\} = \frac{1}{2}\left[\mathrm{erf}\left(\frac{y_2}{\sqrt{2}\sigma_y}\right) - \mathrm{erf}\left(\frac{y_1}{\sqrt{2}\sigma_y}\right)\right], \tag{2}$$

978-1-4244-7092-1/10/$26.00 ©2010 IEEE

where $\text{erf}(\cdot)$ is the error function. The function for $P_z(\mathcal{Z})$ is identical with $(y, Y, \mathcal{Y}) \rightarrow (z, Z, \mathcal{Z})$. To find the function $P_{yz}(\mathcal{Y}, \mathcal{Z})$, we write the joint PDF of Y and Z as

$$p(y,z) = \frac{1}{2\pi|\mathbf{R}|^{1/2}} \exp\left\{-\frac{1}{2|\mathbf{R}|} S(y,z)\right\}, \tag{3}$$

where $S(y,z) = \sigma_x^2(y^2 + z^2 - 2zy) + \sigma_1^2 z^2 + \sigma_2^2 y^2$, and $|\mathbf{R}| = \sigma_x^2(\sigma_1^2 + \sigma_2^2) + \sigma_1^2\sigma_2^2$. The PDF of Z conditioned on Y in a specified interval is

$$p(z|Y \in \mathcal{Y}) = \frac{1}{P_y(\mathcal{Y})} \int_{y_1}^{y_2} p(y,z)dy = \frac{1}{\sqrt{8\pi}\sigma_z P_y(\mathcal{Y})} \exp\left[-\frac{z^2}{2\sigma_z^2}\right] [A_2(z) - A_1(z)], \tag{4}$$

where $A_i(z) = \text{erf}[(\text{y}_\text{i} - \alpha \text{z})\sigma_\text{z}/(\sqrt{2}|\mathbf{R}|^{1/2})]$ and $\alpha = \sigma_x^2/\sigma_z^2$. Finally,

$$P_{yz}(\mathcal{Y}, \mathcal{Z}) = \Pr\{Y \in \mathcal{Y},\ Z \in \mathcal{Z}\} = \int_{z_1}^{z_2} p(z|Y \in \mathcal{Y})dz, \tag{5}$$

which can be computed numerically.

In CQG with a two-way handshake, Alice and Bob share guardband indicator bits (GIBs) which indicate when a node observes the channel in guardband, and the channel observation is discarded if either GIB is set. Here, $\mathcal{Y}_m$ and $\mathcal{Z}_m$ are both $[x_m, x_{m+1} - g]$, and the probability of simultaneous GIB=0 is

$$P_{\overline{\text{GIB}}} = \sum_{m=1}^{2M'} \sum_{n=1}^{2M'} P_{yz}(\mathcal{Y}_m, \mathcal{Z}_n). \tag{6}$$

Defining observation probabilities conditioned on GIB=0 as $P'_{yz}[m,n] = P_{yz}(\mathcal{Y}_m, \mathcal{Z}_n)/P_{\overline{\text{GIB}}}$, $P'_y[m] = P_y(\mathcal{Y}_m)/P_{\overline{\text{GIB}}}$ and $P'_z[m] = P_z(\mathcal{Z}_m)/P_{\overline{\text{GIB}}}$, the probability of symbol error is

$$P_e = \sum_{m=1}^{2M'} \sum_{\substack{n=1 \\ n \neq m}}^{2M'} P'_{yz}[m,n]. \tag{7}$$

Performance of CQA is derived by forming a two-sided set of $4M'$ QIs without the guardband, where the m_{th} raw interval is $\mathcal{W}_m = [w_m, w_{m+1}]$. Alice groups these into pairs of left (L) and right intervals (R),

$$\mathcal{Y}_{L,m} = \mathcal{W}_{2m-1}, \quad \mathcal{Y}_{R,m} = \mathcal{W}_{2m}, \tag{8}$$

and $\mathcal{Y}_m = \mathcal{Y}_{L,m} \cup \mathcal{Y}_{R,m}$. For each observed channel, Alice shares a quantization map (QM) bit with Bob, where QM=0 if $Y \in \bigcup_{m=1}^{2M'} \mathcal{Y}_{L,m}$, and QM=1, otherwise. Bob's QI map depends on the QM bit, or

$$\mathcal{Z}_{L,m} = [w_{2m-1} - \Delta w_{2m-2}, w_{2m} + \Delta w_{2m}],$$
$$\mathcal{Z}_{R,m} = [w_{2m} - \Delta w_{2m-1}, w_{2m+1} + \Delta w_{2m+1}], \tag{9}$$

$\mathcal{Z}_m = \mathcal{Z}_{L,m}$ or $\mathcal{Z}_{R,m}$ for QM=0 and 1, respectively, and $\Delta w_m = (w_{m+1} - w_m)/2$. Probability of symbol error is given by (7) with $P'_{yz}[m,n] = P_{yz}(\mathcal{Y}_{L,m}, \mathcal{Z}_{L,n}) + P_{yz}(\mathcal{Y}_{R,m}, \mathcal{Z}_{R,n})$ and $P_{\overline{\text{GIB}}} = 1$.

For the complex channel with M two-dimensional QSs, the probability of symbol error is $P'_e = 1 - (1 - P_e)^2$. In [3] and [4], only symbol error rate (SER) was considered, and here we derive the exact BER assuming Gray coding. From (7), bit error probability (BER) is

$$P_b = \frac{1}{\log_2(2M')} \sum_{m=1}^{2M'} \sum_{\substack{n=1 \\ n \neq m}}^{2M'} P'_{yz}[m,n]\ T_{mn}, \tag{10}$$

where T_{mn} is the number of error bits when interval (symbol) m is observed by Alice but interval n is observed by Bob. Defining the distance (in intervals) between the m_{th} interval and n_{th} interval as

$$d_{mn} = \min[\ |m-n|\ ,\ 2M' - |m-n|\ ], \tag{11}$$

where $\min[.,.]$ chooses the smaller number, we can express T_{mn} in terms of d_{mn} as

$$T_{mn} = \begin{cases} d_{mn}, & \text{if } d_{mn} = 0,1,2 \\ 2, & \text{if } d_{mn} = 4,8 \\ 1, & \text{if } d_{mn} = 3 \text{ and } s_{mn} = 5+4k \\ 3, & \text{if } d_{mn} = 3 \text{ and } s_{mn} \neq 5+4k \\ 1, & \text{if } d_{mn} = 5,7 \text{ and } s_{mn} = 9+8k \\ 3, & \text{if } d_{mn} = 5,7 \text{ and } s_{mn} \neq 9+8k \\ 2, & \text{if } d_{mn} = 6 \text{ and } (s_{mn} = 8+8k \text{ or } s_{mn} = 10+8k) \\ 4, & \text{if } d_{mn} = 6 \text{ and } (s_{mn} \neq 8+8k \text{ and } s_{mn} \neq 10+8k) \end{cases} \tag{12}$$

where $s_{mn} = m+n$, and k is a positive integer. Eq. (12) is valid for M=256, 64, 16 and 4, where maximum values of $d_{m,n}$ are 8, 4, 2 and 1, respectively.

Simple efficiency is defined as the number of error-free bits per channel observation, or

$$\eta = P_{\text{GIB}}^2 (1-P_b)\log_2(M) \quad \text{(bits/channel).} \tag{13}$$

Results

The BER for CQA (varying M) and CQG (M= 4 and varying g) is plotted in Figure 1(a) for a single complex scalar channel with unit variance and estimation error $\sigma_1^2 = \sigma_2^2 = \sigma^2$, so that SNR=$1/\sigma^2$. Although BER is reduced significantly with CQG, the efficiency is decreased whereas CQA provides comparable BER without reduction in efficiency as seen in Figure 1(b). The efficiency is compared with the information theoretic bound I_k given in [4] for exact BER as well as BER=SER assumption. Although the efficiency of both methods in low SNR seems larger than I_k, error control coding in this regime would reduce the effective number of secure bits and true efficiency must be lower than I_k. As an example, we consider cyclic redundancy check (CRC) error detection of key bits in which the data blocks with errors are discarded. Although the exact number of CRC bits required for a target rate of undetected error is unknown, we make a simple assumption such that the number of CRC bits per block is

$$N_c = \lceil \alpha \; N_e \rceil = \lceil \alpha \; P_{b,raw} \; N_x \rceil, \tag{14}$$

where N_e is the expected error bits per block of key bits having length N_x, P_b is the BER before error detection, and α is a protection factor giving the required CRC bits per expected error bit. Here we take α= 1 and 2 for the comparison of the performance. The efficiency after error detection coding is

$$\eta_c = P_{\text{GIB}}^2 \frac{N_x - N_c}{N_x/\log_2 M}[1-P_b]^{N_x} \quad \text{(bits/channel),} \tag{15}$$

where the value of N_x is chosen to maximize (15). Note that this expression assumes that protection CRC bits are subtracted from the generated key bits, since a protection bit potentially conveys one bit of information about the key to the eavesdropper.

Figure 2 plots the modified efficiency η_c based on (15) considering exact P_b which is below the I_k bound in the low SNR region as opposed to η. Since significant CRC overhead is used due to high P_b, the efficiency decreases. However, η_c for α=1 is still above the bound in some cases, indicating insufficient CRC bits to detect the error to a target level. For CQG with $g = 4\sigma$, η_c is insensitive to α, since only a single bit (parity) is needed to detect at most a single expected bit error per block.

Conclusion

This paper has computed the bit error rate (BER) performance of two practical key generation methods CQG and CQA considering Gray coded mapping. An improved efficiency metric was also presented that gives a more realistic indication of key generation performance.

Acknowledgment

This work was supported by the German Research Foundation (DFG) under the COIN program.

References:

[1] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Trans. Commun.*, vol. 43, pp. 3–6, Jan. 1995.

[2] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Proc. 2008 IEEE Intl. Conf. Acoustics, Speech, and Signal Processing*, Las Vegas, NV, Mar. 31-Apr. 4, 2008, pp. 3013– 3016.

[3] J. Wallace, C. Chen, and M. Jensen, "Key generation exploiting MIMO channel evolution: Algorithms and theoretical limits," in *3rd European Conference on Antennas and Propagation (EuCAP '09)*, Berlin, Germany, Mar. 23-27, 2009, pp. 1499 – 1503.

[4] J. Wallace, "Secure physical layer key generation schemes: Performance and information theoretic limits," in *IEEE International Conference on Communications (ICC '09)*, Dresden, Germany, June 14-18, 2009, pp. 1–5.

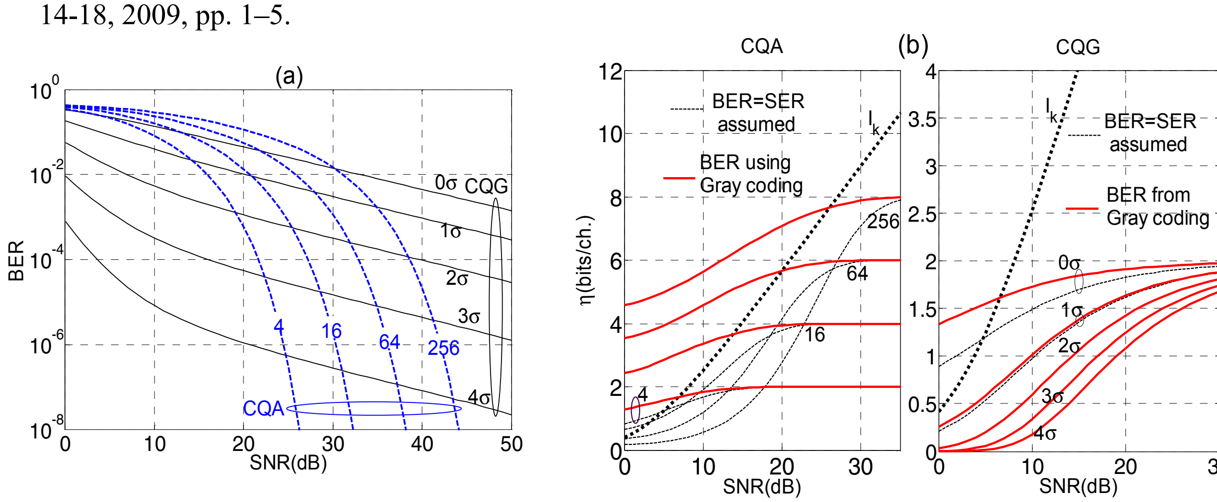

Figure 1: (a) Exact bit error rate (BER) of CQG for M=4 and different guardbands and CQA for different values of M using Gray coding. (b) Simple efficiency of CQA for different levels of M (left) and CQG with M=4 and increasing guardband size (right).

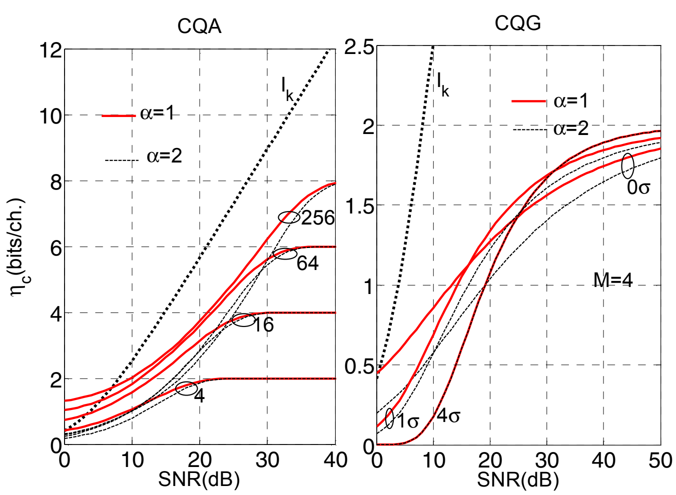

Figure 2: Comparison of improved efficiency definition to I_k, considering CRC bits for error detection