Secure Physical Layer Key Generation Schemes: Performance and Information Theoretic Limits

Jon Wallace

School of Engineering and Science
Jacobs University Bremen, Campus Ring 1, 28759 Bremen, Germany
Phone: +49 421 200 3197 Email: wall@ieee.org

***Abstract*— There is growing interest in wireless security methods that provide strong or even perfect secrecy by taking advantage of features of the physical propagation channel. In advantage-based methods, high channel quality in an average or opportunistic sense is exploited between two legitimate nodes, such that nonzero secrecy capacity can be achieved. Since such methods require bounds on the quality of the eavesdropper channel, they are somewhat impractical. Secret key generation based on tracking channel evolution in time division duplex systems is a more attractive option, where two nodes generate secret key bits based on a mutually known random channel. Since the eavesdropper channel is typically independent of the legitimate channel, the key can only be broken by brute force attacks, which are difficult when new keys are continuously generated. In this paper, the information theoretic limits of key generation schemes are investigated, based on the level of estimation error, temporal correlation, and dependence of the eavesdropper and legitimate channels. Two practical candidate key generation schemes are also considered: channel quantization and channel quantization with guardband.**

I. Introduction

Security is an important concern for wireless networks where by nature signals are transmitted in a broadcast fashion, and there is growing interest in methods that provide strong or even perfect secrecy by taking advantage of the behavior of wireless channels. For example, if the legitimate users have a channel with an SNR advantage relative to a potential eavesdropper, there exists a nonzero secrecy capacity, allowing finite information to be exchanged without giving any information to the eavesdropper [1], [2]. For fading channels, pairs of users can signal opportunistically to create an effective SNR advantage relative to an eavesdropper, thus providing nonzero secrecy capacity even when the eavesdropper has an average SNR advantage. A problem with advantage-based methods is that some knowledge or bound about the eavesdropper channel quality is required.

Alternatively, secret keys can be generated based on fluctuations or evolution of the channel state [3]–[5]. In a wireless system with time-division duplex (TDD), the forward and reverse propagation channels are identical by reciprocity. When there is high multipath, rapid fading causes the channel to the eavesdropper to be independent of the legitimate channel. Even for a line-of-sight (LOS) channel without multipath, random movement can cause channel phase fluctuations that are independent at multiple nodes. The evolving channel state information represents common randomness [6], [7] that can be observed by the legitimate transmitter and receiver, but not at the eavesdropper, allowing keys to be dynamically generated. Since secret key generation only requires channel independence, it may be more practical than advantage-based methods.

In practice, a number of factors limit the rate at which secret key bits can be generated: (1) estimation error, (2) spate-time correlation, and (3) dependence of the eavesdropper and legitimate channel. This paper provides an information theoretic analysis of these factors for vector Gaussian channels, indicating fundamental limits on the number of unique key bits that can be generated per channel realization.

In addition to the information theoretic analysis, two simple and practical key generation schemes are considered: channel quantization (CQ) [4] and a new extension to CQ that includes guardband (CQG). The methods are simulated for a path-based fading channel model, and their performance is compared in terms of efficiency and the mismatch rate of key bits.

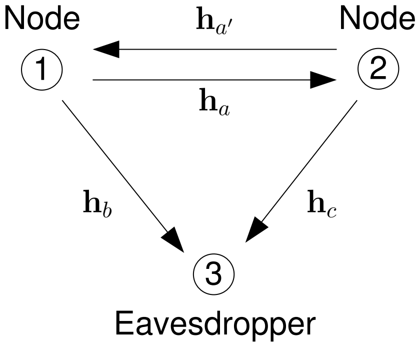

Fig. 1. System model for a wireless communications scenario consisting of legitimate communicating nodes 1 and 2 as well as a node 3 that is an eavesdropper

II. System Model

Figure 1 depicts the model for a wireless communications system. Nodes 1 and 2 are legitimate users that would like to communicate securely, while node 3 is a potential eavesdropper. Reciprocal vector channels $\mathbf{h}_a = \mathbf{h}_{a'}$ are referred to as the *forward* and *reverse* channels for legitimate communications, which are estimated by nodes 2 and 1, respectively. Channels $\mathbf{h}_b$ and $\mathbf{h}_c$, on the other hand, convey information to (and are estimated by) the eavesdropper. Due to noise, the nodes have imperfect estimates of the channels, or

$$\hat{\mathbf{h}}_a = \mathbf{h}_a + \boldsymbol{\epsilon}_2, \;\; \hat{\mathbf{h}}_{a'} = \mathbf{h}_{a'} + \boldsymbol{\epsilon}_1, \;\; \hat{\mathbf{h}}_b = \mathbf{h}_b + \boldsymbol{\epsilon}_3, \;\; \hat{\mathbf{h}}_c = \mathbf{h}_c + \boldsymbol{\epsilon}_3, \tag{1}$$

where $\boldsymbol{\epsilon}_i$ is zero-mean complex Gaussian estimation error at node i having variance σ_i^2. Note that the meaning of the elements in the channel vectors is arbitrary and can refer to multiple frequency bins, stacked elements of a multiple-input multiple-output (MIMO) channel, or both.

In the analysis, it is assumed that the channels are also zero-mean correlated complex Gaussian random processes, characterized by the covariance matrices

$$\mathbf{R}_{rp} = \mathrm{E}\left\{\mathbf{h}_r \mathbf{h}_p^H\right\} \qquad \hat{\mathbf{R}}_{rp} = \mathrm{E}\left\{\hat{\mathbf{h}}_r \hat{\mathbf{h}}_p^H\right\}, \tag{2}$$

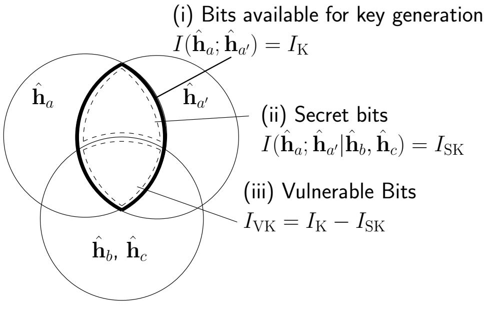
(i) Bits available for key generation
$I(\hat{\mathbf{h}}_a;\hat{\mathbf{h}}_{a'}) = I_{\mathrm{K}}$
$\hat{\mathbf{h}}_a$
$\hat{\mathbf{h}}_{a'}$
(ii) Secret bits
$I(\hat{\mathbf{h}}_a;\hat{\mathbf{h}}_{a'}|\hat{\mathbf{h}}_b,\hat{\mathbf{h}}_c) = I_{\mathrm{SK}}$
(iii) Vulnerable Bits
$I_{\mathrm{VK}} = I_{\mathrm{K}} - I_{\mathrm{SK}}$
$\hat{\mathbf{h}}_b$, $\hat{\mathbf{h}}_c$

Fig. 2. Graphical representation of quantities for key generation

where $\{r,p\} \in \{a,a',b,c\}$. For simplicity, it is assumed that the processes are not temporally correlated, which could be achieved by only sampling the links at intervals much longer than the coherence time or performing a pre-whitening operation. Scenarios with nonzero channel mean can also be handled by subtracting this mean from the channels, as this does not change mutual information.

A two-dimensional path-based channel model will be used to describe the links in Figure 1. The general MIMO channel from transmitter k of node n to receiver i of node m is

$$\begin{aligned} h_{ik}^{(m,n)} = \sum_{\ell} \beta_{\ell}^{(m,n)} \exp\{j2\pi[x_i^{(m)}\cos\phi_{\ell}^{(m,n)} + y_i^{(m)}\sin\phi_{\ell}^{(m,n)} \\ + x_k^{(n)}\cos\phi_{\ell}^{(n,m)} + y_k^{(n)}\cos\phi_{\ell}^{(n,m)}]\}, \end{aligned} \tag{3}$$

where $\beta_{\ell}^{(m,n)}$, $\phi_{\ell}^{(m,n)}$, and $\phi_{\ell}^{(n,m)}$ are the complex gain, angle of arrival, and angle of departure of the ℓth path, and $(x_i^{(m)}, y_i^{(m)})$ is the coordinate of the ith antenna in wavelengths at node m. The general covariance of the links between the nodes is represented as

$$r_{i_1k_1,i_2k_2}^{(m_1,n_1;m_2,n_2)} = \mathrm{E}\left\{h_{i_1k_1}^{(m_1,n_1)} h_{i_2k_2}^{(m_2,n_2)*}\right\}, \tag{4}$$

where i and k are stacked to obtain a standard covariance matrix. Channel variation can arise due to changing gains β_{ℓ}, positions of the nodes, or path angles.

An important special case is that of a common transmitter $n_1 = n_2 = n$ with close receiver nodes, so that the path angles for the two receivers are identical: $\phi_{\ell}^{(m_1,n)} = \phi_{\ell}^{(m_2,n)}$ and $\phi_{\ell}^{(n,m_1)} = \phi_{\ell}^{(n,m_2)}$. Assuming that just the transmitter moves randomly in a large area, the covariance reduces to

$$r_{i_1k_1,i_2k_2}^{(m_1,n;m_2,n)} = \sum_{\ell} |\beta_{\ell}^{(m_1,n)}|^2 \exp(j2\pi\psi_{i_1k_1,i_2k_2}^{(m_1,m_2,n)}) \tag{5}$$

$$\begin{aligned} \psi_{i_1k_1,i_2k_2}^{(m_1,m_2,n)} = \; & (x_{i_1}^{(m_1)} - x_{i_2}^{(m_2)})\cos\phi_{\ell}^{(m_1,n)} \\ & + (y_{i_1}^{(m_1)} - y_{i_2}^{(m_2)})\sin\phi_{\ell}^{(m_1,n)} \\ & + (x_{k_1}^{(n)} - x_{k_2}^{(n)})\cos\phi_{\ell}^{(n,m_1)} \\ & + (y_{k_1}^{(n)} - y_{k_2}^{(n)})\sin\phi_{\ell}^{(n,m_1)}. \end{aligned} \tag{6}$$

III. INFORMATION THEORETIC ANALYSIS

Figure 2 graphically depicts the quantities to be identified in this section, indicating the number of common key bits that can be generated and how many of these may be received by the eavesdropper. The estimated random channels $\hat{\mathbf{h}}_{a'}$ and $\hat{\mathbf{h}}_a$ are observed by nodes 1 and 2, respectively, and the maximum number of information bits extracted from this process for key generation is $I_{\mathrm{K}} = I(\hat{\mathbf{h}}_a;\hat{\mathbf{h}}_{a'})$. The number of secure bits is the remaining mutual information when the eavesdropper channels are already known or $I_{\mathrm{SK}} = I(\hat{\mathbf{h}}_a;\hat{\mathbf{h}}_{a'}|\hat{\mathbf{h}}_b,\hat{\mathbf{h}}_c)$. The number of vulnerable key bits that can be obtained by the eavesdropper is the difference of these two quantities, or $I_{\mathrm{VK}} = I_{\mathrm{K}} - I_{\mathrm{SK}}$.

Assuming correlated zero-mean complex Gaussian random vectors for the links, we have

$$\begin{aligned} I_{\mathrm{K}} &= h(\hat{\mathbf{h}}_a) + h(\hat{\mathbf{h}}_{a'}) - h(\hat{\mathbf{h}}_a, \hat{\mathbf{h}}_{a'}) \\ &= \log_2(\pi e)^{N_a}|\hat{\mathbf{R}}_{aa}| + \log_2(\pi e)^{N_a}|\hat{\mathbf{R}}_{a'a'}| \\ &\quad - \log_2(\pi e)^{2N_a}|\hat{\mathbf{R}}_{AA'}| \\ &= \log_2 \frac{|\hat{\mathbf{R}}_{aa}||\hat{\mathbf{R}}_{a'a'}|}{|\hat{\mathbf{R}}_{AA'}|}, \end{aligned} \tag{7}$$

where N_r is the number of elements in $\mathbf{h}_r$, and covariances of combined (stacked) random vectors are defined as

$$\hat{\mathbf{R}}_{P_1\ldots P_M} = \mathrm{E}\left\{\mathbf{q}\mathbf{q}^H\right\}, \qquad \mathbf{q} = [\mathbf{p}_1^T\mathbf{p}_2^T\ldots\mathbf{p}_M^T]^T. \tag{8}$$

Straightforward evaluation reveals

$$\hat{\mathbf{R}}_{aa} = \mathbf{R}_{aa} + \sigma_2^2\mathbf{I} \tag{9}$$

$$\hat{\mathbf{R}}_{a'a'} = \mathbf{R}_{aa} + \sigma_1^2\mathbf{I} \tag{10}$$

$$\hat{\mathbf{R}}_{AA'} = \begin{bmatrix} \mathbf{R}_{aa} + \sigma_2^2\mathbf{I} & \mathbf{R}_{aa} \\ \mathbf{R}_{aa} & \mathbf{R}_{aa} + \sigma_1^2\mathbf{I} \end{bmatrix}. \tag{11}$$

Substituting into (7) and simplifying results in

$$I_{\mathrm{K}} = \log_2|\mathbf{R}_{aa}\mathbf{R}_{\sigma}^{-1} + \mathbf{I}|, \tag{12}$$

where

$$\mathbf{R}_{\sigma} = (\sigma_1^2 + \sigma_2^2)\mathbf{I} + \sigma_1^2\sigma_2^2\mathbf{R}_{aa}^{-1}. \tag{13}$$

Evaluation of the secret key bits I_{SK} gives

$$\begin{aligned} I_{\mathrm{SK}} &= I(\hat{\mathbf{h}}_a;\hat{\mathbf{h}}_{a'}|\hat{\mathbf{h}}_b,\hat{\mathbf{h}}_c) \\ &= h(\hat{\mathbf{h}}_a|\hat{\mathbf{h}}_b,\hat{\mathbf{h}}_c) + h(\hat{\mathbf{h}}_{a'}|\hat{\mathbf{h}}_b,\hat{\mathbf{h}}_c) - h(\hat{\mathbf{h}}_a,\hat{\mathbf{h}}'_a|\hat{\mathbf{h}}_b,\hat{\mathbf{h}}_c) \\ &= h(\hat{\mathbf{h}}_a,\hat{\mathbf{h}}_b,\hat{\mathbf{h}}_c) + h(\hat{\mathbf{h}}_{a'},\hat{\mathbf{h}}_b,\hat{\mathbf{h}}_c) \\ &\quad - h(\hat{\mathbf{h}}_b,\hat{\mathbf{h}}_c) - h(\hat{\mathbf{h}}_a,\hat{\mathbf{h}}_{a'},\hat{\mathbf{h}}_b,\hat{\mathbf{h}}_c) \\ &= \log_2 \frac{|\hat{\mathbf{R}}_{ABC}||\hat{\mathbf{R}}_{A'BC}|}{|\hat{\mathbf{R}}_{BC}||\hat{\mathbf{R}}_{AA'BC}|}, \end{aligned} \tag{14}$$

where the covariance matrices are again the covariance of the stacked subscripted variables.

For many practical scenarios, the eavesdropper will be far away from both nodes 1 and 2, in which case $\hat{\mathbf{h}}_b$ and $\hat{\mathbf{h}}_c$ are independent of $\hat{\mathbf{h}}_a$ and $\hat{\mathbf{h}}_{a'}$ and

$$I_{\mathrm{SK}} = \log_2 \frac{|\hat{\mathbf{R}}_A||\hat{\mathbf{R}}_{BC}||\hat{\mathbf{R}}_{A'}||\hat{\mathbf{R}}_{BC}|}{|\hat{\mathbf{R}}_{BC}||\hat{\mathbf{R}}_{AA'}||\hat{\mathbf{R}}_{BC}|}, \tag{15}$$

which reduces to (7), meaning all key bits are safe.

The worst case for security, however, is when the eavesdropper is near one of the nodes. Consider the case where the eavesdropper is near node 1 and only movement of node 2 or scatterers causes variation of $\mathbf{h}_c$ and $\mathbf{h}_a$. With the relative positions of node 1 and 3 fixed, $\mathbf{h}_b$ is not random and contains no information, and (14) reduces to

$$I_{\mathrm{SK}} = \log_2 \frac{|\hat{\mathbf{R}}_{AC}||\hat{\mathbf{R}}_{A'C}|}{|\hat{\mathbf{R}}_C||\hat{\mathbf{R}}_{AA'C}|}, \tag{16}$$

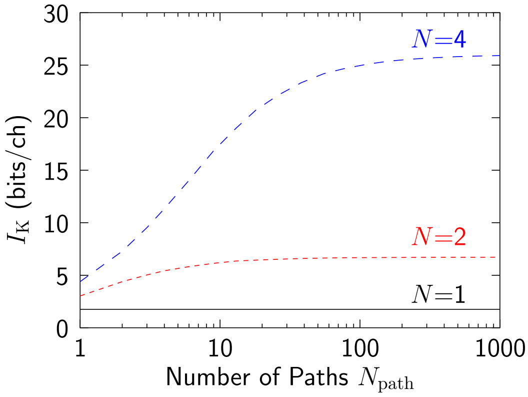

Fig. 3. Theoretical key bits that can be generated for N transmit and receive antennas and different levels of multipath for 10 dB SNR (channel to estimation error power ratio)

and the covariances can be written explicitly as

$$\hat{\mathbf{R}}_{AC} = \begin{bmatrix} \mathbf{R}_{aa} + \sigma_2^2\mathbf{I} & \mathbf{R}_{ac} \\ \mathbf{R}_{ac}^H & \mathbf{R}_{cc} + \sigma_3^2\mathbf{I} \end{bmatrix}, \tag{17}$$

$$\hat{\mathbf{R}}_{A'C} = \begin{bmatrix} \mathbf{R}_{aa} + \sigma_1^2\mathbf{I} & \mathbf{R}_{ac} \\ \mathbf{R}_{ac}^H & \mathbf{R}_{cc} + \sigma_3^2\mathbf{I} \end{bmatrix}, \tag{18}$$

$$\hat{\mathbf{R}}_{C} = \mathbf{R}_{cc} + \sigma_3^2\mathbf{I}, \tag{19}$$

$$\hat{\mathbf{R}}_{AA'C} = \begin{bmatrix} \mathbf{R}_{aa} + \sigma_2^2\mathbf{I} & \mathbf{R}_{aa} & \mathbf{R}_{ac} \\ \mathbf{R}_{aa} & \mathbf{R}_{aa} + \sigma_1^2\mathbf{I} & \mathbf{R}_{ac} \\ \mathbf{R}_{ac}^H & \mathbf{R}_{ac}^H & \mathbf{R}_{cc} + \sigma_3^2\mathbf{I} \end{bmatrix}. \tag{20}$$

A. Example Computations

In this section, numerical values for I_{K} and I_{SK} are presented for the path-based channel model with varying numbers of paths and numbers of antennas. For each plot, the results are averaged over 1000 random covariances, where the paths for each realization have angles uniform on $[0, 2\pi]$ and equal power, scaled to give total average unit power.

Figure 3 plots I_{K} versus the number of paths and the number of transmit and receive antennas N for an SNR of 10 dB, where SNR is the mean squared estimation error divided by mean squared channel gain. For a fixed number of antennas, the shared information saturates with increasing paths, and there is a dramatic increase in the available number of key bits with additional antennas N.

Figure 4 plots the relative number of vulnerable bits $I_{\mathrm{VK}}/I_{\mathrm{K}}$ for a single antenna scenario, where the eavesdropper is located a distance d (in wavelengths) from node 1. Although the eavesdropper can steal most of the key bits for little separation or limited multipath, the key bits are safe for realistic separation and moderate multipath.

Figure 5 considers a similar scenario with 4 antennas per user. In this case, although many more key bits can be generated, far richer multipath and separation are required to keep all bits safe. This suggests that adding antennas to enhance the generation rate of key bits potentially leaks increasing information to the eavesdropper.

How much information can be stolen when the eavesdropper has an advantage in SNR or the number of antennas is considered in Figures 6 and 7. For the single antenna system in Figure 6 the eavesdropper has an SNR of 30 dB compared to 10 dB for the legitimate users. The curves are shifted up slightly, but for moderate multipath and large separation, most key bits are still safe. Figure 7 indicates the result when the eavesdropper has 10 antennas compared to 4 antennas for the legitimate users. Far more paths are required to maintain secrecy of the key, suggesting that key generation schemes may still be vulnerable to eavesdroppers with a large advantage.

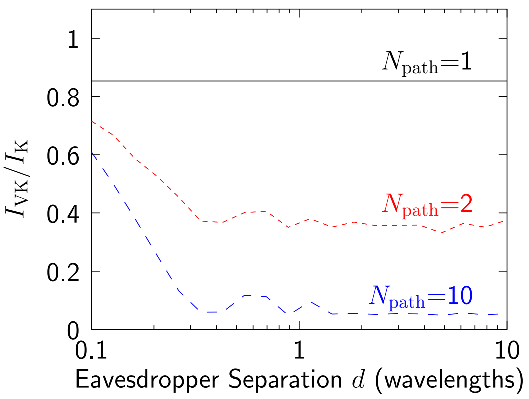

Fig. 4. Relative number of vulnerable key bits for single antenna channels for an eavesdropper at a distance d with varying levels of multipath and 10 dB SNR

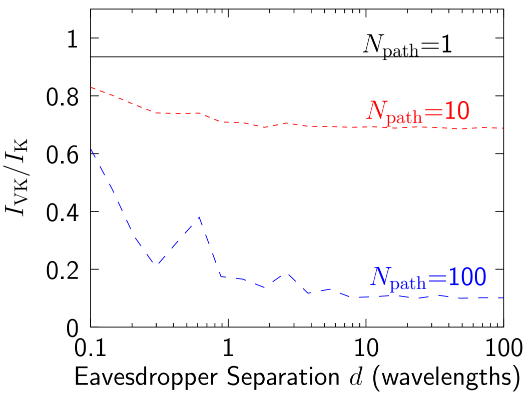

Fig. 5. Relative number of vulnerable key bits for $N = 4$ antennas for an eavesdropper at a distance d with varying levels of multipath and 10 dB SNR

IV. Practical Key Generation Methods

In this section, three different key generation methods are considered and compared in terms of their efficiency as well as their ability to keep key bits secret from an eavesdropper. Only single antenna channels will be considered, but multiple antenna extensions are possible by applying the methods to the multiple dimensions separately. For the following Monte Carlo simulations, curves were generated considering 10^5 channel realizations.

A. Channel Quantization (CQ)

Perhaps the simplest method for generating a random key at nodes 1 and 2 is for the two nodes to simultaneously quantize $\hat{\mathbf{h}}_{a'}$ and $\hat{\mathbf{h}}_a$, respectively [4]. Due to estimation error at the two nodes, sometimes the key bits will not match, necessitating some kind of error correction method over a public channel.

The channel quantization (CQ) is performed by dividing the total space of observable channels into decision regions, each with a unique bit pattern. Ideally the channel has equal probability of landing in any region. For vector channels, quantization can be performed individually to multiple independent channels, yielding more key bits per channel observation. This

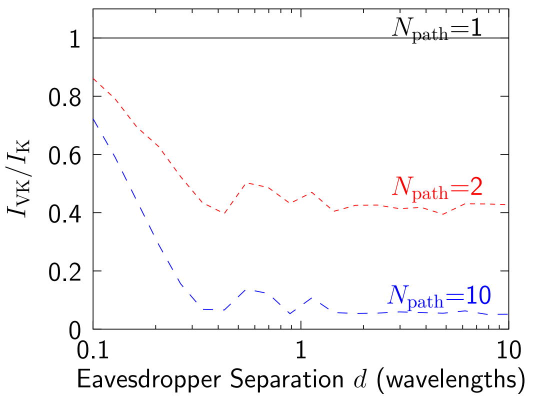

Fig. 6. Relative number of vulnerable key bits for an eavesdropper with an SNR advantage and single-antenna communications. SNR at the eavesdropper is 30 dB, while the SNR at the communicating nodes is only 10 dB.

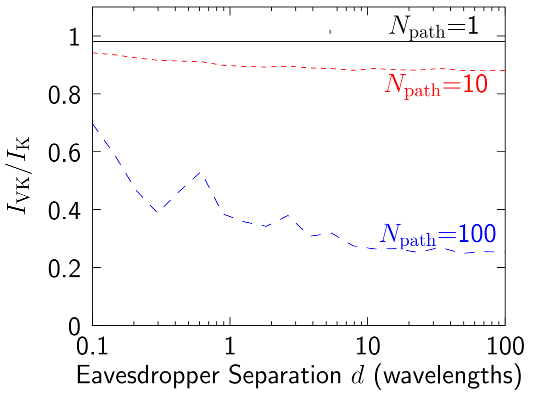

Fig. 7. Relative number of vulnerable key bits for an eavesdropper with an antenna advantage. The eavesdropper has 10 antennas compared to 4 at the communicating nodes, and SNR is 10 dB.

paper considers decision region patterns that are similar to those employed in phase shift keying (PSK) [4] and quadrature amplitude modulation (QAM).

Figure 8 depicts results for key generation with CQ using 4PSK regions versus the SNR. The efficiency (Eff) of the key generation is the number of matching key bits at nodes 1 and 2 that can be generated per channel realization. It is assumed that a symbol mismatch is essentially a deletion, so that all bits for that symbol are discarded. Also plotted is the ideal number of key bits available I_{K}. For the moderate SNR of 15 dB, it is noted that the symbol error rate (SER) is quite high (around 0.25), which may make forward error correction difficult. Although the method has acceptably low SER for high SNR, the efficiency is far below the theoretical limit. The fact that the Eff and I_{K} curves cross for low SNR is due to the simple definition of efficiency, since the good symbols at such high SER could not really be identified.

It should be noted that for practical implementation, any deterministic variation of the channel phase due to carrier offset between nodes should be removed before applying any CQ-like methods, since an eavesdropper can easily derive this variation by looking at the phase difference of channels $\hat{\mathbf{h}}_b$ and $\hat{\mathbf{h}}_c$. Although not rigorously derived or simulated, it is expected that the fraction of bits that can be stolen by the eavesdropper will follow the same behavior studied in Section III, which is to be considered in future work.

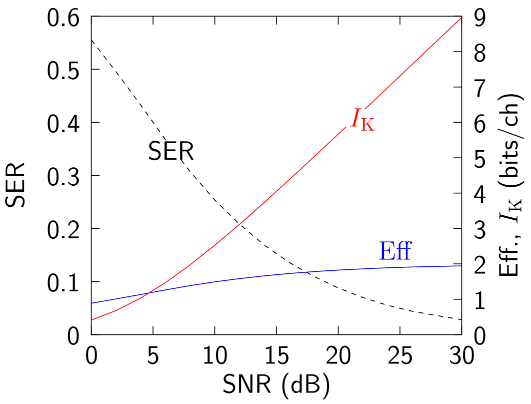

Fig. 8. Performance of key generation using channel quantization for 4PSK versus SNR

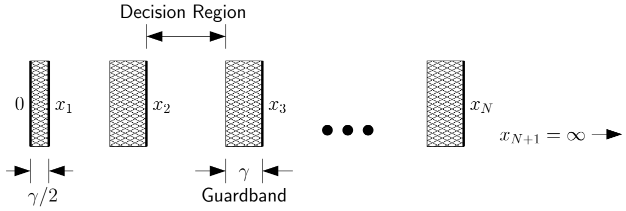

Fig. 9. Parameters for defining decision regions with guardband. Only one positive dimension of the QAM pattern is considered, where x_n is the start of the nth out of N total decision regions separated by guardband of size γ.

B. Channel Quantization with Guardband (CQG)

One of the problems with CQ is that when the channel state is near the boundary between two regions, there is a high probability of a symbol error. To overcome this problem and also to generalize the CQ idea, this work proposes dividing the domain of observable channels into equal probability regions with a specified guardband between those regions. For each observed channel, the nodes only add bits to the key if the observed channel did not fall in the guardband. A handshake mechanism is needed for the nodes to agree on whether a channel symbol should be accepted or not. The handshake can be uni-directional (node 1 always estimates and adds a symbol when node 2 sends the OK bit), or bi-directional (both nodes must agree that the observed channel is not in the guardband). By making the guardband large enough (a few standard deviations of the estimation error), the probability of making a symbol error can be made small.

A simple method for generating optimal decision regions is proposed here based on QAM. Figure 9 depicts the parameters of the QAM decision regions, and for regions symmetric with respect to the I and Q axes, the problem can be considered in just one dimension on the positive I axis. Here, γ is the desired minimum guardband between regions, and $x \in [x_n, x_{n+1} - \gamma]$ is the extent of the nth decision region.

The basic problem is to find the x_n such that the regions are equally probable, or

$$C = \int_{x_n}^{x_{n+1}-\gamma} p(x)dx, \tag{21}$$

for constant C with the required guardband, or

$$\begin{aligned} x_1 &= \gamma/2 \\ x_{n+1} &\geq x_n + \gamma \\ x_{N+1} &= \infty. \end{aligned} \tag{22}$$

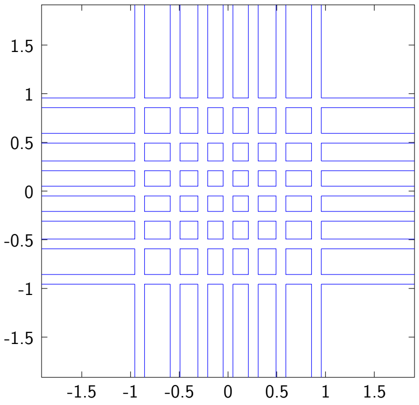

Fig. 10. Example CQG decision regions for 256QAM with $\gamma = 0.1$

The required regions (assuming unit-variance zero-mean Gaussian statistics on x) are obtained using an iterative procedure:

1. Set initial decision regions according to $x_1 = \gamma/2$, $x_{n+1} = x_n + \gamma$ for $n = 1, \ldots, N-1$ and $x_{N+1} = \infty$, which puts all non-guardband probability in the Nth decision region.
2. Compute probability taken by the guardband regions: $g_1 = \text{erf}(x_1)$ and $g_n = \text{erf}(x_n) - \text{erf}(x_n - \gamma)$ for $n = 2, \ldots, N$.
3. Compute updated decision regions by trying to distribute probability not used in guardbands equally to the regions, or for each $n = 2, \ldots, N-1$ compute

$$p_n = \text{erf}(x_n)$$

$$x_{n+1} = \text{erf}^{-1}\left[\frac{1 - p_n - \sum_{m=n+1}^{N} g_m}{N - (n-1)} + p_n\right] + \gamma$$

4. If the probabilities of the decision regions $p_{d,n} = \text{erf}(x_{n+1} - \gamma) - \text{erf}(x_n)$ are nearly equal (within some tolerance), stop. Otherwise, return to step 2.

As an example, Figure 10 shows the results for 256QAM generated with $N = 4$, $\gamma = 0.1$, and a tolerance of 10^{-6}, requiring only 9 iterations.

It is found that a two-way handshake gives significantly lower SER for nearly the same efficiency, so this will be used in the following examples. Figure 11 shows the performance of 4QAM (same as 4PSK for CQ) for 15 dB SNR versus guardband ranging from 0 to 4σ. Although the efficiency drops linearly with the increasing guardband, the SER drops exponentially allowing a level to be chosen that can be overcome with conventional error control techniques. Averaging channel estimates over many training symbols may make it possible to make channel estimation error very low for channels with slower temporal variation. Figure 12 depicts the results for higher SNR (30 dB) and a higher order 16QAM pattern. In this case, higher efficiency can be obtained, and moderate guardband reduces the SER to a manageable level.

A problem with CQG is that the guardband reduces the efficiency of the method since channel information is sometimes discarded. It is expected that an improved method could be developed that uses multiple decision region patterns and the handshake protocol selects the most beneficial pattern to avoid a disagreement. This way, a similar situation to guardband can be obtained, but without discarding observed channels, and this will be studied in future work.

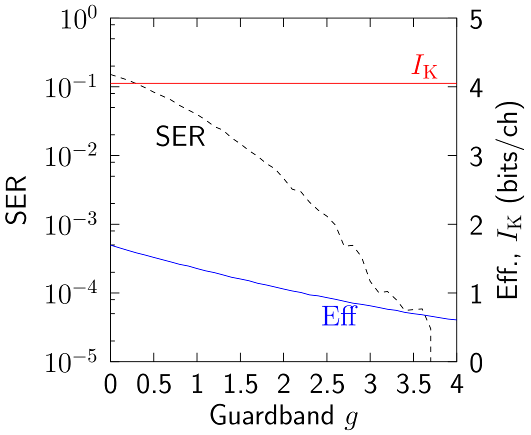

Fig. 11. Performance of channel quantization with guardband (CQG) versus the size of the guardband for 4QAM and 15 dB SNR

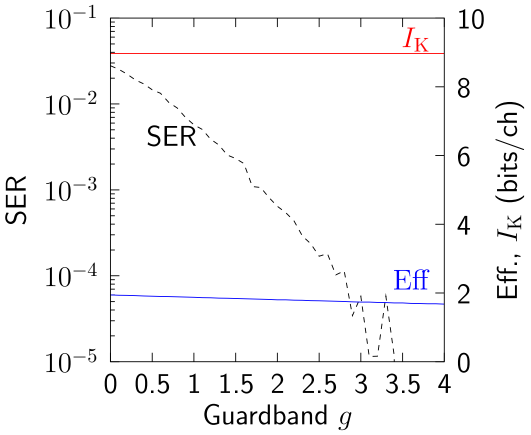

Fig. 12. Performance of CQG versus guardband for 16QAM modulation and 30 dB SNR

V. Conclusion

This paper has presented information theoretic limits for key generation schemes for correlated vector Gaussian channels. Two simple key generation methods were presented, and improving the efficiency and secrecy of these methods is the subject of ongoing work.

References

[1] A. O. Hero, III, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, pp. 3235–3249, Dec. 2003.

[2] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2515–2534, June 2008.

[3] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Trans. Antennas Propag.*, vol. 53, pp. 3776–3784, Nov. 2005.

[4] 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.

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

[6] I. Csiszar and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, pp. 344–366, Mar. 2000.

[7] S. Nitinawarat, "Secret key generation for correlated Gaussian sources," in *Proc. 2008 IEEE Intl. Symp. Inf. Theory*, Toronto, ON, 6-11 July 2008, pp. 702–706.