SECURE WIRELESS COMMUNICATIONS: SECRET KEYS THROUGH MULTIPATH

Akbar Sayeed[†] *and Adrian Perrig*[‡]

[†] University of Wisconsin-Madison
[‡] Carnegie Mellon University

ABSTRACT

Secure wireless communications is a challenging problem due to the shared nature of the wireless medium. Most existing security protocols apply cryptographic techniques for bit scrambling at the application layer by exploiting a shared secret key between pairs of communicating nodes. However, more recent research argues that multipath propagation – a salient feature of wireless channels – provides a physical resource for secure communications. In this context, we propose a protocol that exploits the inherent randomness in multipath wireless channels for generating secret keys through channel estimation and quantization. Our approach is particularly attractive in wideband channels which exhibit a large number of statistically independent degrees of freedom (DoF), thereby enabling the generation of large, more-secure, keys. We show that the resulting keys are distinct for distinct pairwise links with a probability that increases exponentially with the key-size/channel DoF. We also characterize the probability that the two users sharing a common link generate the same key. This characterization is used to analyze the energy consumption in successful acquisition of a secret key by the two users. For a given key size, our results show that there is an optimum transmit power, and an optimum quantization strategy, that minimizes the energy consumption. The proposed approach to secret key generation through channel quantization also obviates the problem of key pre-distribution inherent to many existing cryptographic approaches.

Index Terms— key pre-distribution, channel estimation, quantization, wideband transceivers, energy minimization

1. INTRODUCTION

Secure wireless communications is a challenging problem due to the inherently shared nature of the wireless medium. Existing works on wireless security fall under three main categories. First, there is extensive work on secure protocols at the application layer based on cryptographic methods in which the transmitted bits are scrambled using a shared *secret key* between a pair of communication nodes (see, e.g., [1, 2]). Second, a number of researchers are building on the original information-theoretic formulation of secure communication due to Shannon [3] to characterize fundamental limits to secure communications over wireless channels. In particular, the problem of the wire-tap channel due to Wyner [4] is receiving considerable attention. Third, more recently there has been interest in physical layer security techniques that exploit the characteristics of wireless channels and systems (see, e.g., [5–7]).

In this paper, we propose a physical layer technique that exploits the characteristics of multipath propagation – a salient feature of wireless channels – for secure communication. Specifically, we exploit the fact that for sufficiently rich multipath, the wireless channels associated with pairwise communication links between users with *distinct spatial locations* exhibit statistically independent characteristics. In essence, in time-division duplexed systems, each pair of users shares a common stochastic channel that is statistically independent of all other shared channels in pairwise communication links. Furthermore, the independence of distinct channels increases with the dimension of the signal space, which can be quite large for modern wideband, multiantenna transceivers. Specifically, we propose a method for generating a *secret key* for each pairwise communication link by directly quantizing the phases of the channel coefficients of the shared common channel. Thus, the problem of *key pre-distribution* (see, e.g., [2]), common to many application-layer cryptographic methods, is obviated.

In the context of existing work, our approach is most similar to [5] in which the *differential* phase between two frequency tones is encoded for key generation. Larger keys are generated by repeating the two-tone procedure over time. Error control coding techniques are also proposed in [5] for enhancing the reliability of key acquisition. In contrast, our emphasis is on exploiting the large number of random degrees of freedom in wideband wireless channels for generation of large secret keys. A significant contribution of this paper is the characterization of a key parameter – the probability, $p(\mathrm{SINR}, Q)$, that both ends of a link generate the same quantization index for a particular phase – as a function of the operating signal-to-interference-and-noise ratio SINR and the number of quantization levels Q. This characterization is then exploited for optimizing the protocol for successful key acquisition with minimum energy consumption. Thus, the results of this paper and [5] are complementary: the use of error control coding in [5] could enhance the performance of the scheme proposed here, whereas the characterization of p could facilitate the analysis and optimization of the method in [5]. Finally, we note that [6] builds on the protocol in [5] to propose secure transmission schemes, whereas [7] analyzes the information-theoretic aspects of secure communication in ultra-wideband channels.

2. SYSTEM MODEL

2.1. Physical Layer Model

We consider an OFDM system with $N = TW$ tones: each OFDM packet is of duration T and bandwidth W. The system equation from user i to user j is given by

$$\boldsymbol{r}_j = \boldsymbol{H}_{j,i}\boldsymbol{x}_i + \boldsymbol{w}_j \tag{1}$$

where $\boldsymbol{x}_i$ and $\boldsymbol{r}_j$ denote the N dimensional transmitted and received signal vectors, $\boldsymbol{H}_{j,i} \in \mathcal{C}^{N\times N}$ denotes the (stochastic) channel matrix, and $\boldsymbol{w}_j$ denotes the N dimensional vector of AWGN and interference from other simultaneous transmissions. We consider *reciprocal* channels, $\boldsymbol{H}_{i,j} = \boldsymbol{H}_{j,i}$, as in time-division duplexing.

In slowly time-varying channels, $\boldsymbol{H}$ is diagonal. To capture the statistically independent degrees of freedom (DoF), we consider a simple block fading model for $\boldsymbol{H}$:

$$\boldsymbol{H} = \mathrm{diag}(h(1)\cdots h(1), h(2)\cdots h(2), \cdots, h(D)\cdots h(D)) \tag{2}$$

This work was partly supported by the NSF grant CNS-0627589.

where the frequency band is split into D coherence bands, with $N_c = N/D$ OFDM tones per coherence band. In Rayleigh fading, the channel is characterized by D i.i.d. zero-mean complex Gaussian random variables $\{h(1), \cdots, h(D)\}$ and the N_c coefficients in the i-th coherence band are identical. Without loss of generality, we assume that $h(i) \sim \mathcal{CN}(0,1)$ and define $\boldsymbol{h} = [h(1), \cdots, h(D)]^T$ as the vector of i.i.d. channel coefficients, $\boldsymbol{h} \sim \mathcal{CN}(\boldsymbol{0}, \boldsymbol{I})$.

The basic idea behind cryptographic methods for secure communications is that each pair of communicating nodes share a *secret key*, s, not known to any other nodes, for encrypting their data. For our purposes, the most important property of a key, s, is that it is a *large* integer, e.g. a 128 bit integer. The key idea behind this work to generate secret keys, $\{s_i\}$, associated with distinct pairwise links, is to exploit the inherent randomness in the corresponding (reciprocal) channel vectors, $\{\boldsymbol{h}_i\}$. The randomness of the channel vectors associated with different pairwise communication links is a function of the *richness* of multipath and *minimum* spatial distance between different nodes. In this paper, we assume that the multipath is sufficiently rich and/or the users are sufficiently far apart so that all pairwise channel vectors, $\{\boldsymbol{h}_i\}$, are statistically independent of each other, in addition to having D i.i.d. entries.

Suppose that two nodes in a network want to establish a secure communication link. We propose a generalized request-to-send (RTS) protocol in which: i) both nodes estimate their common channel $\boldsymbol{h}_i$, and ii) generate their secret key s_i from the channel estimates. Note that this generalized RTS protocol requires training signals in both directions to help estimate $\boldsymbol{h}_i$. We consider a MMSE channel estimator for which the channel estimate generally takes the form

$$\hat{\boldsymbol{h}}_i = \boldsymbol{h}_i + \Delta\boldsymbol{h}_i \tag{3}$$

where $\hat{\boldsymbol{h}}_i$ denotes the estimate of $\boldsymbol{h}_i$. The errors in the estimate, $\Delta\boldsymbol{h}_i$, which include the impact of interference, can also be modeled as zero-mean Gaussian under mild assumptions. Furthermore, since the channel coefficients in $\boldsymbol{h}_i$ are i.i.d., it can be shown that the components of $\Delta\boldsymbol{h}_i$ are also statistically independent but are not identically distributed in general. That is, $\Delta\boldsymbol{h}_i \sim \mathcal{CN}(\boldsymbol{0}, \boldsymbol{\Lambda}_i)$ where $\boldsymbol{\Lambda}_i$ is a diagonal error covariance matrix. In this paper, for simplicity, we assume that the component errors, in addition to being independent are also identically distributed; that is,

$$\Delta\boldsymbol{h}_i \sim \mathcal{CN}(\boldsymbol{0}, \sigma^2\boldsymbol{I}) = \mathcal{CN}\left(\boldsymbol{0}, \frac{\boldsymbol{I}}{\mathrm{SINR}}\right) \tag{4}$$

where σ^2 denotes the combined variance of noise and interference, and $\mathrm{SINR} = E[|h_i(k)|^2]/E[|\Delta h_i(k)|^2] = 1/\sigma^2$ the signal-to-interference-and-noise-ratio in the estimate of each channel coefficient in (3). The SINR can be increased by increasing the power of training signals and is a key parameter that governs the performance of the proposed key generation scheme.

2.2. Random Key Generation From Channel Estimates

Let $\hat{\boldsymbol{h}}$ denote the estimate of the common channel in a pairwise communication link. How do we generate a key from $\hat{\boldsymbol{h}}$? A simple strategy is to quantize the phase of each component of the estimate

$$\hat{h}(k) = |\hat{h}(k)|e^{j\hat{\theta}(k)},\ k = 1, \cdots, D \tag{5}$$

$$\hat{\theta}(k) = \tan^{-1}(\mathrm{imag}(\hat{h}(k))/\mathrm{real}(\hat{h}(k))) \tag{6}$$

where $\hat{\theta}(k) \in [0, 2\pi]$ denotes the *random* phase of $\hat{h}(k)$. We uniformly quantize the phase of each component of $\hat{\boldsymbol{h}}$ into Q values. Let $f_Q : \mathcal{C} \to \{1, \cdots, Q\}$ denote this element-wise mapping. For $h = |h|e^{j\theta}$, we have

$$f_Q(h) = f_Q(\theta) = q \text{ if } \theta \in \left[\frac{2\pi(q-1)}{Q}, \frac{2\pi q}{Q}\right),\ q = 1, \cdots, Q\,. \tag{7}$$

Since the phase of each channel coefficient in (6) is random, we have

$$P\left(f_Q(\hat{h}(k)) = q\right) = P\left(f_Q(\hat{\theta}(k)) = q\right) = \frac{1}{Q}. \tag{8}$$

Let $\boldsymbol{f}_Q : \mathcal{C}^D \to \{1, \cdots, Q\}^D$ denote the vector-valued function that maps a D dimensional channel vector $\boldsymbol{h}$ into D quantized values corresponding to *element-wise* Q-level quantization of the phase of each component of $\boldsymbol{h}$; that is,

$$\boldsymbol{f}_Q(\boldsymbol{h}) = [f_Q(h(1)), \cdots, f_Q(h(D))]\,. \tag{9}$$

The key s associated with $\hat{\boldsymbol{h}}$ is defined by the correspondence

$$s\left(\hat{\boldsymbol{h}}\right) \leftrightarrow \boldsymbol{f}_Q\left(\hat{\boldsymbol{h}}\right) \tag{10}$$

Let us elaborate on this correspondence. First, the quantization of each phase value generates $\log_2(Q)$ bits of information since the phase is random. Furthermore, since the different components of $\hat{\boldsymbol{h}}$ in (3) are also statistically independent, applying the quantization to the D elements of $\hat{\boldsymbol{h}}$, as in (10), yields

$$b_{key} = D\log_2(Q) \tag{11}$$

bits of information. Thus, in essence, $f_Q\left(\hat{\boldsymbol{h}}\right)$ generates a b_{key}-bit integer and this integer serves as the key, s, in (10). If s represents a b_{key}-bit integer (say $b_{key} = 128$), then for a given D, the required number of quantization values is given by $Q = 2^{\frac{b_{key}}{D}}$. For example, for $b_{key} = 256$ and $D = 64$ (64 independent coherence bands in an OFDM channel), $Q = 16$.

3. PERFORMANCE OF CHANNEL-BASED RANDOM KEY GENERATION

3.1. Independence of Keys for Distinct Links

From a security perspective, the keys associated with distinct pairwise links should be distinct with high probability. Let $\boldsymbol{h}_1$ and $\boldsymbol{h}_2$ represent the channels corresponding to two distinct pairwise links, which are statistically independent under our assumptions. It follows that the estimates, $\hat{\boldsymbol{h}}_1$ and $\hat{\boldsymbol{h}}_2$, are also statistically independent, and as a result the b_Q-bit integers generated by $\boldsymbol{f}_Q\left(\hat{\boldsymbol{h}}_1\right)$ and $\boldsymbol{f}_Q\left(\hat{\boldsymbol{h}}_2\right)$ are also statistically independent. The following result quantifies the probability of generating distinct keys s_1 and s_2 via (10).

Proposition 1 *Let $s_1 \leftrightarrow \boldsymbol{f}_Q\left(\hat{\boldsymbol{h}}_1\right)$ and $s_2 \leftrightarrow \boldsymbol{f}_Q\left(\hat{\boldsymbol{h}}_2\right)$ represent b_{key}-bit keys. Under the assumption that $\boldsymbol{h}_1$ and $\boldsymbol{h}_2$ are statistically independent D-dimensional vectors*

$$P(s_1 \neq s_2) = P\left(\boldsymbol{f}_Q\left(\hat{\boldsymbol{h}}_1\right) \neq \boldsymbol{f}_Q\left(\hat{\boldsymbol{h}}_2\right)\right) = 1 - \frac{1}{Q^D} = 1 - \frac{1}{2^{b_{key}}} \tag{12}$$

Proof: The proof follows from a direct computation

$$P\left(\boldsymbol{f}_Q\left(\hat{\boldsymbol{h}}_1\right) \neq \boldsymbol{f}_Q\left(\hat{\boldsymbol{h}}_2\right)\right) = 1 - P\left(\boldsymbol{f}_Q\left(\hat{\boldsymbol{h}}_1\right) = \boldsymbol{f}_Q\left(\hat{\boldsymbol{h}}_2\right)\right)$$

$$= 1 - \prod_{k=1}^{D} P\left(f_Q\left(\hat{h}_1(k)\right) = f_Q\left(\hat{h}_2(k)\right)\right) \tag{13}$$

$$= 1 - \prod_{k=1}^{D} \frac{1}{Q} = 1 - \frac{1}{Q^D} \tag{14}$$

where the equality in (13) follows from the independence of the components of channel estimates and the element-wise operation of $\boldsymbol{f}_Q$. The second equality in (12) follows from (11). □

Note that the above result is independent of SINR. It basically says that the inherent channel randomness serves as a random key (number) generator via the proposed phase quantization.

3.2. Secret Key for A Common Link

In this section we analyze the acquisition of a shared secret key by the two nodes forming a pairwise communication link. Each user generates a key from its estimate of the common (reciprocal) channel via (10). For each pair of keys generated, the users do a secure handshake (e.g. along the lines of [2]) to confirm if they have generated identical keys.[1] If the keys are not identical, the users generate a new pair of keys, based on a new (independent) estimate of the channel. The process continues until both users generate the same key. Formally, let p_{key} denote the probability that both users generate the same key in one handshake. Let n denote the number of (independent) handshakes. Each handshake is a Bernoulli trial with p_{key} the probability of success. Then, the probability, $p_{succ}(n)$, that there is at least one successful handshake in n trials is given by

$$p_{succ}(n) = 1 - (1 - p_{key})^n \tag{15}$$

For a given p_{key}, the number of handshakes needed to achieve a desired (sufficiently high) p_{succ} is given by

$$n_{succ} = \frac{\log(1 - p_{succ})}{\log(1 - p_{key})} \ . \tag{16}$$

We now outline our approach for estimating p_{key}. Let $\boldsymbol{h}_o = [h_o(1), \cdots, h_o(D)]^T$ denote the common channel and let $\hat{\boldsymbol{h}}_F$ (forward) and $\hat{\boldsymbol{h}}_B$ (backward) denote the estimates of $\boldsymbol{h}_o$ at the two ends of the link. We model the channel estimates as

$$\hat{\boldsymbol{h}}_F = \boldsymbol{h}_o + \Delta\boldsymbol{h}_F \ , \ \hat{\boldsymbol{h}}_B = \boldsymbol{h}_o + \Delta\boldsymbol{h}_B \tag{17}$$

where $\Delta\boldsymbol{h}_F$ and $\Delta\boldsymbol{h}_B$ are modeled as in (4) and are also independent. The phase of each coefficient is quantized into Q levels resulting in a key with $b_{key} = D\log_2(Q)$ bits. Let p denote the probability that both users generate the same quantization index for a particular phase. By the assumption of uniform SINR across all coefficients (see (4)), p is identical for all coefficients. Thus, the probability that both users generate the same key is given by

$$p_{key} = p^D \tag{18}$$

and the problem of estimating p_{key} boils down to estimating p.

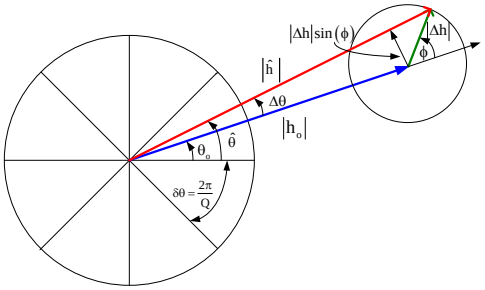

Fig. 1. The channel phase geometry.

[1] In the case of perfect channel estimates (no noise/interference), the two nodes will always generate the same key due to the common channel.

The probability p corresponds to generating a quantization index for one channel coefficient. As illustrated in Fig. 1, we can model the estimate of any one channel coefficient more explicitly as

$$\begin{aligned} \hat{h}_F &= h_o + \Delta h_F \ , \ |\hat{h}_F|e^{j\hat{\theta}_F} = |h_o|e^{j\theta_o} + |\Delta h_F|e^{j\phi_F} \\ \hat{h}_B &= h_o + \Delta h_B \ , \ |\hat{h}_B|e^{j\hat{\theta}_B} = |h_o|e^{j\theta_o} + |\Delta h_B|e^{j\phi_B} \end{aligned} \tag{19}$$

where the amplitudes are Rayleigh distributed and the phases are uniformly distributed over $[0, 2\pi]$. The phases $\hat{\theta}_F$ and $\hat{\theta}_B$ are uniformly quantized into Q levels with a resolution $\delta\theta = 2\pi/Q$, as in (7). Let $\hat{\theta}_{F,Q}$ and $\hat{\theta}_{B,Q}$ denote the quantized values. The probability p is a function of SINR and Q

$$p(\text{SINR}, Q) = P(\hat{\theta}_{F,Q} = \hat{\theta}_{B,Q}) \ , \tag{20}$$

that is, the probability that the two quantized phases lie in the same cell. Since, conditioned on θ_o, the phases at the two ends are independent, we can simply focus on a single phase

$$\hat{\theta} = \theta_o + \Delta\theta \tag{21}$$

where $\Delta\theta$ reflects the perturbation around the true underlying channel phase, θ_o, due to the interference and noise in the channel estimates. There are three key quantities in our analysis (see Fig. 1):

$$X = \frac{|\Delta h|}{|h_o|} - \text{inverse instantaneous SINR} \tag{22}$$

$$\theta_o \quad - \text{phase of } h_o \tag{23}$$

$$\phi \quad - \text{phase of } \Delta h \tag{24}$$

where ϕ is measured relative to θ_o. Due to symmetry, we can focus on computing p when the true channel phase is in the first quantization cell; $\theta_o \in [0, 2\pi/Q)$. As illustrated in Fig. 1, the phase perturbation can be computed as

$$\tan(\Delta\theta) = \frac{|\Delta h|\sin(\phi)}{|h_o| + |\Delta h|\cos(\phi)} = \frac{X\sin(\phi)}{1 + X\cos(\phi)} \approx X\sin(\phi) \tag{25}$$

$$\Delta\theta \approx \tan^{-1}(X\sin(\phi)) \tag{26}$$

where the approximation in (25) is valid at high SINR's ($X \ll 1$ with high probability). Note that $\phi \in [0, \pi) \leftrightarrow \Delta\theta \geq 0$ and $\phi \in [\pi, 2\pi) \leftrightarrow \Delta\theta \leq 0$.

We provide an approximate lower bound to p at high SINR's. Let $\gamma > 0$ denote a threshold and let $A = \{\hat{\theta}_{F,Q} = \hat{\theta}_{F,B}\}$. Then, we have the following lower bound on p

$$\begin{aligned} p(\text{SINR}, Q) &= P(A) = E[1_A] = E\left[1_A | X \leq \gamma\right] + E\left[1_A | X > \gamma\right] \\ &\geq E\left[1_A | X \leq \gamma\right] \end{aligned} \tag{27}$$

where 1_A denotes the indicator function for the set A. The lower-bound can be made arbitrarily tight by making

$$E\left[1_A | X > \gamma\right] \leq P(X > \gamma) = \frac{1}{\gamma^2\text{SINR} + 1} \tag{28}$$

arbitrarily small by choosing γ^2SINR sufficiently large. The last equality follows from the cdf/pdf of X

$$F_X(x) = P(X \leq x) = \frac{x^2}{x^2 + \sigma^2} \ , \ f_X(x) = \frac{2x\sigma^2}{(x^2 + \sigma^2)^2} \ . \tag{29}$$

In particular, we use the following value for the threshold[2] γ as a function of the quantization resolution, $\delta\theta = 2\pi/Q$

$$\gamma = \gamma_{max} = \tan(\delta\theta/2) = \tan(\pi/Q)\ . \tag{30}$$

The following result quantifies the probability $p(\text{SINR}, Q)$, which we state without proof due to lack of space.

Proposition 2 *For sufficiently high* SINR*, the probability that the same quantization index is generated for a particular channel coefficient at both ends of a link can be approximated as*

$$\begin{aligned} p(\text{SINR}, Q) &= P\left(\hat{\theta}_{F,Q} = \hat{\theta}_{B,Q}\right) \geq E[1_A | X \leq \gamma_{max}] \\ &\approx \frac{1}{2}\frac{\tan^2(\delta\theta/2)}{\tan^2(\delta\theta/2)+\sigma^2} + \frac{1}{\delta\theta}\int_0^{\delta\theta/2} \frac{\tan^2(\theta_o)}{\tan^2(\theta_o)+\sigma^2} d\theta_o \\ &\quad + \frac{4}{\pi^2\delta\theta}\int_{\theta_o=0}^{\delta\theta/2}\int_{x=\tan(\theta_o)}^{\tan(\delta\theta/2)} \frac{2x\sigma^2}{(x^2+\sigma^2)^2} \\ &\quad \left[\sin^{-1}(\tan(\theta_o)/x)\right]^2 dx d\theta_o \end{aligned} \tag{31}$$

where $\gamma_{max} = \tan(\delta\theta/2)$*,* $\delta\theta = 2\pi/Q$*, and* $\sigma^2 = 1/\text{SINR}$*.*

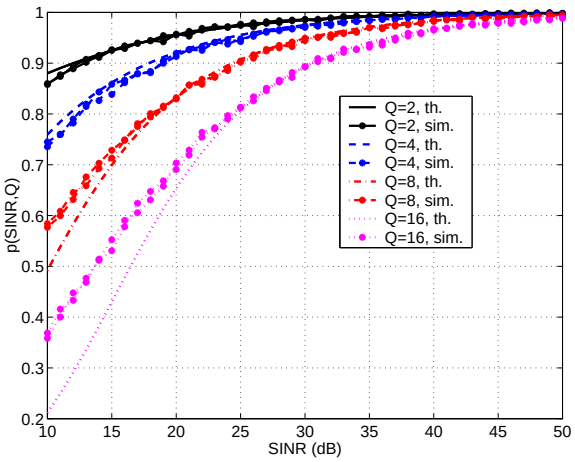

Fig. 2. Analytical vs. simulated values of $p(\text{SINR}, Q)$.

Fig. 2 compares the analytical (Prop. 2) and numerically estimated values of p as a function of SINR for different values of Q. As expected, a higher SINR is needed to achieve a desired p for higher values of Q. Furthermore, the analytical approximation is quite accurate for SINR ≥ 20 dB and $Q \leq 16$.

3.3. Minimum Energy Consumption for Secret Key Acquisition

In this section, we estimate the energy required for successful acquisition of a secret key by the two nodes of a pairwise communication link. For a given key size, b_{key}, and p_{succ}, the energy consumed can be estimated as

$$\mathcal{E} \propto \text{SINR} D n_{succ} = \text{SINR} D \frac{\log(1-p_{succ})}{\log(1-p(\text{SINR}, Q)^D)} \tag{32}$$

since SINR is per channel coefficient, D is the total number of channel coefficients, and n_{succ} is the minimum number of handshakes needed for guaranteeing successful key acquisition with probability p_{succ}. We are particularly interested in achieving a desired p_{succ} (say 0.99) for given b_{key} (say 128 bits) with minimum energy consumption. First, note from (32) that as SINR increases, the first factor in (32) increases, but so does $p(\text{SINR}, Q)$, which reduces $\mathcal{E}$. Thus, we expect an optimum value of SINR that minimizes $\mathcal{E}$. Second, this optimum SINR value is a function of Q and D that are constrained through (11). Thus, overall, we expect an optimum value of Q that minimizes $\mathcal{E}$ for a given p_{succ} and b_{key}:

$$Q_{opt}(p_{succ}, b_{key}) \leftrightarrow \text{SINR}_{opt} \leftrightarrow \mathcal{E}_{min} \tag{33}$$

This is illustrated in Fig. 3 where $\mathcal{E}$ is plotted as a function of SINR

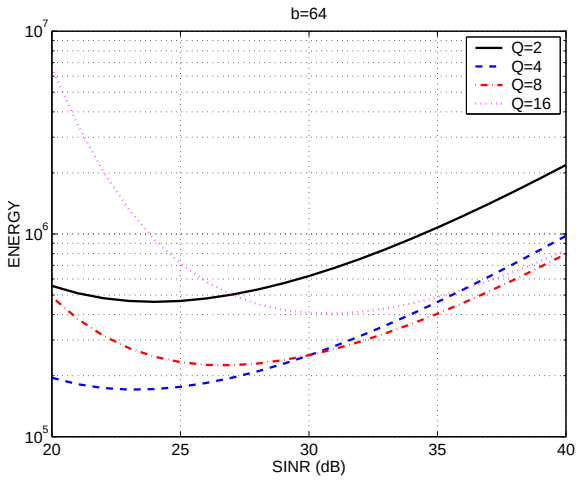

Fig. 3. $\mathcal{E}$ as a function of SINR for different values of Q.

for $b_{key} = 64$, $p_{succ} = 0.99$, and different values of Q. As evident, $Q_{opt} = 4$ ($D_{opt} = 32$) yields the lowest energy at $\text{SINR}_{opt} \approx 23$ dB. We note that the same value of Q_{opt} works for $b_{key} = 128$ or 256, but the corresponding SINR_{opt} gets higher with increasing b_{key} (as expected), resulting in higher $\mathcal{E}_{min}$ for larger values of b_{key}. The corresponding plots are not shown here for lack of space.

4. REFERENCES

[1] L. Zhou and Z. Haas, "Securing ad hoc networks," *IEEE Network Magazine*, pp. 24–30, Nov./Dec. 1999.

[2] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for wireless sensor networks," in *Proc. IEEE Symp. Security Privacy*, May 2003.

[3] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 29, pp. 656–715, 1949.

[4] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, 1975.

[5] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, "Cryptographic key agreement for mobile radio," *Digital Signal Processing*, vol. 6, no. 207-212, 1996.

[6] H. Koorapaty, A. A. Hassan, and S. Chennakeshi, "Secure information transmission for mobile radio," *IEEE Commun. Letts.*, pp. 52–55, Feb. 2000.

[7] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in UWB channels," *IEEE Tran. on Inform. Forens. Sec.*, pp. 364–375, Sep. 2007.

[2] γ_{max} reflects the largest value of X that does not result in an error when $\theta_o = \delta\theta/2$; that is, θ_o is at the center of the quantization cell.