

# On Enhancing the Reliability of Key Extraction Mechanisms from Wireless Channels

Youssef El Hajj Shehadeh<sup>1</sup>, Ammar El Falou<sup>2</sup>, and Dieter Hogrefe<sup>1</sup>

<sup>1</sup> Institute of Computer Science, University of Goettingen, Germany  
shehadeh@informatik.uni-goettingen.de

<sup>2</sup> Telecom Bretagne, Brest, France

**Abstract.** We investigate applying an error correcting code of small block size to enhance the performance of key generation from wireless channels. A trade-off between performance and secrecy is then studied. Preliminary results show that using a simple lower quantization approach achieves better performance than applying a small block size BCH code.

## 1 Introduction

Recently, much attention has been given to the wireless channel in the realm of generating secret keys. Indeed, it has been found that the multipath wireless channel forms by its nature a source of randomness which can be leveraged to derive a shared secret key between two wireless devices.

In our previous work [1], we have proposed intelligent mechanisms for channel quantization and key extraction achieving a high extraction rate of secret bits with a low probability of disagreement. While, in some other related works (ex. [2], [3]), a direct quantization approach has been considered accompanied with applying Error Correcting Codes (ECC) to enhance the performance at the cost of loosing some secrecy.

However, it is still unclear whether using ECC would achieve a good trade-off between performance and secrecy loss; as a matter of fact that the transmission of syndromes and/or parity check bits causes a loss of secrecy dependent on the code rate. Therefore, it is reasonable to question whether using ECC is the right choice to use to enhance the performance, particularly for relatively small block sizes.

In this paper, we investigate the application of a BCH code to increase the performance (measured as probability of error:  $P_e$ ) of the Phase Shifting (PS) mechanism presented in [1]. This mechanism mainly targets lowering  $P_e$  through a phase correction mechanism, and increasing the efficiency by optimizing the quantization precision for a  $P_e < 10^{-3}$ . More precisely, we compare the trade-off performance/secracy-loss between two approaches. In the first approach, we simply apply the PS mechanism with 1bit lower quantization precision than that elaborated in [1]. While in the second approach, we consider enhancing the PS quantization mechanism by including an error correction step. As a result, a lower number of secret bits would be expected but with a lower probability of error.

The rest of this paper is organized as follows. In section II, we present the system model and give an overview of the channel quantization and key extraction procedure. And finally in section III, we show some simulation results and draw out the conclusions.

## 2 Channel Quantization and Key Extraction

The wireless multipath channel can be modeled as a vector of independent channel taps following, without loss of generality, a Rayleigh distribution. Thus, representing each channel tap as a complex Gaussian term, the channel can be expressed as:

$$\mathbf{h} = (h_0, h_1, \dots, h_{L-1}), \quad (1)$$

where  $L$  is the number of taps also called the length of the channel.

We consider that the multipath wireless channel is reciprocal and common between two communicating nodes mainly called Alice and Bob, and uncorrelated from an eavesdropper which is located sufficiently far in space. Each of the legitimate nodes will then observe a noised estimate of the channel:

$$\mathbf{h}_A = \mathbf{h} + \mathbf{z}_A, \text{ and } \mathbf{h}_B = \mathbf{h} + \mathbf{z}_B, \quad (2)$$

where  $\mathbf{z}_A$  and  $\mathbf{z}_B$  are added white Gaussian noise at the two nodes. In this case, the theoretical bound on the maximum number of secret bits that can be generated can be found to be [2]:

$$N_k = I(\mathbf{h}_A, \mathbf{h}_B) = \sum_{i=0}^{L-1} \log_2 \left( 1 + TNR_i \cdot \frac{1}{2 + 1/TNR_i} \right), \quad (3)$$

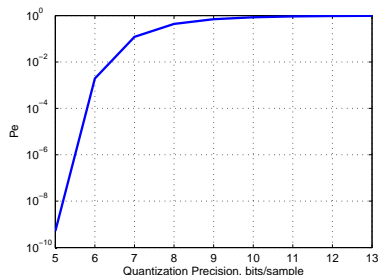
where  $TNR_i$  is here the Tap power to Noise Ratio for channel tap  $i$ .

In our previous work, we have proposed a quantization mechanism, called Phase Shifting (PS) [1], achieving high efficiency in secret bit extraction and low probability of disagreement (less than  $10^{-2}$ ).

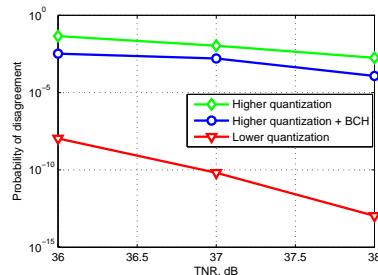
In Fig. 1, we show the probability of error using this quantization mechanism as a function of the quantization precision for a  $TNR = 36 \text{ dB}$ . It is clear here that using lower quantization precision leads to a lower probability of error. Therefore, a trivial approach to enhance the performance and reliability of the key generation mechanism is to use lower quantization precision. However, this leads to a lower number of secret bits extracted. Another approach to enhance the performance is to use ECCs. But using ECCs would also lead to loss in secrecy due to the need of sending syndromes and/or parity check bits. Therefore there is a performance-efficiency trade-off. The aim of this paper is to compare these two approaches in terms of performance at a certain cost of loss of secrecy.

## 3 Simulation Results and Discussions

In this section, we compare the performance of the two proposed approaches. Particularly, we consider using a 1bit lower quantization for the first approach,



**Fig. 1.:** Probability of error as a function of the quantization precision for a TNR=36dB, PS mechanism.



**Fig. 2.:** Probability of disagreement as a function of TNR for the two approaches.

while we use a BCH(127,106) ECC for the second approach. We consider quantizing a channel vector of 21 taps. At a TNR greater than 36 dB, a 6 bits quantization level is used. We will therefore obtain 126 secret bits at a higher probability of disagreement or 105 secret bits at a lower probability of disagreement following the first approach. On the other hand, using the second approach with a BCH(127,106) code, we would obtain 106 secret bits.

In Fig. 2, we plot the probability of disagreement as a function of TNR using these two approaches in addition to the main PS mechanism. We can observe clearly here that both approaches provide better performance. But the lower quantization precision approach provides a much better performance enhancement than the second approach. This is mainly due to the fact that using the BCH(127,106) ECC helps in correcting up to 3 bit errors while using a 1-bit lower quantization decreases dramatically the bit error rate as can be seen in Fig. 1.

Finally, we note that we tended to use small block size ECCs as a small number of secret bits is expected to be extracted from a single channel observation. However, it is interesting to study more powerful ECCs and larger block sizes, and compare their performance against using lower quantization precision for an equal secrecy loss. This would be the subject of our future research.

## References

1. El Hajj Shehadeh, Y., Alfani, O., Tout, K., Hogrefe, D.: Intelligent mechanisms for key generation from multipath wireless channels. In: *IEEE WTS '11*, New York, NY, April 2011.
2. Ye, C., Mathur, S., Reznik, A., Shah, Y., Trappe, W., Mandayam, N.: Information-theoretically Secret Key Generation for Fading Wireless Channels. In: *IEEE Trans. on Information Forensics and Security*, vol. 5, no. 2, pp. 240-254, June 2010.
3. Chen, C., Jensen, M.: Secret Key Establishment Using Temporally and Spatially Correlated Wireless Channel Coefficients. In: *IEEE Transactions on Mobile Computing*, pp. 1-11, July 2010.