ATLANTIS PRESS
Advances in Engineering Research (AER), volume 61
International Conference on Mechanical, Electronic, Control and Automation Engineering (MECAE 2017)

The Channel Quantization Alternating Algorithm in the Secret Key Generation System

Fuxing Guo [a], Dapeng Yu [b] and Gang Xin [c]

National Digital Switching System Engineering and Technological Research Center, Zhengzhou 450001, China

[a]fxingchina@163.com, [b]ydpntm@126.com, [c]downxg@163.com

Keywords: CQA Algorithm, Offset, Log Likelihood Ratio, Quantization Subinterval.

Abstract. In order to solve the problem that the high bit inconsistent rate between the two parties in the legal communication affects the key length , an improved CQA algorithm that calculating the log likelihood ratio that each bit is '0' or '1' after quantization sample value is proposed. Suppose both parties are Alice and Bob. The algorithm uses Alice's position index and Bob's sampling value to compute the conditional probabilities that each bit is '0' or '1' after quantize Alice's corresponding sample value. The probability log likelihood ratio is then calculated and the hard decision of the log likelihood ratio is used as the quantization result without having to quantize the sampled values by moving the quantization threshold. The simulation results show that the initial inconsistent rate of the improved algorithm is lower than that of the original quantization algorithm and the generated key is longer. When the number of quantization intervals is equal and the correlation coefficient between random variables is less than 0.87, the key length generated by the improved algorithm is increased by at least 0.15bits/symbol; When the number of quantization subintervals of the improved algorithm is 1/2 of the original algorithm and the correlation coefficient is less than 0.83, the key length generated by the improved algorithm is increased by at least 0.1bits/symbol.

1. Introduction

In the key generation process based on the wireless channel, both the legitimate communication Alice and Bob adopt the way of time division duplex (TDD) to carry on two-way detection to the wireless channel, by utilizing the reciprocity of the radio channel to extract the channel parameters of the respective received information to generate the secret key. Although the extracted channel information has strong correlation, the initial information sequence of the two parties is not consistent due to the difference of hardware between the two sides of communication and the noise from the outside, and the higher sequence inconsistency ratio not only reduces the efficiency of key reconciliation, but also shortens the key generation length.

In order to generate longer keys and reduce the times of key reconciliation, design a superior performance quantization algorithm is a critical step. In [1], Sana Hamida et al proposed an adaptive quantization algorithm, which adjusts the quantization threshold adaptively to reduce the bit error rate; In [2-3], a two-threshold quantization algorithm is adopted, the algorithm quantizes the value larger than the upper threshold to '1', smaller than the quantization of the lower threshold to '0', and discards the sampling value between the upper and lower thresholds, the uncertainty of quantization interval of sampled value is reduced, but the quantization factor of the algorithm is a fixed value, and there is no specific analysis of the value of the quantization factor to the key generation process; In [4], Wenbing Cai et al taked the key length as the objective function, computed the optimal quantization factor when using the two-threshold quantization to generate the longer key, so that the key length of each sample value increased at least 0.1 bits, but the algorithm quantization deleted a lot of the original information, in essence, or shorten the length of the generated key. In [5], Chan Chen et al proposed a CQA (Channel Quantization Alternating) quantization algorithm, which achieves reducing the error rate by exchanging the quantization error information and moving the quantization threshold of the other communication side; Reference [6] based on [5] taked the key length as the objective function to compute optimal

number of quantization bits for the longest key length. However, the algorithm needs to quantize again after moving the threshold, and ignoring the moving threshold does not necessarily correct the quantization result of Bob.

In order to improve the quantization performance of the algorithm, this paper, based on the CQA quantization model, improves the algorithm by computing the conditional probabilistic log-likelihood ratio of the sampled values of the communicating party, without moving any thresholds. The simulation results show that the proposed algorithm can increase the key length by at least 0.15 bits / symbol when the correlation coefficient of the random variable is less than 0.87.

2. Improvement of CQA Quantization Algorithm

Assume that Alice and Bob transmit the probe signal S in a time-division duplex manner in the coherence time. Alice receives the signal X and Bob receives Y. Because of the reciprocity of the wireless channel, the random variables X and Y received by the two legitimate communication sides have strong correlation, and the relationship between the received and transmitted signals can be expressed as:

$$\begin{cases} X = h_{ba} \bullet S + N_a \\ Y = h_{ab} \bullet S + N_b \end{cases} \tag{1}$$

Where the channel gains from Alice to Bob are expressed as h_{ab}, the channel gains from Bob to Alice are expressed as h_{ba}, N_a and N_b are the channel noise that obey complex Gaussian distribution.

In the original CQA algorithm, after receiving the signals, Alice first divides the X into N intervals with equal probability, then divide each interval i ($0 \le i \le$ N-1) into Q sub-interval with equal probability, Alice sends its subinterval index q ($0 \le q \le Q$)to Bob; Second, Bob calculates the threshold offset according to the received index value and moves all the quantization thresholds, and then quantizes the sampled value [5]. Although this algorithm reduces the quantization inconsistency to a certain extent, there is no guarantee that the quantization interval of the Bob samples after the threshold shift is corrected. To solve this problem, the quantization algorithm will be improved next.

This paper makes some changes on the basis of CQA quantization algorithm [7]. First of all, Alice deals the X similarly with the original algorithm, quantize the every region of X once again that has been quantized equal probability, but this time Bob just saves its sample values; Secondly, Alice sends its subinterval index to Bob according to the original CQA algorithm. Finally, Bob computes the quantization log likelihood ratio according to the sampled value y_i and the subinterval index q. Specific operations are as follows:

① If Alice code (Gray code) each sample into R bits, it will divide X equal probability into 2^R quantization intervals, and then the each interval is quantized into N subintervals. So X is divided into a total of $2^R * N$ sub-interval, set the boundaries of sub-interval are $a_0, a_1, \cdots, a_{2^R * N}$,

$$a_i = F^{-1}(i / (2^R * N)) \tag{2}$$

And $F^{-1}(\bullet)$ is the function of inverse cumulative integral.

②Alice determines the subinterval index q of the sampled values by the boundary of the subinterval and sends it to Bob. When Alice sends q, although the eavesdropping Eve may also wiretap the q, but it does not know the q belongs to which specific quantization interval, so even if the eavesdropper has acquired the index value q, the key information is still security.

③ Bob calculates the conditional probability of each bit being judged as '0' or '1' after encoding x_i according to q and y_i ,and then computes the logarithm of the ratio of their conditional probabilities, as:

$$Y_{i,u} = \log_2 \frac{P(\bigcup_{l_u \in L_u} x_{i,0,l_u} \mid y_i, q)}{P(\bigcup_{k_u \in K_u} x_{i,1,k_u} \mid y_i, q)} \tag{3}$$

Where $Y_{i,u}$ represents the log-likelihood ratio of the u-th bit after encoding y_i, y_i is the i-th sampled value of Bob, x_i is the i-th sampled value of Alice; $x_{i,0,l_u}$ represents the interval that the u-th bit is'0'after encoding x_i, l_u is the number of the interval and $0 \le l_u \le 2^R - 1$, $x_{i,1,k_u}$ represents the interval that the u-th bit is '1' after encoding x_i, k_u is the number of the interval and $0 \le k_u \le 2^R - 1$; L_u denotes the set of interval numbers whose the quantization interval of the L_u-th bit is '0' within the range of X, K_u denotes the set of interval numbers whose the quantization interval of the K_u-th bit is '1' within the range of X, and $1 \le u \le R$.

From equation (3) we can see that the first step of calculating the quantization log likelihood ratio is compute the conditional probability that the bit is '0' or '1' after encoding x_i, and the conditional probability that the u-th bit is '0' after encoding x_i can be expressed as equation(4):

$$P(\bigcup_{l_u \in L_u} x_{i,0,l_u} \mid y_i, q) = \frac{\sum_{l_u \in L_u} \int_{l_u * N + q - 1}^{l_u * N + q} f(x_{i,0,l_u}, y_i) dx}{\int_{-\infty}^{+\infty} f(x, y_i) dx} \tag{4}$$

Equation (4) can be further developed as follow:

$$P(\bigcup_{l_u \in L_u} x_{i,0,l_u} \mid y_i, q) = \frac{P(\bigcup_{l_u \in L_u} x_{i,0,l_u}, y_i, q)}{P(y_i, q)} = \frac{\sum_{l_u \in L_u} \iint f(x_{i,0,l_u}, y_i, q) dx dy}{p(q) \bullet \int f(x, y_i \mid q) dx} \tag{5}$$

And because Bob has known the value q that Alice sends to Bob by the public channel and y_i, it can be directly substituted into equation (5) to deduce the conditional probability that the u-th bit of coding x_i is '0', where $f(x, y)$ is the joint probability density function of random variables X and Y:

$$f(x, y_i) = \frac{1}{2\pi\sigma_1\sigma_2\sqrt{1-\rho^2}} \exp\{-\frac{1}{2(1-\rho^2)}[(\frac{x}{\sigma_1})^2 - 2\rho\frac{x}{\sigma_1} \cdot \frac{y_i}{\sigma_2} + (\frac{y_i}{\sigma_2})^2]\} \tag{6}$$

And the mean value of X and Y are 0, the standard deviations are σ_1 and σ_2, respectively, and the correlation coefficient of random variables is ρ.

Similarly, Bob can also calculate the conditional probability that the u-th bit is '1' after encoding x_i according to equation(7):

$$P(\bigcup_{k_u \in K_u} x_{i,1,k_u} \mid y_i, q) = \frac{\sum_{k_u \in K_u} \int_{k_u * N + q - 1}^{k_u * N + q} f(x_{i,1,k_u}, y_i) dx}{\int_{-\infty}^{+\infty} f(x, y_i) dx} \tag{7}$$

Substituting equation (7) and (4) into (3), we can get the quantization log likelihood ratio.

Finally, we use (8) to hard-decision the quantized log likelihood ratio

$$y(i,u) = \begin{cases} 0 & if \quad \mathrm{Y}_{i,u} \ge 0 \\ 1 & if \quad \mathrm{Y}_{i,u} < 0 \end{cases} \tag{8}$$

The resulting $y(i,u)$ is the value of the u-th bit after quantize y_i.

3. The generated key length

Although both parties can reduce the inconsistent rate of the initial sequence by quantifying the received random variables, it is necessary to negotiate the key agreement to generate the key[8]. And because the performance of the quantization algorithm directly affects the length of generated key, so in

order to analyze the performance of the quantization algorithm, we can use the quantized initial sequence inconsistency rate to deduce the theoretically generated key length [9,10].

$$L = M \cdot [1 + P \cdot \log_2 P + (1-P) \cdot \log_2 (1-P)] \tag{9}$$

And M is the number of quantization bits, P is the initial inconsistent rate of the sequence.

In the CQA quantization algorithm, when Bob and Alice quantify the same, Bob's upper and lower threshold should observe:

$$\begin{cases} Y_{i\_L}(x) = F_A^{-1}[F_A(x) - \frac{1}{2N}] \\ Y_{i\_U}(x) = F_A^{-1}[F_A(x) + \frac{1}{2N}] \end{cases} \tag{10}$$

By taking the average of X, we can get the inconsistent rate of the original information sequence after CQA quantification [6]

$$P(\rho, M) = 1 - \frac{1}{\sqrt{2\pi}\sigma} \int_{-\infty}^{+\infty} e^{-a^2/2\sigma^2} [F_{\Delta a}(Y_{i\_U}(x) - x) - F_{\Delta a}(Y_{i\_L}(x) - x)] dx \tag{11}$$

Where $F_{\Delta a}$ is the cumulative integral function of the observed noise, substituting equation (10) into equation (11) yields the relationship between the initial inconsistent rate and the correlation coefficient. In addition, because the legitimate communication both sides will Gray coded the quantized information sequence, and when $P(\rho, M)$ is relatively small, the relationship between the inconsistency rate before and after Gray encoding can be expressed as [10]:

$$P_G = \frac{P(\rho, M)}{M} \tag{12}$$

Where P_G is the inconsistent rate after Gray coding. Finally, substituting equation (12) into equation (9), can be obtained CQA quantization algorithm theoretically generated key length.

4. Simulation

In order to verify the improved algorithm has better quantization performance, firstly, analyzed the quantization inconsistent rate P of the original algorithm and the improved algorithm; Secondly, simulated the generated key length when the quantization bit number takes different value according to the relationship between P and the key length; Finally, the performance of the two quantization algorithms is further analyzed by comparing the key length of the improved algorithm and the original algorithm.

4.1 The initial inconsistent rate of quantization

Because the most direct way to evaluate the quantization algorithm is to measure the quantization inconsistent rate, so simulated the quantization inconsistent rate of the original and the improved algorithm when the number of quantization bits is $M = 1$, as shown in Figure 1. In addition, in order to analyze the relationship between the quantization bit error rate and the quantization bit number, we also analyzed the quantization initial inconsistency rate when takes different quantization bit numbers, as shown in Figure 2.

It can be seen from Fig. 1 that the improved algorithm has a lower quantization inconsistent rate than the original algorithm, which shows that the improved algorithm has better performance. As can be seen from Fig. 2, the larger the quantization bit number, the larger the A, this is because the quantization bit number increases so that the number of quantization interval to 2 exponential increase, reducing the interval of the quantization zone, the signal jitter slightly larger may lead to quantization out of bounds, and increase of bit error rate. Although the quantization inconsistent rate is very low when the quantization bit number is 1, because the value of the quantization bit number affects the length of the key generation, the appropriate quantization bit number should be selected according to the key length and quantization inconsistent rate.

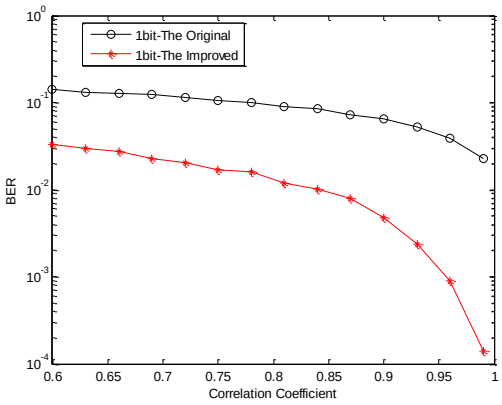

Fig. 1 Performance comparison of two quantization algorithms

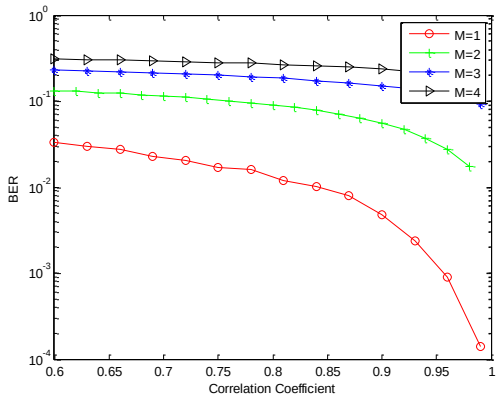

Fig. 2 The quantization inconsistent rate for different quantization bits

4.2 The optimal number of quantization bits

In order to generate a longer key, it is necessary to analyze the performance of different quantization bits and find the optimal quantization bit number. Figure 3 is the simulation results of the generated key length when the quantization bit number respectively is $M = 1、2、3、4$.

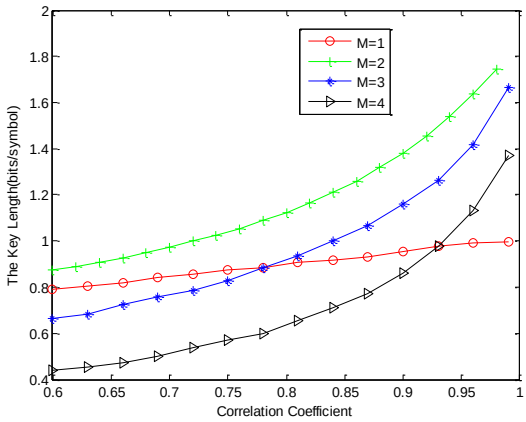

Fig.3 Key length of different quantization bit number

It can be seen from Fig.3 that when the sampled values are quantized to different number of bits, the generated key length increases with the increase of the correlation coefficient. Although the quantization non-coincidence rate of 1-bit quantization in Fig. 1 is low, it can be seen from Fig. 3 that when the number of quantization bits is 2, the generated key is longest, and therefore, in order to generate a longer key, each sample value should be quantized to 2 bits, and the subsequent simulations are performed using a 2-bit quantization analysis algorithm.

4.3 Generated Key Length of the Improved Algorithm and the Original Algorithm

Although the CQA quantization algorithm can reduce the quantization inconsistent rate by increasing the number of quantization intervals Q, when the number of quantization subintervals is greater than 16, the quantization inconsistency rate can't be reduced significantly[7], and the larger the number of subintervals, the more channel resources and computational resources are occupied, deceased the generation efficiency of the key. In order to prove that the improved algorithm is better than the original algorithm, the key length generated by the improved algorithm and original algorithm when $Q = 8$ is simulated as shown in Fig.4, and then simulated the generated key length of the original algorithm when it's Q is 16, as Fig.5.

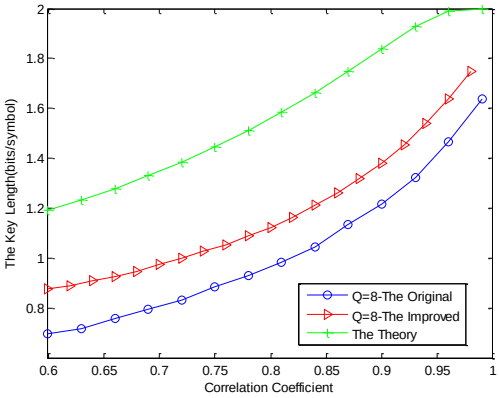

Fig.4 The key length when the Q is 8

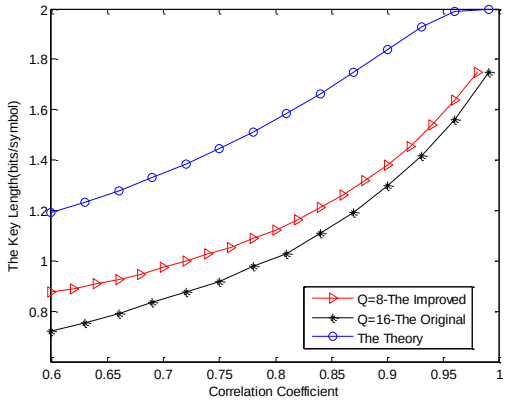

Fig.5 Key lengths generated by different Q

It can be seen from Fig. 4 that the key generated by the improved algorithm is longer than the original algorithm, and when the ρ less than 0.87, the key generated by the improved algorithm is increased by at least 0.15 bits/symbol relative to the original algorithm. And in Figure 5, when the ρ less than 0.83, the key length generated by the improved algorithm that the Q is 8 is increased by at least 0.1-0.15bits/symbol relative to the original algorithm that the Q is16, it not only increases the key length but also reduces the occupation of channel resources and computing resources, and the advantage is more obvious when the channel correlation is weaker. Although the increased key length of each sample value is limited, when the number of samples is large, the key length of the improved algorithm can greatly enhance the security of secure communication. Therefore, the improved quantization algorithm has more excellent quantization performance.

5. Summary

In this paper, the application of CQA algorithm in key generation is studied. The quantitative result of Bob's is corrected by using the hard-decision of the log likelihood ratio of each bit after quantized Alice sampling value, and the quantized inconsistency rate is further reduced. At the same time, the generated key is longer, and the security performance of the system is improved. In the next step, we will study the relationship between quantization and key reconciliation and improve the reconciliation performance of key reconciliation algorithm by improving the quantization algorithm.

References

[1]. Hamida T B, Pierrot J B, and Castelluccia C. “An Adaptive Quantization Algorithm for Secret Key Generation Using Radio Channel Measurements” .New Technologies. Mobility and Security (NTMS), 2009 3rd International Conference on. IEEE , 2009, p.1-5.
[2]. Ali S T, Sivaraman V, and Ostry D. “Secret Key Generation Rate vs. Reconciliation Cost Using Wireless Channel Characteristics in Body Area Networks”. Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on. IEEE , 2010, p.644-650.
[3]. Madiseh M G, He S, and Mcguire M L, et al. “Verification of secret key generation from UWB channel observations”. Environmental science & technology, Vol.35(2009), p.1-5.
[4]. Cai W B, Zhang S L, and Xin G, et al. “Research on Double - threshold Quantization Algorithm in Key Generation System”. Signal Processing, Vol.29(2013) , p.782-787.
[5]. Chen C, Jensen M A. “Secret Key Establishment Using Temporally and Spatially Correlated Wireless Channel Coefficients”. IEEE Transactions on Mobile Computing, Vol.10(2011), p.205-215.
[6]. Cai W B, Zhang S L, “Research on Improved Quantization Algorithm in Key Generation System”. Journal of Information Engineering University, Vol. 14(2013) , p.213-217.
[7]. Cai W B, “Research on Theoretical Limit and Quantization Method of Key Generation Based on

Wireless Channel". People 's Liberation Army Information Engineering University, 2013.
[8]. Shi M R, Jiang Z H, "A Key Agreement Protocol of Wireless Authentication. Computer Engineering", Vol. 35(2009) , p. 142-143.
[9]. Fu Z Y, "Information Theory -Principles and Applications". Beijing: Electronic Industry Press, 2007, p. 73-97.
[10]. Burr, A. "Modulation and Coding for Wireless Communication". Vol. 13(2001), p. 5264 – 5273.