A Physical Layer Secret Key Consistency Enhancement Scheme Using Constellation Decision Information

Zheyuan Deng¹, Liang Jin¹*, Xiaoyan Hu¹, Zhou Zhong¹, Yangming Lou¹, Ge Niu¹

¹ PLA Strategic Support Force Information Engineering University, 450001, China

Received: xx xxxxxxxx 2021 / Revised: xx xxxxx 2022 / Accepted: xx xxxxxxx 2022 / Published online: xx xxxxxx 2023

Abstract Secret key generation based on wireless channel (WC-SKG) is a promising solution to address the security issues in wireless communication. However, the consistency of channel estimation between two legal communication nodes in WC-SKG is often poor due to the receiver noise, signal power, etc., leading to low secret key generation rate (SKGR). Although there are several denoising algorithms such as orthogonal transformation to address this issue, existing schemes overlook the fact that data symbols are also affected by the channel. This results in existing schemes only using the pilot symbols for channel estimation and not fully utilizing the received signal power of the WC-SKG. To address this issue, we propose a consistency enhancement algorithm based on constellation decision information (CEA-CDI), which utilizes both pilot symbols and soft decision information of data symbols to improve SKGR. Monte Carlo simulation and numerical results demonstrate that our proposed scheme can improve performance by approximately 16 dB compared to initial channel estimation.

Keywords Physical secret key generation, consistency enhancement, soft decision

Citation Author A, Author B and Author C. This is Article Title. Security and Safety 2023; x: xxxxxxxx. https://doi.org/10.1051/sands/xxxxxxx

1 Introduction

The inherent openness of wireless channels makes it difficult to thoroughly address wireless communication security issues such as eavesdropping. With the growing popularity of applications such as smart homes, the Internet of Vehicles, and telemedicine, wireless communication’s security problems have become more serious. Therefore, finding a fundamental solution to ensure wireless communication security is an urgent issue that needs to be addressed. In recent years, secret key generation based on wireless channel (WC-SKG) has attracted widespread attention as a potential solution to these security problems. By utilizing the physical characteristics of reciprocity, time-variability, and irrelevance in wireless channels, legitimate communication nodes can generate keys, thereby achieving "information theory" security.

The traditional WC-SKG scheme consists of four steps: channel detection, quantization, information reconciliation, and privacy amplification. During the channel detection step, both legitimate communication nodes broadcast their detection signals to one other to obtain channel state information (CSI), such as channel frequency response (CFR) and channel impulse response (CIR). The CSI is then fed to the quantizer, which transforms it from continuous value into either 0 or 1 bits to generate the initial key bits. Due to various effects such as noise and signal distortion during transmission, both legitimate
parties may end up with different initial key bits. Consequently, it is necessary to eliminate the inconsistency through information reconciliation, i.e., the legitimate communication parties share error correction information through a public error-free channel. Regrettably, this process may expose confidential information via public channels. Hence, privacy amplification step becomes necessary to eliminate any unintentional leakage and create the ultimate secret key bits. In summary, channel detection is essential to the entire key generation, which dictates the upper limit of the scheme’s performance.

The main factors that affect channel consistency include variations in receiver hardware differences, asynchronous transmission measurements, and estimation errors. For the problem of receiver hardware differences, a difference feedback mechanism [1] can be employed as these differences are often fixed across both parties. For the problem of the Doppler shift resulting from asynchronous measurements, Zhang’s [2] theoretical analysis demonstrates that in general slow-fading communication scenarios, this factor has minimal influence and can be ignored. As for the problem of estimation error, it is hard to solve due to factors like the estimation algorithm of the communication system itself and the number of pilots, but it can be mitigated by using smoothing algorithms or orthogonal transformations.

For the smoothing algorithm, Ambekar et al. [3] use polynomial regression to fit the channel. However, this method will smooth the channel into a low-order polynomial, which reduces the achievable secret key generation rate (SKGR). To overcome the limitations of manual parameter design in smoothing algorithms and enhance adaptability, current research primarily focuses on preprocessing methods based on orthogonal transformations. These methods assume that the shared random source between legitimate communication parties is composed of arrival paths with varying delays and noise affects these paths differently. Simply eliminating heavily affected paths by noise can significantly improve overall consistency. Li et al. [4] proposed principal component analysis (PCA) algorithm to improve consistency and conducted a theoretical analysis of orthogonal transformation-based preprocessing methods. The PCA algorithm utilizes the correlation matrix’s feature matrix as the transformation matrix and extracts high-power components for key generation.

In conclusion, channel estimation error, which are influenced by factors such as the number of pilots, channel environment, and channel estimation algorithms used in communication process, are the primary cause of poor consistency between legitimate communication parties. However, the existing WC-SKG scheme relies on orthogonal transformations to reduce key inconsistency rate (KIR) at the expense of sacrificing a portion of SKGR, which is not the most effective solution.

To address the above problem, Wang et al. [3] showed that most of the current research on WC-SKG schemes only focuses on pilot-based approaches, neglecting the potential SKGR gain from the transmitted power of data symbols. Wang discovered not only can channel information be obtained from pilot symbols, but correctly demodulated data symbols can also be used as pilots to obtain channel information. However, Wang only provided a theoretical analysis that utilizing correctly demodulated data symbols as pilots can effectively improve the consistency of channel estimation for legitimate users, without providing a practical algorithm or implementation.

To address this issue, this paper proposes a novel consistency enhancement algorithm that leverages constellation decision information and designs an WC-SKG scheme. The main contributions of this article are as follows:

- A consistency enhancement algorithm based on constellation decision information (CEA-CDI) is
proposed to enhance SKGR. The algorithm is designed based on the principle of EM algorithm and has been improved according to the propagation mechanism of signal.

- We add a consistency enhancement step to the traditional WC-SKG scheme and design a complete key generation scheme. The consistency enhancement step can effectively improve the correlation between the legitimate parties, thereby reducing the KIR and the overhead from information reconciliation, ultimately improving the overall scheme performance.

- We conduct simulations and evaluate the normalized mean square error (NMSE) and SKGR under various signal-to-noise ratios (SNRs) from five perspectives: the number of symbols, the number of subcarriers, bandwidth, channel condition, and channel estimation methods. The simulation results show that the CEA-CDI algorithm makes use of both pilot symbols and soft decision information from data symbols to improve the accuracy of channel estimation and SKGR.

The remainder of this paper is as follows. Section II introduces the system model. Section III presents a key generation scheme based on CEA-CDI. In Section IV, the complexity analysis is provided. In Section V, the simulation analysis of the algorithm’s impact on OFDM signals is conducted. Finally, Section VI concludes this paper.

2 System Model

2.1 Wireless Channel Model

![Communication process between Alice and Bob](image)

The traditional WC-SKG model is considered as the system model [5]. Alice, Bob, and Eve are the three single antenna users in the scene. Alice and Bob are legal communication users, exchanging a frame of pilot-data symbols within the coherence time $T_n (n = 1, 2, \ldots)$). Figure 1 shows the communication process between them. Eve is an illegal eavesdropping user. Assuming that its distance from Alice and Bob exceeds several wavelengths, Eve’s channel can be regarded as independent of Alice and Bob’s channel. Consequently, the impact of Eve will not be considered in subsequent analyses. The communication behavior of Alice and Bob can be represented as

$$
\begin{align*}
    y_a &= h_{ba}x_a + w_a, \\
    y_b &= h_{ab}x_b + w_b,
\end{align*}
$$

where $h_{ab}, h_{ba}$ respectively represent the CIR of Alice to Bob and Bob to Alice, $x_a, x_b$ respectively represent the sending signals of Alice and Bob, and $w_a, w_b$ respectively represent the receiving noise at Alice and Bob. Alice and Bob can obtain the channel through channel estimation as

$$
\begin{align*}
    \hat{h}_a &= h_{ba} + e_a, \\
    \hat{h}_b &= h_{ab} + e_b,
\end{align*}
$$
where $\hat{h}_a, \hat{h}_b$ represent the channel estimation, $e_a, e_b$ represent estimation error.

The wireless signal propagation channel between Alice and Bob, which consists of many electromagnetic waves that are reflected, dispersed, and refracted, is an ideal random source in WC-SKG. The CIR of a multipath Rayleigh fading channel with $L$ taps can be expressed as

$$h(q) = \sum_{l=0}^{L-1} h_l \delta(q - \tau_l),$$

(3)

where $h(q)$ represents the $q$-th sample point of CIR, and $q$ should no larger than the total number of samples for a symbol. $h_l$ represents the $l$-th path of the received signal. When there are abundant paths in the environment, it can be considered $h_l$ as a zero mean cyclic symmetric complex Gaussian (ZMCSCG) random variable, and the different propagation paths are irrelevant. $h_l$ follows $h_l \sim \mathcal{CN}(0, \sigma_l^2)$ and $\sum \sigma_l^2 = P$. $\tau_l$ represents the delay of $l$-th path. $L$ represents the total number of paths. $\delta(\cdot)$ represents pulse function.

2.2 OFDM Model

The current popular communication systems almost use OFDM modulation, such as LTE, Wi-Fi, etc. So, the legitimate users utilize OFDM modulation to communicate are assumed. In each OFDM symbol, the first is pilot symbol, the last $K-1$ are data symbols, and each symbol has equal power. Both Alice and Bob transmit $K$ OFDM symbols on $M$ subcarriers in the coherence time $T_c$. The OFDM system’s basic transmitting and receiving process is shown in Figure 2.

![Figure 2](image)

**Figure 2** Basic transmitting and receiving process of the OFDM system.

When transmitting OFDM signals, the information bits-stream firstly modulates to obtain $D$ data symbols (constellation mapping). $D$ data symbols form the frequency domain signal $X$ which consists of $M$ subcarriers and $K-1$ OFDM symbols ($D = M (K-1)$). Then insert one known pilot symbol and OFDM modulate it to obtain the time domain signal $x$, which can be represented as

$$x_k(q) = \frac{1}{\sqrt{M}} \sum_{m=0}^{M-1} X_k(m) e^{j2\pi mq/M},$$

(4)

where $x_k(q)$ represents the time domain transmission signal of the $q$-th sample point of the $k$-th symbol. $X_k(m)$ represents the frequency domain transmission signal of the $m$-th subcarrier of the $k$-th symbol.

To avoid intersymbol interference, the cyclic prefix (CP) is added to the OFDM signal, which is then transmitted through the multipath fading channel with additive Gaussian white noise (AWGN).

Assuming that the receiver synchronization performs well, the multipath fading channel remains unchanged within $2 \times K$ OFDM symbols (Alice and Bob complete a round of alternating transmitting and receiving), and the CIR length is less than the CP length, the received signal after removing the CP can be
represented as

\[ y_k(q) = \sum_{l=0}^{\frac{L-1}{2}} h(l) x_k(q-l) + w_k(q), \]

where \( y_k(q) \) represents the time-domain received signal of the \( q \)-th sample point of the \( k \)-th symbol. \( w_k(q) \) represents AWGN and follows \( w_k(q) \sim \mathcal{CN}(0, \sigma_w^2) \). Then, the time-domain received signal through OFDM demodulating to obtain an equivalent frequency-domain received signal, which can be expressed as

\[ Y_k(m) = \frac{1}{\sqrt{M}} \sum_{q=0}^{\frac{M-1}{2}} y_k(q) e^{-j2\pi\frac{mq}{M}}, \]

\[ = H(m) X_k(m) + W_k(m), \]

where \( X_k(m) \), \( W_k(m) \) represent frequency-domain symbols and noise at the \( m \)-th subcarrier of the \( k \)-th symbol, respectively. And \( W_k(m) \) follows \( W_k(m) \sim \mathcal{CN}(0, \sigma_w^2) \), \( \sigma_w^2 = M \sigma_w^2 \). Since we have assumed that the channel remains unchanged within a coherence time, the CFR of all symbols at the \( m \)-th subcarrier of the same symbol is expressed as \( H(m) \).

CFR is the frequency-domain representation of CIR, which can be expressed as

\[ H(m) = \sum_{l=0}^{\frac{L-1}{2}} h_l e^{-j2\pi ml/M}. \]

Since \( H(m) \) is a linear change of \( h_l \) and each channel tap \( h_l \) is a ZMCSCG random variable, \( H(m) \) is also a ZMCSCG random variable. It can be deduced from Pascal’s discrete theorem that

\[ \frac{1}{M} \sum_{m=0}^{M-1} |H(m)|^2 = \sum_{l=0}^{\frac{L-1}{2}} |h_l|^2. \]

So, \( H(m) \) also follows \( H(m) \sim \mathcal{CN}(0, P) \). The CFR estimation of Alice and Bob can be expressed as

\[ \hat{H}_A(m) = H_{A\alpha}(m) + E_A(m) \]

\[ \hat{H}_B(m) = H_{Ab}(m) + E_B(m), \]

where \( \hat{H}_A(m), \hat{H}_B(m) \) represent the CFR estimation of Alice and Bob for the received signal, respectively. \( H_{Ab}(m) \), \( H_{A\alpha}(m) \) represent the CFR of the \( m \)-th carrier from Alice to Bob and Bob to Alice, respectively, which follows \( H_{Ab}(m), H_{A\alpha}(m) \sim \mathcal{CN}(0, P) \). \( E_A(m), E_B(m) \) represent the estimation error of CFR, which follows \( E_A(m) \sim \mathcal{CN}(0, \sigma_e^2), E_B(m) \sim \mathcal{CN}(0, \sigma_e^2) \).

For the initial channel estimation of the pilot, we employ the least-squares (LS) method, which is expressed as

\[ \hat{H}^{(0)}(m) = \frac{Y_p(m)}{X_p(m)} = H(m) + \frac{W_p(m)}{X_p(m)} \]

\[ = H(m) + E^{(0)}(m). \]

Due to \( |X_p|^2 = 1 \), the initial estimation error of CFR is \( E^{(0)}(m) \sim \mathcal{CN}(0, \sigma_w^2) \).

The received data symbols are then transmitted to channel equalizer and constellation de-mapping. Finally, bits-stream are obtained through the decision.
3 Secret key generation scheme based on CEA-CDI

3.1 WC-SKG scheme

A general key generation scheme should include channel detection, quantization, information reconciliation, and privacy amplification. To reduce the initial KID and avoid the need for feedback on a large amount of data during information reconciliation, this paper designs the CEA-CDI algorithm to improve channel consistency between legitimate users. Figure 3 shows the WC-SKG scheme.

1) Channel detection

Figure 3 shows that Alice and Bob must complete their communication within the coherence time and each need transmit one pilot symbol and $K-1$ data symbols. This process is consistent with current communication systems based on pilot-data frames, such as LTE uplink signals in which two demodulation reference signal (DMRS) symbols are inserted into a frame for channel estimation [6].

2) Consistency enhancement

Alice and Bob use pilot symbol to complete initial channel estimation, followed by consistency enhancement using the CEA-CDI algorithm (detailed in Section 3.2). The process results of the CEA-CDI algorithm are shown in Figure 4. Figure 4(a) shows the true CFR (without noise). Figure 4(b) shows the initial channel estimation based on the pilot symbol. Noise and poor consistency significantly impact Alice and Bob's initial channel estimation. Figure 4(c) shows the results of consistency enhancement using the CEA-CDI algorithm, which demonstrates intuitively that the CEA-CDI algorithm is more accurate than the initial channel estimation.
3) Quantization

The purpose of quantification is to convert continuous CFR into discrete 0, 1 initial key bits. The equiprobability quantization algorithm is used to achieve a uniform number of 0 and 1 bits after quantization. The quantization interval of the equal probability quantization algorithm can be expressed as

$$\int_{-\infty}^{q_i} p(x) \, dx = \frac{i}{\nu},$$  \hspace{1cm} (11)

where \( \nu \) denotes the number of quantization thresholds, \( q_i \) represents the \( i \)-th threshold value, and \( p(x) \) represents the probability of \( x \) within a quantization interval.

We use secret key inconsistency ratio (KIR) to evaluate the inconsistent number of key bits after quantization, which is not only related to the quantization algorithm, but also to the consistent of channel estimation. KIR is a commonly used indicator that can be expressed as
\[
KIR = \frac{\sum_{i=1}^{\text{LEN}} \text{XOR}(K_A(i), K_B(i))}{\text{LEN}}
\]  \hspace{1cm} (12)

where \( \text{XOR}(\cdot) \) represents XOR operation; \( K_A \) and \( K_B \) represent Alice and Bob's initial key bits after quantization, respectively; \( \text{LEN} \) represents the length of the initial key bit.

4) Information reconciliation

Despite consistency enhancement has been added to the WC-SKG scheme, there may still be incorrect key bits after quantization due to noise. Consequently, information reconciliation is still required to eliminate inconsistent bits between legitimate communication parties to obtain consistent keys for symmetric encryption. We employ a method of information reconciliation based on error-correcting encoding. We can calculate the KIR at various signal-to-noise ratios in advance and then select BCH codes with multiple rates. As stated in consistency enhancement, CEA-CDI can enhance the consistency of channels between legitimate communication parties, thereby reducing KIR. When KIR is low, the higher rate of error correction coding can be used to conserve communication bandwidth because the rate of error correction coding is inversely proportional to KIR. Different KIRs require varying BCH \( (n, k, t) \), where \( n \) is the length of the BCH codeword; \( k \) is the length of the information bit in the BCH codeword, and \( t \) is the maximum number of errors the BCH code can correct.

5) Privacy amplification

Because Alice must send the error-corrected information to Bob through a public channel during information reconciliation, Eve can also use this information to correct his key. Although there may be a significant distinction between Eve and legitimate channels, it is hard to prevent information from leaking. Therefore, based on the residual hash lemma [2], the leaking key bits can be reduced by using the SHA1 function. Then we can generate the final secure key sequence.

3.2 Consistency enhancement algorithm based on constellation decision information

The conventional WC-SKG schemes only use pilot symbols for channel estimation, resulting in low accuracy and inconsistent channel estimation between Alice and Bob. This limitation arises from the fact that these schemes do not fully exploit the power of transmitted signals. To address this issue, we aim to design a method for channel estimation that can simultaneously make use of both pilot symbols and data symbols.

To improve channel estimation accuracy before decoding, we need to consider how to effectively utilize the information obtained from constellation decision. Unfortunately, using pilot-assisted channel estimation methods is not feasible since the receiver needs to know the transmitted data symbols before making constellation decision. The bits obtained after the decision will no longer contain information about the channel impact. Furthermore, once an error in decision-making has occurred and the error bits have been used to correct the initial channel estimation, the expected gain may not be achieved. Therefore, it is crucial for to determine how to make soft decision on the signal after channel equalization, acquire soft symbol information, and use this information to improve the initial channel estimation without knowing the transmission symbol. Based on these considerations, we propose a consistency enhancement algorithm based on constellation decision information (CEA-CDI) that is based on the EM algorithm.
principle.

The EM algorithm [7] is a method for iteratively reaching the maximum likelihood solution in the condition of missing variables. It can iteratively approach the maximum likelihood solution of CFR by calculating the soft symbol information of the received data symbol without knowing the specific transmission data symbol. The Expectation step (E-step) and the Maximum step (M-step) are the two main parts of the EM's iterative process.

Alice or Bob obtains the initial channel estimation at the m-th subcarrier during the channel detection stage, the E-step and the M-step can be written as

E-step:
\[
Q(H(m)|H^{(p)}(m)) = E_{X} \left\{ \log f(Y(m),X(m)|H(m))|Y(m),H^{(p)}(m) \right\}, \quad (13)
\]

M-step:
\[
H^{(p+1)}(m) = \arg \max_{H} Q(H(m)|H^{(p)}(m)), \quad (14)
\]

where \( H^{(p)}(m) \) represents the channel estimation of the \( p \)-th iteration. According to the Bayesian formula, (13) can be written as

\[
Q(H(m)|H^{(p)}(m)) = E_{X} \left\{ \log f(X|H(m))f(Y_{i}(m)|H(m),X)|Y(m),H^{(p)}(m) \right\}
\]

\[
= \sum_{i=1}^{C} \sum_{k=1}^{K} \log \left[ \frac{1}{C} f(Y_{i}(m)|H(m),X_{i}) f(X|Y_{i}(m),H(m)) \right] f(Y_{i}(m)|X_{i},H^{(p)}(m)) f(X|H^{(p)}(m))
\]

\[
= \sum_{i=1}^{C} \sum_{k=1}^{K} \log \left[ \frac{1}{C} f(Y_{i}(m)|H(m),X_{i}) \right] f(Y_{i}(m)|X_{i},H^{(p)}(m)) f(Y_{i}(m)|H^{(p)}(m))
\]

where \( X_i \) is a known constellation symbol, \( C \) is the modulation order. If \( x \) is modulated by QPSK, then \( C = 4 \) and \( X_{i} = \{1+i,1-i,-1+i,-1-i\} / \sqrt{2} \).

According to (6), noise follows ZMCSGG, so when \( H^{(p)}(m) \) and \( X_i \) are known, the conditional probability of \( Y_i(m) \) is

\[
f(Y_{i}(m)|H^{(p)}(m),X_{i}) = \frac{1}{\pi \sigma_{w}^{2}} \exp \left\{ -\frac{Y_{i}(m)-H^{(p)}(m)X_{i}^{2}}{\sigma_{w}^{2}} \right\}, \quad (16)
\]

And when \( H^{(p)}(m) \) is known, the conditional probability of \( Y_i(m) \) is
\[
 f(Y_i(m) | H^{(p)}(m)) = \sum_{i} \frac{1}{\pi \sigma_w^2} \exp \left( - \frac{|Y_i(m) - H^{(p)}(m) X_i|^2}{\sigma_w^2} \right).
\]

According to (16) and (17), (14) can be further written as

\[
 H^{(p+1)}_{mm}(m) = \arg\max_{H} \sum_{i=1}^C \sum_{k=1}^E \log \left( \frac{1}{C} \sum_{i=1}^C f(Y_i(m) | H(m), X_i) f(Y_i(m) | X_i, H^{(p)}(m)) f(Y_i(m) | H^{(p)}(m)) \right)
\]

Taking the derivative of (18) results in

\[
 H^{(p+1)}_{mm}(m) = \left[ \sum_{i=1}^C \sum_{k=1}^E X_i^* f(Y_i(m) | X_i, H^{(p)}(m)) f(Y_i(m) | H^{(p)}(m)) \right]^{-1} \\
 \times \left[ \sum_{i=1}^C \sum_{k=1}^E X_i Y_i f(Y_i(m) | X_i, H^{(p)}(m)) f(Y_i(m) | H^{(p)}(m)) \right].
\]

Furthermore, by incorporating (16) and (17) into (19), the simplified result of the EM algorithm's (p+1)-th iteration is

\[
 H^{(p+1)}_{mm}(m) = \frac{1}{CK} \left[ \sum_{i=1}^C X_i^* \exp \left( - \frac{|Y_i(m) - H^{(p)}(m) X_i|^2}{\sigma_w^2} \right) \right] \left[ \sum_{i=1}^C \exp \left( - \frac{|Y_i(m) - H^{(p)}(m) X_i|^2}{\sigma_w^2} \right) \right]^{-1}.
\]

Extracting a portion of (20) yields (21). \( \Omega^{(p+1)}_i(m) \) represents the soft decision information of constellation symbol, which is based on the weighted average of received data symbols for each symbol in the constellation.

\[
 \Omega^{(p+1)}_i(m) = \frac{\sum_{i=1}^C X_i^* f(Y_i(m) | X_i, H^{(p)}(m))}{\sum_{i=1}^C f(Y_i(m) | X_i, H^{(p)}(m))}.
\]

The EM algorithm calculates the probability of received symbols regarding each modulation symbol and derives the soft decision information of received symbols instead of directly using hard decision. In this way, it can preserve the influence of channel on the received data symbols to the utmost extent.

Since the CIR is usually much shorter than the symbol length, the estimation error in the actual non-existent path can be eliminated by truncating the result of iterative estimation (20) in the time domain. Here we assume that the CIR length \( L \) is known (in reality, \( L \) is an unknown parameter that can be estimated) and we simply use the length of CP as the upper bound of \( L \), since CP is usually set to be longer than \( L \). So, we use inverse Fourier transformation on the result of the EM iterative estimation \( H^{(p+1)}_{mm} \) to
obtain $h^{(p+1)}_{em}$, then, set the $h^{(p+1)}_{em}(q) = 0$ when $q > L$, which can be expressed as

$$h^{(p+1)}_{em}(q) = \begin{cases} h^{(p+1)}_{em}(q) & q \leq L, \\ 0 & q > L. \end{cases}$$ (22)

Then use Fourier transform on $h^{(p+1)}_{em}$ to obtain $H^{(p+1)}$. Once the difference between $H^{(p+1)}$ and $H^{(p)}$ is small enough, i.e., $\|H^{(p+1)} - H^{(p)}\|^2 < \delta$, the iteration process stops.

By using Algorithm 1, the iterative effect in the above formula can be achieved equivalently.

### 3.3 Analysis of secret key generation rate

Secret key generation rate (SKGR) is the most commonly used metric to evaluate WC-SKG schemes. It represents the upper limit of the number of key bits that can be obtained by detecting channel once. The SKGR $R$ can be expressed as
According to (9), \( \hat{H}_A \) and \( \hat{H}_B \) are the ZMCSCG variables, so (23) can be further represented as

\[
R = \log_2 \left| \begin{bmatrix} \hat{R}_{aa} & \hat{R}_{ab} \\ \hat{R}_{ba} & \hat{R}_{bb} \end{bmatrix} \right|
\]  

(24)

The covariance matrices \( \hat{R} \) in the above can be represented as

\[
\hat{R}_{aa} = R_{HH} + \sigma_{\epsilon_A}^2 I_M
\]

(25)

\[
\hat{R}_{bb} = R_{HH} + \sigma_{\epsilon_B}^2 I_M
\]

(26)

\[
\hat{R}_{ab} = \begin{bmatrix} \hat{R}_{aa} & R_{HH} \\ R_{HH} & \hat{R}_{bb} \end{bmatrix}
\]

(27)

where \( R_{HH} \) represents the covariance matrix of the actual channel, \( I_M \) represents the identity matrix with \( M \times M \). Substituting the above covariance matrix into (24) and simplifying it, we can obtain

\[
R = \log_2 \left| R_{HH} \left( \left( \sigma_{\epsilon_A}^2 + \sigma_{\epsilon_B}^2 \right) I_M + \sigma_{\epsilon_A}^2 \sigma_{\epsilon_B}^2 R_{HH} \right)^{-1} + I_M \right|
\]

(28)

According to (28), it can be seen that the SKGR is inversely proportional to estimation error \( \sigma_{\epsilon_A}^2, \sigma_{\epsilon_B}^2 \).

And The simulations are conducted to find the relationship between SKGR and the number of symbols, the number of subcarriers, the channel condition in section 5.

4 Complexity analysis

In this section, the computational complexity of the proposed CEA-CDI, hard decision feedback (HDF) method and LS method are analyzed. Following [8], we use the \( \Theta \)-notation to measure the complexity with respect to \( K \) whereby \( \Theta(f(K)) \) denotes the set of functions which are bounded both above and below by \( f(K) \) asymptotically.

For the CEA-CDI, since the modulation order \( C \) is a constant, the computation of the (21) is \( \Theta(1) \). And the computation of the (19) requires \( \Theta(K) \) operations. According to [9], we also assume that the average number of iterations required for convergence remains almost unchanged with respect to \( K \), i.e. \( \Theta(\bar{n}) = \Theta(1) \), where \( \bar{n} \) is the average number of iterations required for convergence. Then, the computation of time-domain truncation is \( \Theta(M \log M) \) operations due to FFT. So, we can conclude that for the CEA-CDI, the total computational complexity is \( \Theta(M \log M) \).

For the HDF method, we use the result of (29) as extended pilot, it requires \( \Theta(K) \) operations for one subcarrier. And then we take the average of the channel estimation of the extended pilot as the result of HDF. So, the computational complexity of HDF is \( \Theta(MK) \).
\[
\alpha_{k}^{(p+1)}(m) = \arg\min \left| x - X_{i} \right|^2, i = 1, 2, \ldots, C
\]

(29)

For the LS method, since we only using one pilot symbol, the computational complexity is \( \Theta(M) \). The comparison of the computational complexity is summarized in the Table 1.

<table>
<thead>
<tr>
<th>Table 1 Comparison of the computational complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEA-CDI</td>
</tr>
<tr>
<td>( \Theta(MK + M \log M) )</td>
</tr>
</tbody>
</table>

5 Simulation and Analysis

5.1 The Setting of Simulation Parameters

To verify the performance of the proposed scheme, we conducted Monte Carlo simulations, and some basic OFDM parameter settings are shown in Table 2.

<table>
<thead>
<tr>
<th>Table 2 Simulation Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
</tr>
<tr>
<td>Bandwidth</td>
</tr>
<tr>
<td>Number of subcarriers</td>
</tr>
<tr>
<td>CP length</td>
</tr>
<tr>
<td>Number of pilot symbols</td>
</tr>
<tr>
<td>Number of data symbols</td>
</tr>
<tr>
<td>Total number of symbols</td>
</tr>
<tr>
<td>Modulation</td>
</tr>
</tbody>
</table>

Based on the above parameters, the average effective received SNR for each message bit is

\[
\frac{E_{sk}}{N_0} = \left( \frac{L + M}{M(K-1)C} \right) \frac{E_s}{N_0}.
\]

(30)

In the simulation, the total power is fixed, and each symbol shares the total power equally. Meanwhile, in order to test the impact of different environments on the proposed scheme, the following two different fading models are considered in the simulation.

- **Exponential power delay (EPD) model**: This model has \( L+1 \) complex Gaussian distribution taps, and the average power of each tap \( h_i \) satisfies \( \sigma_i^2 = E(\left| h_i \right|^2) = \sigma_0^2 e^{-\tau/s_{rms}}, \sum_{i=0}^{L} \sigma_i^2 = 1 \). The root mean square delay is \( \tau_{rms} = 30ns \), and the channel length is \( L+1=8 \) (at 10 MHz).

- **Tapped Delay Line-A (TDL-A) model**: TDL-A is one of the channel models in 5G-NR, with a frequency range of 0.5GHz to 100GHz and a maximum bandwidth of 2GHz. The root mean square delay is \( \tau_{rms} = 100ns \), and the channel length is \( L+1=26 \) (at 10 MHz).

Unless otherwise specified, the EPD model is used for simulation. Meanwhile, we use data symbols as extended pilots, which is equivalent to improving the signal-to-noise ratio of channel estimation. Therefore, all traditional methods [3],[4],[10]-[12] can continue to be applied after the CEA-CDI, so we have not compared them with traditional methods.
LS method, HDF method, and CEA-CDI method are compared in simulations. HDF method directly use the result of (29) as extended pilot and then take the average of the channel estimation of the extended pilot as the result.

5.2 Simulation Result

In our simulation studies, we focus on the impact of parameters such as the number of data symbols, the number of subcarriers, bandwidth, and channel environment on the performance of the proposed method.

Firstly, we analyzed the impact of the proposed CEA-CDI algorithm as shown in Figure 6. It can be observed that by using the CEA-CDI method, the NMSE and SKGR performances are improved by approximately 16 dB compared to the initial least squares (LS) estimation when increasing the SNR. This improvement is due to the inverse relationship between SKGR and NMSE, as indicated in (28).

Furthermore, Figure 7 illustrates the impact of different methods on the KIR. It is evident that the proposed CEA-CDI algorithm exhibits a lower KIR than other methods. Moreover, even with high quantization bits (3 bits) used, their KIR will still be lower than the LS method using low quantization bits (1 bit). This highlights the superiority of the CEA-CDI algorithm in terms of both SKGR and KIR.

Figures 8, 9, and 10 respectively show the impact of the number of data symbols, the number of
subcarriers, and bandwidth on NMSE and SKGR. Only the declared parameters are modified in the Figures 8, 9, and 10, while the other parameters remain the same as Table 2.

**Figure 8** The impact of the number of data symbols.

**Figure 9** The impact of the number of subcarriers.
The impact of bandwidth.

Figure 8 illustrates the impact of the number of data symbols. The results of 8 symbols adopt the parameters in Table 2. We then evaluate the performance of three methods by increasing the number of data symbols to 15 while keeping one pilot symbol (the total number of symbols is 16). It is observed that both CEA-CDI method and HDF method exhibit an increase in SKGR as the number of data symbols increases. This is because they utilize data symbols as extended pilots, resulting in improved channel estimation. In contrast, NMSE and SKGR of the LS method remains unchanged.

Figure 9 shows the impact of the number of subcarriers. We can be observed that as the number of subcarriers increases, the NMSE of LS and HDF will not change. It means that once the environment and other basic parameters are determined, the number of carriers will not affect channel estimation. However, the NMSE of CEA-CDI increase as the number of subcarriers increases. This is because the number of time domain points for each OFDM symbol increases, but the channel length remains unchanged. It can obtain gain from time-domain truncation step. We can also find that the NMSE and SKGR are not completely related, since the SKGR of LS and HDF increase as the number of subcarrier increase. This is because there is $I_M$ in SKGR according to (28) that is related to the number of subcarriers.

Figure 10 shows the impact of the bandwidth. It can be observed that only changing bandwidth will not affect the NMSE and SKGR of LS and HDF. However, it can be found that bandwidth is inversely proportional to NMSE and SKGR of CEA-CDI. This is because we add time-domain truncation in CEA-CDI method, LS method and HDF method do not have this step. In the simulation of 10M bandwidth, we set the delay path to 8 consecutive points (the channel length is 8 in EPD model). We keep the delay of the path unchanged (0.1ms interval between each path), so there will be 16 intermittent points under 20M bandwidth, which means our time-domain truncation step cannot remove extra noise. It can be observed an increase in bandwidth and a decrease in performance.

Finally, Figure 11 shows the impact of different channel conditions. For the proposed CEA-CDI algorithm, the SKGR performance is improved by about 19 dB compared to the initial LS estimation. Moreover, under
the same SNR conditions, the SKGR improvement is up to 43.25 bits. It is noted that the delay path length of the TDL-A model is \( L = 25 \) and that of the EPD model is \( L = 7 \), which means that the delay path of the TDL-A model is more complex than that of the EPD model. We find that as the SNR increases, the performance of the CEA-CDI algorithm under the TDL-A model is consistently worse than that under the EPD model in the NMSE simulation, which is due to the increase of \( L \) resulting in an increase in the difficulty of channel estimation.

Furthermore, it is noted that \( L \) has different effects on NMSE and SKGR. An increase in \( L \) may lead to an increase or decrease in SKGR, but it has little effect on NMSE. The reason for the above is that the SKGR is influenced by both the number of delay paths \( L \) and the SNR in the environment. A larger \( L \) and a higher SNR respectively mean a larger number of random sources and more accurate estimation of random sources. Therefore, in a high SNR environment, an increase in \( L \) can lead to an improvement in SKGR. On the contrary, in low SNR environments, it is difficult to accurately estimate each random source, resulting in a decrease in SKGR as \( L \) increases.

Based on the simulation results and the complexity analysis in section 4, it can be seen that although the CEA-CDI can effectively improve the SKGR compared with the initial channel estimation result (LS), it still has the following limitations: 1) As shown in Figure 8, the higher the number of symbols, the higher SKGR can be improved by CEA-CDI. This may mean that the CEA-CDI is not applicable to the low-rate communication scenarios, such as IoT. Because the low communication rate means that the number of symbols sent at one time will not be much, then the performance improvement brought by the CEA-CDI is limited. 2) As shown in section 4, the computational complexity of the CEA-CDI has increased, which may pose challenges for less capable terminals. 3) Since CEA-CDI requires iterative processing, it may cause latency overhead. However, we believe that this impact is relatively small. Unlike communication, key generation requires less real-time performance. Because the channel detection step can be asynchronous with the consistency enhancement step as shown in Figure 3. After obtaining the initial channel estimation in a coherent time, it can be processed slowly.

6 Conclusion

We start from solving the problem of low SKGR caused by channel inconsistency in the WC-SCK scheme and find that the current scheme did not fully utilize the received signal power. To address this issue, we employ the EM algorithm to derive and propose CEA-CDI. By making soft decisions on the received data symbols, the influence of the channel is preserved for each symbol. This iterative approach improves channel estimation accuracy, resulting in improved key consistency between legitimate communication users. The simulation results demonstrate that compared to the initial channel estimation, the proposed algorithm enhance performance by approximately 16dB, effectively improving SKGR.

Funding

This work was supported by the National Natural Science Foundation of China (No.U22A2001), and by the National Key Research and Development Program under Grants 2022YFB2902202.

References

Security and Safety, For Peer Review Only.

Zheyuan Deng et al.: Using Constellation Decision Information for Channel Consistency Enhancement in Secret Key Generation


Zheyuan Deng received the M.S. degree from the PLA Strategic Support Force Information Engineering University, China, in 2022. And he is currently pursuing the Ph.D. degree at the PLA Strategic Support Force Information Engineering University. His research interests include wireless communication, physical layer security.

Liang Jin received the Ph.D. degree from Xi’an Jiaotong University. He is currently a Professor and Ph.D. Supervisor of the PLA Strategic Support Force Information Engineering University, Zhengzhou, China. His research interests include wireless communication, physical layer security, and smart antenna.

Xiaoyan Hu received the M.S. degree and Ph.D. degree in information and communication engineering from PLA Strategic Support Force Information Engineering University. He is currently an assistant researcher of PLA Strategic Support Force Information Engineering University. His research interests include physical layer security and information security.

Zhou Zhong received the M.S. degree and Ph.D. degree in information and communication engineering from PLA Strategic Support Force Information Engineering University. He is currently an associate professor of PLA Strategic Support Force Information Engineering University. His research interests include physical layer security and wireless communication.
Yangming Lou received the M.S. degree in information and communication engineering from PLA Strategic Support Force Information Engineering University. He is currently an assistant researcher of PLA Strategic Support Force Information Engineering University. His research interests include physical layer security and wireless communication.

Ge Niu received the M.S. degree in information and communication engineering from Zhengzhou University. He is currently an assistant engineer of PLA Strategic Support Force Information Engineering University. His research interests include physical layer security and information security.