Adaptive and Efficient Key Extraction for Fast and Slow Fading Channels in V2V Communications

Mahmoud A. Shawky†, Muhammad Usman†, Muhammad Ali Imran†,
Qammer H. Abbasi†, Shuja Ansari†, and Ahmad Taha†
†James Watt School of Engineering, University of Glasgow, Glasgow, G12 8QQ, United Kingdom
Email: m.shawky.1@research.gla.ac.uk,
{Muhammad.Usman, Muhammad.Imran, Qammer.Abbasi, Shuja.Ansari, Ahmad.Taha}@glasgow.ac.uk

***Abstract*—Securing data exchange between intercommunicating terminals, e.g., vehicle-to-everything, constitutes a technological challenge that needs to be addressed. Security solutions must be computationally efficient and flexible enough to be implemented in any wireless propagation environment. Recently, physical layer security has gained popularity, which exploits the randomness of wireless channel responses for extracting high entropy secret cryptographic keys. The current state-of-the-art relies on the independently varying channel sources of randomness, e.g., received signal strength (RSS) and phase. However, the limited capability of RSS-based extraction techniques has motivated researchers to investigate alternative approaches. Although phase-based approaches have emerged in many studies, optimising the extraction performance by adapting the algorithm to the non-reciprocal components of static and dynamic channels remains a challenge. In this paper, we propose an adaptive multi-level quantisation approach that adjusts the size of the quantisation region to the channel responses' non-reciprocity parameters, thus optimising the trade-off between the bit generation rate (BGR) and the bit mismatch rate (BMR). The probability of error has been theoretically formulated. Accordingly, the order of the quantisation process is adapted for acceptable mismatching probability. Moreover, simulation analysis is conducted to prove the ability of the proposed approach to provide flexible adaptation of the quantisation order at different signal-to-noise ratios (SNRs), achieving fast secret bit generation rates $1.1 \sim 2.85$ bits/packet at SNRs of $10 \sim 25$ dB for acceptable BMR $\leq \mathbf{0.1}$.**

***Index Terms*—Physical layer security, Multi-level quantisation, Secret key extraction, Vehicle-to-vehicle communication.**

I. Introduction

Nowadays, modern vehicles have become increasingly dependent on wireless technology, which facilitates the exchange of vital information about location, heading, and speed to provide drivers with real-time traffic situations. The matter that helps to prevent potential road accidents and chaos. Unfortunately, adversaries can abuse the wireless channel shared medium to intercept, alter, and replay the broadcasted traffic-related messages [1]. Thus, securing data packets and verifying senders' identities are crucial for security and privacy. Public-key cryptography (PKC) is commonly used to provide these security services, e.g., authenticity, confidentiality, etc. However, PKC-based key management is not a practical solution due to its drawbacks regarding power consumption and computational complexity ($\sim msec$) [2]. Recent studies have investigated the physical (PHY) characteristics of wireless channels for providing authentication and setting up a symmetric shared key [3]–[9]. In this regard, the development of a physical-layer-based method for generating secret keys may provide an alternative to existing encryption-based key exchanging protocols, e.g., Diffie-Hellman. The major source of randomness in the key extraction process is unexpected variations in channel responses, i.e., received signal strength and phase [4]. The former is a random function resulting from the significant and unpredictable spatial and temporal fluctuations in each multipath component's path loss and shadowing, whereas the latter is a function of the delay, frequency offset, and Doppler shift. The key point is that a pair of communicating devices can observe reciprocal estimates of the spatially and temporally varying channel responses within a limited time interval, known by the coherence time [4]. These highly correlated observations are quantised to form the extracted key. Unfortunately, the imperfect reciprocity of the channel and the inherent hardware imperfections lead to occasional discrepancies/errors in the extracted bits [5]. An indicator of how many bits are mismatched to the total number of channel samples is known as the bit mismatch rate. Wireless cards are readily available for the acquisition of the RSS, which is why RSS is widely used [3]. However, RSS-based techniques suffer from limited scalability and low bit generation rates, defined by the total number of bits extracted from channel samples. In addition, it has limited capabilities for generating group keys due to the difficulty of safely accumulating RSS observations over multiple nodes [4]. A further disadvantage is its inability to cope with slow channel variations (static or indoor cases) due to a lack of sufficient randomness (roughly static path loss and shadowing). Therefore, phase-based quantisation has emerged due to the high sensitivity of the channel-phase response to the distance between terminals, allowing the high dynamicity of vehicular networks to be an advantage for obtaining high entropy cryptographic keys. Unfortunately, the impact of the unpredictable shadowing of adjacent vehicles and infrastructures over vehicular ad-hoc networks causes channel fading variations, fluctuating between high and low levels of fading in urban and rural areas, respectively, posing a significant challenge [3]. Several phase-based techniques have been developed so far that guarantee high secret bit generation rates (SBGRs) [6]–[9], defined by the number of correct or matched bits out of the total number of channel samples. However, optimising the trade-off between BGR and

BMR is extremely challenging, particularly under conditions of significant channel variations. The larger the quantisation region, the smaller the BMR and BGR, and vice versa. In this sense, optimising the size of the quantisation region enhances the extraction performance, which is the main objective of this study. This study contributes the following:

- We evoke the channel gain complement (CGC) method presented in [5] to learn the randomly varying non-reciprocity parameters sensed by two communicating nodes. Upon learning these parameters, the observed channel phase response is then complemented in order to mitigate the channel non-reciprocity impact; also, the order of the phase-based quantisation levels is adapted for optimum performance (i.e., high SBGR).
- Our proposed method is applied for pairwise key extraction, employing several channel observations obtained from orthogonal frequency division multiplexing (OFDM) sub-channels for high BGRs. Theoretical and simulation analyses prove the existence of an optimal multi-level quantisation order at different SNRs of the 3D scattering vehicle-to-vehicle (V2V) channel modelled in [10]. Results show that this approach is effective in obtaining high entropy secret keys.

The rest of this paper is structured as follow. Section II reviews existing phase-based key extraction algorithms. Section III presents the proposed thresholding optimising technique. Section IV evaluates the key extraction performance. Finally, Section V concludes this work.

II. Related Works

In [6], the phase difference between two orthogonal sinusoids of different frequencies is utilized as a source of randomness in an attempt to reduce the non-reciprocity impact, thereby reducing the BMR. For improved BGR, reference [7] employs both phase differentials and amplitudes as two independent randomness sources. Reference [4] proposes a theoretical round-trip group key generation mechanism, in which initial random phases are encapsulated for each extraction, passing through a group of nodes in the clockwise and anticlockwise directions, having the same phase offset estimates for both directions at each node over the same coherence interval. However, the number of the group members is restricted due to the accumulated noises across multiple nodes and the short coherence period of high-speed terminals.

In all the above works, the quantisation process is designed without invalid regions; however, observations near the region's boundaries may result in a greater BMR. To address this issue, [8] employs guard intervals in order to achieve a low BMR. The idea that larger boundary regions will lead to a decrease in the mismatching probability is logical, but this will be accompanied by a decrease in the bit extraction rate since more observations are likely to be dropped. In OFDM systems, the frequency interference is minimized by splitting the signal into parallel streams of separately modulated subcarriers, which is considered to be a number of narrowband sub-channels that can be treated as multiple sources of randomness, resulting in an increased BGR. Reference [9] developed a single side probing mechanism in which random phase sequences are initiated for N subcarriers OFDM system and the corresponding terminal employs the channel's reciprocal characteristics to encrypt a preliminary secret key. Unfortunately, there is not a clear answer yet on how to optimise the multi-level quantisation process for fast and slow fading channels.

III. PHY-Layer Secret Key Extraction

This section provides a brief review of the CGC method described in [5], followed by a description of the procedures and theoretical analysis of the proposed work.

A. Review of the channel gain complement method in [5]

Let us consider a scenario in which Alice and Bob, which are trusted wireless communication devices, employ the randomness and reciprocity characteristics of the wireless channel attributes, e.g., RSS and channel phase response, to establish a symmetric shared key. In that case, the received signal consists of several L multipath components, each of which has a different phase delay ξ_l, fading coefficient $|h_l|$, and doppler shift v_l, as shown in Fig. 1. A simple formulation for Bob's channel response h_b at time t is

$$h_b(t) = \sum_{l=1}^{L} |h_l| \, e^{(j\xi_l)} e^{2\pi v_l t} \tag{1}$$

During channel probing, the frequency domain received probe signals, $R_a(f)$ and $R_b(f)$, at both communicating terminals can be simplified for the OFDM system of N subcarriers as

$$\left.\begin{array}{l} R_a\left(f_i\right) = X\left(f_i\right) H_a\left(f_i\right) + \omega_a\left(f_i\right) \\ R_b\left(f_i\right) = X\left(f_i\right) H_b\left(f_i\right) + \omega_b\left(f_i\right) \end{array}\right\} i = 1, \ldots, N \tag{2}$$

where $X\left(f_i\right)$ is a pre-known probe symbol at a particular frequency f_i, and ω_a and ω_b are additive noises at the side of Alice and Bob, respectively. The estimated (noisy) channel responses, $\widehat{H}_a$ and $\widehat{H}_b$, at timestamps, t_a and t_b, can be formulated as

$$\begin{array}{l} \widehat{H}_a^{t_a}\left(f_i\right) = H_a\left(f_i\right) + N_a\left(f_i\right) \\ \widehat{H}_b^{t_b}\left(f_i\right) = H_b\left(f_i\right) + N_b\left(f_i\right) \end{array} \tag{3}$$

where N_a and N_b are noise estimates resulting from ω_a and ω_b in (2). Since probing the channel is conducted in the half-duplex mode for $t_a - t_b \leq$ coherence time T_c, the estimated responses, $\widehat{H}_a$ and $\widehat{H}_b$, are not identical. Furthermore, the RF front-end imperfections, e.g., antenna gain and coerced carrier frequency, also contribute to imperfect channel reciprocity. Thus, (3) leads to

$$\begin{array}{l} \widehat{H}_a^{t_a}\left(f_i\right) = H\left(f_i\right) + \varepsilon_a\left(f_i\right) + N_a\left(f_i\right) \\ \widehat{H}_b^{t_b}\left(f_i\right) = H\left(f_i\right) + \varepsilon_b\left(f_i\right) + N_b\left(f_i\right) \end{array} \tag{4}$$

where ε_a and ε_b are the non-reciprocity components estimated at both terminals. After exchanging a sufficient number of

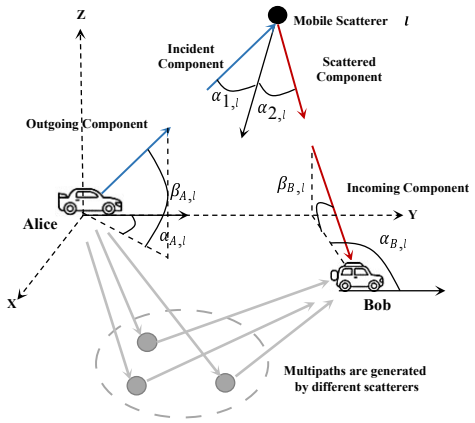


Fig. 1: Non-Line-of-Sight V2V channel model [2].

m probing packets and having channel estimates at both ends, both terminals exchange their estimates $\widehat{H}_a$ and $\widehat{H}_b$ at timestamp t_a and t_b, respectively. Then, both test whether $\|t_a - t_b\| \leq T_c$. If holds, the difference between $\widehat{H}_a$ and $\widehat{H}_b$ in (4) can be simplified as

$$\begin{aligned} \varepsilon_{a,b}(f_i) &= \widehat{H}_a^{t_a}(f_i) - \widehat{H}_b^{t_b}(f_i) \\ &= (\varepsilon_a(f_i) - \varepsilon_b(f_i)) + (N_a(f_i) - N_b(f_i)) \end{aligned} \tag{5}$$

The authors of [5] assumed that N_a and N_b are normally distributed random variables $N(v, \sigma^2)$ with mean v and variance σ^2. Therefore, the distribution of $\varepsilon_{a,b}(f_i)$ is approximated by $N(\mu_{\varepsilon,i} = \varepsilon_a(f_i) - \varepsilon_b(f_i), var_{\varepsilon,i} = 2\sigma^2)$, where the mean $\mu_{\varepsilon,i}$ and the variance $var_{\varepsilon,i}$ are measured from m channel difference estimates of (5) as

$$\begin{aligned} \mu_{\varepsilon,i} &= \frac{1}{m}\sum_{x=1}^{m}\left(\widehat{H}_a^{t_a}(f_i) - \widehat{H}_b^{t_b}(f_i)\right) \\ var_{\varepsilon,i} &= \frac{1}{m-1}\sum_{x=1}^{m}\left(\widehat{H}_a^{t_a}(f_i) - \widehat{H}_b^{t_b}(f_i) - \mu_{\varepsilon,i}\right)^2 \end{aligned} \tag{6}$$

Thus, Alice can complement the subsequent channel estimates $\widehat{H}_a$ at timestamp t'_a as

$$\widehat{H}_a^{t'_a}(f_i)^{new} = \widehat{H}_a^{t'_a}(f_i) - \mu_{\varepsilon,i} \tag{7}$$

After complementing Alice's channel estimates, the distribution of $\varepsilon_{a,b}(f_i)$ in (5) can be approximated as

$$\varepsilon_{a,b}(f_i) = \widehat{H}_a^{t'_a}(f_i)^{new} - \widehat{H}_b^{t'_b}(f_i) \sim N(0, 2\sigma^2) \tag{8}$$

This CGC method is used in our study for two primary reasons: 1) Alleviating the adverse impact of the channel non-reciprocity components to achieve a high BGR and low BMR. 2) Employing the computed variance $var_\varepsilon = 2\sigma^2$ in (6) as an indicator to adjust the quantisation level for optimal key extraction performance.

B. Scheme description

The proposed scheme employs the CGC algorithm in [5] to learn the non-reciprocity components modelled in (4). Thus, optimising the quantisation thresholding levels based on the measured mean μ_ε and variance var_ε of the channel responses difference operation in (6), minimising the BMR, and maximising the BGR of the key extraction process. Fig. 2 shows the flowchart of the proposed scheme. In this work, a channel-phase response-based quantisation scheme is proposed in which the preliminary key is generated by one of the communicating terminals, mapped and masked by the channel-phase response in a challenge-response process. After learning the non-reciprocity parameters, the extraction process comprises three stages, i.e., channel probing and quantisation, information reconciliation, and privacy amplification. All network terminals are assumed to be at least half the wavelength apart ($2.5\text{ cm} \sim 5.9\text{GHz}$) to maintain a high degree of decorrelation between legitimate and wiretap channels. Furthermore, the subcarriers' frequencies are well separated to support independent fading.

C. Channel probing and quanisation thresholding stage

The current state-of-the-art employs the RSS for channel probing in an interleaved approach. However, the extracted key must be sufficiently random with a high degree of entropy, which is hard to be achieved in conditions of slow fading channel variations. Contrary to many existing approaches, this work is based on the reciprocity of the uplink and downlink channel-phase responses between two terminals within the coherence interval T_c. In this context, the challenge signal is generated by Alice with uniformly distributed random phases $\theta_a \sim U[0, 2\pi)$, which makes it hard for an eavesdropper, Eve, to deduce the channel-phase response ξ_i. A robust and high entropy preliminary secret key sk_b is generated by Bob, mapped, and masked by ξ_i, generating the response signal related to the received challenge, as shown in Fig. 3. This way allows for probing the channel multiple times within the same coherence interval since the random choice of the mapped sk_b overcomes the insufficient randomness of stationary environments. The following three steps constitute this stage.

a) Challenge initialisation: In this step, Alice initiates a uniformly distributed random phases modulated sinusoids of N subcarriers OFDM system at time t_0, which can be formulated as

$$s_a(t_0) = \sum_{i=1}^{N}\sqrt{\frac{2E_s}{T}}\cos(2\pi f_i t_0 + \theta_{a,i}),\ i = 1, \ldots, N \tag{9}$$

The signal received by Bob at time t'_0 can be expressed as

$$r_b(t'_0) = \sum_{i=1}^{N}\sqrt{\frac{2|h_i|^2 E_s}{T}}\cos(2\pi f_i t'_0 + \theta_{a,i} + \xi_{b,i}) + \omega_{b,i} \tag{10}$$

where $\omega_{b,i}$ is the complex additive gaussian noise $\sim \mathcal{CN}(0, \sigma_n^2)$ of the i^{th} subcarrier at the side of Bob. In a similar way to (4), $\xi_{b,i} = \xi_i + \varepsilon_{b,i}$, where ξ_i and $\varepsilon_{b,i}$ are the reciprocity and non-reciprocity components, respectively. Then, Bob computes the phase of $r_b(t'_0)$ as

$$\begin{aligned} \theta_{b,i} = \angle(r_{b,i}) &= \arctan\left(\frac{imag(r_{b,i})}{real(r_{b,i})}\right) \\ &= \theta_{a,i} + \xi_i + \varepsilon_{b,i} + N_{b,i} \end{aligned} \tag{11}$$

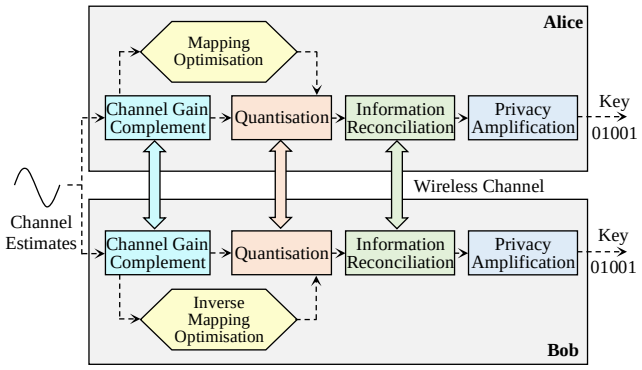


Fig. 2: Flowchart of the proposed key extraction scheme.

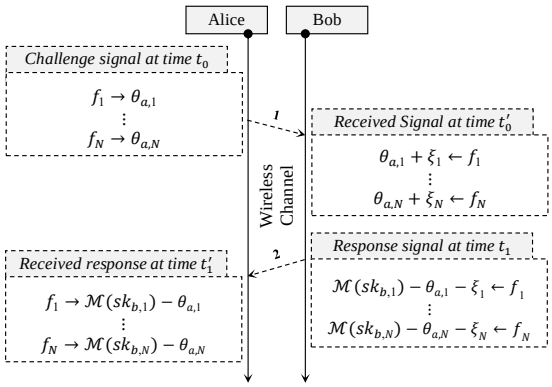


Fig. 3: The process of channel probing in a noiseless channel.

b) Response generation: In this step, n-bits Gray-code mapping operation $\mathcal{M}(.)$, e.g., 2-PSK, 4-PSK, and 8-PSK, is used by Bob to map the preliminary secret key $sk_b = \{\kappa_1, \kappa_2, \ldots, \kappa_N\}$ for $|\kappa_i| = n$ bits, as shown in Fig. 4(a). For simplicity, a 2-bits mapping can be described as

$$\mathcal{M}(\kappa_i) = \begin{cases} 0 & \kappa_i = [\ 0 \quad 0\ ] \\ \frac{\pi}{2} & \kappa_i = [\ 0 \quad 1\ ] \\ \pi & \kappa_i = [\ 1 \quad 1\ ] \\ \frac{3\pi}{2} & \kappa_i = [\ 1 \quad 0\ ] \end{cases}, i = 1, \ldots, N \tag{12}$$

Note that, a Gray-code is chosen to ensure that adjacent codes are one hamming distance apart, reducing the BMR of the extracted keys. Finally, Bob replies to Alice's challenge as

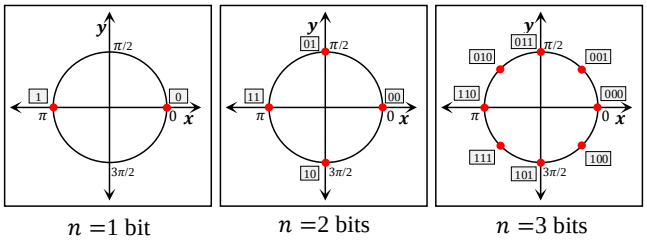
$$s_b(t_1) = \sum_{i=1}^{N} \sqrt{\frac{2E_s}{T}} \cos\left(2\pi f_i t_1 + \mathcal{M}(\kappa_i) - \theta_{b,i}\right) \tag{13}$$

The signal received by Alice at time t'_1 can be formulated as

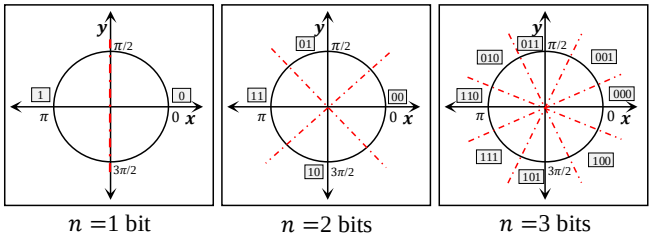
$$r_a(t'_1) = \sum_{i=1}^{N} \sqrt{\frac{2|h_i|^2 E_s}{T}} \cos\left(2\pi f_i t'_1 + \mathcal{M}(\kappa_i) - \theta_{b,i} + \xi_{a,i}\right) + \omega_{a,i} \tag{14}$$

for $\xi_{a,i} = \xi_i + \varepsilon_{a,i}$, and phase equals

$$\begin{aligned} \angle(r_{a,i}) &= \arctan\left(\frac{imag(r_{a,i})}{real(r_{a,i})}\right) \\ &= \mathcal{M}(\kappa_i) - \theta_{b,i} + \xi_i + \varepsilon_{a,i} + N_{a,i} \end{aligned} \tag{15}$$



(a) n-bits Gray-code mapping operation.



(b) n-bits Gray-code inverse mapping operation.

Fig. 4: Mapping and inverse-mapping operations.

for $t'_1 - t_0 \leq T_c$, by substituting (11) into (15) yields:

$$\angle(r_{a,i}) = \mathcal{M}(\kappa_i) - \theta_{a,i} + (\varepsilon_{a,i} - \varepsilon_{b,i}) + (N_{a,i} - N_{b,i}) \tag{16}$$

c) Signal equalization: In this step, Alice equalizes the received signal by computing

$$\begin{aligned} c_i(t) &= \angle\left(r_{a,i}(t'_1)\, s_{a,i}(t_0)\right) \\ &= \mathcal{M}(\kappa_i) + (\varepsilon_{a,i} - \varepsilon_{b,i}) + (N_{a,i} - N_{b,i}) \end{aligned} \tag{17}$$

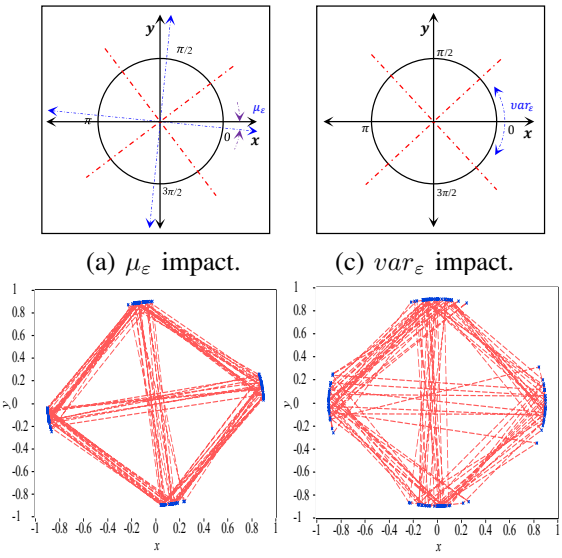
In a noiseless channel with ideal channel reciprocity, the computed $c_i(t)$ is equal to $\mathcal{M}(\kappa_i)$. In this case, Alice can retrieve the mapped preliminary key sk_b by inversely mapping $c(t) = \{c_1, c_2, \ldots, c_N\}$, as shown in Fig. 4(b), so that $sk_{a,i} = \mathcal{M}^{-1}(c_i)$. For simplicity, the inverse-mapping operation $\mathcal{M}^{-1}(.)$ of order 2-bits can be described as

$$\mathcal{M}^{-1}(c_i) = \begin{cases} 00 & c_i \in \left[-\frac{\pi}{4}, \frac{\pi}{4}\right) \\ 01 & c_i \in \left[\frac{\pi}{4}, \frac{3\pi}{4}\right) \\ 11 & c_i \in \left[\frac{3\pi}{4}, -\frac{3\pi}{4}\right) \\ 10 & c_i \in \left[-\frac{3\pi}{4}, -\frac{\pi}{4}\right) \end{cases}, i = 1, \ldots, N \tag{18}$$

The order of the inverse-mapping operation $\mathcal{M}^{-1}(.)$ at the side of Alice must be the same as that of $\mathcal{M}(.)$ at the side of Bob. Due to the non-reciprocity component $\varepsilon_{a,b}(f_i) \sim N(\mu_\varepsilon, var_\varepsilon)$ of the wireless channel modelled in (5), the impact of the mean value μ_ε makes the constellation of the inverse mapping operation $\mathcal{M}^{-1}(.)$ deviates, as shown in Fig. 5(a) and 5(b). Fig. 5(b) denotes the simulation of the received signal in (17) with hardware imperfection specifications tabulated in Table I. To address these issues, Alice employs the estimated μ_ε from the CGC stage in (6) to compensate the final estimation of $c(t)$ as

$$c(t)^{new} = c(t) - \mu_\varepsilon \tag{19}$$

So that, the distribution of $c(t)^{new}$ is $N(\mathcal{M}(\kappa_i), var_\varepsilon)$ for $i = 1, \ldots, N$. Both terminals use the pre-estimated var_ε of



(a) μ_ε impact. (c) var_ε impact.

(b) μ_ε simulation result. (d) var_ε simulation result.

Fig. 5: The impact of the non-reciprocity component $\varepsilon_{a,b}(f_i)$.

$\varepsilon_{a,b}(f_i)$ in (6) to optimise the order of $\mathcal{M}^{-1}(.)$ and $\mathcal{M}(.)$ at the side of Alice and Bob, respectively, as shown in Fig. 5(c) and 5(d). A high order of $\mathcal{M}/\mathcal{M}^{-1}$ denotes high BGR while low order denotes low BMR, as shown in Fig. 6.

The quantisation stage departs from the work presented in [9]. However, the authors use a fixed order of the mapping operation regardless of channel variations conditions. In contrast to [9], the proposed technique adjusts the thresholding levels at different fading conditions, thus optimising the key extraction performance.

d) Theoretical analysis of mismatching: Estimating the probability of mismatching/error P_e is crucial for performance evaluation. In this way, and since the distribution of the complemented estimate $c(t)^{new}$ in (19) is $N\left(\mathcal{M}(\kappa_i), var_\varepsilon = 2\sigma^2\right)$, the cumulative distribution function $\Phi(.)$ can be formulated as

$$\Phi(x) = \frac{1}{2}\left[1 + \mathrm{erf}\left(\frac{x - \mathcal{M}(\kappa_i)}{2\sigma}\right)\right], \qquad \mathrm{erf}(z) = \frac{2}{\sqrt{\pi}}\int_0^z e^{-t^2}dt \tag{20}$$

where $\mathrm{erf}(z)$ is the error function. Then, P_e is the probability that $c_i^{new} \notin [-\pi/2^n, \pi/2^n)$ for $\mathcal{M}(\kappa_i) = 0$, given by

$$P_e = 2\Phi\left(\frac{\pi}{2^n}\right)\Big|_{\mathcal{M}(\kappa_i)=0} \tag{21}$$

where n is the order of $\mathcal{M}/\mathcal{M}^{-1}$. For acceptable $P_e \leq$ the scalar value α, n can be obtained as follow.

$$x' = \arg\max_{x'} \mathrm{erf}\left(\frac{x' - \mathcal{M}(\kappa_i)}{2\sigma}\right)\Big|_{\mathcal{M}(\kappa_i)=0} \leq \alpha - 1 \tag{22}$$

Given x', n can be computed as

$$n = \arg\max_{n'} 2^{n'} \leq \frac{\pi}{x'} \quad \text{for } n' = 1, 2, 3 \tag{23}$$

TABLE I: Hardware Imperfection Specifications

Specifications	**Fig. 5 (b)**	**Fig. 5 (d)**
Carrier frequency	5.9GHz	5.9GHz
Carrier frequency offset	100 Hz	0 Hz
Quadrature skew	4°	0°
IQ gain imbalance	1 dB	0 dB
SNR	20 dB	15 dB

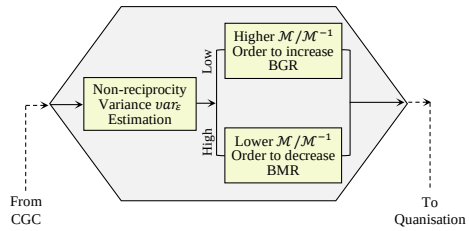


Fig. 6: Flowchart of the $\mathcal{M}/\mathcal{M}^{-1}$ optimisation engine.

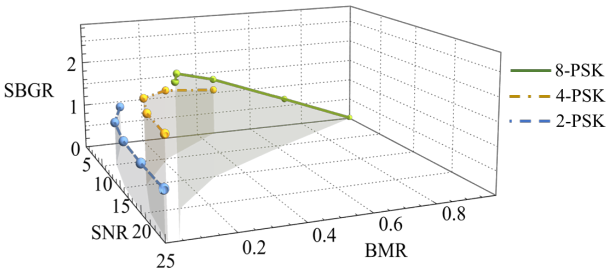
IV. Simulation and Performance Evaluation

In this section, performance evaluation is carried out using Monte-Carlo simulations of 100,000 runs. Since the frequency range of the dedicated short-range communication protocol of vehicular network is from 5.85 to 5.925GHz [11]. The simulation is conducted at 5.9GHz carrier frequency with 64 subcarriers of the OFDM system, and *m* equals 100 learning samples in (6), as recommended in [5]. Results are derived using 16-multipath components of a Rayleigh fading vehicle-to-vehicle channel modelled in [10], see Fig. 1. According to [3], the speed of the scatterers obeys the Weibull distribution, and Tx/Rx maximum speeds are up to 30 m/s. The simulated channel parameters are listed in Table II (for details, see reference [10]). In this study, we refer to the key extraction performance as the relationship between the SBGR and the BMR. Fig. 7(a) and 7(b) show the extraction performance from different viewpoints at different SNRs added at both sides of the communicating terminals. Let us consider that acceptable key performance is the achievable SBGR at a low BMR ($\alpha \leq 0.1$). In that case, it can be noted from Fig. 7 that 2^n-PSK for $n = 1, 2, 3$ denote low BMR ≤ 0.1 at high SNR (25 dB). However, 8-PSK achieves the highest SBGR in the order of 2.85bits/ch, which makes it the best choice for high SNRs. In cases of SNR equal to 15 and 20 dB, 4-PSK achieves higher SBGR compared with 2-PSK for $\alpha \leq 0.1$. In low SNR situations, 2-PSK is evidently the only order that delivers acceptable performance. Fig. 8 shows simulation results for the CDF $\Phi(x)$ of c_i^{new} in (19) at different SNRs and $n = 1, 2, 3$ compared to its theoretical formulation in (20). This specifies the probability of error $P_e = 2\Phi(x)$ for $x = \frac{\pi}{2^n}$ and proves the existence of optimum $\mathcal{M}/\mathcal{M}^{-1}$ order at different SNR values, also demonstrates the capability of the proposed technique to optimise the trade-off relationship between the BMR and the BGR based on the computed variance var_ε in (6).

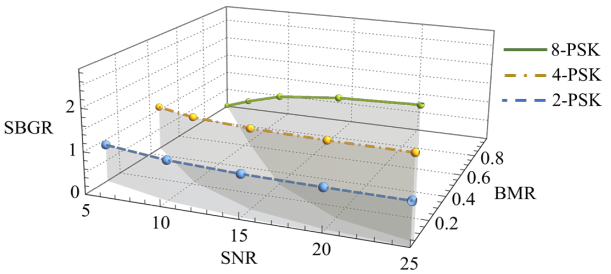
Using the widely used randomness statistical test suite designed by the National Institute of Standards and Technology (NIST) [12], the extracted secret key is evaluated for its randomness. It is assumed that sk is hard to forge if

TABLE II: Channel Parameters

Description	Value
No. of multipath components (L)	16
Tx/Rx maximum speeds	30 m/s
Scatterers' maximum speed	30 m/s
Azimuth angels of departure/arrival $(\alpha_{A(B),l})$	$U[-\pi, \pi)$
Elevation angels of departure/arrival $(\beta_{A(B),l})$	$U[-\pi, \pi)$
Scatterers' angels of incident/departure $(\alpha_{1(2),l})$	$U[0, \pi/3)$
Scale coefficient of the Weibull distribution (ρ)	2.985
Shape coefficient of the Weibull distribution (a)	0.428



(a) Side view.



(b) Front view.

Fig. 7: Secret key extraction performance at different SNRs.

the returned P-value from each test is at least greater than the significance level (0.01). Table III shows the P-values of selected typical tests that prove the randomness of the extracted bit sequence sk of length 128 bits. According to the listed P-values, the extracted bit sequence passed the tests.

V. Conclusion

In this paper, we proposed an adaptive secret key extraction technique that is applicable to any wireless propagation environment. With the aid of the CGC method in [5], we introduced an optimisation engine that can act as a forward indicator for the extraction process, combating the varying non-reciprocity of the channel responses. The selection of the quantisation order has been determined analytically for an acceptable probability of error. Furthermore, simulation analysis is conducted to evaluate the efficacy of the proposed method for a 3D scattering V2V channel scenario at different SNRs. Finally, the NIST tests suite was used to analyse whether the extracted keys are robust enough to be used as cryptographic keys. Results clearly demonstrated that the extracted bits had sufficient randomness. Our future research will explore the possibility of extending our key extraction approach to the design of a dynamic PHY-layer authentication scheme that supports forward and backward secrecy in vehicular networks.

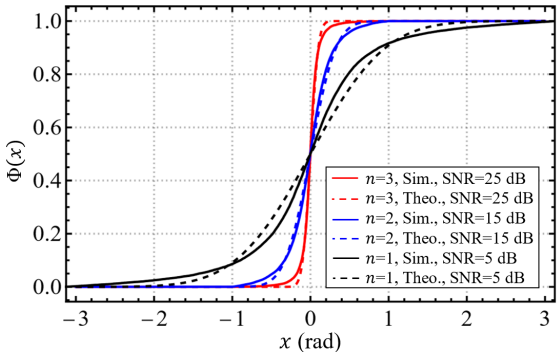


Fig. 8: CDFs of c_i^{new} at different n and SNRs.

TABLE III: Randomness Evaluation

NIST Statistical Test Suite	P-value
Block Frequency Test	0.483
Long Runs Test	0.476
Monobit Test	0.518
Key Entropy	0.299
Maurer Universal Statistical Test	0.186
Discrete Fourier Transform (Spectral) Test	0.475
Overlapping Template Matchings Test	0.483

References

[1] M. Al-Shareeda, M. Anbar, and I. Hasbullah, "Survey of Authentication and Privacy Schemes in Vehicular Ad Hoc Networks", *IEEE Sensors Journal*, vol. 21, no. 2, Jan. 2021.

[2] M. Bottarelli, P. Karadimas, G. Epiphaniou, D. Kbaier, and C. Maple, "Adaptive and Optimum Secret Key Establishment for Secure Vehicular Communications and Sensing", *IEEE Trans. on Vehic. Tech.*, Feb. 2021.

[3] M. Bottarelli, G. Epiphaniou, D. Kbaier, P. Karadimas, and H. Al-Khateeb, "Physical Characteristics of Wireless Communication Channels for Secret Key Establishment: A Survey of the Research", *Computers and Security*, vol. 78, pp. 454-476, Aug. 2018.

[4] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and Scalable Secret Key Generation Exploiting Channel Phase Randomness in Wireless Networks", Proceedings of IEEE INFOCOM., pp. 1422-1430, Jun. 2011.

[5] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response", Proceedings of IEEE INFOCOM., pp. 3048–3056, Apr. 2013.

[6] H. Koorapaty, A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio", *IEEE Communications Letters*, vol. 4, no. 2, pp. 52–55, Feb. 2000.

[7] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "ProxiMate: proximity-based secure pairing using ambient wireless signals", Proceedings of MobiSys. conference, pp. 211-224, Jun. 2011.

[8] Y. Shehadeh, and D. Hogrefe, "An Optimal Guard-Intervals Based Mechanism for Key Generation from Multipath Wireless Channels", Proceedings of 4th IFIP International Conference on New Technologies, Mobility and Security, pp. 1–5, Feb. 2011.

[9] L. Cheng, L. Zhou, B. Seet, W. Li, D. Ma, and J.Wei, "Efficient Physical-Layer Secret Key Generation and Au-thentication Schemes Based on Wireless Channel-Phase", *Mobile Info. Systems*, vol. 2017, Jul. 2017.

[10] P. Karadimas, and D. Matolak, "Generic stochastic modeling of vehicle-to-vehicle wireless channels", *Vehicular Communications*, vol. 1, no. 4, pp. 153–167, 2014.

[11] X. Wang, P. Hao, and L. Hanzo, "Physical-Layer Authentication for Wireless Security Enhancement: Current Challenges and Future Developments", *IEEE Communications Magazine*, vol. 54, Jun. 2016.

[12] NIST, *A Statistical Test Suite For Random and Pseudorandom Number Generators For Cryptographic Applications*, 800th ed., National Institute of Standards and Technology, 2001.