Inform : Jurnal Ilmiah Bidang Teknologi Informasi dan Komunikasi
Vol.10 No.2 July 2025, P-ISSN : 2502-3470, E-ISSN : 2581-0367

Secure Authentication in Vehicular Networks: Integrating Zero-Knowledge Protocols with RSS Key Generation

M. Cahyo Kriswantoro[1], Eko Handoyo[2], Mutsna Sa Yu Zakka[3]

[1,3]*Medical Informatics Department, Universitas Muhammadiyah Lamongan, Indonesia*

[2]*Computer Engineering Department, Universitas Muhammadiyah Lamongan, Indonesia*

[1]cahyo.krizt@gmail.com(*)

[1,2][m.cahyokriswantoro, eko_handoyo]@umla.ac.id

[3]mtsnasyzkk@gmail.com

Received: 2024-12-27; Accepted: 2025-06-04; Published: 2025-06-11

Abstract— Zero Knowledge Authentication protocol is a cryptographic method used to identify users through interactive communications without exposing confidential. The identification scheme is an example of a real-world application of the Zero-Knowledge protocol, which provides a mechanism for actors in possession of a secret key to verify their identity using the corresponding public key. Several prominent identification schemes have been proposed in the literature, including the Feige-Fiat-Shamir (FFS), Guillou-Quisquater (GQ), and Schnorr protocols. In conjunction with these schemes, mechanisms for key generation and key updates have been developed to enhance privacy in zero-knowledge cloud-based file storage systems. To ensure data integrity within cloud environments, the Shacham-Waters auditing protocol has been employed. The FFS identification scheme, in particular, utilizes a public-private key pair in a parallel verification structure. To improve computational efficiency, this scheme has been enhanced by incorporating parallel constructions. Researchers utilize the Zero-Knowledge Authentication Feige-Fiat-Shamir protocol by combining the key generator obtained from Received Signal Strength (RSS) in vehicle communications, thereby replacing the channel in the Feige-Fiat-Shamir protocol with the key generator derived from RSS. The existing combination combines stages 1 and 4 in FFS. The change is that the channel sent is replaced with a key generator obtained from the RSS key generator**.** The results of this study are expected to serve as a reference for the implementation of vehicle communication technology, which is anticipated to experience rapid growth in the future.

Keywords— Zero Knowledge Authentication; Feige-Fiat-Shamir; Vehicular Ad-Hoc Network; Received Signal Strength; Key Generator.

I. INTRODUCTION

Zero-Knowledge Authentication is a cryptographic protocol involving two entities: the Claimant and the Verifier. Within this framework, the Claimant does not disclose any information that could potentially compromise the confidentiality of the underlying data, thereby preserving its secrecy throughout the authentication process [1]. The Claimant is only required to demonstrate to the other party, referred to as the verifier, that they possess knowledge of a secret, without disclosing the secret itself. The protocol is specifically designed to neither expose nor obscure the secret beyond what is necessary for verification. After the message exchange, the verifier can only conclude whether the Claimant does or does not know the secret, resulting in a binary (yes/no) outcome with minimal information disclosure. In this context, three key Zero-Knowledge Authentication protocols have been implemented, including the Fiat-Shamir protocol. [2] and the Guillou-Quisquater protocol [3], and their performance is compared. The Zero Knowledge Convention enables the verifier to demonstrate that they know the mystery without revealing any information about it [4]. By evaluating indicators of commitment and responsiveness, the evaluator can assess whether the observed reaction aligns with established normative parameters [5]. This allows the verifier to check the data without knowing the private mystery of the Verifier [6]. This method can facilitate anonymous authentication on devices such as RFID tags, particularly in contexts where safeguarding sensitive information is critical. For instance, in the case of travel documents, RFID tags implementing Zero-Knowledge protocols can be employed to protect specific data while simultaneously verifying the authenticity of individuals holding passports [7].

A Zero-Knowledge Proof is a cryptographic technique that allows one party to demonstrate possession of certain information to another party without disclosing the actual content of that information [8]. Zero-Knowledge Proofs were initially conceptualized by Shafi Goldwasser, Silvio Micali, and Charles Rackoff in 1985 through their foundational paper, *"The Knowledge Complexity of Interactive Proof Systems,"* which laid the groundwork for the theoretical understanding of interactive proof systems [9]. The fundamental principle of Zero-Knowledge Proof lies in the interaction between a prover and a verifier, wherein the prover seeks to demonstrate knowledge of a certain piece of information without revealing the information itself to the verifier [10]. This process must satisfy three essential properties: completeness, soundness, and zero-knowledge [11]. *Completeness* refers to the property that, if the prover is honest and possesses the correct knowledge, the verifier will accept the proof with high probability. *Soundness* ensures that a dishonest prover cannot deceive the verifier into accepting a false statement. Conversely, the *Zero-Knowledge* property guarantees that the

DOI : https://doi.org/10.25139/inform.v10i2.9488

verifier gains no knowledge about the prover's secret beyond the validity of the claim itself [12].

The Feige-Fiat-Shamir (FFS) identification scheme is a parallelized approach that utilizes public and private key pairs. In this context, the original Feige-Fiat-Shamir (FFS) scheme has been improved through the integration of parallel structures, aiming to enhance the algorithm's computational efficiency [13]. To the best of our knowledge and understanding, this enhancement is novel and has a significant impact on the performance of the authentication scheme. The Feige-Fiat-Shamir (FFS) protocol consists of two primary phases: key generation and authentication. Its novelty resides in the integration of Zero-Knowledge Authentication within the FFS framework. This combination involves merging the 1st and 4th stages of FFS. The change is that the channel sent is replaced with a key generator obtained from the RSS key generator [14]. It is expected to obtain a new key for vehicle communication.

A Vehicular Ad hoc Network (VANET) is a communication system that facilitates data exchange between vehicles and Road Side Units (RSUs) within a limited transmission range, typically spanning from 100 to 300 meters. [15]. The main purpose of deploying VANET is to overcome the problem of accidents. It has various applications for enhancing human safety and enabling drivers to navigate urban roads safely. The accident rate is increasing day by day, along with the growing vehicle population; therefore, vehicles must implement VANET systems [16]. For example, let us assume that vehicle A is traveling before vehicle B and suddenly A meets with a collision by a storm and affects its brakes, the does not want B to face the same trouble, then again, the sensor of vehicle A drives a signal and sends it to the road side unit and then broadcasts the warning information to other vehicles [17]. After receiving the notification message, B moves back from the vehicle. Efficient and reliable communication between vehicles is essential during road journeys [18].

VANET is a driven network that focuses on smart and intelligent transportation systems, providing facilities for vehicle end-users to exchange information quickly and enhance their welfare[19]. VANET utilizes specialized guidelines, such as DSRC and WAVE, for the rapid and efficient exchange of information. The United States Federal Communications Commission (FCC) has allocated a 75 MHz bandwidth within the 5.9 GHz frequency band specifically for Dedicated Short-Range Communications (DSRC). This spectrum is divided into seven channels, each occupying 10 MHz. [20]. Among the seven allocated channels, one is designated as the control channel, primarily intended to support safety-critical applications. [21]. In VANET, there are two types of safety-related communications passing through the control channel; the first is an event-driven message sent to the target vehicle when a hazard situation has occurred and another is a periodic beacon message indicating the vehicle's current location information such as position, speed, to nearby vehicles [22]. Researchers utilize the Zero-Knowledge Authentication Feige-Fiat-Shamir protocol by combining the key generator obtained from the Received Signal Strength (RSS) of vehicle communication, thereby replacing the channel in the Feige-Fiat-Shamir protocol with the key generator derived from RSS. Here, it is expected to obtain a new key for vehicle communication. To ensure safer data communication during the exchange of existing data information.

II. Research Methodology

A Vehicular Ad hoc Network (VANET) is a communication system that facilitates data exchange between vehicles and Road Side Units (RSUs) within a limited transmission range, typically spanning from 100 to 300 meters. The main purpose of deploying VANET is to overcome the problem of accidents. It has various applications for enhancing human safety and enabling drivers to drive properly on urban roads. The accident rate is increasing daily, in tandem with the growing number of vehicles on the road. Therefore, vehicles must incorporate Vehicle-to-Everything (V2X) or Vehicle-to-Everything (V2E) systems. For example, let us assume that vehicle A is traveling before vehicle B and suddenly collides with a storm, affecting its brakes. Then, it does not want B to face the same trouble. Again, the sensor of vehicle A drives the signal and sends it to the roadside unit, which then broadcasts the warning information to other vehicles. After receiving the notification message, B moves back from the vehicle. So, efficient and reliable communication between vehicles is needed during the journey on the road.

Researchers utilize the Zero-Knowledge Authentication Feige-Fiat-Shamir protocol by combining the key generator obtained from the Received Signal Strength (RSS) of vehicle communication, thereby replacing the channel in the Feige-Fiat-Shamir protocol with the key generator derived from RSS. It is expected to obtain a new key for vehicle communication. To ensure safer data communication during the exchange of existing data information.

Feige-Fiat-Shamir Protocol Zero Knowledge Authentication. The Feige-Fiat-Shamir (FFS) identification protocol employs a parallel approach grounded in public-private key cryptography. To improve the algorithm's performance, the scheme is refined through the integration of parallel structures. To the best of our knowledge and understanding, this enhancement is novel and has a significant impact on the performance of the authentication scheme.

There are two main phases in FFS, namely, key generation and authentication. The first phase involves key generation to produce public and private key pairs, which are used in communication. The prover and verifier choose k different numbers: *v1, v2, ..., vk*, where each number is the square of the residual modulus. Then both of them choose the same number *vi from x2* $\equiv$ *vi mod n* and have a solution *v-1 i mod n*, where *i k*. String *v 1kv2k ... kvk* is the user's public key. Both parties calculate a very small number *si*, where *si = qv − 1 i mod n.* The string *s1ks2k ... ksk* is the user's private key. The second phase, authentication, occurs whenever *a* legitimate

DOI : https://doi.org/10.25139/inform.v10i2.9488

user is authenticated using an interactive protocol. The authentication phase consists of three steps, namely, witness, challenge, and response. (i)The prover generates a random number *r*, where *r<n*. Then he computes *x=r2 mod n*, and sends *x* to the verifier (witness). (ii)The verifier then sends a number k of random bits, namely, *b1, b2, ..., bk* (challenge). Rather than transmitting each bit individually, the verifier may opt to send the entire block of random bits simultaneously to improve efficiency.

The objective of implementing this parallel mechanism is to maximize the number of verifications performed per iteration, thus minimizing the communication overhead between the participating entities. The prover computes *y = r (sb1 1 sb2 2 ... sbk k) mod n*. Intuitively, If the value of a given bit in the challenge sequence is 1, the corresponding *sis_isi* contributes to the computation of *y*; conversely, if the bit is 0, sis_isi is excluded from the multiplication. The prover then transmits the resulting *y* value as the response. The verifier checks the value *x0 = y2 (vb1 1 vb2 2 ... vbk k) mod n*. This authentication process is iterated t times to ensure the verifier gains sufficient confidence that the prover possesses the correct values of *s1, s2, ..., sk*. The likelihood of a dishonest prover successfully deceiving the verifier in all iterations is *1/2 t*.

Fig.1. Received Signal Strength (RSS) Stages

The initial phase of this study involves channel probing using Received Signal Strength (RSS) measurements. As illustrated in Fig. 1, Alice and Bob, acting as legitimate users, exploit the wireless environment to obtain RSS estimates during their communication. Meanwhile, a third party, Eve, passively intercepts the wireless channel between Alice and Bob and attempts to capture all communication data. Through this eavesdropping, Eve may potentially reconstruct the secret key utilized by Alice and Bob for secure message exchange during transmission.

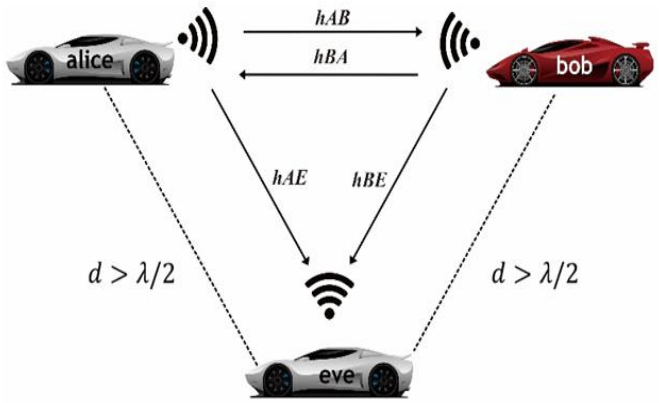

Fig.2. RSS Collection Scenario

The exchange of RSS values between Alice and Bob is conducted using the ping command, which operates based on the ICMP protocol. As illustrated in Fig. 2, it is assumed that the channel response observed by Bob from Alice is denoted as hAB, while the response measured by Alice from Bob is represented as hBA. Meanwhile, Eve obtains channel information from Alice as hAE and from Bob as hBE. Given that the distance between Eve and both Alice and Bob exceeds half the transmission wavelength, it follows that $hBA \neq hAE$ and $hAB \neq hBE$. Alice and Bob exchange information through mutual information within a specified time frame, as defined by Equation (1).

$$hAB = \{hAB(t1), hAB(t2),...,hAB(tn)\} \quad (1)$$
$$hBA = \{hBA(t1'), hBA(t2'),...,hBA(tn')\}$$

The probing interval between two users is determined based on the coherence time to ensure that both Alice and Bob observe equivalent RSS (Received Signal Strength) values. In wireless communication systems, coherence time refers to the time duration over which the channel's impulse response remains stable. Within the context of secret key generation for Vehicle-to-Vehicle (V2V) communication, this parameter is critical for achieving a high degree of signal correlation. Furthermore, when Alice and Bob engage in V2V communication at higher speeds, the Doppler shift effect becomes significant. Notably, the maximum Doppler frequency is inversely related to the coherence time.

After the Received Signal Strength (RSS) stage is complete, which starts from getting the Key Generator using the Rasberry Pi Tool, the next step is Zero Knowledge Authentication here, which combines the Zero Knowledge Authentication FFS (Feige-Fiat-Shamir Protocol), in Fig.3 we see the existing combination is combining stages 1 and 4 in FFS. The existing changes are in the channel sent, replaced with the key generator obtained from the RSS key generator. It is expected to obtain a new key for vehicle communication.

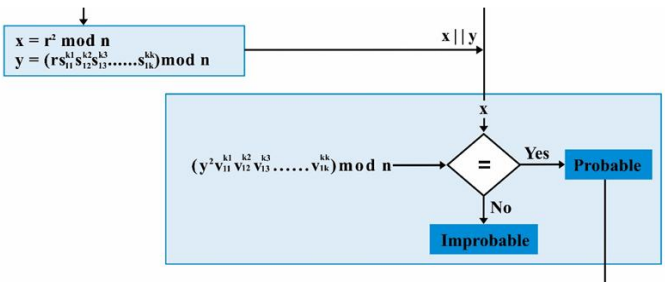

Fig.3. Combination Feige-Fiat-Shamir Protocol

III. Result and Discussion

A. Channel Probabilistic Data Retrieval

The system's performance is assessed by evaluating its reliability in generating cryptographic keys that demonstrate a high degree of consistency and confidentiality. The testing scenario is conducted in an outdoor environment, specifically along a highway. During the key generation process, mobile

DOI : https://doi.org/10.25139/inform.v10i2.9488

nodes operating at varying speeds can synchronize their measurements accordingly.

The system evaluation employs a TL-WN722N wireless USB adapter, which supports IEEE 802.11b/g/n standards and operates in the 2.4 GHz frequency band for communication. In the experimental setup, Alice serves as the initiator, while Bob functions as the responder. The distance between Alice and Bob is maintained at approximately 3 meters. Eve, the eavesdropper, is positioned around 3 meters away from them and moves in the same direction and at the same speed. The data collection takes place on a smooth and densely trafficked road.

The speeds used are 0, 20, 40, and 60 km/h. Following the study of the secret key creation process, a suitable speed can be determined. The second parameter involves the variation of ping intervals, which directly influences the measurement data obtained from the two nodes. In this context, the ping interval is selected based on the calculated coherence time and must exceed the coherence time corresponding to a given vehicle speed. The evaluated interval values are 7 ms, 10 ms, and 20 ms.

Vehicles 1 and 2 use the same channel and an ad hoc (peer-to-peer) arrangement for communication. The tcpdump command in monitor mode is used to perform the RSS (Received Signal Strength Indicator) measurement procedure. The RSS signal intensity of Vehicle 2 will be measured by Vehicle 1, and while probing, Vehicle 2 measures the Received Signal Strength (RSS) of signals transmitted by Vehicle 1. The encryption key used to transmit text messages from Vehicle 1 to Vehicle 2 securely is generated by Vehicle 1 and applied within a symmetric key cryptographic framework, where the same key is used for both encryption and decryption processes. This is feasible under the condition that both vehicles obtain identical RSS (Received Signal Strength) values and the randomness requirements are satisfied.

Table I outlines the experimental scenarios designed to evaluate the effectiveness of utilizing secret keys. A total of nine scenarios (labeled A through I) are implemented. These scenarios are structured around two main parameters: vehicle speed and the time interval between measurements.

TABLE I
MEASUREMENT SCENARIOS

Scenario	Speed	Ping Interval
A	20 km/h	7 ms
B		10 ms
C		20 ms
D	40 km/h	7 ms
E		10 ms
F		20 ms
G	60 km/h	7 ms
H		10 ms
I		20 ms

B. *Universal Hash*

In symmetric cryptographic communication systems, the NIST randomness test is used to verify that the generated encryption and decryption keys meet the standards for randomness required by the NIST. Within the NIST testing framework, several statistical parameters are evaluated, each requiring a p-value greater than 0.01 to be considered valid. Only the best-performing parameter from among the generated keys or the evaluation of 1 to 3 selected keys is used as a benchmark for key suitability. Afterward, the key is processed using the SHA-256 algorithm.

The NIST test determines whether the key exhibits sufficient randomness by analyzing various metrics, including entropy, frequency test, block frequency analysis, longest run of ones test, cumulative sum (forward), and cumulative sum (backward). To successfully pass the test, the resulting p-value for each parameter must exceed the threshold of 0.01. Since there are fifteen keys, the NIST test can also be used to identify the key winner, the key that will be utilized in the cryptography procedure. To proceed with the Zero Knowledge Authentication process, the key that exhibits the highest approximate entropy and successfully passes all parameters of the NIST statistical test suite is considered the optimal (or winning) key.

Fig. 4 shows that the 40k10ms Approach produces the highest value of 0.7352 according to the Average Entropy Estimation Results. This number will then be used as input for the Zero Knowledge Authentication procedure.

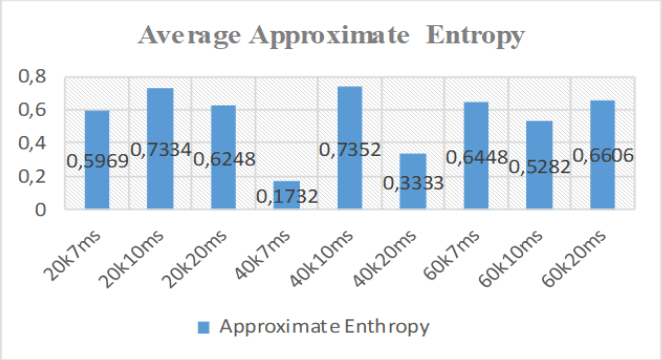

Fig. 4. Average Approximate Entropy Results

C. *Testing of Proposed Algorithm Authentication Time Against Changed Distance with Dynamic Scenario*

Following the previous simulation testing process, the proposed algorithm is now implemented on a Raspberry Pi for further evaluation. The testing was conducted on *Jalan Soekarno Hatta Lamongan*. Fig.5 shows the location where the algorithm is tested. The location shown in Fig. 5 illustrates the dynamic scenario of the verifier, with distances from the Claimant at intervals of 5 meters, 10 meters, 15 meters, 20 meters, and 25 meters. The existing testing was conducted on busy, smooth roads with heavy vehicle traffic. Each distance will be authenticated by the Claimant to the Verifier 3 times, and the average time will be recorded.

DOI : https://doi.org/10.25139/inform.v10i2.9488

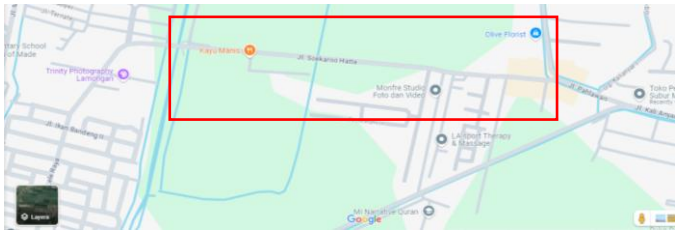

Fig.5. Proposed Algorithm Testing Location

Both the Claimant and the Verifier are in the same condition, moving at a speed of 40 km/h during the test, because the Approximate Entropy used is 40 k10 ms. Table II shows the results of the dynamic scenario test. This system is automated and operates using wireless communication media. This system utilizes a Raspberry Pi 3 mini-computer as its embedded system. For its communication device, it utilizes IEEE 802.11n wireless technology. In its communication, it can only be done in one direction, namely from the transmitter device installed on the vehicle as a message sender to the receiver installed on public or private vehicles that act as message recipients. The design and realization of communication system devices between vehicles generally consist of two main parts: the transmitter and receiver parts, also known as Claimant or Verifier.

For the transmitter and receiver parts, a Raspberry Pi 3 mini-computer is equipped with a wireless connection using IEEE 802.11n technology, and Raspbian Linux is installed. Similarly, the verifier is equipped with Raspbian Linux to run message sending applications or perform authentication. In software design, this device utilizes the Raspbian Linux operating system, which has been installed with several supporting software packages to establish an ad hoc wireless network connection.

TABLE II
AUTHENTICATION TIME TEST RESULTS OF THE PROPOSED ALGORITHM

Distance (Meters)	Authentication Time (Seconds)	Average Authentication Time (Seconds)
5 Meter	0.000456	0.000442
	0.000405	
	0.000466	
10 Meter	0.000375	0.000367
	0.000326	
	0.000402	
15 Meter	0.000280	0.000283
	0.000275	
	0.000294	
20 Meter	0.000291	0.000344
	0.000378	
	0.000364	
25 Meter	0.000441	0.000418
	0.000396	
	0.000419	

Table II shows the test results with a dynamic scenario. In dynamic conditions, it can be observed that the greater the distance between the Verifier and Claimant, the less authentication time is required. However, the difference in authentication time values from one distance to another is not that significant. Indeed, at a distance of 20 meters, there is an increase in the existing authentication time, which persists up to a distance of 25 meters. However, the highest value occurs when the Verifier and Claimant are at a distance of 5 meters, namely 0.000442. This is due to the influence of crowded vehicles during the testing process.

D. Single Brute Force Attack Testing On The Proposed Algorithm With A Dynamic Scenario

The next experiment is testing the authentication security of the proposed algorithm using brute force penetration testing. The Verifier test scenario involves measuring distances from the Claimant at intervals of 5 meters, 10 meters, 15 meters, 20 meters, and 25 meters. In each scenario, three brute force attack attempts will be carried out on the verifier. If, in the three tests, the attacker fails to perform a brute force attack, then the proposed algorithm's security effectiveness is 100%. In the security testing of the proposed algorithm, a single-attacker scenario is considered. The single-attacker scenario is a Verifier attack scenario involving a single attacker. The results of the test in dynamic conditions are presented in Table III.

TABLE III
RESULTS OF SINGLE BRUTE FORCE ATTACK TESTING ON THE ALGORITHM

Distance	Testing	Single Attacker Dinamis
5 Meter	1	Failed
	2	Failed
	3	Failed
10 Meter	1	Failed
	2	Failed
	3	Failed
15 Meter	1	Failed
	2	Failed
	3	Failed
20 Meter	1	Failed
	2	Failed
	3	Failed
25 Meter	1	Failed
	2	Failed
	3	Failed

As shown in the test results above, the proposed algorithm achieves 100% security effectiveness, specifically in both the dynamic scenario and the single-attacker scenario. This indicates that the attacker was unable to authenticate the system during the experiment.

IV. CONCLUSION

From the results of the experiments and analysis conducted in the study. A total of nine scenarios (A-I) have been tested in the secret key generation process, considering two main parameters: vehicle speed and time interval. Based on the results obtained from the Modified Quantization Log, the average Key Disagreement Rate Metric (KDRM) between Alice and Bob is observed to be 9.4%. Meanwhile, the average Key Generation Rate (KGR) is recorded at 71.4 bits per second (bps). This value indicates that the level of bit mismatch between the two legitimate users after the Modified

DOI : https://doi.org/10.25139/inform.v10i2.9488

Quantization Log process is relatively low, as the pre-processing stage was previously carried out using the Kalman Filter.

When the Modified Quantization Log is integrated with the BCH coding scheme, a Key Disagreement Rate (KDR) of 0% is achieved between Alice and Bob. Additionally, the average number of generated bits exceeds 1,512 bits, indicating that the previous quantization process is capable of producing high-quality keys. This is possible because about half of the bits that match during the quantization process can be further processed into keys, as shown by the results of the BCH code.

The output of the Universal Hash has been evaluated using the NIST test suite, and the results align with expectations, particularly by satisfying the required p-value threshold, which must exceed 0.01. In the dynamic condition authentication time test, it can be seen that the further the distance between the Verifier and Claimant, the less authentication time is needed. However, the difference in authentication time values against the distance from one another is not that significant. The highest value, when the Verifier and Claimant are at a distance of 5 meters, is 0.000442. In the Dynamic Single Brute Force test, the proposed algorithm achieves 100% security. This indicates that the attacker was unable to authenticate the system during the experiment. The results of this study are expected to serve as a reference for the implementation of vehicle communication technology, which is anticipated to experience rapid growth in the future.

ACKNOWLEDGMENT

The researcher would like to express his gratitude to the Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi Republik Indonesia, which has allowed the researcher to participate in Skema Penelitian Dosen Pemula. The researcher and the team can gain more insight from this opportunity and, in the future, will be more enthusiastic about conducting other research. The researcher would also like to thank Universitas Muhammadiyah Lamongan for its support, which has enabled this research to be carried out properly.

REFERENCES

[1] Abhijit Ambekar and Hans D. Schotten, *Enhancing Channel Reciprocity for Effective Key Management in Wireless Ad-hoc Networks*. 2014.

[2] U. Feige, A. Fiat, and A. Shamir, "Zero-Knowledge Proofs of Identity," 1988.

[3] M. Bellare and A. Palacio, "GQ and Schnorr Identification Schemes: Proofs of Security against Impersonation under Active and Concurrent Attacks," Springer-Verlag, 2002.

[4] S. Paramanik, "Comparison of Zero Knowledge Authentication Protocols," 2014.

[5] Mike Yuliana, Wirawan, and Suwadi, *Performance Evaluation of the Key Extraction Schemes in Wireless Indoor Environment*. 2017.

[6] B. Sharma, M. Satya, P. Sharma, and R. Singh Tomar, "A Survey: Issues and Challenges of Vehicular Ad Hoc Networks (VANETs) under responsibility of International Conference on Sustainable Computing in Science, Technology and Management," 2019.

[7] I. A. Kalmykov, A. A. Olenev, N. I. Kalmykova, and D. V. Dukhovnyj, "Using Adaptive Zero-Knowledge Authentication Protocol in VANET Automotive Network," *Inf.*, vol. 14, no. 1, Jan. 2023, doi: 10.3390/info14010027.

[8] M. C. Kriswantoro, A. Sudarsono, and M. Yuliana, "Secret Key Establishment Using Modified Quantization Log For Vehicular Ad-Hoc Network," *Inf. J. Ilm. Bid. Teknol. Inf. dan Komun.*, vol. 6, no. 2, pp. 103–109, Jul. 2021, doi: 10.25139/inform.v6i2.4037.

[9] A. F. Septano, A. Kusyanti, and R. A. Siregar, "Implementasi Feige-Fiat-Shamir Identification Scheme untuk Autentikasi antara Node dan Gateway pada Module Lora," 2021.

[10] M. Yuliana, Wirawan, and Suwadi, "A simple secret key generation by using a combination of pre-processing method with a multilevel quantization," *entropy*, vol. 21, no. 2, Feb. 2019, doi: 10.3390/e21020192.

[11] Amang Sudarsono, Mike Yuliana, and Prima Kristalina, *A Reciprocity Approach for Shared Secret Key Generation Extracted from Received Signal Strength in The Wireless Networks*. IEEE, 2018.

[12] C. Weiß, "V2X communication in Europe - From research projects towards standardization and field testing of vehicle communication technology," *Comput. Networks*, vol. 55, no. 14, pp. 3103–3119, 2011, doi: 10.1016/j.comnet.2011.03.016.

[13] I. Arnomo, "Authentication Comparison of Telecommunications Technology Using A3, A8, A5 and Rijndael Algorithms," *Inf. J. Ilm. Bid. Teknol. Inf. dan Komun.*, vol. 3, no. 2, pp. 74–83, 2018, doi: 10.25139/inform.v3i2.1031.

[14] L. Cheng, L. Zhou, B. C. Seet, W. Li, D. Ma, and J. Wei, "Efficient Physical-Layer Secret Key Generation and Authentication Schemes Based on Wireless Channel-Phase," *Mob. Inf. Syst.*, vol. 2017, 2017, doi: 10.1155/2017/7393526.

[15] S. Goldwasser, "Interactive proof systems," vol. 18, no. 1, pp. 108–128, 1989, doi: 10.1090/psapm/038/1020812.

[16] J. A. L. Calvo and R. Mathar, "Secure Blockchain-Based Communication Scheme for Connected Vehicles," *2018 Eur. Conf. Networks Commun. EuCNC 2018*, pp. 347–351, 2018, doi: 10.1109/EuCNC.2018.8442848.

[17] M. C. Kriswantoro and A. H. Ayatullah, "Manajemen Bandwidth Pada Jaringan Pemerintah KotaSurabaya Menggunakan Metode Queue Tree," *Aicoms 2023*, vol. 2, no. 2, pp. 1–8, 2023.

[18] M. F. Falah *et al.*, "Comparison of cloud computing providers for development of big data and internet of things application," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 22, no. 3, pp. 1723–1730, 2021, doi: 10.11591/ijeecs.v22.i3.pp1723-1730.

[19] E. M. Member, E. Hasan, and G. Student, "Concept Drift Aware Wireless Key Generation in Dynamic LiFi Networks," *IEEE Open J. Commun. Soc.*, vol. PP, p. 1, 2024, doi: 10.1109/OJCOMS.2024.3524497.

[20] J. Petit and S. E. Shladover, "Potential Cyberattacks on Automated Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 546–556, 2015, doi: 10.1109/TITS.2014.2342271.

[21] Y. Yu, Y. Li, M. H. Au, W. Susilo, K. K. R. Choo, and X. Zhang, "Public cloud data auditing with practical key update and zero knowledge privacy," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9722, pp. 389–405, 2016, doi: 10.1007/978-3-319-40253-6_24.

[22] G. Hussain, S. J. Nawaz, S. Wyne, and M. N. Patwary, "On Channel Transforms to Enhance Reciprocity and Quantization in Physical-Layer Secret Key Generation," *IEEE Access*, vol. 13, no. November 2024, pp. 256–272, 2024, doi: 10.1109/ACCESS.2024.3523105.

DOI : https://doi.org/10.25139/inform.v10i2.9488