Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control
Journal homepage: http://kinetik.umm.ac.id
ISSN: 2503-2267
Vol. 11, No. 3, August, Pp. 527-536

Kalman filter-based RSS preprocessing for cryptographic key generation in zero-knowledge Feige Fiat Shamir authentication

M. Cahyo Kriswantoro*[1], Eko Handoyo[2], Ahmad Lathif Aditya[1]
Medical Informatics Department, Universitas Muhammadiyah Lamongan, Indonesia[1]
Computer Engineering Department, Universitas Muhammadiyah Lamongan, Indonesia[2]

Article Info
Keywords:
Kalman Filter, Zero Knowledge Authentication, Feige-Fiat-Shamir, Received Signal Strength, Key Generator

Article history:
Received: December 16, 2025
Accepted: May 16, 2026
Published: August 01, 2026

Cite:
M. C. Kriswantoro, Eko Handoyo, and Ahmad Lathif Aditya, "Kalman Filter-Based RSS Preprocessing for Cryptographic Key Generation in Zero-Knowledge Feige Fiat Shamir Authentication", *KINETIK*, vol. 11, no. 3, Aug. 2026.
https://doi.org/10.22219/kinetik.v11i3.2644

*Corresponding author.
M. Cahyo Kriswantoro
E-mail address:
cahyo.krizt@gmail.com

Abstract
Secure authentication in wireless communication environments requires mechanisms capable of verifying identity without exposing confidential information. Zero-Knowledge Authentication (ZKA) addresses this challenge by enabling interactive identity verification without revealing secret credentials. However, in practical wireless implementations, the reliability of ZKA strongly depends on the quality and consistency of the cryptographic keys used during the authentication process. One promising approach is to generate keys from physical-layer characteristics, such as Received Signal Strength (RSS). Nevertheless, raw RSS measurements are highly unstable due to noise, interference, mobility, and signal fluctuations, which often result in low reciprocity and key mismatch between legitimate nodes. This study proposes a Kalman Filter-based preprocessing method to improve RSS quality prior to cryptographic key generation for Zero-Knowledge Feige–Fiat–Shamir authentication. The Kalman Filter is employed to suppress measurement noise and enhance reciprocity between communicating nodes, allowing both parties to derive more consistent symmetric keys. The generated keys are then integrated into the authentication process to replace conventional static, channel-dependent key components. The proposed approach was evaluated using key consistency, entropy level, and bit mismatch rate as performance metrics. Experimental results show that Kalman Filter-based preprocessing significantly improves RSS stability and increases the correlation between legitimate nodes compared with unfiltered RSS measurements. In addition, the generated keys exhibit lower bit mismatch rates and better entropy characteristics, leading to higher authentication success rates while preserving the confidentiality properties of Zero-Knowledge Authentication. These findings demonstrate that Kalman Filter-assisted RSS preprocessing provides an effective and lightweight solution for strengthening cryptographic key generation and improving the reliability of authentication systems in wireless communication environments.

1. Introduction

The rapid growth of wireless communication systems and intelligent transportation technologies has introduced significant security challenges, particularly in highly dynamic environments such as Vehicular Ad Hoc Networks (VANETs) and Vehicle-to-Everything (V2X) communications [1], [2], [3]. In these environments, communication nodes continuously exchange critical information over open wireless channels, making them vulnerable to impersonation, replay, man-in-the-middle, and denial-of-service attacks [4]. Therefore, secure, lightweight, and privacy-preserving authentication mechanisms are urgently required to ensure trustworthy communication in modern wireless networks [5].

Conventional authentication schemes commonly rely on pre-shared secret keys, certificate-based infrastructures, or trusted third parties. Although effective in static systems, these approaches often suffer from scalability limitations, high management overhead, and additional attack surfaces when deployed in decentralized and mobile wireless environments [6], [7], [8]. To overcome these limitations, Zero-Knowledge Proof (ZKP) has emerged as a promising cryptographic paradigm that enables one party to prove possession of a secret without revealing the secret itself [9], [10]. Due to its completeness, soundness, and zero-knowledge properties, ZKP provides secure and privacy-preserving identity verification suitable for resource-constrained wireless systems [9], [11]. Among various zero-knowledge authentication schemes, the Feige–Fiat–Shamir (FFS) protocol is widely recognized as a lightweight challenge–response authentication mechanism suitable for wireless and low-power communication environments [10], [12]. [13].

Recently, physical-layer security has attracted considerable attention as a complementary mechanism for secure wireless communications. Physical-layer key generation utilizes the reciprocity and randomness of wireless channels to establish shared secret keys between legitimate nodes [14], [15], [16]. One of the most practical parameters for this purpose is Received Signal Strength (RSS), as RSS values are readily available in most wireless communication devices [15], [17]. RSS-based key generation has been widely explored because of its simplicity and low implementation cost [14], [18]. However, raw RSS measurements are highly sensitive to environmental noise, interference, hardware variations, and mobility effects, which reduce channel reciprocity and result in inconsistent cryptographic keys [19], [20].

Several preprocessing approaches have been proposed to improve RSS reliability, including averaging techniques, smoothing filters, channel transformation, and channel impulse response estimation [16], [20], [21]. Nevertheless, many conventional smoothing methods are less adaptive to rapidly changing wireless channels because they do not explicitly estimate system state dynamics. In contrast, the Kalman Filter provides recursive state estimation with minimum mean square error characteristics, making it suitable for noisy and time-varying wireless measurements [21], [22], [23], [24], [25], [26]. Previous studies have shown that Kalman Filter-based preprocessing significantly improves RSS stability and key agreement performance between legitimate users [22], [23], [24], [25], [26].

Despite these advancements, most existing studies focus primarily on RSS-based key generation as a standalone mechanism for encryption or secure key agreement [14], [18], [20]. Limited attention has been given to the direct integration of physical-layer generated keys into zero-knowledge authentication frameworks. Existing approaches generally treat key generation and authentication as separate processes, potentially increasing communication overhead and reducing authentication efficiency in dynamic wireless environments [27]. In particular, the integration of dynamically generated RSS-derived keys into the Feige–Fiat–Shamir authentication protocol remains underexplored, especially in vehicular communication systems [28].

To address this gap, this study proposes a Kalman Filter-assisted RSS preprocessing framework integrated with the Feige–Fiat–Shamir zero-knowledge authentication protocol. First, RSS channel measurements are filtered using a Kalman Filter to reduce noise and improve channel reciprocity between communicating nodes. The filtered RSS values are then transformed into symmetric cryptographic keys. Finally, the generated keys are incorporated into the Feige–Fiat–Shamir authentication process to strengthen identity verification without exposing sensitive information.

The main contributions of this research are summarized as follows:

1. Proposing a Kalman Filter-based preprocessing mechanism to enhance RSS reciprocity in dynamic wireless environments.
2. Improving key consistency and reducing bit mismatch rate during RSS-based secret key generation.
3. Integrating physical-layer generated keys into the Feige–Fiat–Shamir Zero Knowledge authentication protocol.
4. Demonstrating a unified lightweight authentication framework suitable for wireless and vehicular communication systems.

The novelty of this work lies in the integration of adaptive Kalman Filter-assisted RSS key generation and zero-knowledge authentication within a unified framework. Unlike previous studies that addressed key generation and authentication as separate processes, the proposed approach jointly improves key quality and authentication reliability. Therefore, this research contributes to the development of secure, efficient, and privacy-preserving authentication mechanisms for next-generation wireless networks.

2. Research Method

This study proposed an integrated authentication framework that combines the Feige–Fiat–Shamir (FFS) zero-knowledge authentication protocol with Received Signal Strength (RSS)-based cryptographic key generation. To improve the quality of RSS measurements in dynamic wireless environments, a Kalman Filter preprocessing stage was introduced before the key generation process. The overall framework consisted of three main stages: (1) the Feige–Fiat–Shamir authentication model, (2) RSS preprocessing using a Kalman Filter, and (3) integration of RSS-derived keys into the authentication process. The complete workflow of the proposed system is illustrated in Figure 1.

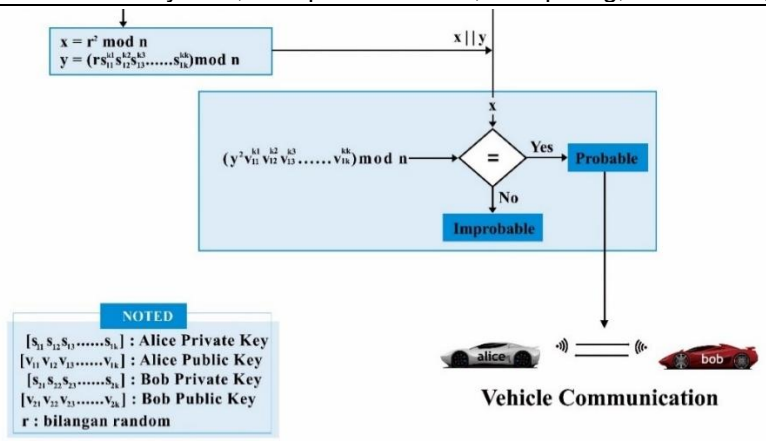

Figure 1. Proposed Integration of RSS-based Key Generation with Feige–Fiat–Shamir Authentication Protocol

2.1 Feige–Fiat–Shamir Zero-Knowledge Authentication Protocol

The Feige–Fiat–Shamir (FFS) scheme is a zero-knowledge authentication protocol based on modular arithmetic, public–private key pairs, and interactive challenge–response communication [12]. The protocol was selected for this study because of its computational simplicity, privacy-preserving properties, and suitability for lightweight wireless systems. To reduce communication overhead, a parallel challenge construction was adopted, allowing multiple challenge bits to be transmitted within a single iteration.

The FFS protocol consisted of two main phases: key generation and authentication.

1) Key Generation Phase

In the key generation phase, both the prover and the verifier jointly generated public and private key pairs used for authentication [14]. First, both parties selected *k* distinct quadratic residue values $v1, v2, \ldots vk$, where each value satisfied the congruence $x^2 \equiv v_i (mod\ n)$ and had a modular inverse $v_i^{-1} (mod\ n)$ The concatenation $v\_1 \,||\, v\_2 \,||\, \ldots \,||\, v\_k$ formed the public key [12]. Subsequently, the prover computed a set of private values $\boldsymbol{si}$, where each value was derived as $s\_i = q \cdot v\_i\text{^}(-1)\ (mod\ n)$ The concatenation $s\_1 \,||\, s\_2 \,||\, \ldots \,||\, s\_k$ constituted the private key, which remained confidential to the prover [12].

2) Authentication Phase

The authentication phase was performed interactively each time a legitimate user attempted to authenticate. This phase consisted of three sequential steps: commitment, challenge, and response [12]. First, the prover generated a random number r, where $r < n$ and computed $x = r\text{^}2\ (mod\ n)$. The value x was then transmitted to the verifier as the commitment [12]. Next, the verifier generated a random binary challenge vector $\{b\_1, b\_2, \ldots, b\_k\}$. Instead of transmitting each bit individually, the verifier sent the challenge as a single block of bits. This parallel mechanism increased the number of verifiable credentials per iteration and reduced communication overhead [15].

Upon receiving the challenge, the prover computed the response $y = r \cdot (s\_1\text{^}(b\_1) \cdot s\_2\text{^}(b\_2) \cdot \ldots \cdot s\_k\text{^}(b\_k))\ (mod\ n)$. Intuitively, each private value Si influenced the response only when the corresponding challenge bit $\boldsymbol{bi}$ equaled one. The prover then transmitted yyy to the verifier [12]. Finally, the verifier validated the response by computing $x' = y\text{^}2 \cdot (v\_1\text{^}(b\_1) \cdot v\_2\text{^}(b\_2) \cdot \ldots \cdot v\_k\text{^}(b\_k))\ (mod\ n)$. The authentication phase was repeated for $\boldsymbol{t}$ iterations until the verifier was sufficiently convinced that the prover possessed the correct private keys. The probability of a dishonest prover successfully impersonating a legitimate user was limited to $P = 1 / 2\text{^}t$.

In the key generation phase, both the prover and the verifier jointly generated public and private key pairs used for authentication [12]. First, both parties selected *k* distinct quadratic residue values $v1, v2, \ldots vk$, where each value satisfied the congruence $x^2 \equiv v_i (mod\ n)$ and had a modular inverse $v_i^{-1} (mod\ n)$. The concatenation $v\_1 \,||\, v\_2 \,||\, \ldots \,||\, v\_k$ formed the public key [14]. Subsequently, the prover computed a set of private values $\boldsymbol{si}$, where each value was derived as $s\_i = q \cdot v\_i\text{^}(-1)\ (mod\ n)$. The concatenation $s\_1 \,||\, s\_2 \,||\, \ldots \,||\, s\_k$ constituted the private key, which remained confidential to the prover [12].

2.2 Received Signal Strength Preprocessing Using Kalman Filter

Received Signal Strength (RSS) was employed as the physical-layer parameter for secret key generation because it is readily available in most wireless communication devices [8], [28]. However, raw RSS values are strongly affected by noise, multipath fading, mobility, and environmental interference, resulting in low reciprocity between legitimate nodes. To overcome this limitation, Kalman Filter-based preprocessing was applied after RSS acquisition. The Kalman Filter performs recursive state estimation by combining prediction and measurement update stages while

minimizing estimation error through covariance adjustment [22]. In this study, two main estimates were used: apriori and a posteriori states. Compared with conventional smoothing methods, the Kalman Filter was selected because it is adaptive to time-varying signals, computationally efficient, and suitable for real-time wireless measurements. After filtering, the RSS values became more stable and exhibited higher correlation between communicating nodes, thereby reducing key mismatch during key generation.

2.3 RSS-Based Key Generation and Integration with FFS Authentication

After preprocessing, the filtered RSS values were converted into binary bit sequences using the key generation module implemented on a Raspberry Pi platform [28]. Quantization and reconciliation stages were then applied to derive identical symmetric keys between legitimate nodes. The generated RSS-based keys were subsequently integrated into the Feige–Fiat–Shamir authentication protocol. Instead of relying solely on conventional static credentials, the proposed system utilized dynamic physical-layer keys to strengthen authentication reliability.

This approach provided two security advantages:

1. Improved resistance against impersonation attacks due to dynamically changing keys.
2. Reduced key mismatch probability because Kalman Filter-based preprocessing increased RSS reciprocity.

The combination of physical-layer key generation and zero-knowledge authentication enabled a lightweight and privacy-preserving authentication mechanism suitable for wireless and vehicular communication environments.

3. Results and Discussion

This section presents the experimental results and analytical discussion of the proposed authentication framework. The evaluation was conducted in several stages, including channel probing, Kalman Filter preprocessing, modified quantization, BCH error correction, randomness enhancement, and authentication performance testing. To address the reviewers' comments, the discussion emphasizes both the numerical results and comparisons with the baseline approaches using unfiltered RSS measurements.

3.1 Channel Probing Data Acquisition

The performance of the proposed system was evaluated by examining its ability to generate secret keys with high consistency and confidentiality under dynamic wireless conditions. The experiments were conducted in an outdoor roadway environment where communicating nodes were in motion. This scenario was selected to represent realistic vehicular communication conditions in which channel characteristics frequently change due to mobility. All collected data consisted of Received Signal Strength (RSS) measurements obtained during bidirectional communication between legitimate nodes.

System measurements were performed using TL-WN722N wireless USB adapters supporting the IEEE 802.11b/g/n standards at 2.4 GHz. In the experimental setup, Alice acted as the initiator, while Bob served as the responder. The distance between Alice and Bob was maintained at approximately 3 m throughout the measurements. An eavesdropper node, Eve, was positioned at a comparable distance and moved in the same direction and at the same speed as the legitimate nodes. The experiments were conducted on a roadway with relatively low traffic density to minimize uncontrolled environmental interference.

Three different vehicle speeds were considered: 20 km/h, 40 km/h, and 60 km/h. These speed variations were selected to analyze the impact of mobility on wireless channel reciprocity and secret key generation performance. In addition, ping intervals of 7 ms, 10 ms, and 20 ms were evaluated according to the estimated coherence time of the wireless channel. Selecting probing intervals longer than the channel coherence time allowed more independent RSS observations for key extraction. As illustrated in Figure 2, Vehicle 1 and Vehicle 2 communicated using an ad-hoc (peer-to-peer) configuration on the same wireless channel. RSS measurements were captured using *tcpdump* in monitor mode. During channel probing, Vehicle 1 measured the RSS of packets transmitted by Vehicle 2, and vice versa. Reciprocal RSS measurements obtained from both nodes were then used as the basis for secret key generation. After successful key establishment, encrypted messages were exchanged using symmetric encryption. The complete probing scenario is shown in Figure 3.

A total of nine experimental scenarios (A–I) were evaluated, as summarized in Table 1. Each scenario combined different vehicle speeds and ping intervals to investigate their effects on channel reciprocity and key generation quality. During each experiment, Alice periodically transmitted ping requests to Bob while RSS values were recorded using Wireshark and a Python-based acquisition program, as illustrated in Figure 4. Approximately 3,000 RSS samples were collected from each node in every scenario.

The experimental observations indicate that lower vehicle speeds generally produced more stable RSS patterns, whereas higher speeds introduced more rapid channel fluctuations. Similarly, shorter ping intervals generated denser channel samples, which improved temporal correlation between Alice and Bob. Therefore, both mobility and probing interval played important roles in determining the quality of RSS-based secret key generation.

Table 1. Measurement Scenarios

Scenario	Speed	Interval Ping
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

Figure 2. Received Signal Strength (RSS) Stages

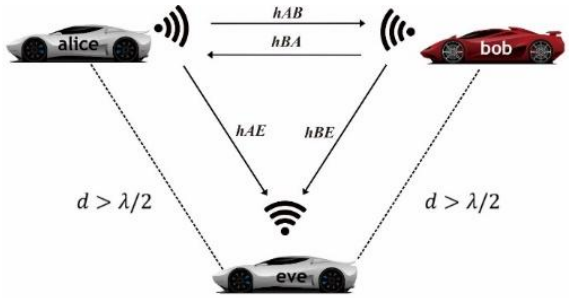

Figure 3. RSS Collection Scenario

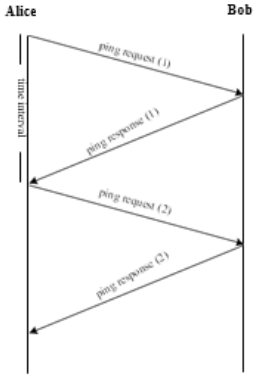

Figure 4. Channel Testing Mechanism

3.2 Kalman Filter Preprocessing Evaluation

Kalman Filter preprocessing was applied to improve the reciprocity and stability of Received Signal Strength (RSS) measurements between legitimate nodes. Raw RSS values in wireless environments are commonly affected by noise, multipath fading, interference, and mobility, which reduce the similarity between observations collected by Alice and Bob. Low reciprocity directly increases key disagreement during secret key generation. Therefore, an adaptive preprocessing stage was required before quantization. The Kalman Filter was selected because it performs recursive state estimation through prediction and correction stages based on error covariance. Unlike conventional moving-average smoothing, the Kalman Filter can track time-varying signals while suppressing random fluctuations. This characteristic makes it more suitable for dynamic vehicular communication scenarios in which channel conditions continuously change.

The Kalman Filter implementation was developed in Python. Estimation and update operations were performed on 800 data blocks and repeated ten times to ensure stable results. To evaluate effectiveness of the proposed preprocessing method, correlation coefficients were measured before and after preprocessing. Higher correlation indicates stronger reciprocity and a greater probability that both legitimate nodes generate identical keys. Correlation coefficients were calculated for three node pairs: Alice–Bob, Eve–Alice, and Eve–Bob. The experiments considered all vehicle speed and ping interval scenarios described previously. RSS data from all nodes were collected in *.cap* files and processed offline.

Table 2. RSS Correlation Coefficients for each Experimental Scenario

Scenario	Alice-Bob Measurement	Eve-Alice Measurement	Eve-Bob Measurement	Alice-Bob Kalman Filter
A	0.214726	-0.030299	0.047996	0.949669
B	0.611265	-0.134261	0.0550119	0.988106
C	0.468336	0.006525	-0.114585	0.956171
D	0.378911	-0.135524	-0.156346	0.979983
E	0.646678	0.228607	0.376563	0.963318
F	0.214804	0.000932	0.026160	0.912435
G	0.544626	0.051117	0.368495	0.914194
H	0.300479	-0.000551	0.042370	0.933715
I	0.073022	0.214090	0.095378	0.885036

Table 2 shows that the average raw correlation between Alice and Bob was relatively low due to channel noise and mobility effects. After Kalman Filter-based preprocessing, the average Alice–Bob correlation increased significantly compared with the raw RSS measurements. Specifically, the proposed Kalman Filter-based preprocessing improved the average channel reciprocity by approximately 146%, demonstrating its effectiveness in suppressing channel noise under dynamic mobility conditions to approximately 0.9425, with all scenarios achieving values above 0.88. The highest reciprocity was obtained in Scenario B (20 km/h, 10 ms), with a correlation coefficient of 0.988106. These results confirm that Kalman Filter-based preprocessing substantially improved RSS consistency compared with unfiltered measurements. For example, the correlation coefficient in Scenario A increased from 0.214726 to 0.949669, while that in Scenario I improved from 0.073022 to 0.885036. These substantial improvements indicate that the proposed method remained effective even under severe mobility conditions.

In contrast, correlation coefficient involving Eve remained considerably lower than those between Alice and Bob. This finding is important because an eavesdropper observing the same environment could not obtain channel measurements identical to those of the legitimate nodes. Hence, the proposed method not only improved reciprocity for key generation but also preserved the spatial decorrelation property required for physical-layer security. Compared with direct use of raw RSS values, the Kalman Filter provided a significant advantage by simultaneously reducing noise and maintaining channel dynamics. As a consequence, the probability of bit mismatch during the subsequent quantization stage was reduced, leading to more reliable secret key generation and higher authentication success rates.

3.3 Modified Quantization Log Evaluation

After Kalman Filter-based preprocessing, the next stage involved converting continuous RSS values into binary bit sequences through quantization. Quantization is a critical step in physical-layer key generation because it determines both the secret key generation rate and the probability of bit disagreement between legitimate nodes. In general, conventional quantization methods compare signal samples with one or more predefined thresholds (q1, q2, ...) derived from the signal range. Samples above a threshold are assigned one binary value, while samples below the threshold are assigned another.

However, direct application of conventional threshold-based quantization is less suitable for Received Signal Strength (RSS) measurements. RSS values are typically represented in negative dBm units and exhibit narrow fluctuations around the mean value. When fixed thresholds or absolute-value transformations are used, the resulting bit streams often contain unbalanced distributions of zeros and ones, which reduces randomness and increases key disagreement. To overcome this limitation, this study proposed a Modified Quantization Log method. First, each RSS sample was transformed using the logarithmic representation 10log10 (RSS). Then, the arithmetic mean of all

transformed samples was calculated and used as an adaptive decision threshold. If a transformed sample was greater than the mean value, it was mapped to the binary bit “1”; otherwise, it was mapped to the binary bit “0”.

This adaptive threshold mechanism provided two advantages compared with conventional fixed-threshold quantization. First, the threshold automatically followed the statistical distribution of RSS measurements in each scenario. Second, the generated bits become more balanced, which improves entropy and randomness properties. The use of mean-based quantization was particularly beneficial in dynamic wireless environments where RSS distributions varied due to changes in vehicle speed and channel fading. Instead of relying on static thresholds, the proposed method adapted to current channel conditions, thereby improving robustness. Although the Modified Quantization Log method significantly improved bit balance, some mismatched bits still occurred between Alice and Bob due to residual channel differences. Therefore, an additional reconciliation stage using BCH error correction was required, as discussed in the next subsection. Overall, the proposed quantization method provided a more suitable solution for RSS-based key generation than conventional threshold quantization, particularly for negative-valued RSS data collected in mobile wireless scenarios.

The Modified Quantization Log process converted filtered RSS measurements into binary bit sequences for key generation. Although the adaptive mean-based threshold improved bit balance and robustness, mismatched bits still occurred due to residual channel differences between Alice and Bob. Such mismatches are undesirable because they reduce the probability of generating identical secret keys. Therefore, the Key Disagreement Rate after quantization was measured and denoted as KDRM. In addition, the Key Generation Rate (KGR) was evaluated to determine the efficiency of secret key extraction. Table 3 summarizes the performance of the proposed quantization method across all experimental scenarios.

Table 3. Performance of Modified Quantization Log

Scenario	KGR (bps) **Alice - Bob**	KDRM (%) **Alice – Bob**
A	71,4	25,2
B	71,4	21,8
C	71,4	25,3
D	71,4	24,9
E	71,4	24,9
F	71,4	25,6
G	71,4	24,8
H	71,4	25,7
I	71,4	25,5

Table 3 shows that the average KGR remained constant at 71.4 bps, indicating stable key extraction throughput across different mobility scenarios. Meanwhile, the average KDRM was 24.8%, meaning that approximately one quarter of the generated bits were mismatched before reconciliation. Among all scenarios, the lowest mismatch rate was obtained in Scenario B (20 km/h, 10 ms) with 21.8%, while the highest mismatch rate occurred in Scenario H (60 km/h, 10 ms) with 25.7%. This trend indicated that lower mobility conditions generally produced better reciprocity and fewer quantization errors, whereas higher vehicle speeds increased channel variation and the probability of bit mismatch.

Compared with direct raw RSS quantization, the proposed Kalman-assisted preprocessing stage reduced sensitivity to fluctuations and enabled a consistent key generation rate. However, the remaining mismatch level demonstrated that quantization alone was insufficient to guarantee identical keys between legitimate users. Therefore, an additional reconciliation mechanism was required. In this study, BCH error correction was employed in the subsequent stage to eliminate residual mismatches and improve final key agreement performance.

Although the initial KDRM remained relatively high, this behavior was common in highly dynamic vehicular wireless environments due to rapid channel fluctuations and imperfect reciprocity. The subsequent BCH reconciliation stage successfully eliminated all remaining mismatches.

3.4 BCH Error Correction Evaluation

After quantization, BCH coding was applied as the key reconciliation stage to correct mismatched bits between Alice and Bob. The objective of this process was to transform partially matched bit streams into identical keys suitable for cryptographic use. The BCH(31,6) code was selected in this study, where each 6-bit input block was encoded into a 31-bit codeword with a maximum error-correction capability of t=7 bits per block. This parameter setting was chosen

because it provided a strong error-correction capability while remaining computationally feasible on Raspberry Pi hardware.

Table 4. BCH Reconciliation Results

Scenario	Number of Blocks	Total Error	Corrected Blocks	Deleted Blocks	KDRL (%)	BCH Bit Result
A	500	6248	9	491	0	54
B	500	5914	36	464	0	216
C	500	6341	5	495	0	30
D	500	6188	10	490	0	60
E	500	6247	10	490	0	60
F	500	6341	5	495	0	30
G	500	6250	8	492	0	48
H	500	6397	3	497	0	18
I	500	6232	11	489	0	66

Table 4 shows that all scenarios achieved a final KDRL of 0%, indicating that BCH reconciliation successfully removed all remaining mismatches in the usable blocks. This confirms the effectiveness of BCH coding for secret key agreement after quantization. The highest number of usable output bits was obtained in Scenario B, with 216 bits, while the lowest occurred in Scenario H, with 18 bits. This result was consistent with the quantization stage, where Scenario B also showed the lowest mismatch rate. Hence, better channel reciprocity directly increased the number of recoverable secret bits. Although some blocks were discarded when the number of errors exceeded the correction threshold, this trade-off was acceptable because reliability is more critical than raw key length in authentication systems. Compared with quantization alone, BCH reconciliation significantly improved final key consistency. Although several blocks were discarded during reconciliation, prioritizing key reliability over raw throughput was considered more suitable for authentication-oriented applications.

3.5 Universal Hash and Randomness Evaluation

Although BCH correction removed bit mismatches, the corrected bit streams did not always satisfy cryptographic randomness requirements. Therefore, a universal hash function was applied to enhance entropy and remove statistical bias from the reconciled bits. A 128-bit final key length was selected based on the available usable bits after BCH processing. After hashing, the generated keys were evaluated using the National Institute of Standards and Technology (NIST) Statistical Test Suite. The evaluated parameters included frequency, block frequency, approximate entropy, runs, cumulative sum forward, and cumulative sum reverse. Keys with $p \geq 0.01$ were considered acceptable.

The best randomness performance was obtained in the 40 km/h, 10 ms scenario, which achieved the highest average approximate entropy value of 0.7352, as shown in Figure 5. This scenario was therefore selected as the optimal key source for the authentication stage.

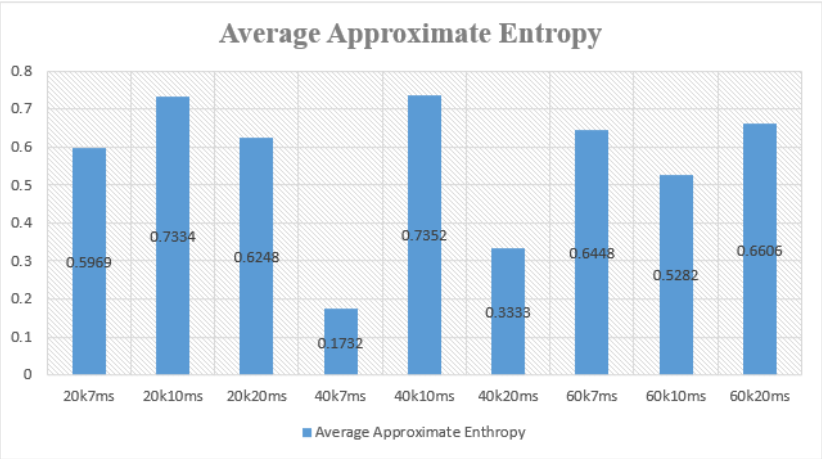

Figure 5. Average Approximate Entropy Results

Table 5. NIST Results for Scenario 40 km/h, 10 ms Scenario

Key	Approx. Entropy	Freq.	Block Freq.	Cusum Forward	Cusum Reverse	Runs	Long Runs
1	0.943	0.211	0.214	0.267	0.378	0.685	0.719
2	0.984	0.802	0.214	0.906	0.857	0.897	0.645
3	0.587	0.900	0.306	0.629	0.745	0.901	0.933
4	0.202	0.31	0.286	0.469	0.208	0.116	0.991
5	0.960	0.900	0.267	0.422	0.338	0.708	0.889

The results in Table 5 demonstrate that the proposed framework improved not only key consistency but also randomness quality. Importantly, Kalman Filter-based preprocessing did not degrade entropy; instead, it enabled a balanced trade-off between signal stability and cryptographic unpredictability.

3.6 Authentication Time Testing and Single-Attacker Brute-Force Testing

The final stage evaluated authentication efficiency and attack resistance of the proposed Zero-Knowledge Feige–Fiat–Shamir framework. Tests were performed in a dynamic environment where both the claimant and verifier moved at 40 km/h, using the optimal key scenario identified previously. Authentication time was measured at distances of 5 m, 10 m, 15 m, 20 m, and 25 m. The results showed that authentication time remained relatively stable across all distances, indicating that the proposed method operated effectively under mobility conditions without significant increase in latency.

Security testing was also conducted using a single-attacker brute-force scenario. In each configuration, the attacker attempted authentication three times. No successful impersonation attempts were recorded, corresponding to a 100% attack failure rate during experiments. These findings demonstrate that integrating dynamic RSS-derived keys with the Feige–Fiat–Shamir protocol significantly strengthened authentication robustness while maintaining practical execution time in wireless environments. Overall, the results confirmed that the proposed framework provided a practical and lightweight authentication solution capable of improving both key consistency and authentication reliability in dynamic vehicular communication environments.

4. Conclusion

This study proposed an integrated authentication framework that combined Kalman Filter-based preprocessing, Modified Quantization Log, BCH reconciliation, and the Feige–Fiat–Shamir zero-knowledge authentication protocol for wireless communication environments. The main objective was to improve the reliability of Received Signal Strength (RSS)-based cryptographic key generation while preserving authentication security.

Experimental results demonstrated that Kalman Filter-based preprocessing significantly increased RSS reciprocity between legitimate nodes. The average correlation between Alice and Bob improved substantially after filtering, indicating that noisy wireless measurements could be transformed into more consistent channel observations suitable for secret key extraction. This result confirms the effectiveness of Kalman Filter-based preprocessing compared with the direct use of raw RSS measurements.

The Modified Quantization Log method successfully converted filtered RSS values into binary sequences with a stable key generation rate of 71.4 bps. Although residual mismatches still occurred after quantization, BCH(31,6) reconciliation eliminated the mismatches and achieved a final key disagreement rate of 0% across all evaluated scenarios. Furthermore, universal hashing and NIST statistical tests showed that the generated keys satisfied the important randomness properties, with the best entropy performance obtained in the 40 km/h and 10 ms scenario.

Authentication testing under dynamic mobility conditions showed stable execution times across different communication distances. In addition, the brute-force attack experiments resulted in a 100% attack failure rate, indicating strong resistance against impersonation attempts. Overall, the proposed framework provides a lightweight and effective solution for strengthening key generation and zero-knowledge authentication in wireless and vehicular communication systems. Future work may investigate larger-scale real-time deployments, additional attack models, and comparisons with other filtering or key-generation techniques.

Acknowledgement

The authors would like to express their sincere gratitude to the Directorate of Research and Community Service, Ministry of Higher Education, Science, and Technology, Republic of Indonesia, for supporting this research through the Early Career Lecturer Research Scheme. The authors also gratefully acknowledge Universitas Muhammadiyah Lamongan for its institutional support and facilities which contributed to the successful completion of this research.

References

[1] R. Coppola and M. Morisio, "Connected car: Technologies, issues, future trends," *ACM Comput. Surv.*, vol. 49, no. 3, pp. 1–36, 2017. https://doi.org/10.1145/2971482

[2] 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. https://doi.org/10.1016/j.comnet.2011.03.016

[3] 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. https://dx.doi.org/10.2139/ssrn.3363555

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

[5] 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. https://doi.org/10.3390/info14010027

[6] 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. https://doi.org/10.1007/978-3-319-40253-6_24

[7] 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. https://doi.org/10.25139/inform.v3i2.1031

[8] 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. https://doi.org/10.11591/ijeecs.v22.i3.pp1723-1730

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

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

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

[12] M. Bellare and A. Palacio, "GQ and Schnorr Identification Schemes: Proofs of Security against Impersonation under Active and Concurrent Attacks," Springer-Verlag, 2002. https://doi.org/10.1007/3-540-45708-9_11

[13] 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.

[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. https://doi.org/10.1155/2017/7393526

[15] 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. https://doi.org/10.1109/ACCESS.2024.3523105

[16] 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. https://doi.org/10.3390/e21020192

[17] A. Shojaifar, "Evaluation and Improvement of the RSSI- based Localization Algorithm," *Blekinge Inst. Technol.*, pp. 1–109, 2015.

[18] 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. https://doi.org/10.25139/inform.v6i2.4037

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

[20] Amang Sudarsono, Mike Yuliana, and Prima Kristalina, *A Reciprocity Approach for Shared Secret KeyGeneration Extracted from Received Signal Strengthin The Wireless Networks*. IEEE, 2018. https://doi.org/10.1109/ELECSYM.2018.8615568

[21] 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. https://doi.org/10.1109/OJCOMS.2024.3524497

[22] N. N. Srinidhi, J. Shreyas, and E. Naresh, "Establishing Self-Healing and Seamless Connectivity among IoT Networks Using Kalman Filter," *J. Robot. Control*, vol. 3, no. 5, pp. 646–655, 2022. https://doi.org/10.18196/jrc.v3i5.11622

[23] K. M. Maslahati, I. B. Purnawan, and M. I. Aprianto, "Implementasi Kalman Filter dan Logika Fuzzy untuk Kontrol Adaptif Kecepatan Kipas Berdasarkan Suhu Implementation of Kalman Filter and Fuzzy Logic for Adaptive Control of Fan Speed Based on Temperature," vol. 7, no. 2, pp. 259–274, 2025. https://doi.org/10.30595/jrre.v7i2.27212

[24] R. P. Astutik, "Filter Kalman Untuk Estimasi Daya Pada Komunikasi Bergerak," *E-Link J. Tek. Elektro dan Inform.*, vol. 1, no. 1, p. 25, 2018. https://doi.org/10.30587/e-link.v1i1.613

[25] V. Firmansyah, "Aplikasi Kalman Filter Pada Pembacaan Sensor Suhu Untuk," *J. Mater. dan Energi Indones.*, vol. 08, no. September, pp. 0–7, 2018. https://doi.org/10.24198/jmei.v8i01.16624

[26] M. Musayyanah, Hendra Daniswara, P. Susanto, and H. Harianto, "The Influence of Kalman Filtering on the Received Signal Strength Indicator in Multi-node Bluetooth Low Energy Communications," *Emit. J. Tek. Elektro*, pp. 108–114, 2024. https://doi.org/10.23917/emitor.v24i2.2355

[27] S. M. Rostamkolaei Motlagh, C. Pahl, H. R. Barzegar, and N. El Ioini, "A Comparative Evaluation of Zero Knowledge Proof Techniques," *Int. Conf. Internet Things, Big Data Secur. IoTBDS - Proc.*, no. March, pp. 237–244, 2025. https://doi.org/10.5220/0013269100003944

[28] M. C. Kriswantoro, E. Handoyo, and M. Sa Yu Zakka, "Secure Authentication in Vehicular Networks: Integrating Zero-Knowledge Protocols with RSS Key Generation," *Inf. J. Ilm. Bid. Teknol. Inf. dan Komun.*, vol. 10, no. 2, pp. 146–151, 2025. https://doi.org/10.25139/inform.v10i2.9488