Adaptive Reciprocal Differential Encoding Quantization for the Physical Layer Key Generation

Abdullah Alshamdayn
Louisiana Tech University
Ruston, Louisiana 71270
aal132@latech.edu

Manki Min
Louisiana Tech University
Ruston, Louisiana 71270
mankimin@latech.edu

***Abstract*—Physical layer secret key generation (PLSKG) is a lightweight, information-theoretically secure alternative to classical cryptography, exploiting the randomness of the wireless channel to generate symmetric keys.The quantization phase is crucial for the efficient key generation process, as it determines both the key generation rate and the key disagreement rate. This work proposes a lossless, lightweight adaptive quantization method for PLSKG designed for resource-constrained devices. The quantizer is based on the reciprocal differential encoding method with a guard band, which adaptively extracts secret bits from channel variations to improve key agreement while reducing bit mismatches. A comprehensive simulation evaluation demonstrates that the generated keys achieve a low key disagreement rate and strong randomness, passing the NIST statistical test suite.**

***Index Terms*—Physical-Layer Secret Key Generation (PLSKG), Resource-constrained devices, Quantization, Adaptive lossless, Embedded systems**

I. Introduction

The expansion of resource-constrained devices is driven by diverse applications across multiple sectors, such as smart home devices, wearable health monitors, industrial automation, military defense, and smart city infrastructure. It is projected that by 2030, the connected devices will exceed 40 billion units. There are two main approaches to establish secret keys for secure communication: classical cryptography and physical-layer security. Classical methods, such as public key cryptography or preshared keys, are often impractical for these devices. Resource-constrained devices lack the computational power for the public key algorithms and the large-scale or ad-hoc deployments, making manual key distribution and management infeasible. On the other hand, Physical-layer security is an alternative lightweight method that is suitable for such devices.

Physical layer security can be categorized into channel-based secret key generation and secrecy coding. Channel-based secret key generation utilizes the inherent randomness of the wireless channel to generate symmetric keys. Furthermore, physical-layer secret-key generation relies on three channel properties: channel reciprocity, which allows both endpoints to obtain highly correlated measurements; spatial decorrelation, meaning an eavesdropper a few wavelengths away observes a different channel and cannot reproduce the same key bits; and temporal variation, where motion and environmental changes provide entropy.

Moreover, the quantization step transforms continuous channel measurements into a shared binary sequence for key generation. This paper introduces a physical-layer secret key generation scheme using a lossless quantization algorithm. Our contributions include an adaptive, lightweight quantization method based on reciprocal differential encoding with a dynamic guard band, and run in linear-time complexity of $O(N)$.

II. Background and Related Work

Channel-based secret key generation systems rely on natural randomness found in the physical world, such as the motion of individuals and objects causing signals to scatter or reflect, or

on the distinct hardware imperfections caused by the manufacturing process. The key generation system comprises several stages, including channel probing, signal preprocessing, quantization, information reconciliation, and privacy amplification, which collectively establish an efficient and secure process. The key generation goal is to produce symmetric matching keys for cryptographic applications. The quantization step [1] is critical, as it directly determines the Key Generation Rate (KGR) and the Key Disagreement Rate (KDR).

A. Lossy Quantization Schemes

Chen et al. [2] proposed an adaptive lossy quantization (AQ–KG) scheme for PLKG employing multi-level quantization combined with a guard-band mechanism to control the KDR. Their method partitions the channel measurements into blocks and uses the Lempel–Ziv 1976 (LZ76) complexity metric as a predictor of channel variability. They also utilized an offline-trained linear regression models to map the complexity values to two key parameters: the number of quantization levels and the guard-band size parameter. The scheme discards samples that fall within the guard band area.

In MobiKey [3], the authors use phase measurements from commercial smart home devices to generate keys. They propose an adaptive, lossy, multi-level quantization method with CDF-based thresholds and a custom double-Gray coding scheme. The signal is preprocessed with a Savitzky–Golay filter and a sliding mean filter to reduce high-frequency noise and smooth the waveform. To resist deducing attacks, the authors discard some successive observations so an eavesdropper cannot infer quantization levels. When phase variation is limited or observations are few, achieving strong randomness is difficult, so they delete some bits at random to meet the randomness requirement.

B. Lossless Quantization Schemes

Guo et al. [4] proposed a Moving Average Filtering-Bidirectional Difference Quantization (MAF-BDQ) scheme to improve the reliability and efficiency of physical layer key generation. Their quantization method has two stages: moving average filtering to smooth the channel measurements, and bidirectional difference quantization to convert the filtered measurements without using fixed thresholds. In their process, each measurement is compared to its neighbors, producing two bits per sample. The first bit shows whether the current measurement is greater than or equal to the previous one, while the second compares it to the next measurement.

Zhao et al. [5] proposed a lossless adaptive quantization technique where they segment the RSS time series into blocks based on the location of peaks within the data to then run the quantizer within each block. In every round, the block's statistics are recomputed (mean, maximum, minimum), and two thresholds are defined by taking the mean and shifting it up and down by a fraction α of the block's amplitude (i.e., the distance between its maximum and minimum). Channel samples that fall above the upper threshold are assigned to 1, the ones below the lower threshold are assigned to 0, and any samples in between are carried forward to the next round until all measurements are assigned.

Ambekar et al. [6] propose a lossless multi-bit adaptive quantization that operates on blocks of RSS measurements. In their scheme, each node enhances reciprocity by curve-fitting its RSS time series with a low–order polynomial to obtain an enhanced channel profile. The profile is then divided into fixed–size blocks, and within each block, the quantizer forms four intervals by placing two thresholds around the block mean and variance. Then, each interval is assigned to a two–bit to map every sample. Alice transmits the positions of samples that fall into the {levels 1,3} and {levels 2,4}, and Bob acknowledges the commonly agreed positions before reconciliation.

Patwari et al. [7] proposed a multi-bit adaptive quantization (MAQ) algorithm. In their scheme, each decorrelated component $y_a(i)$ at the leader (Node A) is mapped into equally likely bins, with the number of bins set to four times the number of m-bit codewords ($K = 4 \cdot 2^m$). The bin edges are determined by the component's cumulative distribution function (CDF), so each bin has the same probability. Each bin is labeled with an m-bit Gray code so that adjacent bins differ by one bit. The leader also sends a one-bit value per component, selecting the Gray code table used by both nodes to keep the labeling consistent across the nodes.

III. Proposed Work

This work proposes a physical-layer secret key generation scheme employing an adaptive quantizer algorithm. The system consists of five steps: (1) Channel Probing, where Received Signal Strength (RSS) is measured; (2) Signal Preprocessing using Exponential Smoothing Filters to reduce noise; (3) Quantization using the proposed Reciprocal Differential Encoding Quantizer; (4) Information Reconciliation with a Reed-Solomon error correction code to correct bit mismatches; and (5) Privacy Amplification applying a Secure Hash Function to distill the final secret key, as shown in Figure 1 below.

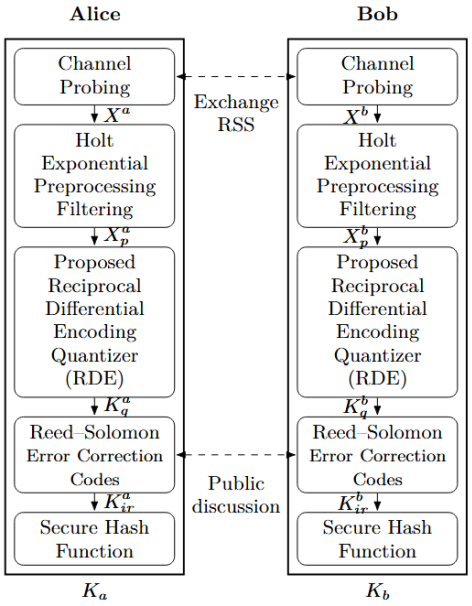

Fig. 1. Proposed Scheme

This scheme enables secret key generation between two resource-constrained transceivers, Alice and Bob, who communicate over a bidirectional wireless channel. The system operates under the assumption that a passive eavesdropper, Eve, is located at a distance of at least half a wavelength from either legitimate node. The detailed steps of the proposed system are as follows:

1. **Channel Probing** Both nodes utilize channel probing to gather the RSS channel measurements. An advantage of using RSS as the foundation for key generation in wireless sensor networks is that it can be deployed and is accessible to higher layers on off-the-shelf wireless sensor network devices without requiring any hardware modification. As a result, realistic techniques in Wireless Sensor Networks must rely on employing rough indicators of channel unpredictability.
2. **Signal Preprocessing** The observed raw RSS contains slow variations (path loss, shadowing, device offsets) and fast fluctuations, as well as independent receiver noise that can create small differences between the transceivers. We apply Holt's [8] double-exponential smoothing to separate each sample x_i into a slow part and a fast part. To the best of our knowledge, Holt's method has not previously been used for preprocessing in the PLSKG literature.
3. **Quantization** This step transforms the analog network readings into digital binary values, enabling the transmission of data between the endpoints. Channel reciprocity is one of the physical layer secret key generation principles, which implies that the two endpoints of the connection experience almost the same multi-path fading in the channel. Based on this principle, this work proposes a lossless quantization algorithm that exploits the reciprocal nature of the channel measurements by applying an adaptive thresholding mechanism and a dynamic guard band to reduce bit disagreements while having a high bit generation rate.
   The proposed quantization algorithm's objective is to convert the reciprocal local variations in the channel measurements into shared binary sequences. The primary challenge is to ensure that the algorithm is robust against small noise fluctuations while maintaining a lightweight design and achieving high bit generation with low key disagreement rates.
   Unlike some existing quantization algorithms that rely on the signal level (value), the proposed approach is based on the increment (difference), which is defined by the change in the signal value between consecutive samples. The proposed method consists of: reciprocal differential encoding, local scaling of differences, thresholds, and a dynamic guard band. Within this algorithm, for the preprocessed RSS channel measurements: $x = \{x_1, x_2, \ldots, x_n\} \in \mathbb{R}$. The process is as follows:
   - Compute the increment: in this step,

instead of using the raw signal levels, the algorithm utilizes the adjacent increments in samples. For each pair of neighboring samples, the algorithm computes the successive difference as $d_i = x_i - x_{i-1}$, for $i = 2, \ldots, n$.

To compute the signal direction d_i, the algorithm only needs the current sample x_i and the previous x_{i-1}. If d_i is positive, the signal went up, if negative, down, and if $d_i = 0$, then it stayed the same.

Typically, the increments of $d_i^{(A)}$and $d_i^{(B)}$ are highly correlated. If the signal exhibits slow drift, then the increment tends to be small. The algorithm adjusts the thresholds based on the local slope, not the global level.

- Take the absolute difference mean: instead of using the variance or the standard deviation, the proposed quantizer relies on a simpler yet more robust method using the mean absolute successive difference. It is defined as $\overline{\Delta} = \frac{1}{N-1}\sum_{i=2}^{N}|d_i| = \text{mean}(\,|x_i - x_{i-1}|\,)$.

  The $\overline{\Delta}$ measures the size of local changes naturally.
- Thresholds and Dynamic Guard Band: the algorithm defines two symmetric thresholds around zero and a guard band area. A guard band is the buffer zone around the quantization thresholds, preventing errors caused by small signal fluctuations.

  The algorithm uses two parameters, ($\beta > 0$) and ($\alpha > 0$), to control the quantizer. β sets how far the thresholds are from the mean, and α sets how wide the middle zone (guard band) is. A larger α widens this zone, making decisions less sensitive to noise; a smaller α narrows it, causing the system to react more to small changes. Larger β moves the thresholds farther from the mean so that only large changes cross them, while smaller β brings them closer so that smaller changes are more likely to cross them.

  These parameters are used to define the quantization regions as $T_{\text{up}} = +\beta\,\overline{\Delta}$, $T_{\text{low}} = -\beta\,\overline{\Delta}$, and $G = \alpha\,\overline{\Delta}$. The algorithm constructs three areas: 1) Upper Area as $[T_{\text{up}} + G, \infty)$, 2) Lower Area as $[T_{\text{low}} - G, -\infty)$, and 3) Guard Band Area as $[T_{\text{low}} - G, T_{\text{up}} + G]$. The areas are used to produce a bit as: $b_i = 1$ if (d_i is in the Upper Area) or (in the Guard Band Area and $d_i > 0$), $b_i = 0$ otherwise.
4. **Information Reconciliation**
   Half-duplex communication mode causes post-quantization results to differ due to noise issues. We applied Reed–Solomon [9] error correction codes, RS(15, 11).
5. **Privacy Amplification**
   The scheme utilized the secure hash function, SHA-256.

Algorithm 1: Reciprocal Differential Encoding

Input: Block $[x_1, \ldots, x_n]$; $\alpha > 0$, $\beta > 0$
Output: Initial key $[b_1, \ldots, b_{n-1}]$

Function *RDEQ*($x[1..n]$, α, β)
  $\overline{\Delta} \leftarrow \frac{1}{n-1}\sum_{i=2}^{n}|x_i - x_{i-1}|$;
  $T_{\text{up}} \leftarrow +\beta\,\overline{\Delta}$;
  $T_{\text{low}} \leftarrow -\beta\,\overline{\Delta}$;
  $G \leftarrow \alpha\,\overline{\Delta}$;
  for $i \leftarrow 1$ **to** $n-1$ **do**
    $d \leftarrow x_i - x_{i-1}$;
    if $d > T_{\text{up}} + G$ **then**
      $b_i \leftarrow 1$
    else if $d < T_{\text{low}} - G$ **then**
      $b_i \leftarrow 0$
    else
      if $d > 0$ **then**
        $b_i \leftarrow 1$
      else
        $b_i \leftarrow 0$
  return $\{b_1, \ldots, b_{n-1}\}$;

IV. Results and Discussion

To ensure the effectiveness of secure mechanisms in information security, cryptographic algorithms must undergo randomness testing. The performance metrics considered are KDR and NIST randomness. To verify that the final keys are indistinguishable from random, we applied the NIST Statistical Test Suite (STS) to the keys generated by our scheme. In the NIST STS, we focused on the subset that examines different aspects of randomness. For each test, a high p-value (above a significance level, typically 0.01) means the sequence passes the test (appears random in that aspect).

All tests produce a p above 0.1 (between 0.163 and 0.784), thus none of the null hypotheses (that the sequence is random) were rejected.

This confirms that the keys exhibit uniform distribution of 0/1 and no detectable patterns. In addition, the proposed quantizer RDE is a single-pass method with $O(N)$ complexity and $O(1)$ memory that generates $N-1$ bits from the N channel samples. In the simulation with typical indoor wireless fading scenarios with low mobility, the observed raw bit mismatch rates were below 2%, for different preprocessing filtering techniques.

AQ–KG [2] adaptive value-domain quantizer has parameters chosen per segment using an estimate of randomness and is a pre-trained offline linear regression model. Their design introduces extra per-segment processing, the LZ-complexity evaluation and model inference, and a calibration loop during reconciliation. Our proposed quantizer is a single-pass, difference-domain rule with constant-time updates per sample with no pre-trained model.

MobiKey [3] value-domain quantizer constructs keys by the distribution of channel samples using a virtual threshold line and the CDF for equal probability. That can give balanced bits based the distribution of the samples in each segment, requiring $O(NlogN)$ computational complexity. Our RDE avoids distribution fitting entirely; it thresholds increments with a guard band, so it stays $O(N)$.

The MAF–BDQ [4] design combines a moving-average filter with a bidirectional differential quantizer, achieving low implementation complexity $O(N)$ and feasibility on constrained devices. However, it depends heavily on the MAF, which gives equal weight to all samples and therefore suppresses noise poorly. Our scheme remains lightweight, incorporating a dynamic guard band into the differential rule. As the channel conditions change, adaptive thresholds produce uniformly distributed bits, reducing mismatches and minimizing reconciliation overhead.

V. CONCLUSION

In this work, we introduced an adaptive lossless reciprocal differential encoding, a difference-domain quantizer with a dynamic guard band and sign fallback. The quantizer method is $O(N)$ linear-time with a constant-memory of $O(1)$, relying only on local increments, generating $N-1$ bits from the N samples. During our low-mobility indoor simulation experiments, the scheme passed the NIST randomness test, achieving p-values above 0.01 across all applicable tests. The scheme achieved KDR below $\leq 2\%$ applying different signal preprocessing methods. We utilized Holt's double-exponential smoothing for the preprocessing. The advantage of Holt over a simple moving average is that it explicitly tracks both the changing level and the slope of the signal, which improves the stability in the slow mean drift over time. These results confirm that our scheme keys are statistically random and suitable for cryptographic use. This further indicates that our method is an efficient and secure solution for key generation in scenarios like smart home device pairing, wearable device communications, or industrial sensor networks.

References

[1] A. D. Alshamdayn and M. Min, "A Survey of Quantization Techniques for Physical Layer-Based Secret Key Generation in IoT Systems," 2024 IEEE International Conference on Computing (ICOCO), Kuala Lumpur, Malaysia, 2024, pp. 36-41, doi: 10.1109/ICOCO62848.2024.10928207.

[2] C. Chen, J. Zhang, and Y. Chen, "Adaptive quantization for key generation in low-power wide-area networks," 2023, arXiv:2310.07853.

[3] L. Wang, H. An, H. Zhu and W. Liu, "MobiKey: Mobility-Based Secret Key Generation in Smart Home," in IEEE Internet of Things Journal, vol. 7, no. 8, pp. 7590-7600, Aug. 2020, doi: 10.1109/JIOT.2020.2986399.

[4] D. Guo, K. Cao, J. Xiong, D. Ma and H. Zhao, "A Lightweight Key Generation Scheme for the Internet of Things," in IEEE Internet of Things Journal, vol. 8, no. 15, pp. 12137-12149, 1 Aug.1, 2021, doi: 10.1109/JIOT.2021.3060438.

[5] H. Zhao, Y. Zhang, X. Huang, Y. Xiang and C. Su, "A Physical-Layer Key Generation Approach Based on Received Signal Strength in Smart Homes," in IEEE Internet of Things Journal, vol. 9, no. 7, pp. 4917-4927, 1 April1, 2022, doi: 10.1109/JIOT.2021.3119053.

[6] A. Ambekar, M. Hassan and H. D. Schotten, "Improving channel reciprocity for effective key management systems," 2012 International Symposium on Signals, Systems, and Electronics (ISSSE), Potsdam, Germany, 2012, pp. 1-4, doi: 10.1109/ISSSE.2012.6374318.

[7] N. Patwari, J. Croft, S. Jana and S. K. Kasera, "High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements," in IEEE Transactions on Mobile Computing, vol. 9, no. 1, pp. 17-30, Jan. 2010, doi: 10.1109/TMC.2009.88.

[8] P. Goodwin, "The holt-winters approach to exponential smoothing: 50 years old and going strong," Foresight, pp. 30–33, 2010.

[9] J.S. Reed and G. Solomon, "Polynomial codes over certain finite fields," J. Soc. Indust. Appl.Math., vol. 8, pp. 300-304, 1960.