Performance Improvement Based on Modified Lossless Quantization (MLQ) for Secret Key Generation Extracted from Received Signal Strength

Muhammad Taufiq Sumadi
Dept. of Information and Computer Engineering
Electronic Engineering Polytechnic Institute of Surabaya
Surabaya, Indonesia
sumadi11895@gmail.com

Mike Yuliana
Dept. of Information and Computer Engineering
Electronic Engineering Polytechnic Institute of Surabaya
Surabaya, Indonesia
mieke@pens.ac.id

Amang Sudarsono
Dept. of Information and Computer Engineering
Electronic Engineering Polytechnic Institute of Surabaya
Surabaya, Indonesia
amang@pens.ac.id

***Abstract*— In symmetric cryptography systems have problems in the distribution of secret keys. The two users who will communicate require sharing keys through the public channel. The proposed solution to overcome these problems is to utilize information from the physical layer (e.g. RSS). Received Signal Strength (RSS) is an indicator for measuring the power received by wireless devices. The advantage of secret key extraction using physical layer information from a wireless channel is that it allows both devices within the transmission range to extract the secret key together. In this paper, we propose a secret key generation scheme adopted from an existing scheme with modifications to improve performance. Our proposed system is applied to static and dynamic conditions to test performance. The proposed algorithm is able to obtain a reduction in KDR (Key Disagreement Rate) up to 48.42% and an increase in the KGR (Key Generation Rate) up to 23.35% when compared to the existing scheme. Our proposed system also successfully passed the randomness using the NIST test with the approximate value of entropy generated 0.80 in static conditions and 0.81 in dynamic conditions.**

Keywords—symmetric cryptography, RSS, secret key generation, key disagreement rate, key generation rate.

I. INTRODUCTION

Symmetric cryptography systems have problems in distributing secret keys. Of the two users who will communicate requires sharing the secret key through the public channel. At present the method used to generate the secret key is the asymmetric cryptography system. Asymmetric cryptography systems require large resources to compute and may not be available in certain scenarios (e.g. adhoc network). From this problem was born research one of them about quantum cryptography to overcome them [1]. However, the application of quantum cryptography in recent years is still very rare and very expensive.

An inexpensive and effective solution to overcome these problems is to utilize information from the physical layer (e.g. RSS) on a wireless channel that can be obtained from two devices that will communicate. Two communicating users utilize the randomness and uncertainty of the wireless channel to generate secret keys [2], [3], [4]. The advantage of secret key extraction using physical layer information from a wireless channel is that it allows two wireless devices within transmission range to extract symmetric keys together without the need for a fixed key distribution infrastructure. Third parties, which are more than half the wavelength of legitimate users, can be tapped but it is very difficult to get the same key in diverse environments [5], [6].

Various kinds of implementations and experiments have been carried out by utilizing received signal strength (RSS) as a source of data to extract secret keys [7]. We use RSS as a data source because it is easily available using the available network card adapters. To get RSS that will be used for secret key generation both devices send probing frames. There are several factors that make it possible for two devices to not have a truly identical channel, such as the non-simultaneous measurement with half-duplex mode, device limitations, and the different types of devices used. This can be overcome by reconciliation information, to correct the difference in bits between the two devices [2].

To improve the performance of systems that include entropy, key generation rate (KGR), key disagreement rate (KDR), and randomness [4] [5] several studies discuss simulations of key extraction or theoretical analysts, discussions of key extraction mechanisms by measuring RSS in the environment indoor [8] with static and dynamic scenarios added to compare various quantization methods [9]. Some studies focus on efforts to reduce KDR but KGR also decreases [3]. There is also an increase in KGR but KDR also increases [4].

In this paper, we propose a secret key generation SKG scheme using RSS on wireless communication to extract secret keys. The method used in the quantization phase is the adoption and modification of the method [9]. By eliminating the process of division per block and utilizing the mode value to determine the threshold value, it can reduce the KDR and increase the KGR value compared to the existing method [9]. The SKG scheme that we propose has four phases, channel probing, quantization, information reconciliation, privacy amplification. Through the RSS probing channel is obtained by sending the ping command via ICMP protocol. After getting RSS (in dBm) the device performs a quantization process to convert into bits. The two devices allow differences in bits affected by various factors and then corrected in the reconciliation information phase. In the privacy amplification phase bits increase in randomness.

978-1-7281-9530-8/20/$31.00 ©2020 IEEE

II. PROPOSED SYSTEM

In this section, we will describe the proposed system. There are two entities that will communicate (i.e., Alice and Bob). First, Alice will communicate with Bob and try to get the secret key through extracted key generation from RSS. In addition, there is Eve able to eavesdrop on an Alice and Bob's channel. In Fig. 1. show the proposed system scenario.

Our propose to adopt and modifies the scheme [9]. There are four phases in secret key generation in Fig. 2. channel probing, quantization, information reconciliation, and privacy amplification. To increase the key generation rate and decrease the key disagreement rate, we proposed a modified lossless quantization (MLQ) algorithm which is the development of self-adaptive lossless quantization [9].

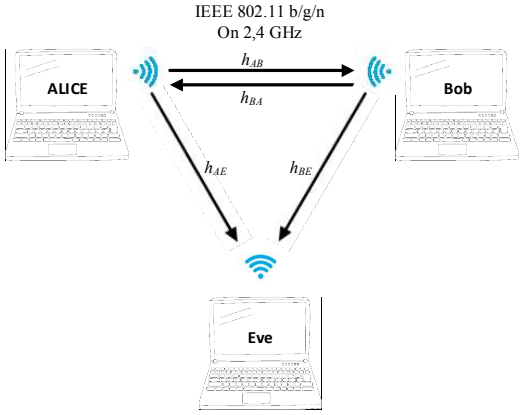

Fig. 1. Proposed System Scenario

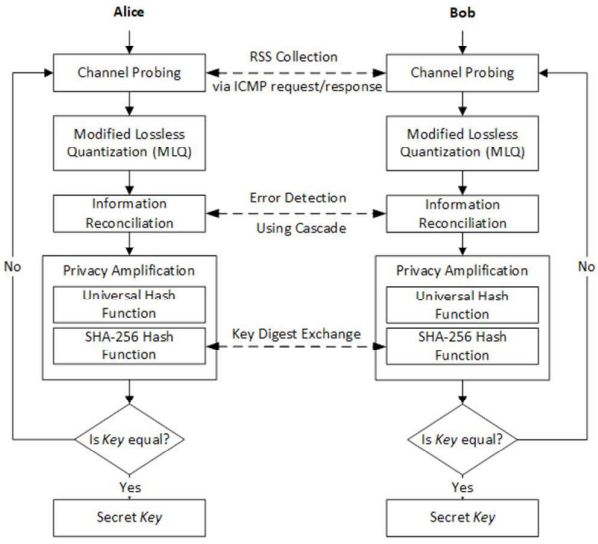

Fig. 2. Proposed System Mechanism

A. Channel Probing

We capture and probe RSS values between two legitimate users (Alice and Bob) by utilizing *ping* command which uses ICMP protocol. The time interval for probing between two legitimate users is depending on coherence time (*Tc*). Based on [10], $T_c = \frac{1}{f_D}$ where f_D maximum droppler frequency. Meanwhile, $f_D \frac{v}{\lambda}$ Where v speeds movement legitimate users (i.e. 1.1 m/s walking people speed). $\lambda = \frac{c}{f_c}$, c is the speed of light, and f_c denotes the carrier frequency of the channel. We use carrier frequency 2,4 GHz in our system, $\lambda = \frac{3\ x\ 10^8}{2.4\ x\ 10^9} = 0.125$ m. As a result coherence time T_c is 113.6 ms We set *ping* interval time of 110 ms, in our best measurement. The experiment was implemented in static and dynamic conditions in a semi-indoor environment. The details of our experiments are explained in section III.

B. Quantization

After channel probing and getting RSS (in dBm) the next process is the quantization phase. At the quantization phase of RSS value is changed to 0 or 1. This value will represent a binary number. In the proposed quantization process RSS the results of channel probing do not divide multiple blocks. RSS obtained has then calculated the value of mode, max, and min. After getting the value, then calculate the value q^+ (used for the upper limit) and q^- (used for the lower limit). If the RSS value is less than equal to q^- it will be changed to 0 and if the RSS value is more than q^+ it will be changed to 1. Then if the RSS value is not in the range of values q^+ and q^- it will be discarded. Modified lossless quantization (MLQ) showed in Algorithm 1.

Algorithm 1: Modified Lossless Quantization (MLQ)

Input: collected RSS measurements T = [t_1, t_2… t_n]
n: number of RSS;
Output: B = Q_1, Q_2, …, Q_s the generated bits stream
1. **for** j=1 to n **do**
2. $M_o \leftarrow$ mode(t), max $\leftarrow$ max(t), min $\leftarrow$ min(t);
3. $q^+ \leftarrow M_o + \alpha \times (\max + \min)$, $q^- \leftarrow M_o - \alpha \times (\max + \min)$;
4. **if** $t_j \leq q^-$ **then**
5. $t_j \leftarrow 0$;
6. **else if** $t_j > q^+$ **then**
7. $t_j \leftarrow 1$;
8. **else** $t_j \leftarrow t_j$;
9. B $\leftarrow Q_1, Q_2, \ldots, Q_s$

C. Information Reconciliation

The communication that occurs in Alice and Bob is half-duplex so that the probe channel that occurs cannot be done at the same time. This results in an inconsistent channel information between Alice and Bob. Besides the random noise that occurs in the environment also affects the channel information obtained. In the quantization phase the channel information is collected on the two devices and then produces an output in the form of a bit stream, therefore the bit stream obtained by the two devices allows for unequal bits. To detect unequal bits we use the information reconciliation protocol cascade [11] to eliminate the bit differences between the two devices. In the error correction process between the two bit stream devices are divided into many blocks and do a parity check for each group in the block to get unequal bit positions in the bit stream. In the information reconciliation phase, it is possible for Eve to get some information, thus allowing Eve to get some of the keys shared.

D. Privacy Amplification

In the information reconciliation phase, it is possible for Eve to obtain some information from the extracted key. To overcome some of the key information obtained by Eve, both

devices perform the universal hash function [12] at the privacy amplification phase. The output bit from universal hash will produce several keys which will be tested using NIST Test. The key bits will be tested with several NIST Test parameters with the condition that the p-value is above 0.01. In this paper use a key with a length of 256 bits. This allows Alice and Bob to get key more than 1. Key with the highest approximate entropy indicates that the key has the highest randomness. The key that will be used is the key with the highest approximate entropy result as the winner key. Then the winner key that is obtained will run the SHA-256 process to get a digest. The acquired digest will be exchanged between Alice and Bob. If Alice and Bob's digest is the same, the secret key can be used for both the cryptographic process.

III. Result and Performance Evaluation

In this section, we will explain the prototype implementation of our scheme. Then we will evaluate the performance of the proposed scheme with other previous schemes.

A. Experimental Setup

We experimentally implemented the proposed scheme, and the experiments were carried out in the building D4 Politeknik Elektronika Negeri Surabaya 1st floor and 2nd floor. In this experiment using the wifi module TL-WN722N wireless adapter standard IEEE802.11b/g/n with frequency 2.4 GHz. There are two scenarios used in generating secret keys in this study. Scenarios with static conditions and scenarios with dynamic conditions. Fig. 3. shows the scenario with static conditions in semi-outdoor multi-storey buildings. Alice as the initiator is on the 1st floor while Bob and Eve are on the 2nd floor. The distance between the floor and the ceiling on each floor is 3.5 meters and has a floor thickness of 0.5 meters. The distance between Eve and Bob is 1 meter. All three devices at the time of measurement are in a stationary position. Fig. 4. show the measurement scenario with dynamic conditions the initial condition of the distance between Bob and Eve is 1 meter. Then Bob moved straight away and approached Eve four meters away.

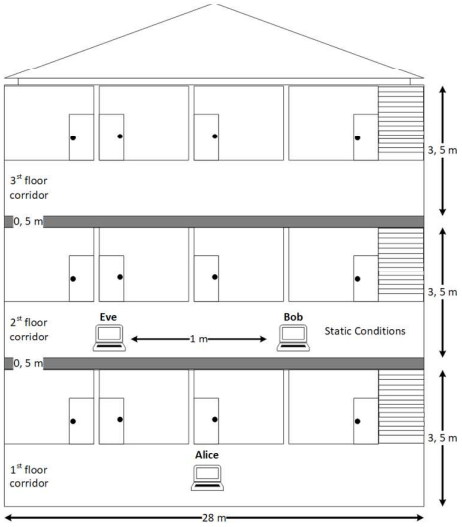

Fig. 3. Experimantal Scenario in static condition

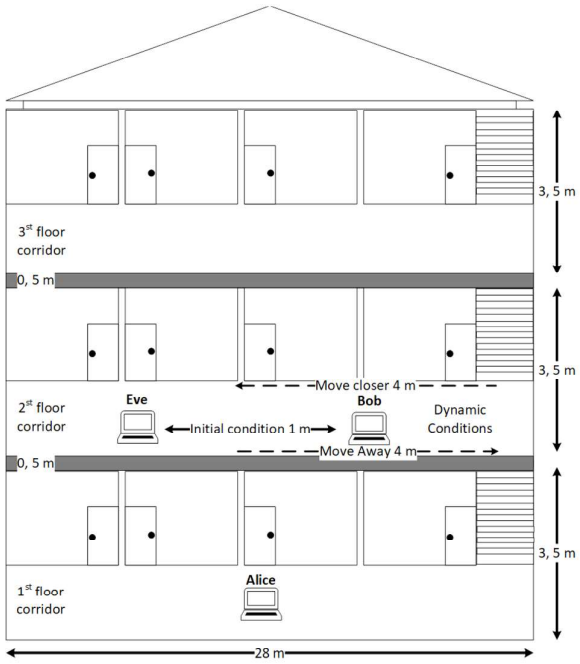

Fig. 4. Experimantal Scenario in dynamic condition

B. Measurement Result

RSS obtained at the time of measurement with static and dynamic conditions is 1400 RSS. 100 measured RSS data are displayed graphically in Fig. 5. for static conditions and Fig. 6. for dynamic conditions. RSS values obtained in static conditions range between -64 to -87 and in dynamic conditions range between -69 to -90. Based on Table 1. the correlation coefficient between Alice and Bob is 0.7874 in static conditions and 0.3369 in dynamic conditions. This shows that the value of the correlation coefficient in static conditions is higher than in dynamic conditions because in dynamic conditions Bob experiences movement so that there is a change in distance resulting in multipath propagation. While the correlation coefficient of Eve with Alice and Bob is quite low so it is very difficult for Eve to get the same RSS as Alice and Bob.

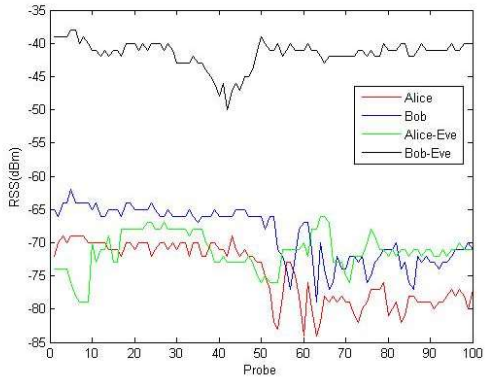

Fig. 5. RSS measurement in static condition

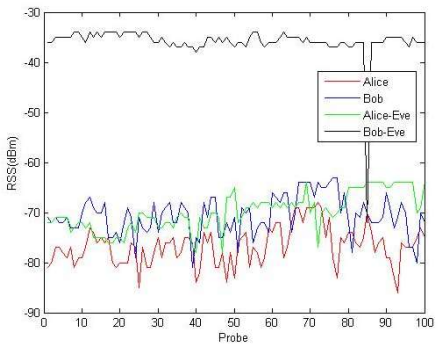

Fig. 6. RSS measurement in dynamic condition

TABLE I. THE CORRELATION COEFFICIENT RESULT

Scenario	Correlation Coefficient		
	Alice and Bob	*Eve and Alice*	*Eve and Bob*
Static	0,7874	-0,0185	-0,0723
Dynamic	0,3369	0,0982	-0,0409

C. Performance Evaluation

In this subsection, we will show the performance of the proposed secret key generation scheme. Performance evaluation of the proposed scheme is measured using KDR, KGR and randomness. In general, the value of α is a constant value with a range of values from 0 to 1. We set the value of α in the range of 0.05 to 0.02 because the α value of more than 0.2 in this experiment will result non-random bits in quantization process. For each scenario a change in the α value fluctuation factor will affect the performance of our scenario.

Key Disagreement Rate (KDR): The key disagreement rate is the percentage of unequal bits produced between the two devices from proposed quantization. From measurements on static and dynamic conditions, variations in fluctuation factors affect the KDR value. We denoted by M_{bits} the number of mismatch bits between 2 devices and denoted by R_{bits} the total number of RSS send and receive between 2 devices. In our scheme, KDR is defined as.

$$KDR = \frac{M_{bits}}{R_{bits}} \text{ x } 100$$

The results of the KDR obtained after the quantization process is shown in Table II. Based on Table II. The KDR with the lowest value is when the value of α = 0.2 with the KDR value for static conditions is 13.64% and for dynamic conditions is 28.64%. This shows that increasing the value of α will result in a lower KDR value.

TABLE II. KDR VALUE WHEN $\alpha = 0.05$ TO $\alpha = 0.2$

Scenario	*KDR(%) α = 0.05*	*KDR(%) α = 0.1*	*KDR(%) α = 0.15*	*KDR(%) α = 0.2*
Static	20.71	18.64	16.14	13.64
Dynamic	51.71	45.00	36.36	28.64

Key Generation Rate (KGR): The key generation rate defines how many bits are produced from the measurement process. The number of bits obtained in this probing experiment channel is 1400 data (in dBm) in both scenarios. We denoted by R_{bits} The total number of RSS send and receive between 2 devices and denoted by T time of the computation process. In out scheme KGR is defined as.

$$KGR = \frac{R_{bits}}{T}$$

In Table III. the highest KGR value is when the value of α = 0.2 with the KGR value obtained 10,980 for static conditions and 9,073 for dynamic conditions. The average KGR produced was 10,517 for static conditions and 7,574 for dynamic conditions.

TABLE III. KGR VALUE WHEN $\alpha = 0.05$ TO $\alpha = 0.2$

Scenario	*KGR(bits/s) α = 0.05*	*KGR(bits/s) α = 0.1*	*KGR(bits/s) α = 0.15*	*KGR(bits/s) α = 0.2*
Static	10.081	10.345	10.662	10.980
Dynamic	6.139	6.993	8.092	9.073

Randomness: Randomness characterizes the patternless randomness of the resulting key. The key bit length used in this study is 256 key bits. In this process allows keys generated more than 1 key. The key is then tested using the NIST Test. The key must meet the randomness standard with a p-value of more than 0.01 for 7 parameters. The number of keys generated and KGR are shown in Table IV.

TABLE IV. NUMBER OF KEY AND KGR

Scenario	*Number of Key*	*KGR(bits/s)*
Static	4	9.234
Dynamic	3	6.933

In Table IV it can be observed that the resulting KGR value for static conditions is 9.234 and the KGR for dynamic conditions is 6.933. The key generated for static conditions is 4 keys and for dynamic conditions is 3 keys. Then each key is tested by NIST Test using 7 parameters. The key with the highest approximate entropy value is called the winner's key and will be used as the symmetric key cryptography. The NIST test results shown in Table V. are the keys with the highest approximate entropy values in static and dynamic conditions.

TABLE V. NIST TEST RESULT WINNER KEY

Parameters	*Static*	*Dynamic*
Frequency	0.45	0.45
Block Frequency	0.82	0.62
Runs	0.30	0.68
Longest Runs	0.08	0.18
Cumulative Sum (Forward)	0.63	0.63
Cumulative Sum (Reversed)	0.80	0.69
Approximate Entropy	0.80	0.81

D. Comparisons with Existing Scheme

In the scheme [9] the quantization process uses a self-adaptive lossless quantization algorithm by utilizing the average value as a threshold value. The proposed algorithm adopts and modifies the scheme algorithm [9] to improve its

performance. Modification of the proposed algorithm using the mode value as a threshold. In Fig. 7. is a comparison of the proposed KDR value of the scheme with the existing scheme [9].

Fig. 7. Comparison between proposed scheme and scheme [9] in term of KDR

From Fig. 7. shows a reduction in KDR up to 48.42% of the proposed scheme compared to the scheme [9]. This is because the proposed algorithm eliminates the division of blocks and uses a value that often appears as a threshold determinant. So the proposed algorithm is able to obtain a better KDR than the algorithm scheme [9].

Fig. 8. Comparison between proposed scheme and scheme [9] in term of KGR

In Fig. 8. there is an increase in KGR produced up to 23.35% compared to the scheme [9]. With the high increase occurred at α = 0.2 with the value of KGR obtained was 10.979. In scheme [9] the number of bits produced in the quantization process depends on the number of blocks used. The number of blocks is calculated by dividing the length of RSS data by the amount of data in each block (interval). So that many bits are wasted and the resulting KGR value becomes small.

IV. Conclusion

In this paper, we propose a secret key generation scheme adopted from the scheme [9] with modifications to improve performance and apply to static and dynamic conditions. The proposed algorithm is able to obtain a KDR reduction of up to 48.42% and an increase in KGR up to 23.35% when compared to the scheme [9]. The best KGR at the stage of reconciliation information is 10.980 in static conditions and 9.073 in dynamic conditions. Our proposed system also successfully passed the randomness test using the NIST test with the approximate entropy value is 0.80 in static conditions and 0.81 in dynamic conditions.

References

[1] M. S. Sharbaf, "Quantum cryptography: A new generation of information technology security system," *ITNG 2009 - 6th Int. Conf. Inf. Technol. New Gener.*, pp. 1644–1648, 2009, doi: 10.1109/ITNG.2009.173.

[2] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key Generation from Wireless Channels: A Review," *IEEE Access*, vol. 4, pp. 614–626, 2016, doi: 10.1109/ACCESS.2016.2521718.

[3] A. Sudarsono, M. Yuliana, and P. Kristalina, "A Reciprocity Approach for Shared Secret Key Generation Extracted from Received Signal Strength in the Wireless Networks," *2018 Int. Electron. Symp. Eng. Technol. Appl. IES-ETA 2018 - Proc.*, pp. 170–175, 2019, doi: 10.1109/ELECSYM.2018.8615568.

[4] M. Yuliana, Wirawan, and Suwadi, "Performance Analysis of Loss Multilevel Quantization on the Secret Key Generation Scheme in Indoor Wireless Environment", *Int. J. on Advanced Science Engineering and Information Technology, vol.9, no.1, pp. 100-108, 2019,* doi: http://dx.doi.org/10.18517/ijaseit.9.1.7583.

[5] Y. Gan, X. Lei, Y. Xiao, H. Hou, and X. Zhou, "Improved Channel Information Extraction toward Efficient Secret Key Generation," *Int. Conf. Commun. Technol. Proceedings, ICCT*, pp. 97–101, 2019, doi: 10.1109/ICCT46805.2019.8947050.

[6] M. F. Awan, K. Kansanen, S. Perez-Simbor, C. Garcia-Pardo, S. Castello-Palacios, and N. Cardona, "RSS-Based secret key generation in wireless in-body networks," *Int. Symp. Med. Inf. Commun. Technol. ISMICT*, vol. 2019-May, pp. 0–5, 2019, doi: 10.1109/ISMICT.2019.8743933.

[7] Z. Li, Q. Pei, I. Markwood, Y. Liu, and H. Zhu, "Secret key establishment via RSS trajectory matching between wearable devices," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 3, pp. 802–817, 2018, doi: 10.1109/TIFS.2017.2768020.

[8] J. Li, A. Ru, and G. Li, "Analysis of Non-Reciprocity Factors in Extracting Secret Key from Wireless Channels for Practical Indoor Scenarios Key Generation Procedure," *2016 2nd IEEE Int. Conf. Comput. Commun. Anal. Int. Conf. Comput. Commun. Anal.*, pp. 227–231, 2016.

[9] H. Zhao, Y. Zhang, X. Huang, and Y. Xiang, "An adaptive physical layer key extraction scheme for smart homes," *Proc. - 2019 18th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. IEEE Int. Conf. Big Data Sci. Eng. Trust. 2019*, pp. 499–506, 2019, doi: 10.1109/TrustCom/BigDataSE.2019.00073.

[10] M. Yuliana, Wirawan, and Suwadi,"An Efficient Key Generation for the Internet of Things Based Synchronized Quantization", *Sensors, 19, 2674, 2019,* doi: 10.3390/s19122674.

[11] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 765 LNCS, pp. 410–423, 1994, doi: 10.1007/3-540-48285-7_35.

[12] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *J. Comput. Syst. Sci.*, vol. 18, no. 2, pp. 143–154, 1979, doi: 10.1016/0022-0000(79)90044-8.