Physical Layer Secret Key Generation with Kalman Filter Detrending

Miroslav Mitev, Arsenia Chorti, Gerhard Fettweis

▶ **To cite this version:**

Miroslav Mitev, Arsenia Chorti, Gerhard Fettweis. Physical Layer Secret Key Generation with Kalman Filter Detrending. 2023 IEEE Global Communications Conference (GLOBECOM 2023), Dec 2023, Kuala Lumpur, Malaysia. pp.5007-5012, 10.1109/GLOBECOM54140.2023.10437062 . hal-04520311

HAL Id: hal-04520311
https://hal.science/hal-04520311

Submitted on 25 Mar 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Physical Layer Secret Key Generation with Kalman Filter Detrending

Miroslav Mitev[1], Arsenia Chorti[2,1], Gerhard Fettweis[1,3]
[1]Barkhausen Institut, 01187 Dresden, Germany;
[2]ETIS, UMR 8051 CY Cergy Paris Université, ENSEA, CNRS, 95000, Cergy, France;
[3]Vodafone Chair for Mobile Communications Systems, Technische Universität Dresden, 01062 Dresden, Germany;
{miroslav.mitev, gerhard.fettweis}@barkhauseninstitut.org, arsenia.chorti@ensea.fr

***Abstract*—The massive deployment of low-end wireless Internet of things (IoT) devices opens the challenge of finding de-centralized and lightweight alternatives for secret key distribution. A possible solution, coming from the physical layer, is the secret key generation (SKG) from channel state information (CSI) during the channel's coherence time. This work acknowledges the fact that the CSI consists of deterministic (predictable) and stochastic (unpredictable) components, loosely captured through the terms large-scale and small-scale fading, respectively. Hence, keys must be generated using only the random and unpredictable part. To detrend CSI measurements from deterministic components, a simple and lightweight approach based on Kalman filters is proposed and is evaluated using an implementation of the complete SKG protocol (including privacy amplification that is typically missing in many published works). In our study we use a massive multiple input multiple output (mMIMO) orthogonal frequency division multiplexing outdoor measured CSI dataset. The threat model assumes a passive eavesdropper in the vicinity (at 1 meter distance or less) from one of the legitimate nodes and the Kalman filter is parameterized to maximize the achievable key rate.**

I. Introduction

The sixth generation wireless networks (6G) are anticipated to facilitate the extensive deployment of Internet of Things (IoT) devices. However, the high computational demands of many cryptographic schemes, particularly in the field of public key encryption (PKE), can significantly impact performance and drain the battery of power-limited devices [1], [2]. Furthermore, the emergence of quantum computing makes existing PKE algorithms insecure. To address this concern, physical layer security (PLS)-based secret key generation (SKG) is identified as a viable quantum-secure alternative. This lightweight approach (first proposed in [3] and [4]) allows the extraction of shared randomness directly from the wireless channel and provides means for secure communication.

Despite the existence of vast theory behind the SKG scheme, real-world implementations are scarce. The openness of the wireless medium creates a challenge, as eavesdroppers in the vicinity might observe similar channel state information (CSI) and obtain partial knowledge on the "secret" key if information leakage is not explicitly considered. Therefore, correlations between legitimate and adversarial channel observations must be taken into account. To ensure independence in time, frequency and antenna domains, simple approaches, e.g., subsampling, can be used. However, accounting for dependencies in space and in particular near-by locations, requires explicit consideration.

While small-scale fading effects de-correlate rapidly over short distances, large-scale fading phenomena vary slowly and can remain stable in time [5] (making it predictable by nearby nodes [6]). In this sense, it is important that large-scale effects are removed from the CSI and keys are generated only from the unpredictable and random part [7]. Recent work has presented pre-processing steps to address this issue [8]. The authors propose the use of principal component analysis (PCA) and autoencoders (AE) to separate the components of the channel. However, such algorithms might require high computational power [9], making them unsuitable for low-end devices.

In this work, we present a lightweight detrending approach based on Kalman filters. Kalman filter is a standard technique to smooth noisy measurements and extract location-dependent trends. Such trends are mainly represented by path-loss and shadowing (i.e., large-scale fading). Following from that, we propose to isolate the entropy rich, small-scale fading, present in the wireless channel, by treating the output of the Kalman filter as a predictable component which must be removed before SKG. This concept was first introduced in our earlier work [10], where SKG was combined with location information in a zero round-trip-time (0-RTT) authentication protocol. In [10] we focused mainly on authentication and provided security proofs assuming that secret keys can be generated at sufficient rates.

The current work is a proof of concept aiming at demonstrating the feasibility of executing a lightweight SKG. All steps of the SKG protocol are implemented and evaluated using massive multiple input multiple output (mMIMO) real-life outdoor measurements provided by Nokia Bell-Labs [11]. The dataset consists of CSI measurements of mobile users that pass by nearby locations that are 1 meter (or less) apart but are separated in time. Each user generates secret keys from CSI measurements which are reconciled using Slepian-Wolf implementations of Polar codes. This work aims at evaluating spatial correlations in time, i.e., we evaluate leakages to malicious users who pass by similar location as legitimate users but at different time instances. To derive the final SKG rate we perform conditional min-entropy evaluation on the legitimate reconciled sequences with respect to the information obtained by the attacker in order to determine the required amount of privacy amplification.

The rest of this paper is organized as follows: Section II gives a detailed overview of the SKG protocol. It also presents our system model and introduces the proposed Kalman filter-based

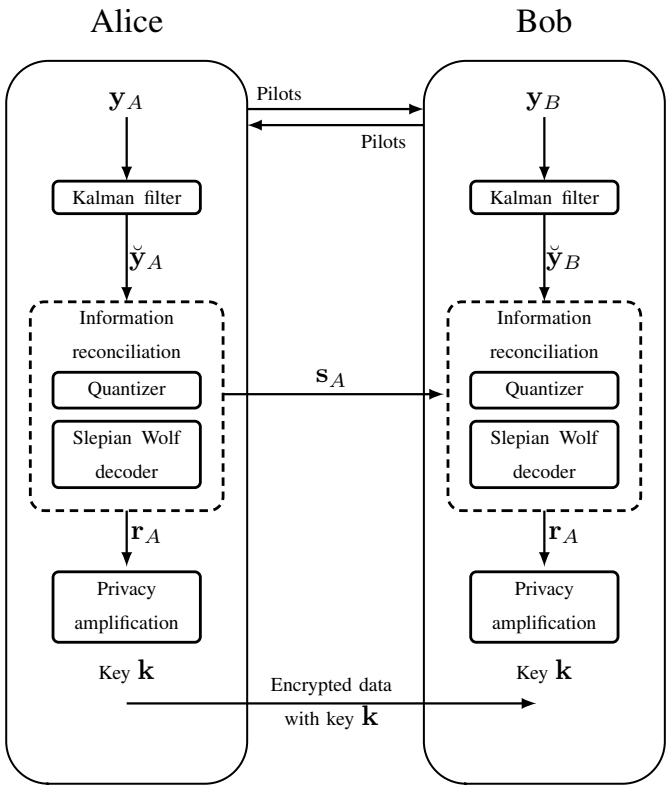


Fig. 1. Secret key generation between Alice and Bob using Kalman filter. Thanks to reciprocity in wireless channels, the outputs of the quantizers are highly correlated variables but not the same (due to noise). Using $\mathbf{s}_A$ and his Slepian Wolf decoder Bob corrects the errors to obtain $\mathbf{r}_A$. Final keys are obtained after privacy amplification.

randomness extraction. Section III, presents the details on the dataset used for this study. Next, a step-by-step evaluation of the SKG protocol is given in Section IV. Finally, Section V concludes this paper.

II. Kalman Filter Based Deternding for Secret Key Generation

The system model in this work consists of two legitimate users, Alice and Bob and a malicious user within the network, Eve. A sketch of the SKG protocol used in this paper is depicted in Figure 1 and described below.

1) *Advantage distillation with Kalman filtering:* To estimate their reciprocal CSI Alice and Bob exchange orthogonal frequency-division multiplexing (OFDM) probe signals in a time-division duplex manner[1]. Due to noise and possible imperfect CSI estimation, the two estimates will be different. At different point in time, Eve passes in a similar location as Bob and aims at obtaining correlated measurements. The complex signals received at Alice, Bob and Eve can be denoted as:

$$\mathbf{y}_A = \mathbf{h}X + \mathbf{n}_A, \tag{1}$$

$$\mathbf{y}_B = \mathbf{h}X + \mathbf{n}_B, \tag{2}$$

$$\mathbf{y}_E = \mathbf{h}_E X + \mathbf{n}_E, \tag{3}$$

where $X \in \mathbb{C}$ is the transmit probe symbol, $\mathbf{n}_A, \mathbf{n}_B, \mathbf{n}_E \in \mathbb{C}^{N\times 1}$ are additive white Gaussian noise variables and $\mathbf{h}, \mathbf{h}_E \in \mathbb{C}$ denote the channel coefficients between Alice and Bob, Alice and Eve, respectively. We note that real-world measurements were used to produce the results in this work (as opposed to simulated channel models), hence, no assumptions on the PDFs of the variables above can be made.

To extract randomness from the channel we propose a lightweight fast Kalman filter-based approach. Fast Kalman filter has computational complexity of $\mathcal{O}(N)$ [13], which allows for real-time execution on resource constrained devices [14]. The filter assumes that a state $G_{A,m}$ is related to the previous $G_{A,m-1}$ as:

$$G_{A,m} = G_{A,m-1} + K_{A,m}(Y_{A,m} - G_{A,m-1}), \tag{4}$$

where $Y_{A,m}$, $G_{A,m}$, for sample index $m = 1, 2, \ldots, M$ are the values of raw and filtered measurements, respectively, and $K_{A,m}$ is Kalman gain which determines the convergence of the filter. The Kalman gain is computed as:

$$K_{A,m} = \frac{P_{A,m}}{P_{A,m} + R}, \tag{5}$$

where $P_{A,m}$ is a prediction error which updates iteratively during the filtering process and R denotes variance of the expected error in the raw measurement data, this is a pre-defined constant. From (4) and (5) it is clear that R has an important role and defines how much to "trust" the raw measurements. At the end of this step Alice obtains a vector $\mathbf{g}_A = [G_{A,1}, \ldots, G_{A,M}]$ containing the filter output which is of the same size as her raw measurement vector $\mathbf{y}_A = [Y_{A,1}, \ldots, Y_{A,M}]$. To remove predictable components, Alice subtracts the filter output from her raw measurements and obtains the residual $\breve{\mathbf{y}}_A = \mathbf{y}_A - \mathbf{g}_A$. The process is defined identically for Eve and Bob who obtain $\breve{\mathbf{y}}_E$ and $\breve{\mathbf{y}}_B$, respectively.

To demonstrate how the value of R affects the filter output, Figure 3 shows an example for $R = 10^{-2}$, $R = 10^{-3}$ and $R = 10^{-5}$. The figure illustrates raw measurements, filter outputs and residuals (that are result of subtracting the previous two vectors).

It can be seen that depending on the value of R the filter output can follow the raw measurements loosely (for $R = 10^{-2}$) or closely (for $R = 10^{-5}$) resulting into residual with large or small-scale variations, respectively. It can be seen that when $R = 10^{-2}$ the residual follows the trend of the original data. Next, when $R = 10^{-3}$ the residual becomes closer to zero-mean and large predictable variations are minimized. Finally, for $R = 10^{-5}$, the residual is almost constant with values close to zero. This shows that a large value of R might result in leaving predictable components in the residual, however, if R becomes too small the filtering removes not only predictable but also random components from the raw measurements.

[1]In multiple attack scenarios it has been demonstrated that Alice and Bob should optimally use equal power distribution for channel probing [12].

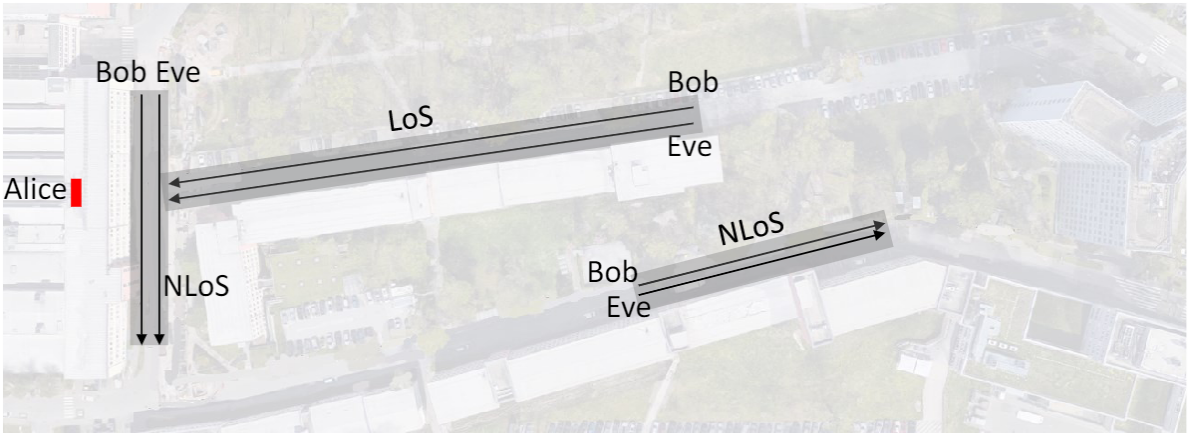


Fig. 2. Snapshot of the measurement campaign from [11]. Only the highlighted tracks are considered in this work.

2) *Information reconciliation:* Alice, Bob and Eve quantize their observations to binary vectors $\mathbf{r}_A, \mathbf{r}_B, \mathbf{r}_E$, respectively. To correct errors at the output of the quantizer one of the legitimate users (Alice) generates syndrome information, $\mathbf{s}_A$, using distributed source coding techniques (e.g., Slepian-Wolf coding). The syndrome is send to the other legitimate party (Bob) on a public channel. Bob uses the syndrome to correct errors in his observations using a DSC decoder. Considering successful reconciliation, at the end of the step Alice and Bob possess identical sequence, $\mathbf{r}_A$. Due to the public transmission we assume that $\mathbf{s}_A$ is also fully accessible to Eve. Using the syndrome she tries to correct errors in her observations, $\mathbf{r}_E$. At the output of her decoder, Eve obtains $\mathbf{r}'_E$ which, depending on initial channel correlations, could be close or not to $\mathbf{r}_A$.

3) *Privacy amplification:* This step is performed to remove leakage that occurred in the previous steps. The length of the final key $\mathbf{k} \in \mathcal{K}$ between Alice and Bob should be [15], [16]:

$$|\mathbf{k}| \leq H_\infty(\mathbf{r}_A|\mathbf{r}_E, \mathbf{s}_A, \mathbf{r}'_E), \tag{6}$$

where [17]:

$$H_\infty(\mathbf{r}_A|\mathbf{r}_E, \mathbf{s}_A, \mathbf{r}'_E) = -\log_2 \max_{\mathbf{r}_A, \mathbf{r}_E, \mathbf{r}'_E \in \mathcal{R}, \mathbf{s}_A \in \mathcal{S}} p(\mathbf{r}_A|\mathbf{r}_E, \mathbf{s}_A, \mathbf{r}'_E), \tag{7}$$

denotes conditional min-entropy, and $\mathcal{R}, \mathcal{S}$ denote the space of quantization outputs and syndromes, respectively. The total amount of leaked information to Eve can be evaluated as [18]:

$$\text{Leakage} = H_\infty(\mathbf{r}_A) - H_\infty(\mathbf{r}_A|\mathbf{r}_E, \mathbf{s}_A, \mathbf{r}'_E), \tag{8}$$

where $H_\infty(\mathbf{r}_A)$ is min-entropy of the sequence $\mathbf{r}_A$. A standard way to remove the leakage from the reconciled information is by using a one-way collision-resistant compression function, e.g., hash function. This last phase ensures that the generated key sequence is uniformly distributed and unpredictable by an adversary [19].

III. Experimental Campaign and Dataset Description

The dataset used to conduct this study comes from a measurement campaign done by Nokia crew on their campus in Stuttgart, Germany [11]. It consists of outdoor mMIMO channel measurements taken while moving along different paths. The paths we consider in this study are illustrated in Figure 2. The transmit antenna array (Alice) is placed on a roof top of a building. The array has 64 antenna elements with a rectangular geometry of 4 rows each with 16 single-polarization patch antennas. Horizontal and vertical spacing between antenna elements are $\lambda/2$ and λ, respectively.

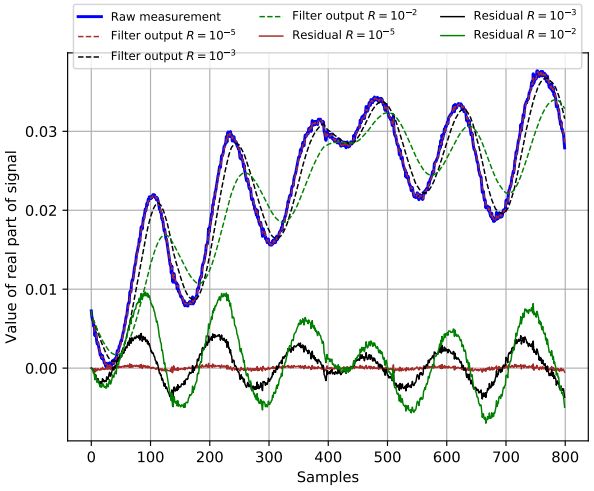


Fig. 3. Kalman filtering outputs for $R = 10^{-2}$, $R = 10^{-3}$, $R = 10^{-5}$. The resulting residuals (i.e., subtracting raw and filtered data) are also illustrated.

In this setting, Alice transmits 64 pilot signals following the 10 MHz LTE numerology (600 subcarriers with 15 kHz spacing). The waveform is OFDM with center frequency of 2.18 GHz. To obtain channel measurements 50 sub-bands are sounded, i.e., 12 consecutive subcarriers are used per sub-band. A pilot burst over all sub-bands requires 0.5 ms, hence bursts are sent with periodicity of 0.5 ms. This results in 1 ms to perform two-way exchange (e.g., Alice - Bob and Bob - Alice).

Two user equipment (Bob and Eve) are mounted on mobile carts, each having a single monopole antenna at 1.5 m. Users

TABLE I
MISMATCH PROBABILITY AFTER QUANTIZATION AT ALL PARTIES CONSIDERING DIFFERENT VALUES FOR R.

Nodes	Alice and Bob		Eve	
Filtering parameter	LoS	NLoS	LoS	NLoS
No filtering	0.019	0.037	0.51	0.47
$R = 10^{-1}$	0.023	0.039	0.47	0.46
$R = 10^{-2}$	0.030	0.046	0.46	0.45
$R = 10^{-3}$	0.040	0.062	0.47	0.45
$R = 10^{-4}$	0.054	0.091	0.48	0.45
$R = 10^{-5}$	0.072	0.124	0.49	0.47
$R = 10^{-6}$	0.083	0.143	0.49	0.47

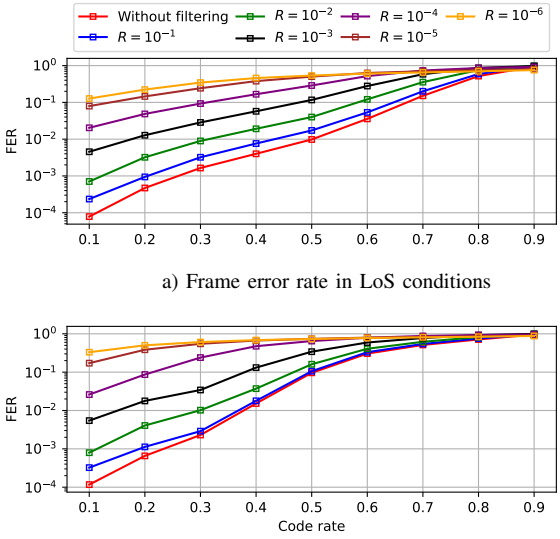
are equipped with Rohde & Schwarz TSMW receivers and Rohde & Schwarz IQR hard disc recorders which continuously measure and store the signals from Alice. As depicted in Figure 2, Bob and Eve move in parallel tracks; note the distance between Bob's and Eve's tracks is kept ≤ 1 m. During measurements, devices are synchronized via GNSS. Bob and Eve move along the tracks at different time instances but at identical speed of 3.6 km/h. In accordance to the periodicity of the pilot bursts this results in approximately 0.1 mm of sampling in the spacial domain.

In a previous work it has been demonstrated that by subsampling in frequency, time and antenna domains correlations can be removed [20]. Similarly here, to account for correlation along these domains we consider measurements at every 4-th antenna, at every 10-th subcarrier, and we keep every 5-th channel sample. Taking every 5-th samples results in time sampling factor $T = 5$ ms. Furthermore, as the dataset contains only uplink measurements we use subsequent samples to mimic the downlink, i.e., odd samples are considered as downlink and even samples are uplink. A statistical analysis on the dataset can be found in [20].

At this point, each party possesses a vector of raw channel measurements over which applies fast Kalman filter detrending with parameter R. As discussed in Section II, Alice, Bob and Eve then subtract the output of the filter from their initial raw channel measurements and obtain the residual vectors $\breve{\mathbf{y}}_A, \breve{\mathbf{y}}_B$ and $\breve{\mathbf{y}}_E$, respectively. To perform quantization and reconciliation and arrive at the desired size, the vectors at each party are reshaped into a matrix of size $\frac{|\breve{\mathbf{y}}_A|}{512} \times 512$. Rows from the resulting matrices are quantized independently. In this work, we assume a linear quantizer with 4 quantization levels. This gives $\log_2(4) = 2$ bits per sample, hence, each row of the matrix produces a sequence of 1024 bits. The quantization levels are chosen uniformly between the minimum and maximum values in the corresponding row. The resulting matrices of quantized residuals are used for key generation. In the next section we evaluate each step of the SKG protocol and show how the proposed Kalman filtering approach affects the performance.

IV. PERFORMANCE EVALUATION

Following from the previous section, we first evaluate the the mismatch probability between Alice and Bob. After quantizing



a) Frame error rate in LoS conditions

b) Frame error rate in NLoS conditions

Fig. 4. Frame error rate in LoS and NLoS conditions after reconciliation between Alice and Bob. Different code rates and filtering parameters are illustrated.

mismatch is measured using Hamming distance over all generated bits. The resulting probability values are given in Table I. As expected decreasing R increases the mismatch between Alice and Bob. A smaller value of R can make the residual more unpredictable, such that it does not follow the trend of the original measurements (see Figure 3), however, as observed here, this comes at the cost of decreased reciprocity. This can be observed for both LoS and NLoS conditions. On the other hand, the mismatch at Eve remains almost stable around 50%. The filtering process has a negligible impact on her mismatch probability. This is a desired behavior as the Kalman filter does not bring improvement at her end.

After quantization the parties perform information reconciliation using Slepian Wolf implementation of Polar codes. Particularly, Polar codes with unique decoding as in [21] are used. Here, Alice generates a syndrome $\mathbf{s}_A$ and sends it to Bob. The syndrome size varies depending on the code rate, i.e., low code rates require longer syndrome. This gives better chances for successful reconciliation, however, leaks more information as $\mathbf{s}_A$ is also observed by Eve. At this step we evaluate the frame error rate (FER) between Alice and Bob.

This is ilustrated in Figure 4. The figure shows the FER for both LoS (Figure 4a) and NLoS (Figure 4b) scenarios. It can be seen that the FER decreases in NLoS conditions. This is an expected result, as the absence of the dominant LoS path naturally decreases the SNR between the two parties. As FER is directly impacted by the bit mismatch probability, we see a similar behaviour as in Table I, i.e., a smaller value of R gives a lower performance in terms of FER. Another important parameter for the success of this step is code rate. At lower code rate the FER is negligible, however, as noted above this requires the exchange of larger syndrome sequence $\mathbf{s}_A$.

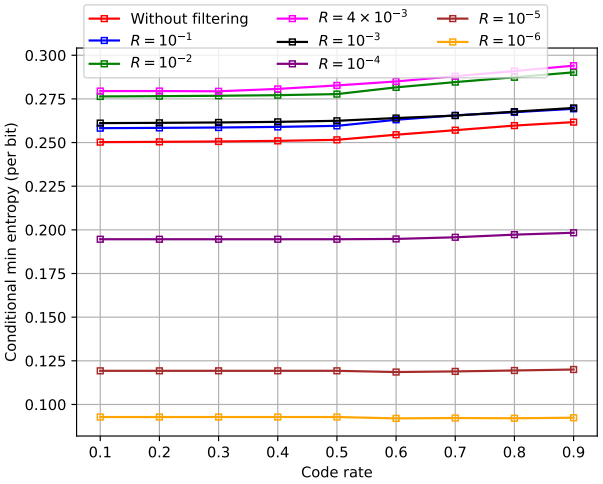


Fig. 5. Conditional min-entropy in LoS condition considering different code rates and values of R.

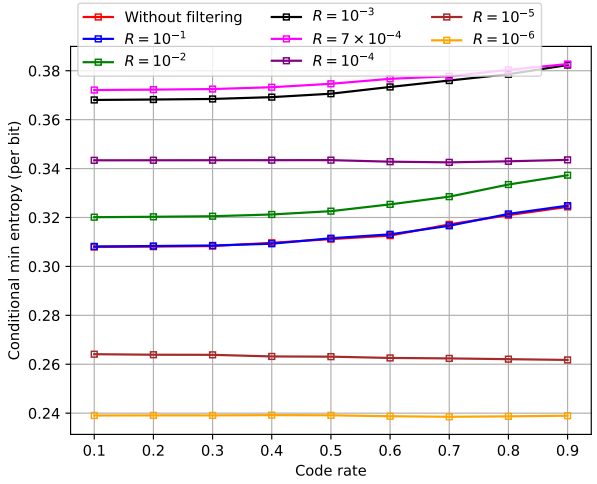


Fig. 6. Conditional min-entropy in NLoS condition considering different code rates and values of R.

After reconciliation we evaluate the secure and random number of bits by considering the leakage at Eve. In our work, this is performed using the FBLEAU estimator [22]. The evaluation is done in accordance to Equation (7), i.e., the estimator takes as inputs $\mathbf{r}_A, \mathbf{r}_E, \mathbf{s}_A, \mathbf{r}'_E$ and outputs a scalar value for the conditional min-entropy. The results are illustrated in Figure 5 for LoS and Figure 6 for NLoS. Several observations can be drawn from the figures.

First, we can see that LoS can in general offer less randomness, hence, lower conditional min entropy. This may be attributed to the fact that main contributors for unpredictability in wireless channels are multipath components (MPCs) that arrive at different times and result from different reflectors. While MPCs are present also in the LoS setup, the received signals are mainly affected by direct path as she contains the most of the power. On the other hand, in NLoS conditions

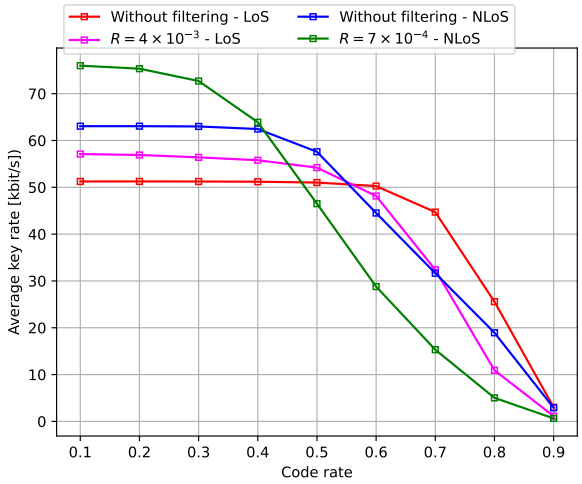


Fig. 7. Average key rate for LoS and NLoS conditions considering different code rates and filtering paratemers.

the reflected components are more pronounced which results in higher unpredictability of the received signals.

Second, applying Kalman filter can improve the performance in terms of conditional min-entropy. However, this is valid only up to a certain R value. For the LoS scenario we see that applying the filter with $R = 10{-}1$ gives a slight improvement. The increase in conditional min-entropy continuous for $R = 10{-}2$ and $R = 4 \times 10^{-3}$ (this value was found with numerical search in the space). However, after these values a sudden drop is observed reaching conditional min-entropy < 0.1 for $R = 10^{-6}$. A similar tren is observed for the NLoS scenario shown in Figure 6 with the optimal value identified, $R = 6 \times 10^{-4}$. Given these results it is clear that an optimal value of R exists and it is determined by the channel conditions. In the LoS case less filtering is required to separate the unpredictable components as compared to the NLoS case. Similar, to the conclusion above we believe that this is a result of the lower randomness in LoS scenarios.

Finally, we can see that the code rate could also affect the conditional min-entropy. This result is expected as increasing the code rate decreases the length of the syndrome. As noted earlier, the syndrome is shared on a public channel and is available to Eve. Therefore, higher code rate leaks less information and brings an increase in conditional min-entropy.

At this step we can evaluate the average key rate for the presented scenarios. For the setup in this work we represent the key rate in $[b/s]$ as a function of several parameters: i) number of bits generated at the output of the quantizer $= 1024$; ii) FER after performing reconciliation; iii) conditional min-entropy as denoted in Equation (7); iv) time sampling factor, T, which as noted in Section III for the current setup equals to 5 ms. Based on that the average key rate is defined as:

$$R[b/s] = \frac{F \times (1 - \text{FER}) \times H_\infty(\mathbf{r}_A | \mathbf{r}_E, \mathbf{s}_A, \mathbf{r}'_E)}{T}. \quad (9)$$

Figure 7 provides an evaluation using subset of the combi-

TABLE II
RANDOMNESS EVALUATION USING NIST-APPROVED TESTS [23].

Test	Success rate
Frequency (monobit) test	0.9926
Frequency within a block test	0.9838
Runs test	0.9868
Longest run of ones in a block test	0.9868
Serial test	0.9874
Cumulative sum test	0.9926

nations above. The figure shows the average key rate in LoS and NLoS conditions when Kalman filter is applied (with parameters $R = 4 \times 10^{-3}$ and $R = 7 \times 10^{-4}$) and when it is not. The values of R are chosen in accordance to the results on conditional min-entropy. For low code rates it can be seen that the filter provides substantial improvement. Particularly, improvement of > 5 [kbit/s] for LoS and > 10 [kbit/s] for NLoS. It can also be observed that increasing the code rate results in decrease in performance. This aligns with our results in Figure 4 as high code rate corresponds to high FER.

Finally, as noted in Section II, to generate the final keys, hashing must be performed. We execute this step using SHA-256 hashing function. The output of SHA-256 has a fixed length of 256 bits. To comply with Equation 6 we fix the input of the function to size $256/H_\infty(\mathbf{r}_A|\mathbf{r}_E, \mathbf{s}_A, \mathbf{r}'_E)$. After hashing we verify the randomness of the generated keys, by passing them through the NIST randomness test collection [23]. The tests evaluate uniformity, independence and unpredictability, of the key bits and output a binary decision (yes/no). All generated keys for LoS $R = 4 \times 10^{-3}$ and NLoS $R = 7 \times 10^{-4}$ and code rate 0.1 are evaluated. The resulting success rates are given in Table II. We can see that the values are close to one, proving that the generated keys are high randomness properties.

Overall, our results demonstrate that Kalman filter can be an efficient and lightweight approach to extract random components from the wireless channel. As a future work we plan to further investigate our approach by optimizing the parameterization throughout the SKG protocol.

V. CONCLUSION

This work provides an experimental validation of the PLS-based secret key generation. All steps of the protocol are performed on a real-life outdoor dataset. In general, our findings illustrate that the utilization of the Kalman filter can be a viable method for extracting random elements from the wireless channel. Based on our evaluation, it is evident that the information accessible for SKG is highly dependent on the characteristics of the channel, i.e., in LoS or NLoS. Therefore devices need to be channel-aware and their system parameters must be chosen accordingly.

ACKNOWLEDGEMENT

This work is financed on the basis of the budget passed by the Saxon State Parliament. The work has also been funded by the German Ministry of Education and Research, joint project: 6G Integrated Communication & Sensing for Mobility – 6G-ICAS4Mobility, funding label 16KISK231. Furthermore, A. Chorti was supported by INEX Funding of Excellence, project PHEBE.

REFERENCES

[1] A. Mukherjee, "Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints," in *Proc. IEEE*, vol. 103, no. 10, Oct 2015.
[2] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," in *Proc. IEEE*, Oct 2015.
[3] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, May 1993.
[4] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. i. secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, July 1993.
[5] A. Goldsmith, *Wireless Communications*. Cambridge Univ. Press, 2005.
[6] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "Proximate: Proximity-based secure pairing using ambient wireless signals," in *Proc. of the 9th International Conference on Mobile Systems, Applications, and Services*, ser. MobiSys '11. New York, NY, USA: Association for Computing Machinery, 2011, pp. 211–224.
[7] A. Chorti, A. N. Barreto, S. Köpsell, M. Zoli, M. Chafii, P. Sehier, G. Fettweis, and H. V. Poor, "Context-aware security for 6G wireless: The role of physical layer security," *IEEE Communications Standards Magazine*, vol. 6, no. 1, pp. 102–108, 2022.
[8] M. Srinivasan, S. Skaperas, M. S. Herfeh, and A. Chorti, "Joint localization-based node authentication and secret key generation," in *IEEE Int. Conf. Commun. (ICC)*, 2022, pp. 32–37.
[9] H. Cardot and D. Degras, "Online principal component analysis in high dimension: Which algorithm to choose?" *International Statistical Review*, vol. 86, no. 1, pp. 29–50, 2018.
[10] M. Mitev, M. Shakiba-Herfeh, A. Chorti, M. Reed, and S. Baghaee, "A physical layer, zero-round-trip-time, multifactor authentication protocol," *IEEE Access*, vol. 10, pp. 74 555–74 571, 2022.
[11] M. K. Shehzad, L. Rose, S. Wesemann, and M. Assaad, "Ml-based massive mimo channel prediction: Does it work on real-world data?" *IEEE Wireless Communications Letters*, vol. 11, no. 4, pp. 811–815, 2022.
[12] M. Mitev, A. Chorti, E. V. Belmega, and H. V. Poor, "Protecting physical layer secret key generation from active attacks," *Entropy*, vol. 23, 2021.
[13] K. Nishiyama, "An H_∞ optimization and its fast algorithm for time-variant system identification," *IEEE Transactions on Signal Processing*, vol. 52, no. 5, pp. 1335–1342, 2004.
[14] C. K. Chui and G. Chen, *Kalman Filtering with Real-Time Applications*. Germany: Springer, Berlin, Heidelberg, 1987.
[15] D. Brown, "Formally assessing cryptographic entropy," *IACR Cryptol. ePrint Arch.*, p. 659, 2011.
[16] C. T. Zenger, J. Zimmer, M. Pietersz, J.-F. Posielek, and C. Paar, "Exploiting the physical environment for securing the internet of things," in *Proc. ACM New Secur. Paradigms Workshop (NSPW)*, Sep., 2015.
[17] L. Reyzin, "Some notions of entropy for cryptography," in *Information Theoretic Security*, S. Fehr, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 138–142.
[18] G. Smith, "On the foundations of quantitative information flow," in *Foundations of Software Science and Computational Structures*, L. de Alfaro, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 288–302.
[19] M. Mitev, A. Chorti, M. Reed, and L. Musavian, "Authenticated secret key generation in delay-constrained wireless systems," *Eurasip J. Wirel. Commun. Netw.*, 2020.
[20] M. Srinivasan, S. Skaperas, M. Mitev, M. S. Herfeh, M. K. Shehzad, P. Sehier, and A. Chorti, "Smart channel state information pre-processing for joint authentication and symmetric key distillation," *Under review in IEEE Tran. on Machine Learning in Com. Netw.*, 2023.
[21] M. Shakiba-Herfeh and A. Chorti, "Comparison of short blocklength slepian-wolf coding for key reconciliation," in *2021 IEEE Statistical Signal Processing Workshop (SSP)*, 2021, pp. 111–115.
[22] G. Cherubin, K. Chatzikokolakis, and C. Palamidessi, "F-BLEAU: Fast black-box leakage estimation," in *2019 IEEE Symposium on Security and Privacy (SP)*, May 2019.
[23] L. Bassham, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Special Publication Nat. Inst. Standards Technol. (SP NIST), Gaithersburg, MD, USA, Tech. Rep., 2010.