Blind Synchronization of Channel Impulse Responses for Channel Reciprocity-based Key Generation

Paul Walther*, Elke Franz*, and Thorsten Strufe*†
*Chair for Privacy and Security, Technische Universität Dresden
†Centre for Tactile Internet with Human-in-the-Loop (CeTI)
{<firstname>.<lastname>}@tu-dresden.de

***Abstract*—Local, blind synchronization of Channel Impulse Responses for key generation algorithms without leaking details to adversaries is challenging, due to noise from transmission and measurements. Extracting the channel characteristics as a common source of randomness using CIR promises notable improvements in key bit rates for Physical Layer Security, however, reciprocity requirements necessitate successful synchronization at both ends.**

We propose a one-dimensional Gaussian filter towards this end, which is simple, more robust, and outperforms competing approaches in almost all settings. To evaluate the quality of our approach, we assess the synchronization accuracy on extensive datasets. Experiments using data generated synthetically with the standardized IEEE 802.15 UWB channel model indicate a performance improvement of up to 31%. Performance on par or better than all alternatives in real measurements underlines its superior robustness against synchronization errors.

I. Introduction

Channel Reciprocity-based Key Generation (CRKG) is a variation of PhySec that aims at efficient shared secret generation [18], [21]. It has been formalized and proven information theoretically secure [2] and consumes significantly less energy than competing key generation approaches (over 61 time less than ECDH, for instance [21], [8]). It leverages that volatile properties of wireless channels between two partners, Alice and Bob, are reciprocal, but hidden from parties observing the medium from a third location. This allows Alice and Bob to derive a shared secret, which is impossible to guess for an eavesdropper Eve.

A severe drawback of current CRKG approaches is their low secret key rate of around 2 $bits$ per second. This is commonly due to their employment of the received signal strength indicator (RSSI) as a shared source of randomness, with a rather low resolution: It only provides a single value per channel utilization [22].

Quantizing channel state information may help leverage much richer and more detailed reciprocal characteristics, while maintaining the security properties. Some authors hence propose to use Channel Impulse Responses (CIR) [4], [10], [17].

The measurements at higher resolution require synchronization at both ends: local timing offsets, even at small scales, inevitably lead to mismatches in the quantized sequences at the communication partners. They hence would erroneously observe reduced channel correlation, leading to mismatching inputs to the key generation algorithms. It hence is crucial for CIR-based CRKG to properly synchronize the remote observed measurements.

This synchronization must not jeopardize the security: In the context of key exchange, this means to leak as little information as possible about the key material and its source. Synchronization hence should be implemented as a *blind* protocol, which processes local data exclusively and does not exchange any information over the public channel.

Despite its importance for CRKG, the challenge of synchronization has not yet been addressed. Moreover, our studies show that intuitive synchronization approaches of adjacent research fields, e.g. [14], [11], are unsuitable in this case.

To address this challenge, we first analyze the problem theoretically and define an appropriate methodology for solution design and evaluation. We then propose a new approach for blind CIR synchronization in time. In this new approach, we apply a one-dimensional Gaussian filter to mitigate deviations in corresponding, remote measurements. Thereby, a robust anchor for synchronization can be determined within the resulting filtered signal at both parties.

This work is partly supported by the German Research Foundation (DFG) through CRC 912 “HAEC” and EXC 2050 “CeTI”.

978-1-7281-1028-8/19/$31.00 ©2019 IEEE

To evaluate our scheme, we compared it to common solutions from related fields. We use data from real world measurements, which we conducted in this context [19], to assess applicability and performance. As the measurements represent only specific setups, we also synthesize data for scenarios ranging from benign to highly adverse settings, using the IEEE 801.15 UWB channel model. The results demonstrate the exceptional performance of our scheme, with advantages of up to 31% over the second best approach.

To summmarize, we make the following *contributions* in this paper:

- we introduce a new blind synchronization scheme for CIR
- we develop a methodology for assessing CIR synchronization
- we thoroughly evaluate the proposed approach against alternative solutions using data from real world measurements and simulation.

The remaining paper is structured as follows: In Sec. II, the system model is described and the methodology developed. Section III covers the problem definition and solution design. In Sec. III-B, our new approach is proposed. Sec. IV describes our evaluation and Sec. V concludes and gives an outlook.

II. System Model and Methodology

Although the approaches presented in this paper are not restricted to a particular use case, we will briefly describe the system model used. Based on this model we will develop the methodology used for solution design and realization in Sec. III.

A. System Model

CRKG is a resource efficient approach of generating a shared secret between wirelessly connected communication partners. It is a realization of Physical Layer key generation based on the source model described by Maurer and Ahlswede [13], [1], where the shared channel is treated as common source of randomness. Due to the unique wave propagation of wireless signals, the channel properties are specific to the terminals' positions and reciprocal at both ends [9]. Additionally, as described by Jake's scattering theorem, an eavesdropper residing more than half of a wavelength away, will observe an uncorrelated realization due to spatial decorrelation [7]. Thereby, the channel characteristics of the legitimate partners are hard to predict for such an eavesdropper.

Fig. 1 depicts the general setup of CRKG. The legitimate partners, Alice and Bob, exchange messages over the shared channel to estimate the respective channel

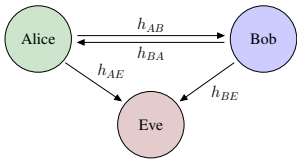


Fig. 1. General system model for CRKG

characteristics, denoted as $X = h_{AB}$ and $Y = h_{BA}$ respectively. Eve is a local passive attacker, which overhears the communication to gain information about the prospective shared secret.

To generate reciprocal observations, X and Y are taken within the channel coherence time. Although the channel properties per se are highly similar at both receivers, the realizations contain differences due to movements and electromagnetic interference within the coherence time, as well as noisy measurements. To compensate these differences, the further processing employs algorithms to equalize the observations, which is crucial to generate a matching secret in the end [2].

Fig. 2(a) depicts typical realizations of estimated channel characteristics, which were derived from the received signals. These signals are composed of a known probe signal x as input convoluted with the channel characteristics h. Additionally, distortion like noise are modeled trough Additive Gaussian White Noise n.

$$y_{AB}(t) = h_{AB}(t, \tau) * x(t) + n(t) \tag{1}$$

Since $x(t)$ is known to both parties, they can estimate h from this signal. As h_{XY} is mainly determined by multipath propagation, we follow the assumptions of the widely applied UWB multipath propagation model defined by Goldsmith [7].

The estimated channel characteristics are further processed as input for the key derivation. This derivation's effective key rate is governed by the amount of information about this input present at Alice (A) and Bob (B), which is described by the mutual information $I(A; B)$. Additionally, the *maximal* key rate is limited by the information leakage towards Eve (E) (Eq. (2)), since she overhears all communication:

$$C_{k,max} \leq min(I(A; B), I(A; B|E)) \tag{2}$$

To minimize this leakage, as little information as possible about the input data should be exchanged.

B. Problem Statement

Since CRKG, especially in terms of secret key rate and secure key bits, is driven by the reciprocity of the

respective channel estimations, it is crucial to minimize any influence diminishing this reciprocity. Mismatches in synchronization will inherently lead to decreased reciprocity, since even equal reciprocal measurements will differ, if they are out of sync. In state-of-the-art approaches to CRKG, this problem has not been addressed yet.

Our analysis shows that state-of-the-art as well as common approaches to related problems like maximum based algorithms, leading edge detection algorithms, and their modern derivates employed in millimeter range UWB location applications [14], [11] do not perform sufficiently in the described scenario.

Therefore, to make CRKG as efficient as possible, an approach is needed, which can determine a sufficient synchronization while keeping the information leakage low. To fulfill the second part, we will only consider approaches without interaction between the single communication partners, as this keeps the leaked information at zero (Eq. (2)). Since such approaches only work with local information, they are also called *blind*.

In consequence, this means that such *blind* approaches have solely local knowledge, i.e. no information about the reciprocal measurement is available. Hence, there is no feedback about the performance of the respective applied algorithm.

C. Methodology

The notation used throughout this section and the remaining paper is shown in Table I.

TABLE I
NOTATION

Symbol	Meaning	Alias
X^i, Y^i	CIR instance measured at time i Vector of samples in time domain	*realization, observation*
X_j, Y_j	Data point j with single CIR	*sample, data point*
t	Time offset	*offset, difference*
t^A	Time offset of approach A	
t_{XY}	Time offset between observations X,Y	

To adequately assess the stated problem, we will develop an appropriate methodology by the following means: First, an optimal solution needs to be defined, which will act as baseline for evaluating our newly proposed approach. Based on this optimal solution, we define a metric, which shows the performance of the compared approaches in relation to each other. Finally, we define another metric to show the impact of the approaches in the context of overall CRKG processing.

It is worth noting, that the defined metrics employ a global view on the reciprocal measurements. This means, the metrics integrate knowledge about differences between the measurements, which are not available to the algorithms per se.

1) Theoretical Optimal Solution: The optimal solution for determining time offsets between two signals is a function which perfectly identifies the actual offset of 2 given signals. This means, that such a functions uniquely identifies a time shift, for which the "overlapping" of the given signals is maximal.

Due to the nature of its calculation, the *discrete cross-correlation* becomes maximal, if two signals "overlap" optimally. For a given offset k, the discrete cross-correlation of the signals X and Y is calculated as:

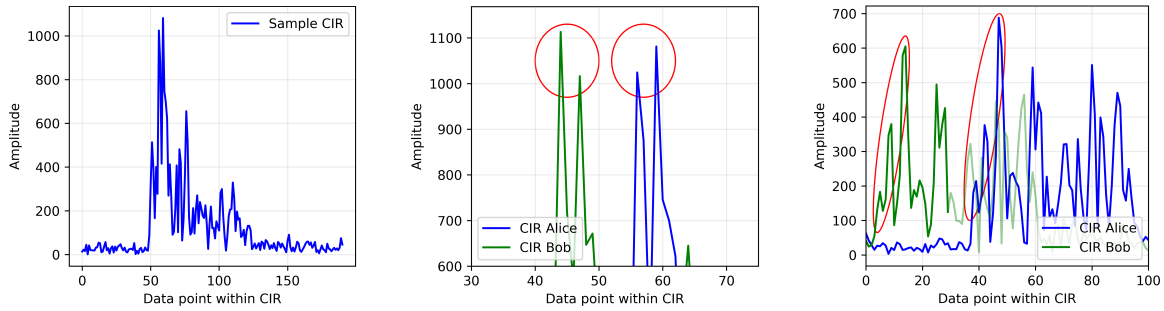
$$(X \star Y)[k] = \sum_{i=-\infty}^{\infty} X_{i+k} Y_i^*$$

By computing the cross-correlation for $k \in [-|X|, |X|]$ a vector of results for the respective offsets is generated. The maximum of this vector corresponds with the optimal time shift, which needs to be applied to achieved maximal time synchronization of the signals X and Y. Hence, we treat the offset t_{XY}^C as the theoretical, optimal solution for synchronization:

$$t_{XY}^C = \max\{k \in [-|X|, |X|] : (X \star Y)[k])\} \quad (3)$$

2) Metrics for Synchronization: Proceeding from this optimal solution, we now define a metric for assessing different CIR time synchronization approaches. The different approaches A will locally define a unique anchor in time at each communication participant. This anchor is a unique data point within the measurement, which acts as the origin of the time axis for this measurement. By using the global view of this analysis, these local anchors can be related to each other to calculate a time offset. The closer a given approach's time offset is to the optimal shift t_{XY}^C, the better is the respective approaches synchronization performance.

We implement the metrics as follows: The difference between the optimal time offset t_{XY}^C and an approaches A time offset is shown in Eq. (4). By applying this difference to all n available CIR observations we obtain the vector $\Delta(A)$. This vector is used in a twofold manner: First, it is used to calculate the aforementioned mean and standard deviation of the time differences. And second, it is used to computed the final metric $\Delta^0(A)$, which is the fraction of optimal time offset generated by the current approach (Eq. (6)). An optimal



(a) Example (b) Maximum (c) Leading Edge Detection

Fig. 2. CIR realization which yield mismatches for different common synchronization approaches.

solution is an approach with $\Delta = (0, \dots 0)$, i.e. $\Delta^0 = 1$.

$$\Delta_i(A) = t^A_{X^i Y^i} - t^C_{X^i Y^i} \tag{4}$$

$$\Delta(A) = (\Delta_1(A), \Delta_2(A), \dots \Delta_n(A)) \tag{5}$$

$$\Delta^0(A) = \frac{|\{d \in \Delta(A) : d = 0\}|}{|\Delta(A)|} \tag{6}$$

3) Metrics for overall CRKG: Finally, we define how the different approaches are evaluated in the context of the overall CRKG processing. Since it is crucial for the key generation to produce the same key at both partners, the *information reconciliation* step needs to be successful. State-of-the-art approaches facilitate error correction codes for reconciliation. By employing perfect codes, the success of this step is determined by the number of bit errors between the quantized observations. Hence, regarding the overall CRKG processing impact, the bit error rate (BER) is a suitable metric [21].

In order to assess the BER, the observed real-valued observations X^i, Y^i are quantized into bit-strings b_{X^i}, b_{Y^i} locally at both communication partners Eq. (7). As quantization algorithm, the best solution from [19] is implemented. Afterwards, to identify the differences between quantized bit-strings, i.e. the resulting error, the Hamming distance between b_X and b_Y is calculated:

$$b_{X^i} = f_{quant}(X^i) \qquad b_{Y^i} = f_{quant}(Y^i) \tag{7}$$

$$e_i = |\{j \in \{1, \dots, |b_{X^i}|\} : b_{X^i_j} \neq b_{Y^i_j}\}| \tag{8}$$

From Hamming distance and bit-strings length the BER of a single realization at time i is computed. Finally, the BER metric is defined as the expected value $\mathbf{E}$ over all single observation BERs as shown in Eq. (10).

$$BER_i = \frac{e_i}{|b_{X^i}|} = \frac{e_i}{|b_{Y^i}|} \tag{9}$$

$$BER = \mathbf{E}[BER_i] \tag{10}$$

The optimal case would be $BER = 0$, which is unachievable due to the noisy nature of the physical measurements.

III. Achieving Blind Synchronization

A. Requirements

In this section we will define the requirements for an appropriate solution.

Our analysis of common as well as state-of-the-art approaches showed, that in the worst case, i.e the worst analyzed scenario, the best of these approaches only achieves $\Delta^0(MR) = 0.49$. This means, that none of the traditional and modern approaches achieves optimal synchronization in more the 49% of the observed CIRs. To visualize the reasons for this lacking performance, Fig. 2 shows two examples in which the straight forward approaches fail and their respective causes: First, the existence of multiple local maxima within the first arriving cluster with non-reciprocal amplitude differences (Fig. 2(b)), where it causes synchronization errors for maximum based approach. Second, non strictly monotonous increasing first edges (Fig. 2(c)), which are especially hard for leading edge detection algorithms.

In relation to the described error causes, an optimal algorithm would expose 2 major properties:

Uniqueness A single data point within an observation needs to be identified, which thereupon acts as this CIRs anchor for synchronization.

Robustness The same unique time anchor needs to be identified in the reciprocal measurements, irregardless of noise and interference.

An explicit non-requirement is the preservation of edges. Since the error cause in Fig. 2(c) are superfluous edges in the leading edge, it is not necessary to preserve such artifacts. Even more, the removal of such interference based edges would be favorable. In consequence, this non-requirement rules out filtering solution, which

aim for perfect waveform structure preservation, e.g. wavelet filtering [20].

Finally, we disregard solutions which exchange information about the received CIRs. Although they might exhibit good performance, following the argumentation in Sec. II-A surplus information exchange about the CIR should be avoided due to information leakage towards the attacker.

B. Solution

The two major requirements for the solution will be achieved by the following means.

Uniqueness can be achieved by selecting the global maximum of a given signal. As shown in Sec. III, this approach alone does not perform well, since it is lacking *robustness*. Hence, we propose to combine it with an algorithm which provides this second requirement.

The *robustness* property can be achieved through two approaches: The first approach is the application of *noise reduction*. This can be realized by employing classical digital FIR filters like Butterworth or Chebyshev filters in low- or band-pass mode [15]. Although, they are very powerful, they need careful fine-tuning regarding the transmission properties, e.g. baseband and bandwidth.

The second approach, what we are proposing, is the usage of blurring or smoothing filters originating from image processing. These have the advantage of independence of transmission properties. Additionally, they fulfill the requirements from Sec III — through the application of such filters with appropriate parameters, the noisy artifacts of the signal can be eradicated.

Due to their proven strong performance in the fields of image noise reduction and image edge detection [3], as well as signal processing for localization [12], [5], we propose to use a one dimensional Gaussian filter for the time synchronization.

According to the system model the single CIR are vectors of values. Hence, we apply a *one dimensional* Gaussian filter to this signal, which is defined as:

$$G_{1D}(x) = \frac{1}{\sqrt{2\pi\sigma}}\, exp(-x^2/2\sigma^2) \qquad (11)$$

By applying this filter to the single CIRs, a unique synchronization anchor can be identified by taking the maximum of the resulting filtered signal.

Fig. 3 shows the CIR of Fig. 2 after applying a Gaussian 1D filtering. It depicts that the filter successfully removed the aforementioned major error causes.

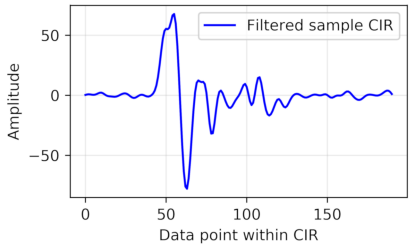


Fig. 3. Sample CIR from Fig. 2(a) after Gaussian 1D filter.

IV. Evaluation

We are interested in both the performance and robustness of our approach compared to alternative solutions. Employing the metrics as introduced in Sec. II, we assess to which extent it independently identifies identical anchors in corresponding Channel Impulse Response observations.

We set out to evaluate all alternatives on a large dataset we acquired in an extensive measurement campaign. It resembles a characteristic office scenario, considering two static terminals representing Alice and Bob, and with static or mobile sources of interference. The measurements are representative only for the given rather specific scenario. For a broader evaluation of the robustness we hence subsequently evaluate all approaches on synthetic data, generated with accepted UWB models from literature and simulating broad ranges of interference.

We finally evaluate the impact of the improved synchronization for the actual CRKG case, comparing the achieved bit error rate (BER) after quantization with algorithms tailored to key generation [19].

A. Compared approaches

While synchronization in CRKG has not been addressed, there exist alternative solutions for time calibration. We apply these approaches to the same data sets for comparison.

A simple maximum detection (*MAX*) and state of the art leading-edge detection mechanisms (*LED*, and *MR*)[14], [11] are used as baselines.

In addition, we compare our one-dimensional Gaussian filter to other, more complex digital FIR filters, for which we choose Butterworth and Chebyshev Type II filters, both realized as low-pass and band-pass, as representative candidates. These filters as parameterized to the acquired real world measurements — additionally, low and high cut frequencies as well as the filter order were determined manually to minimze $1 - \Delta^0$.

To assess the difference between Gaussian and other smoothing filters, we also compare to moving average

TABLE II
SOLUTION PERFORMANCE IN DIFFERENT PHYSICAL SCENARIOS

Algorithm	Δ^0 and (μ, σ) of Δ						
	Scenarios						
	IA	IB	IC	SA	SB	SC	SD
MAX	0.61 (0.19, 1.20)	0.65 (0.57, 2.74)	0.56 (0.09, 0.65)	0.64 (-0.00, 0.59)	0.66 (0.10, 0.57)	0.59 (0.00, 0.63)	0.69 (0.05, 0.96)
LED	0.69 (0.04, 0.61)	0.67 (-0.54, 9.25)	0.59 (0.12, 10.19)	0.61 (-0.60, 9.52)	0.59 (1.15, 18.1)	0.56 (0.45, 12.11)	0.56 (0.64, 14.06)
MR	0.82 (0.06, 0.41)	0.74 (-0.04, 0.62)	0.82 (0.09, 0.40)	0.83 (0.07, 0.39)	0.77 (0.10, 0.46)	0.85 (0.07, 0.38)	0.81 (0.09, 0.42)
Butterworth Low	0.61 (0.20, 1.21)	0.65 (0.57, 2.74)	0.57 (0.10, 0.65)	0.65 (-0.01, 0.59)	0.66 (0.11, 0.57)	0.60 (0.01, 0.64)	0.70 (0.06, 0.96)
Butterworth Band	0.87 (0.38, 3.41)	0.77 (0.02, 1.95)	0.93 (0.00, 0.25)	**0.96 (0.00, 0.18)**	**0.91 (-0.00, 0.29)**	**0.92 (0.01, 0.27)**	0.92 (0.13, 0.82)
Cheby2 Low	0.83 (0.17, 0.81)	0.76 (0.37, 1.89)	0.93 (0.13, 0.81)	0.95 (0.04, 0.21)	0.87 (0.09, 0.45)	0.91 (0.06, 0.30)	0.79 (0.98, 2.55)
Cheby2 Band	0.88 (0.04, 0.78)	0.77 (0.38, 1.66)	0.93 (0.05, 0.25)	**0.96 (0.01, 0.18)**	**0.91 (0.00, 0.29)**	0.91 (0.01, 0.29)	**0.95 (0.03, 0.20)**
Uniform	0.80 (0.24, 1.33)	0.72 (0.38, 1.87)	0.91 (0.10, 0.47)	0.90 (0.04, 0.30)	0.88 (0.03, 0.33)	0.89 (0.05, 0.31)	0.68 (0.95, 1.98)
Hilbert	0.61 (0.19, 1.20)	0.65 (0.57, 2.74)	0.56 (0.09, 0.65)	0.64 (-0.00, 0.59)	0.66 (0.10, 0.57)	0.59 (0.00, 0.63)	0.69 (0.05, 0.96)
SavGol	0.82 (0.16, 0.87)	0.76 (0.18, 1.20)	0.91 (0.10, 0.47)	**0.96 (0.02, 0.18)**	0.86 (0.07, 0.35)	0.89 (0.08, 0.32)	0.90 (0.12, 0.93)
Sobel	0.42 (0.27, 2.90)	0.34 (0.10, 5.08)	0.39 (0.16, 2.26)	0.43 (0.14, 2.42)	0.34 (0.78, 6.17)	0.41 (0.01, 2.06)	0.28 (0.01, 6.31)
Wiener	0.64 (0.20, 1.19)	0.66 (0.38, 1.76)	0.57 (0.10, 0.64)	0.66 (0.01, 0.58)	0.72 (0.10, 0.51)	0.62 (0.00, 0.61)	0.76 (0.07, 0.92)
Spline Interpolation	0.77 (0.61, 2.06)	0.67 (0.57, 2.28)	0.85 (0.27, 1.06)	0.65 (0.92, 2.07)	0.78 (0.10, 0.45)	0.80 (0.51, 1.50)	0.76 (0.43, 1.63)
Gaussian 1D	**0.90 (0.12, 1.54)**	**0.78 (0.13, 1.39)**	**0.94 (0.00, 0.23)**	**0.96 (0.01, 0.19)**	**0.91 (0.03, 0.29)**	**0.92 (0.02, 0.27)**	0.93 (0.04, 0.26)

or one dimensional uniform filter, Savitzky-Golay filter, Sobel filter, Hilbert filter, Wiener filter, and the spline interpolation. Again, the respective algorithm parameters are determined a priori, to optimize their performance with respect to $1 - \Delta^0$.

B. Real World Measurements

To compare the different approaches in terms of performance, we used data from previous real world measurements of realistic communication scenarios [19]. These scenarios were designed to resemble communication situations in typical office environments.

The first set of scenarios realizes static patterns — Alice and Bob are stationary within an office environment, with an additional stationary source of interference (3rd terminal). Four different positions in the room were evaluated, where the respective measurements are called *static A,..., static D* (SA, SB, SC, SD). Additionally, three scenarios incorporate movement for additional interference: First, the 3rd terminal moves randomly in the room; Second, it continuously crosses the line-of-sight (LOS) of Alice and Bob perpendicularly; Third, it moves *on* the LOS between Alice and Bob. The respective cases are called *interference A, B, C* (IA, IB, IC).

Within these scenarios, the measurements were conducted in the following manner: Two wireless terminals are measuring the CIR using UWB signal of 500 MHz bandwidth in the 4 GHz band. Alice and Bob transmit messages under LOS conditions in a typical office environment. After receiving a signal, the respective CIR is estimated. Both terminals are stationary and placed five meters apart. The receivers are placed 1 m above ground to ensure optimal transmission quality. Alice and Bob transmit messages every 370 ms, generating 6 CIRs per second. Single measurements consist of 200 data points. In our hardware, the sample interval is 1 ns, which allows detection of multipath components with a spatial resolution of 30 cm. The resolution of the ADC is 12 bit and is implemented with COTS components.

C. Synthetic Impulse Responses

To test for robustness, we also generate synthetic input data of a broader range of potential scenarios.

The basis for these synthetic data is the IEEE 802.15 UWB channel model as presented in [6], which is a slight modification of the Saleh-Valenzuela UWB model [16]. In addition to the channel model itself, [6] also defines 3 parameter sets for typical indoor UWB propagation. The first parameter set represents a strong LOS scenario, whereas the second and third models describe typical NLOS setups. Finally, a fourth parameter set is defined, which is artificially generated and tries to resemble an extreme non-line-of-sight (NLOS) case.

Since the model does not support the generation of correlated measurements, we adapted it to support this in the following manner: In accordance with the channel model described in Sec. II, the correlated observations were realized by adding two different realizations of independent AWGN to a single observation. This allows us to generate highly correlated observations X_i and Y_i, to also include edge cases, as described in Sec. III

Since the main task of the approaches is time synchronization, an additional time offset was added to one of the generated observations. Theoretically, the value of

TABLE III
SOLUTION PERFORMANCE IN DIFFERENT SYNTHETIC SCENARIOS

Algorithm	Δ^0 and (μ, σ) of Δ			
	Saleh-Valenzuela Models			
	Model 1	Model 2	Model 3	Model 4
MAX	0.50 (0.01, 3.47)	0.42 (-0.03, 5.96)	0.36 (0.53, 9.63)	0.36 (0.23,16.37)
LED	0.76 (0.04, 1.26)	0.66 (0.02, 1.80)	0.61 (-0.11,12.12)	0.49 (0.18,13.01)
MR	**0.88 (-0.03, 1.37)**	0.77 (0.16, 5.56)	0.62 (0.46,12.38)	0.44 (-0.03,17.11)
Butterworht Low	0.47 (-0.05, 4.33)	0.40 (0.01, 6.20)	0.41 (-0.22, 9.27)	0.36 (0.23,16.37)
Butterworth Band	0.56 (0.15, 3.79)	0.46 (-0.08, 5.42)	0.42 (0.47,10.36)	0.37 (0.29,17.73)
Cheby2 Low	0.53 (-0.03, 3.12)	0.45 (0.06, 5.71)	0.40 (0.24, 9.24)	0.38 (0.19,15.57)
Cheby2 Band	0.54 (0.21, 4.36)	0.46 (0.21, 6.16)	0.41 (-0.01,10.87)	0.38 (0.77,16.31)
Uniform	0.68 (-0.08, 2.42)	0.49 (-0.01, 4.84)	0.46 (0.05, 8.26)	0.43 (-0.26,13.59)
Hilbert	0.50 (0.01, 3.47)	0.42 (-0.03, 5.96)	0.36 (0.53, 9.63)	0.36 (0.23,16.37)
SavGol	0.83 (0.02, 2.30)	0.59 (0.90, 2.69)	0.55 (0.32, 7.86)	0.49 (-0.42,15.17)
Sobel	0.33 (0.24, 8.57)	0.27 (-0.34, 9.39)	0.27 (-0.17,16.85)	0.26 (-0.90,22.32)
Wiener	0.51 (-0.02, 3.29)	0.42 (0.05, 5.67)	0.38 (0.27, 9.18)	0.37 (0.14,13.88)
Spline Interpolation	0.50 (0.01, 3.47)	0.42 (-0.03, 5.96)	0.36 (0.53, 9.63)	0.36 (0.23,16.37)
Gaussian 1D	0.86 (0.45, 11.61)	**0.83 (-0.01, 15.72)**	**0.82 (-0.21,11.27)**	**0.80 (-0.82,16.49)**

this offset does not matter, since the algorithms identify the unique data points within a single realization as anchors. This means, they do not have a global view on both realizations and thereby the actual time offset is irrelevant. It would suffice to show that the approach identifies the same data point in both observations, to demonstrate their feasibility. But to keep the results comparable to the real world, we added similar offsets between the two observations.

Analyzing the real world data indicated typical offsets in $t \sim \mathcal{N}(8.3, 11.4)$. We hence used this distribution to generate artificial offsets in the synthetic data.

D. Results

Table II shows the performance of all solutions, the results of our Gaussian filter are shown in the last row. Superior results are highlighted for each scenario. Our Gaussian filter outperforms all other approaches in all but one scenarios.

Only in scenario SD, the manually optimized Chebyshev band-pass performs slightly better (0.95/0.93). Two band-pass approaches (Butterworth Band and Chebyshev Band) fare equally well in the other static scenarios.

In the dynamic scenarios with interference, which are most relevant to the CRKG problem, our Gaussian filter performs better than all competing algorithms with advantages up to 13%, even over the *best* baseline approach with global knowledge.

It is also the most robust approach with consistently high performance across all different measurement scenarios.

A similar comparison of the performance of all solutions for the synthetically generated CIRs is presented in Tab. III. Again, the new approach shows highest robustness, outperforming all others in all but one model.

By recalling the model setup of Model 1 is clear, why the simple leading edge detection algorithm is slightly better in this single case: Model 1 represents a strong LOS channel, as described in [6], which is characterized by a strong first cluster in the CIR. This is distinguished by an unusually strong leading edge, which is also strictly monotonously rising. These two properties are highly advantageous for leading edge detection algorithms. Nevertheless, the Gaussian 1D approach still performs almost on par, even in this case (0.88/0.86).

For the generic NLOS models, our Gaussian filter again significantly outperforms all other approaches, with advantages of up to 31% over the *second best* approach.

In conclusion, the Gaussian 1D approach delivers best results in most cases: it comes in second only for two scenarios that have minor relevance for CRKG, achieving almost identical performance with the respective winner. It achieved optimal synchronization for over 90% of the comparisons in measured datasets, and for over 80% even of the synthetic inputs simulating artificially bad conditions. This consistent good performance indicates a good general applicability, since it performs stable and robust under a broad variety of potential settings.

Fig. 4 shows the bit error rates when applying our filter before quantization according to CRKG. While the BER remains high for all scenarios, the results clearly

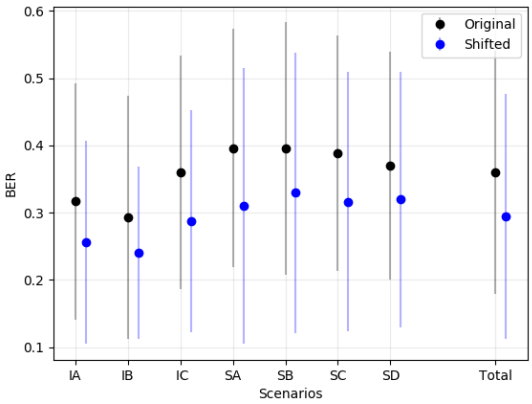


Fig. 4. Improved BER after application of the proposed algorithm.

demonstrate the benefit of applying our approach: Single improvements reach up to 21% reduction in BER, averaging over all obtained measurements the improvement exceeds 18%.

This resulting BER over the total measurements verifies that the slightly higher standard deviation our approach exhibits has no significant influence on the final performance.

V. Summary and Conclusion

In this paper we showed the importance of synchronization of channel impulse responses for Channel Reciprocity-based Key Generation (CRKG). Here, synchronization has to be *blind*: performed local without communicating details of measurements to the peer, to avoid leaking sensitive details to any adversary. This rules out several intuitive solutions, and optimizations according to current environments and settings.

We first analyzed the characteristics of the problem, developed methods and metrics to assess possible solutions, and suggested the application of a Gaussian 1D filter to help uniquely identify anchors in the CIR observations for blind synchronization.

To evaluate our scheme, we exposed it to real world- and synthetically generated observations of realistic to extremely adverse settings. Both resemble different CRKG scenarios, the latter are based on the statistical IEEE UWB channel model.

The results from all scenarios underline the superiority of our approach. It achieves synchronization rates that are better, or at least on par, even with manually optimized, non-blind solutions throughout all scenarios, which underlines its robustness. The improvement reaches 31% over the second best approach, which yields a BER reduction of 18% on average after quantization.

We are currently integrating the Gaussian 1D filters into an overall CRKG implementation, to evaluate the impact on the final key generation rate.

References

[1] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, 1993.

[2] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[3] G. Deng and L. W. Cahill, "An adaptive gaussian filter for noise reduction and edge detection," in *IEEE Conf. Record Nuclear Science Symposium and Medical Imaging Conference*, 1993.

[4] Y. El Hajj Shehadeh, O. Alfandi, K. Tout, and D. Hogrefe, "Intelligent mechanisms for key generation from multipath wireless channels," in *Wireless Telecommunications Symposium*, 2011.

[5] B. Etzlinger and H. Wymeersch, *Synchronization and Localization in Wireless Networks*. now, 2018.

[6] J. Foerster, "Channel modeling sub-committee report final," *IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)*, 2003.

[7] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.

[8] C. S. F. Huth, "Physical-layer security architectures for the internet of things," Ph.D. dissertation, Ruhr University Bochum, Germany, 2018.

[9] W. C. Jakes and D. C. Cox, *Microwave mobile communications*. Wiley-IEEE Press, 1994.

[10] H. Koorapaty, A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *Comm. Letters, IEEE*, 2000.

[11] M. J. Kuhn, J. Turnmire, M. R. Mahfouz, and A. E. Fathy, "Adaptive leading-edge detection in UWB indoor localization," in *Radio and Wireless Symposium*, 2010.

[12] R. K. Mahapatra and N. S. V. Shet, "Localization Based on RSSI Exploiting Gaussian and Averaging Filter in Wireless Sensor Network," *Arabian Journal for Science and Engineering*, 2018.

[13] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. on Information Theory*, vol. 39, no. 3, 1993.

[14] B. Merkl, "The Future of the Operating Room: Surgical Preplanning and Navigation using High Accuracy Ultra-Wideband Positioning and Advanced Bone Measurement," Ph.D. dissertation, University of Tennessee, 2008.

[15] T. Parks and C. Burrus, *Digital Filter Design. Topics in Digital Signal Processing*. John Wiley & Sons, New York, 1987.

[16] A. Saleh and R. Valenzuela, "A statistical model for indoor multipath propagation," *IEEE Journal on selected areas in communications*, vol. 5, no. 2, 1987.

[17] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *2008 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2008.

[18] Y.-S. Shiu *et al.*, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, 2011.

[19] P. Walther, C. Janda, E. Franz, M. Pelka, H. Hellbrück, T. Strufe, and E. Jorswieck, "Improving quantization for channel reciprocity based key generation," in *LCN*, 2018.

[20] A. B. Wiltschko, G. J. Gage, and J. D. Berke, "Wavelet filtering before spike detection preserves waveform shape and enhances single-unit discrimination," *Jrnl of Neurosci. Methods*, 2008.

[21] C. T. Zenger *et al.*, "Exploiting the Physical Environment for Securing the Internet of Things," in *New Security Paradigms Workshop*, 2015.

[22] ——, "Authenticated key establishment for low-resource devices exploiting correlated random channels," *Computer Networks*, 2016.