Intelligent Reflecting Surface-Assisted Wireless Key Generation for Low-Entropy Environments

Paul Staat[1], Harald Elders-Boll[2], Markus Heinrichs[2],
Rainer Kronberger[2], Christian Zenger[3,4], and Christof Paar[1]

[1]Max Planck Institute for Security and Privacy, Bochum, Germany
[2]TH Köln – University of Applied Sciences, Cologne, Germany
[3]PHYSEC GmbH, Bochum, Germany
[4]Ruhr University Bochum, Germany

Abstract—**Physical layer key generation is a promising candidate for cryptographic key establishment between two wireless communication parties. It offers information-theoretic security and is an attractive alternative to public-key techniques. Here, the inherent randomness of wireless radio channels is used as a shared entropy source to generate cryptographic key material. However, practical implementations often suffer from static channel conditions which exhibit a limited amount of randomness. In the past, considerable research efforts have been made to address this fundamental limitation. However, current solutions are not generic or require dedicated hardware extensions such as reconfigurable antennas. In this paper, we propose a novel wireless key generation architecture based on randomized channel responses from an intelligent reflecting surface (IRS). Due to its passive nature, a cooperative IRS is well-suited to provide randomness for conventional resource-constrained radios. We conduct the first practical studies to successfully demonstrate IRS-based physical-layer key generation with an OFDM system. In a static environment, using a single subcarrier only, our IRS-assisted prototype system achieves a key generation rate (KGR) of $97.39\,\mathrm{bps}$ with $6.5\,\%$ key disagreement rate (KDR) after quantization, while passing standard randomness tests.**

I. Introduction

Pervasive wireless networks such as used for IoT systems, are a central aspect of today's connected world and must be thoroughly protected against attacks. In this context, symmetric encryption schemes such as AES play an important role for providing confidentiality as well as message integrity and authentication. However, this requires a key exchange mechanism.

As an alternative to classical public-key techniques for secret sharing over public channels such as the wireless radio channel, significant research efforts have been devoted to primitives from the realm of physical layer security (PLS) [7]. In particular, channel reciprocity-based key generation (CRKG) leverages randomly behaving wireless radio channels to establish shared cryptographic keys to achieve information-theoretic security.

Despite the large body of work exploring CRKG in recent years [17], the acceptance for real-world deployment is rather low as the performance of CRKG is tied to the wireless channel conditions. For instance, static radio channels can only provide a limited amount of entropy and substantially impede

the key generation process: Establishing sufficiently random keys is impractically time-consuming at low key generation rates. This issue affects a wide range of wireless applications with limited mobility, i.e., where channel conditions tend to be static. Examples include warehouses, enclosures, and at night also many other indoor environments.

The ability to work properly in static environments has been outlined as one of the major challenges for physical-layer key generation [17]. Therefore, several previous works investigate approaches to tackle static channel conditions, e. g., reconfigurable antennas, jamming, and beamforming [1], [6], [17]. However, none of them is generically applicable to existing CRKG systems as dedicated hardware extensions or special modulation schemes are required. This is a serious hurdle for the wide-range adoption of the technology, especially for low-resource devices such as found in many IoT systems, for which CRKG in general is desirable.

In this paper we pursue a generic solution based on an intelligent reflecting surface (IRS) to enable CRKG in static environments for arbitrary devices while being compatible with existing CRKG implementations. Here, the IRS serves as an entropy source for the wireless channel, offering an entirely new range of applications for future IRS deployments.

The IRS concept has evolved from research on metamaterials, which are synthetic structures with tailored EM characteristics to realize non-standard wave manipulation capabilities. Cost-effective digitally tunable and flat metamaterial variants paved the way for IRS to become attractive for future communication systems beyond 5G. It has gained significant research interest [2] due to its innovative nature: Adding control to the wireless propagation environment, the IRS enables what is coined *smart radio environments*. The IRS intelligently interacts with radio waves in an entirely passive manner with moderate hardware complexity and low energy consumption.

In the context of this work, we use a cooperative IRS to diminish static channel conditions, assisting CRKG. In particular, we deliberately randomize the wireless channel and generate temporal variation to provide an entropy source which is independent of user terminals. We implement a prototype system using commodity Wi-Fi transceivers and low-complexity IRS prototypes operating in the $5\,\mathrm{GHz}$ fre-

quency range. A key characteristic of our approach is that we consider the wireless channel to provide an additional degree of freedom when designing a wireless key generation system. To the best of our knowledge, this is the first work to implement a practical CRKG system incorporating an IRS. The paper at hand contains the following key contributions:

- We propose physical layer key generation assisted by an IRS to overcome otherwise static propagation environments. Our approach addresses critical real-world requirements of low-resource CRKG systems.
- We show that IRS-assisted CRKG can achieve arbitrary and adjustable key generation rates, while ensuring random key material. Further, we introduce a channel oversampling technique to reduce bit mismatch in the generated key material.
- We implement a functional proof-of-concept system based on low-cost IRS prototypes and commodity MIMO radio transceivers. We present a comprehensive evaluation based on measurements, showing that IRS-assisted CRKG is practically feasible.

II. BACKGROUND

A. Channel Reciprocity-Based Key Generation

The fundamental principles of *channel reciprocity* and *spatial decorrelation* [5] allow to exploit the wireless channel as a mutual keying variable, i. e., for CRKG. Secret key agreement over authenticated two-way public channels from dependent random variables has been pioneered by Maurer [12]. Since then, much work has dealt with practice-oriented wireless CRKG protocols, including prominent examples by Mathur et al. [11], Patwari et al. [11], and Aono et al. [1]. These protocols follow the same rationale: In a first step, the two participants exchange a series of messages to collect channel measurements, e. g., received signal strength (RSS) or channel state information (CSI). Then, a quantization stage maps the channel observations to bits, producing correlated bit sequences K^A and K^B at both nodes. An error correcting code is used for information reconciliation, i. e., to combat bit mismatch. Finally, privacy amplification (via hashing) removes information that has leaked during the exchange of helper data for error correction. Important metrics for CRKG systems include the similarity of channel observations at both ends (e. g., mutual information and correlation measures), the key generation rate (KGR), and the key disagreement rate (KDR).

Most of the current CRKG schemes gather data from time-variant channels and were designed under the assumption of user movement and random channel variation and in view of statistical channel models such as Rayleigh fading. However, these schemes fail to work with static radio channels. Previous solutions to combat static channels come at the cost of significantly increased complexity: For instance, [1] leverages an electronically steerable antenna, while [6] describes a jamming-based technique.

B. Intelligent Reflecting Surface

An IRS, sometimes also referred to metasurface in the literature, is a man-made planar structure with digitally controllable electromagnetic reflection behavior. The IRS adds control to the propagation of radio waves and thereby can optimize wireless radio channels. IRS' are sometimes considered a paradigm shift towards *smart radio environments* [10] and are already in discussion for future communication networks beyond 5G [2].

The IRS has potential for innovation at relatively low hardware complexity. Typically fabricated in microstrip technology on low-cost printed circuit board (PCB) substrate, the IRS consists of many individually tunable reflector elements. For instance, the IRS controller can adjust the phase shift of reflections across the surface to optimize the signal-to-noise ratio (SNR) at a receiver [2] or to enhance spatial diversity [4]. Due to the mostly passive and reflecting nature, the IRS does not require active RF chains and is inherently capable of full duplex operation, while being energy efficient.

In the PLS context, previous work with IRS addressed degradation of the eavesdropper's channel, e. g., from exclusion [10]. For CRKG, [9] has outlined an IRS-assisted approach to reduce information leakage to the eavesdropper.

C. System and Adversary Model

In this work, we consider two legitimate parties Alice and Bob who seek to establish a shared cryptographic key. Alice and Bob deploy a standard time-divison duplex (TDD) wireless communication protocol, e. g., IEEE 802.11n Wi-Fi with orthogonal frequency-division multiplexing (OFDM), and obtain CSI as an essential part of their communication. Using their respective CSI data, both parties implement a CRKG procedure. Furthermore, we assume that a passive IRS is within reach of Alice and/or Bob and thus can partially control the wireless propagation channel. The passive eavesdropper Eve can capture messages sent by Alice and Bob and also obtains CSI, representing the effective channels between Eve and the legitimate parties Alice and Bob, respectively. Eve is aware of the key generation procedure of Alice and Bob and thus can derive own key material.

All parties operate in a normally static indoor environment, i. e., the parties do not move, nor do objects in the environment. Hence, the environment does not contribute to temporal variation and thus exhibits a limited amount of randomness. We assume the passive IRS to be the only source of channel variation.

III. IRS-ASSISTED KEY GENERATION

Our IRS-assisted CRKG scheme follows a standard architecture which includes channel probing, quantization, information reconciliation, and privacy amplification stages. The key difference of our scheme is the channel probing which is performed in conjunction with a channel randomization step from the IRS (see Fig. 1). We review the protocol initiation, channel randomization and probing, synchronization, and quantization steps. We do not elaborate on information reconciliation
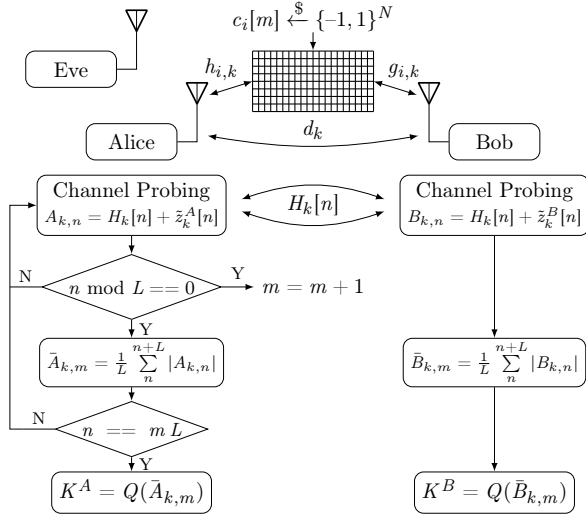
Fig. 1. Key generation procedure assisted by an IRS.

and privacy amplification since well-known approaches from literature can be used [3].

1) Initiation: During protocol initiation, the nodes and the IRS exchange the timing for channel probing, the total number of surface configurations m, and the oversampling factor L. The latter determines the number of bidirectional samples per surface configuration. In addition, the nodes can verify the IRS' channel impact.

2) Channel Randomization: The generalized reflection co-efficients for the N-element IRS can be expressed as:

$$\phi_i[n] = \alpha_i e^{j\varphi_i[n]} = c_i[n] \qquad i = 1, ..., N \qquad (1)$$

where $\alpha_i = 1$. In the context of this work, we consider a binary-tunable IRS with 1-bit phase control per element, restricting $\varphi_i \in \{0, \pi\}$. Hence, we can substitute $\phi_i[n]$ with the surface control signal $c_i[n] \in \{-1, 1\}^N$.

Since the prototype system is implemented by a set of com-mercial off-the-shelf Wi-Fi Network Interface Cards (NICs), we assume that the complex OFDM baseband signal transmit-ted by Alice is generated by taking the inverse discrete Fourier transform of the complex modulated data symbols $X_k^A[n]$ of all K, $k = 0, \ldots, K - 1$, subcarriers of the nth OFDM symbol. In the time domain, a cyclic prefix, which is assumed to be longer than the channel's maximum delay spread, is then prepended to each OFDM symbol. Then, after time- and frequency synchronization, removal of the cyclic prefix and discrete Fourier transform, the received baseband signal of Bob corresponding to the kth subcarrier of the nth OFDM symbol in the frequency domain is given by:

$$Y_k^B[n] = \left(\sum_{i=0}^{N} h_{i,k} c_i[n] g_{i,k} + d_k\right) X_k^A[n] + z_k^B[n], \quad (2)$$

where $h_{i,k}, g_{i,k}, d_k \in \mathbb{C}$, respectively, are the complex channel gains of the link between Alice and the ith IRS element, Bob and the ith IRS element, the direct link between Alice and

Bob for the kth subcarrier, and $z_k^B[n] \sim \mathcal{CN}(0, \sigma^2)$ is additive white Gaussian noise (AWGN). As all links are reciprocal, the received baseband signal $Y_k^A[n]$ of Alice can be noted in the same manner by exchanging A and B in (2). For CRKG, we are interested in the effective channel

$$H_k[n] = \sum_{i=0}^{N} h_{i,k} c_i[n] g_{i,k} + d_k. \qquad (3)$$

We assume that the surface configurations $c_i[n]$ are selected randomly. From the central limit theorem, we gain a first insight into the effectiveness of the IRS for channel random-ization: If the surface is sufficiently large, i.e., $N \gg 1$, $H_k[n]$ converges to a complex normal distribution with variance linearly scaling with N.

3) Channel Probing: During channel probing, Alice and Bob exchange packets in a ping-pong manner. At the receiver side, Alice and Bob use a standard Least-Squares (LS) channel estimator to obtain CSI:

$$\hat{H}_k^A[n] = \frac{Y_k^A[n]}{X_k^B[n]} = H_k[n] + \frac{z_k^A[n]}{X_k^B[n]} = H_k[n] + \tilde{z}_k^A[n], \quad (4)$$

$$\hat{H}_k^B[n] = \frac{Y_k^B[n]}{X_k^A[n]} = H_k[n] + \frac{z_k^B[n]}{X_k^A[n]} = H_k[n] + \tilde{z}_k^B[n]. \quad (5)$$

Note that we assume the IRS to be the only source of channel variation. As the IRS switches channel states, Alice and Bob effectively observe a static channel during one IRS configuration period. Thus, averaging over L consecutive samples obtained per IRS configuration can help Alice and Bob to reduce noise components (see Fig. 1).

4) Synchronization: The nodes are either aware of or can alternatively measure the IRS modulation frequency. The latter is possible since the IRS modulates the channel response periodically (cf. Fig. 3 (a)). Then, Alice and Bob can time-align their channel probing to coarsely match the IRS timing. Naturally, the ping-pong packet exchange needs to be shorter than the IRS update interval. This step may also be performed as part of the protocol initiation.

5) Quantization: A quantization stage maps Alice' and Bob's channel observations to bits to derive key material from channel measurements. As input to the quantizer, we use a series of m samples for a fixed single subcarrier k. Each of the m samples is obtained from averaging over L consecutive normalized magnitude channel estimates (see Fig. 3 (b)). Due to its simplicity and equiprobable output, we here use a cumulative distribution function (CDF)-based quantization scheme with gray coding from the literature [13].

IV. PROTOTYPE IMPLEMENTATION

We now describe our prototype system consisting of an IRS and commodity Wi-Fi transceivers.

1) IRS prototype: We use two low-cost IRS prototypes with 64 binary-phase tunable elements each, offering $2^{128} \approx 3.4 \times 10^{38}$ surface configurations. One IRS consists of structurally identical elements that are arranged in an 8×8 array on
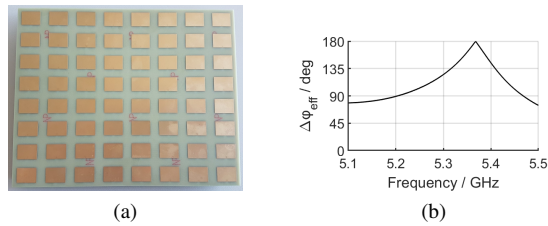
Fig. 2. Intelligent reflecting surface prototype. (a) Front view with patch elements (20 cm x 16 cm). (b) Unit cell phase response.
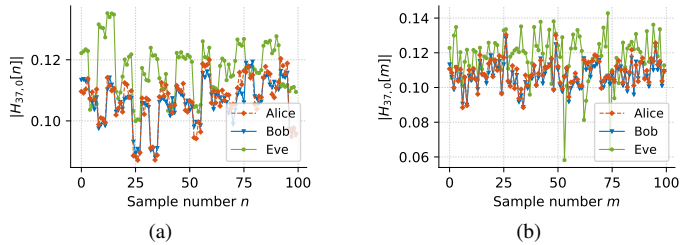

Fig. 3. Time domain samples taken by Alice, Bob, and Eve on the exemplary subcarrier $k = 37$ of spatial channel $j = 0$. (a) Raw signals with $L = 4$. (b) Signals after downsampling from block averaging.
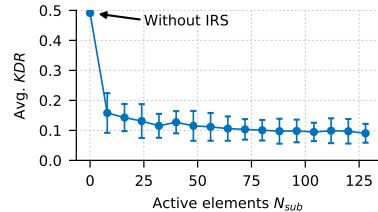
standard FR4 PCB substrate (see Fig. 2 (a)). The elements are linearly polarized rectangular patch reflectors on top of a ground plane. The resonance frequency of the elements can be individually switched using a PIN diode to shift the phase response. Each element has a power consumption of approximately $1.5\,\mathrm{mW}$ when the corresponding PIN diode is switched on, resulting in an average power consumption of $0.75\,\mathrm{mW}$ per element for randomized configurations. The IRS is configured by a conventional microcontroller with shift registers.

To obtain the maximum phase alteration, the reflection factor of the IRS is measured under the two extreme conditions when all elements are switched on and off. The measured phase difference of the IRS prototype is shown in Fig. 2 (b) and is by definition limited to the range of $0°$ to $180°$. The measurements were taken with the direction of both the incident wave and the reflected wave perpendicular to the IRS.

In our experimental setup, we synchronize the node's packet exchange and the surface configuration timing. We use the ISAAC pseudorandom number generator (PRNG) [8] seeded from /dev/random [15] to generate random surface configurations $c_i[n]$. The configurations should be erased and remain secret to prevent environment reconstruction attacks.

2) Wi-Fi NICs: In our prototype system, each party Alice, Bob, and Eve consists of a single-board computer equipped with an ath9k-based PCIe NIC [16] for IEEE 802.11n Wi-Fi in a 2x2 MIMO configuration, using off-the-shelf linearly polarized Wi-Fi antennas. The participants transmit at $5\,\mathrm{dBm}$ and allocate a $40\,\mathrm{MHz}$ wide channel at $5{,}300\,\mathrm{MHz}$ (Wi-Fi channel 60), close to the IRS' optimum operation frequency. During channel probing, the devices rapidly exchange packets in a ping-pong manner. For each packet and spatial MIMO channel, we obtain a complex vector containing the CSI data for each of the 114 non-zero OFDM subcarriers. Extending (4) and (5), we denote them as $\hat{H}_{k,j}^A$ and $\hat{H}_{k,j}^B$, with the jth entry in the MIMO channel matrix.

V. PERFORMANCE EVALUATION

We now present measurement results from experiments with our prototype IRS-assisted key generation system.

A. Number of Active Elements

From (3), we expect the effectiveness of channel randomization to scale with the IRS size, i.e., the number of elements N. Intuitively, a large IRS increases the likelihood that a portion of

Fig. 4. KDR against the number of active IRS elements N_{sub} with indication of mean and standard deviation.

the transmitted signal falls on the surface to affect the channel between Alice and Bob. Furthermore, as N increases, more clearly distinctive channel states will be available.

To investigate the impact of N, we randomly select N_{sub} elements from the surface to be used for $m = 10000$ random configurations. The remaining $128 - N_{sub}$ elements are configured randomly but remain static. For all configurations, we measure the channels $\hat{H}_{k,j}^A[n]$ and $\hat{H}_{k,j}^B[n]$ with Alice and Bob $3\,\mathrm{m}$ and $1.5\,\mathrm{m}$ apart from the IRS. Then, we derive keys K^A and K^B for each subcarrier and spatial channel and calculate the KDR as the number of bit errors N_e per N_K key bits. As expected, the KDR decreases with increasing N_{sub} as shown in Fig. 4. Note that we have also included $N_{sub} = 0$ as a special case where the IRS remains static. Here, it is evident from the KDR of approximately 50% that key generation is infeasible in the static environment, i.e., without the IRS.

B. Distance Variation

We evaluate IRS-assisted CRKG under varying distances of Alice and Bob to the IRS and for multiple distances of Eve to Alice. Therefore, we conduct experiments in the basement of our institute building, which is a long-term static environment.
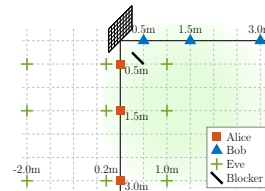

Fig. 5. Floorplan of the measurement setup indicating the relative positions of the parties and the approximate area of IRS radiation (green).
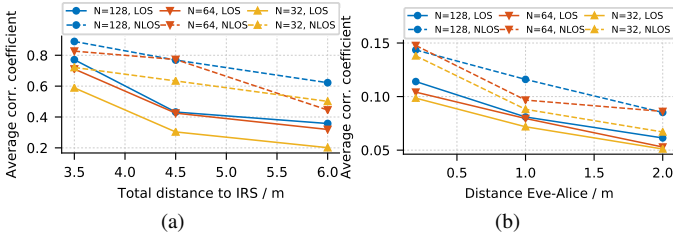
Fig. 6. (a) Average correlation coefficient of signals received by Alice and Bob for varying distances to the IRS. (b) Average correlation coefficient between signals gathered by Alice end Eve for varying positions of Eve relative to Alice.
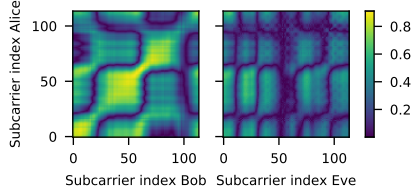

Fig. 7. Pearson correlation coefficient matrices of Alice and Bob (left) and Alice and Eve (right).

The experimental setup is illustrated in Fig. 5 and indicates the positions of Alice, Bob, Eve, and the IRS.

We fix Alice' distance to the IRS to $3\,\mathrm{m}$ and vary Bob's distance to the IRS between $0.5\,\mathrm{m}$, $1.5\,\mathrm{m}$, and $3\,\mathrm{m}$. Then, we invert the order, fixing Bob at $3\,\mathrm{m}$ and varying Alice' distance. For each setting, we vary (i) Eve's distance to Alice between $0.2\,\mathrm{m}$, $1\,\mathrm{m}$, and $2\,\mathrm{m}$, (ii) the number of active IRS elements between 32, 64, and 128, and (iii) LOS and NLOS conditions between Alice and Bob by placing a metallic blocker. For every iteration, Alice and Bob measure $m = 400$ surface configurations with $L = 4$.

To assess the IRS-induced channel variations, we calculate the average of the absolute Pearson correlation coefficients $\rho_{k,j}^{A,B}$ of Alice' and Bob's magnitude channel measurements across MIMO channels and subcarriers. We plot the results over the total node distance to the IRS for 32, 64, and 128 active elements and for LOS and NLOS conditions in Fig. 6 (a). Here, increasing the distance to the IRS reduces the IRS impact, as the loss of the channels to the IRS, $h_{i,k}$ and $g_{i,k}$, increases. Further, in accordance to the previous experiment, more surface elements help to increase the channel variation. Further, the surface impact rises for NLOS channel conditions as the surface-independent direct component d_k in (3) is reduced.

In the same manner as before, we calculate the average of the absolute Pearson correlation coefficients $\rho_{k,j}^{A,E}$ between Eve's and Alice' channel observations, made from the signals transmitted by Bob. We plot the results over Eve's distance in Fig. 6 (b) for LOS and NLOS scenarios with varying number of active surface elements N. As expected and in accordance with spatial decorrelation properties [5], the correlation of Eve's channel observations reduces with distance.

Fig. 7 shows the two-dimensional Pearson correlation ma-

trices of Alice, Bob, and Eve for exemplary spatial channels, illustrating covariance relationships across the parties and subcarriers. In the experiment, Eve was at $0.2\,\mathrm{m}$ distance from Alice. As expected, Alice and Bob (left) make strongly dependent observations on the same subcarriers, as indicated by the diagonal matrix entries. The off-diagonal components reveal that care should be taken when using frequency diversity for key generation, since some subcarriers seem to share a certain covariance. Fig. 7 (right) shows the correlation of Eve's observations which are mostly uncorrelated, however, medium correlation values occur occasionally.

C. Rates

The KGR is obtained by $\frac{N_K}{T_K}$, where N_K is the number of key bits obtained per time interval T_K. In the context of this work, we measure the KGR at the output of the CDF quantizer.

Note that the channel changes at the rate the IRS configuration is updated, allowing to boost key generation rates. That is, in contrast to traditional channel models, the IRS allows immediate switching of channel characteristics. Hence, IRS-assisted CRKG is not bounded by the classical channel coherence time to achieve sufficient randomness. Assuming extraction of a single bit from each IRS configuration, the KGR is upper bounded by $(T_{su} + L\,T_p)^{-1}$, where T_{su} is the surface update time, T_p is the channel probing interval, and L is the oversampling factor.

In our implementation, a bi-directional packet exchange T_p takes approx. $2\,\mathrm{ms}$ and the surface update time T_{su} is approx. $2\,\mathrm{ms}$, which can be further reduced through technical optimization. From the measurement data used in Section V-A with $N = 128$, we calculate the KGR and KDR shown in Table I. The results for varying oversampling factors L at two exemplary subcarriers demonstrate that a trade-off between measurement time and KDR reduction is possible. We emphasize that only a single subcarrier from a single spatial channel is used and therefore we expect that the KGR can easily be further increased. The residual KDR of Alice and Bob stems from the CDF quantizer, when input values are close to the quantizer thresholds.

TABLE I
SINGLE SUBCARRIER KGR AND KDR

	$L = 1$	$L = 2$	$L = 3$	$L = 4$
KGR [bit/s]	237.45	160.58	121.30	97.39
KDR A/B, $k = 25$	0.260	0.157	0.108	0.083
KDR A/B, $k = 94$	0.218	0.120	0.082	0.065

D. Randomness

Using the NIST's statistical test suite for random number generators [14], we assess the randomness of binary sequences generated from the prototype IRS-assisted CRKG system on a single subcarrier with $L = 4$ to cover $m = 300{,}000$ surface configurations. In the experiments, Alice and Bob are located $0.5\,\mathrm{m}$ and $3\,\mathrm{m}$ away from the IRS, respectively, (C, D), and

in a metallic shielding box together with the IRS (A, B). Using the CDF quantizer [13] with 1 bit and 2 bit resolution, we produce binary sequences of lengths 300,000 (A, C) and 600,000 bits (B, D). We apply the tests that are applicable to the given sequence lengths and list the results in Table II, showing that all sequences pass the tests.

TABLE II
NIST STATISTICAL TEST SUITE p-VALUE RESULTS [14].

	A	B	C	D
Frequency	1.00000	1.00000	1.00000	1.00000
Block Frequency	0.86108	0.64011	0.28217	0.83365
Runs	0.85513	0.99588	0.28984	0.26890
Longest Runs	0.77137	0.32486	0.34298	0.07352
Binary Matrix Rank	0.09973	0.04950	0.09466	0.68954
DFT	0.69998	0.85895	0.93210	0.79094
Non-overl. Templ. Matching	0.02935	0.46983	0.87188	0.48896
Universal	-	0.13809	-	0.133209
Serial	0.59214	0.54280	0.34804	0.73928
	0.88924	0.78167	0.32932	0.76001
Approx. Entropy	0.81847	0.12792	0.403202	0.16795
Cum. sums (Fwd)	0.12669	0.27253	0.190075	0.22361
Cum. sums (Rev)	0.12669	0.27253	0.190075	0.22361

VI. DISCUSSION AND FUTURE WORK

Our prototype system with commodity Wi-Fi transceivers demonstrates that conventional radios can successfully perform wireless key generation in static environments complemented by an IRS. Although utilizing a MIMO system, we considered single-subcarrier signals, showing that the concept is applicable to resource-constrained IoT devices with single carrier radios as well. However, larger IRS deployments are needed for a sufficient impact on coarse channel measurements such as RSS. An actively cooperating IRS for key generation requires a trust model between devices and their environment. However, an IRS could alternatively also randomize the channel continuously without participation in the CRKG protocol.

Building on our prototype system, future work will investigate how the IRS could improve the channel conditions of Alice and Bob while providing randomness for key generation. Also, future work could investigate requirements to enhance channel randomization, e. g., from spatial and frequency diversity, the number, size, and placement of IRS elements, the surface modulation signal, and inter-element correlations. More work is needed to evaluate the approach in non-static environments. Finally, we stress the need for a sound security analysis of IRS-assisted CRKG.

VII. CONCLUSION

In this paper, we outline a novel wireless key generation system assisted by an IRS, i.e., a smart radio environment. Here, we leverage a time-dependent randomization of the IRS configuration to overcome static radio environments which are not suited for wireless key generation. The passive IRS provides an entropy source, allowing arbitrary near-by users to perform key generation. The proposed system works with conventional CRKG implementations, completely eliminating

special measures for static environments at the user terminals, e. g., complex hardware extensions. Demonstrating the practical feasibility to establish cryptographic key material, we have implemented a functional prototype system using commodity Wi-Fi transceivers and a low-cost IRS prototype.

REFERENCES

[1] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Transactions on Antennas and Propagation*, vol. 53, no. 11, pp. 3776–3784, Nov. 2005.

[2] E. Basar, M. D. Renzo, J. D. Rosny, M. Debbah, M. Alouini, and R. Zhang, "Wireless Communications Through Reconfigurable Intelligent Surfaces," *IEEE Access*, vol. 7, pp. 116 753–116 773, 2019.

[3] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless Information-Theoretic Security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[4] P. del Hougne, M. Fink, and G. Lerosey, "Optimally diverse communication channels in disordered environments with tuned randomness," *Nature Electronics*, vol. 2, no. 1, pp. 36–41, Jan. 2019. [Online]. Available: http://www.nature.com/articles/s41928-018-0190-1

[5] A. Goldsmith, *Wireless Communications*. USA: Cambridge University Press, 2005.

[6] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *2011 Proceedings IEEE INFOCOM*. Shanghai, China: IEEE, Apr. 2011, pp. 1125–1133, 00149.

[7] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1773–1828, 22. [Online]. Available: https://ieeexplore.ieee.org/document/8509094/

[8] R. J. Jenkins, "ISAAC: a fast cryptographic random number generator," 1996. [Online]. Available: https://burtleburtle.net/bob/rand/isaacafa.html

[9] Z. Ji, P. L. Yeoh, D. Zhang, G. Chen, Y. Zhang, Z. He, H. Yin, and Y. li, "Secret Key Generation for Intelligent Reflecting Surface Assisted Wireless Communication Networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 1030–1034, Jan. 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9298937/

[10] C. Liaskos *et al.*, "A novel communication paradigm for high capacity and security via programmable indoor wireless environments in next generation wireless systems," *Ad Hoc Networks*, vol. 87, pp. 1–16, May 2019.

[11] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM international conference on Mobile computing and networking - MobiCom '08*. San Francisco, California, USA: ACM Press, 2008, p. 128.

[12] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[13] N. Patwari, J. Croft, S. Jana, and S. Kasera, "High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 17–30, Jan. 2010.

[14] A. Rukhin *et al.*, "A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications," NIST, NIST Pubs Special Publication (NIST SP) - 800-22 Rev 1a, 2010.

[15] Ubuntu Manpage, "random, urandom - kernel random number source devices," 2019. [Online]. Available: http://manpages.ubuntu.com/manpages/bionic/en/man4/random.4.html

[16] Y. Xie, Z. Li, and M. Li, "Precise Power Delay Profiling with Commodity WiFi," in *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '15. New York, NY, USA: ACM, 2015, pp. 53–64, Paris, France.

[17] 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.