On-line Entropy Estimation for Secure Information Reconciliation

Christian T. Zenger, Jan Zimmer, Jan-Felix Posielek, Christof Paar
Horst Görtz Institute for IT-Security (HGI), Ruhr-University Bochum, Germany
{christian.zenger, jan.zimmer, jan-felix.posielek, christof.paar}@rub.de

ABSTRACT

The random number generator (RNG) is a critical, if not in fact the most important, component in every cryptographic device. Introducing the symmetric radio channel, represented by estimations of location-specific, reciprocal, and time- variant channel characteristics, as a common RNG is not a trivial task. In recent years, several practice-oriented protocols have been proposed, challenging the utilization of wireless communication channels to enable the computation of a shared key. However, the security claims of those protocols typically rely on channel abstractions that are not fully experimentally substantiated, and (at best) rely on statistical off-line tests. In the present paper, we investigate on-line statistical testing for channel-based key extraction schemes, which is independent from channel abstractions due to the capability to verify the entropy of the resulting key material. We demonstrate an important security breach if on-line estimation is not applied, e.g., if the device is in an environment with an insufficient amount of entropy. Further, we present real-world evaluation results of 10 recent protocols for the generation of keys with a verified security level of 128-bit.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: Security and Protection

Keywords

Channel-based key extraction, physical layer security, on-line entropy estimation, information reconciliation

1. INTRODUCTION

The symmetric characteristic of the wireless channel allows the establishment of a common secret between two (or more) parties that can be used as an encryption key. To do so, the wireless channel needs to be measured in both directions by exchanging a known (pseudo noise) signal. The received signal is affected by various phenomena which characterize the channel. Since full duplex capabilities on a single channel are not feasible with off-the-shelf hardware so far, we successively transmit and receive a signal to estimate the wireless channel. Two important parameters for the common channel measurements are the probing rate r_p and the maximum sampling rate r_s, as illustrated in Figure 1.

A communications engineering rule of thumb, also applied in previous works [18, 2, 3, 14, 13, 12, 15, 1], states that a common channel measurement (let's say between Alice and Bob) needs to be done within the coherence time T_c in which the channel can be assumed to be fixed [9]. Further, a follow-up common channel measurement is assumed to be independent from the previous one if $r_s^{-1} > T_c$ holds. It is important to note that these rules originally address broad channel abstractions for (robust) communication and not security systems. In many cases, the coherence time is a non-fixed physical parameter changing over time and space. If the probing rate r_p of the channel coefficients is high compared to the inverse of the coherence time T_c^{-1}, the channel coefficients of the reciprocal channel estimations obtain a temporal correlation [19]. In other words: The randomness of the underlying fading process of the communication channel is usually based on unpredictable changes within the physical environment [9]. If no channel variations occur, such as due to moving scatterers, transmitter and receiver nodes, no new entropy is generated. If such a static or *slow-fading channel* is given, the important requirement of an *independent and identically distributed* (IID) source is not given anymore and the security of a system may collapse.

The wireless radio channel for key extraction, represented by location-specific, reciprocal, and time-varying channel measurement, has to be considered as an RNG for cryptography. In particular this includes a secure modus operandi for the potential case of a breakdown of the entropy source as well as a thorough evaluation of the physical source of randomness with respect to:

- Bias (unequal distribution, leaked information),
- Correlation (temporal dependency),
- Agility (spectrum), and

MOBIQUITOUS 2015, July 22-24, Coimbra, Portugal

DOI 10.4108/eai.22-7-2015.2260196

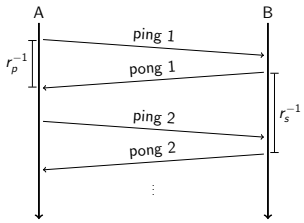


Figure 1: Important time parameter of the channel measurement process.

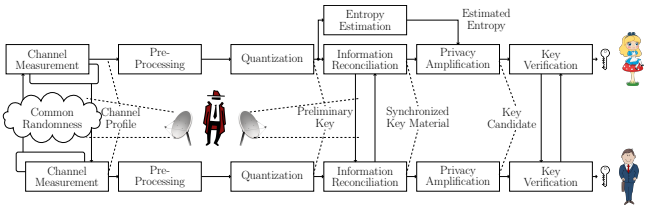


Figure 2: Overview of the components involved in the security architecture for key agreement systems from correlated observations.

- Manipulability (i.e., as shown by Eberz et al. [7]).

As we demonstrate later, on-line statistical testing is essentially relevant to security by considering statistical defects (during runtime) of an RNG in combination with the unavoidable revelation of information during error correction.

1.1 Contributions

We assume that the classical channel model, describing a stationary random process, is only partially given over time. Modeling the channel behavior as a non-IID source introduces realistic drawbacks of static environments such as a Faraday cage. Further, our source model differs from existing models insofar as it involves all kinds of channel statistics in a time-varying manner, without involving idealized requirements which cannot be guaranteed.

Therefore, we introduce design criteria for securing information reconciliation and a system extension for operation with a non-IID source which are suitable for previous security architectures. The extension consists of an on-line entropy estimation-based verifier, e.g., to achieve a key with a security level of 128-bit. Further, we demonstrate practical evaluation results of ten practice-oriented key extraction protocols, by reference [18, 2, 3, 14, 13, 12, 15, 1, 19].

1.2 Related Work

Recent works, e.g., [19], address biased channel profiles by applying quantization schemes with equal probabilities for the output symbols, and/or it is argued that the output passed a number of off-line statistical tests, e.g., a subset of the NIST suite [16]. As discussed above, we disagree with the assumption that temporal correlation is simply preventable by applying a pre-defined channel probing rate r_p which is derived from a maximum Doppler frequency f_d [14]. Recent publications suggest the use of decorrelation techniques by both Alice and Bob [15, 10]. Those techniques may successfully cover possible statistical defects of temporal correlation: Karhunen-Loéve transform, discrete cosine transform, Haar transform, and Walsh-Hadamard transform. Jana et al. [13] proposed an analysis of several quantization schemes introducing off-line Shannon entropy estimations.

Edman et al. [8] introduced an experimental security analysis covering passive eavesdropper nodes based on learning the conditional min-entropy. For the first time the authors call attention to security-related connections between the conditional entropy of potential passive attackers and the conditional entropy due to information reconciliation. The analysis is focused on a one-to-one quantization scheme (without entropy loss) and a $(255, 229)$-RS code. The results are based on 8000 channelsamples. The average-case min-entropy contained in 100 samples is evaluated.

2. CONNECTION BETWEEN ON-LINE ENTROPY ESTIMATION AND INFORMATION RECONCILIATION

The generic security architecture for the extraction of keys from correlated random variables is shown in Figure 2. Note that the variables might originate from channel measurements or other shared sources of physical randomness. These readings are quantized into vector bits to obtain an initial preliminary key. The non-perfect reciprocity in measurement and noise leads to errors in the vector bits of the preliminary key. These errors are detected and corrected in the information reconciliation stage by using error correcting techniques. Since information for error correction is exchanged over the channel, further enhancement of entropy is done in the privacy amplification stage.

Next, we focus on reconciliation- as well as on-line statistical testing- schemes from the literature and show why a connection of both is especially important for the security of a key extraction scheme.

2.1 On-line Statistical Testing

By preventing manipulations of the physical source (which is not addressed in this paper), applying decorrelation techniques, and knowing the cumulative distribution function (CDF) of a random source, we can calculate a min-entropy estimation (of course on condition that no information is revealed during reconciliation). However, in real-world scenarios, the CDF of the wireless channel is changing over time or may be unknown. Therefore, off-line evaluation of the preliminary key material is not sufficient; an on-line statistical testing is urgently needed especially to guarantee that possible statistical defects of the channel profiles combined with the publicly transmitted reconciliation data do not eliminate the entire conditional entropy of the key material (assuming that no predictable pseudo-random characteristic occurs). Given that fact, based on the estimated leftover en-

tropy, the required security level needs to be verified. This is essentially important for the security of the whole system.

2.1.1 Health Test

The on-line health check unit of Intel's Ivy Bridge random number generator [11] is a so called *total break down* or *health* test. Fresh entropy is assumed if at least 128 of the most recent 256 samples are *healthy*, whereby one sample is represented by a 256-bit vector. The test provides only a binary result about the freshness of a 65536-bit block.

2.1.2 Reduced p-value Test

On-line statistical testing could be realized by applying so called *on-the-fly* tests, which are lightweight implementations of reduced complexity of statistical and arithmetic operations of conventional NIST tests [16]. The test provides a binary result on a per block basis, e.g., with a block size of 128 or 256 bits. Recent works (e.g., [17]) addressed problems of time-consuming processes and high memory consumption. Unfortunately, these works are based on independent blockwise calculation of p-values without addressing block-overlapping defects.

2.1.3 Entropy Estimation

The estimation of the min-entropy $H_\infty(X)$ for non-IID random variables as demonstrated in the draft $800-90$B of NIST [4] provides an entropy value on a per-sample basis (e.g., of a 2-bit valued quantizer's output). This enables a continuous bit-entropy estimation $H_\infty(X) \in [0;1]$. The draft recommends five tests: collision test, partial collection test, Markov test, compression test, and frequency test. For security applications, the worst case has to be assumed and therefore the lowest estimation has to be considered as $H_\infty(X)$. This on-line test suite enhances our security model by a block, where the successfully reconciled channel profiles get weighted with the min-entropy (under consideration of further information loss).

2.2 Information Reconciliation

The information reconciliation is responsible for detecting and correcting errors in the preliminary key material between the two communicating parties. These errors are caused by differences during the measurement process. These differences originate from noise due to effects such as hardware impairments. Several techniques for reconciliation have been presented in the past and are summarized below.

2.2.1 Thresholding

One category of reconciliation techniques is based on the selection of channel profiles with strong deviations and the rejection of probably noisy channel profiles. Examples for such techniques are the guard interval techniques (e.g., [14]) or single threshold-based approaches (e.g., [3]). The idea is that due to the robustness of the approach with a high probability no errors occur. Unfortunately, such quantization-combined reconciliation techniques have several open security questions: First, Edman et al. [8] addressed the fact that there might be no conditional entropy left due to the required interactions. Second, robust (against noise etc.) system designs, e.g., guard-band-based approaches, are vulnerable against (partial) key recovery attacks as deductively shown by Eberz et al. [7]. Third, given the fact that the regarded common entropy has its origin in strong physical characteristics, simple side channels for key prediction attacks such as positioning or movements of scatters have to be considered. Jana et al. [13] already demonstrate a first approach of a simple channel-prediction attack.

2.2.2 CASCADE

The approach by Jana et al. [13] relies on Brassard et al.'s iterative, interactive information reconciliation protocol CASCADE [5]. In this protocol, Alice divides the preliminary key material into small blocks and sends parity information of each block to Bob. Bob divides his key material in the same way, computes parity check bits and checks for mismatches. For each mismatch, Bob performs a binary search on the block to find a correction vector which may fix the errors. These steps are iterated a number of times to ensure a high probability of success. However, CASCADE requires interaction that may result in potentially zeroing the conditional entropy [8].

2.2.3 Parity-Based Information Reconciliation

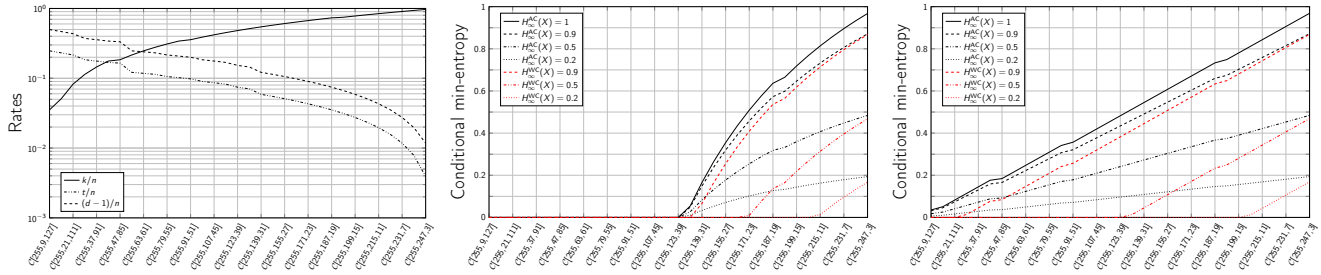
Zhang et al. [20] proposed a reconciliation scheme based on linear block codes. In this protocol, Alice and Bob divide the preliminary key material into k-bit vectors. By utilizing a linear block code $\mathcal{C}[n,k,d]$, Alice calculates and sends the parity check bits to Bob. Bob applies the corresponding decoder, whereby the required code word is composed of Bob's information vector and the received parity bits. If the number of bit disagreements is smaller than $t = \lfloor \frac{d-1}{2} \rfloor$, synchronized key material is guaranteed.

2.2.4 Reconciliation Using Secure Sketches

Edman et al. [8] suggest the usage of a syndrome-based reconciliation approach for channel-based key establishment systems which uses secure sketches as defined by Dodis et al. [6]. Our analysis shows that this scheme is the most efficient one towards minimizing the information loss.

Figure 4 shows the process of the scheme. First, the channel profiles are divided into blocks of n bits, with n being the code word length of a $\mathcal{C}[n,k,d]$ BCH code. Alice and Bob both start with the first block of quantized channel measurements y_x that is given as the common channel x with a unique error vector e_x. Alice computes the syndrome $\mathrm{syn}(y_a)$ of her block and sends it to Bob. Due to the broadcast nature of the wireless channel, an eavesdropper can overhear this message and therefore learn about the common key material.

2.2.5 Correction Capabilities vs. Security



(a) (b) (c)

Figure 3: Parameters of information reconciliation schemes using BCH code (generic $\mathcal{C}$[255,k,d]): (a) Classically considered properties, such as code rate and error correction/detection capability, are given. Further, the leftover conditional min-entropy $H_\infty(X|Y)$ of parity-based (b) and syndrome-based (c) reconciliation are illustrated for several min-entropy values $H_\infty(X)$.

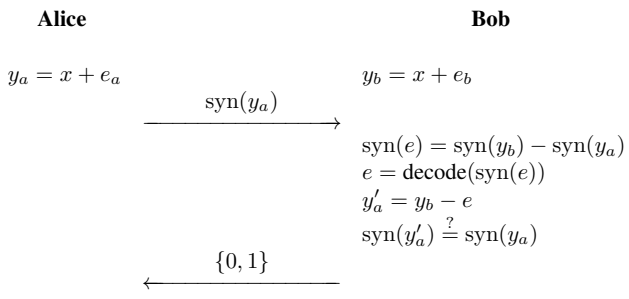


Figure 4: Information reconciliation using secure sketches.

Providing a robust communication over a noisy channel is the traditional application for error correction techniques. As an example, code rates as well as the error correction and detection capabilities for BCH codes (generic $\mathcal{C}$[255,k,d]) are given in Figure 3(a). However, with respect to security applications, the priority lies in the remaining conditional min-entropy an adversary is not able recover, rather than on the classical correction capabilities as we will show next.

We start analyzing the secure sketch approach assuming the *best case*. This means that there are (**1**) no statistical defects on preliminary key material, (**2**) no entropy losses due to public communication of quantizers, and (**3**) no potential eavesdropper measuring correlated channel profiles. Therefore, the bitwise min-entropy of the code word y_a can be assumed as $H_\infty(X) = 1$. The amount of information that an attacker can infer from eavesdropping $\mathrm{syn}(y_a)$ corresponds to the number of transmitted bits: $p = n - k$. Therefore, k bits entropy for each block are retained.

In the next step we consider statistical defects in the preliminary key material and estimate those by applying on-line entropy estimation, e.g., by draft $800 - 90$B of NIST [4] as proposed above. For simplicity, we assume that no potential attacker is close enough to measure correlated channel profiles, and further that a secure quantization scheme is applied. The entropy per bit $H_\infty(X)$, as provided by the draft, may vary between $[0, 1]$. Addressing the information loss Y due to the reconciliation interactions in combination with the (estimated) min-entropy $H_\infty(X)$, the leftover conditional min-entropy $H_\infty(X|Y)$ is given for the average case (AC) as well as for the worst case (WC):

$$H_\infty^{\mathrm{AC}}(X|Y) = H_\infty(X) \cdot \frac{k}{n} \tag{1}$$

$$H_\infty^{\mathrm{WC}}(X|Y) = H_\infty(X) - \frac{n-k}{n} \tag{2}$$

for a code word with the length of n bit and rank k. Further, as an example, an illustration of the leftover conditional min-entropy for $\mathcal{C}$[255,k,d] BCH codes is given in Figure 3(c). The results for the approach [20] are illustrated in Figure 3(b). For future work $H_\infty(X)$ could also consider losses due to correlated observations of an eavesdropper and revealed information of further public interactions.

3. PERFORMANCE EVALUATION

We implemented a channel measurement protocol on the hardware platform Raspberry Pi. We equipped this small computer with a TP-Link TLWN722N wireless USB adapter, utilizing IEEE 802.11g and providing *received signal strength indicator* (RSSI) values on a per-packet basis, as well as a battery for mobility. The setup is specifically designed to obtain synchronized measurements between three parties within $r_p^{-1} \leq 5\,\mathrm{ms}$ with a sampling rate of $r_s^{-1} \approx 10\,\mathrm{ms}$. Further, we implemented a Matlab framework, including quantization protocols from the literature [18, 2, 3, 14, 13, 12, 15, 1, 19] as well as the reconciliation schemes [20, 6] with the on-line entropy estimation [4].

In the present paper, we focused on the following indoor setup: Alice was positioned on a *randomly moving robotic platform* (RMRP). Alice and Bob are separated by a distance of on average $10\,\mathrm{m}$ and a standard deviation of $4.6\,\mathrm{m}$.

3.1 Results

The results of the on-line entropy estimation over time are given in Figure 5(a). Here the draft $800 - 90$B of NIST [4] is applied and the worst-case estimation result of the five

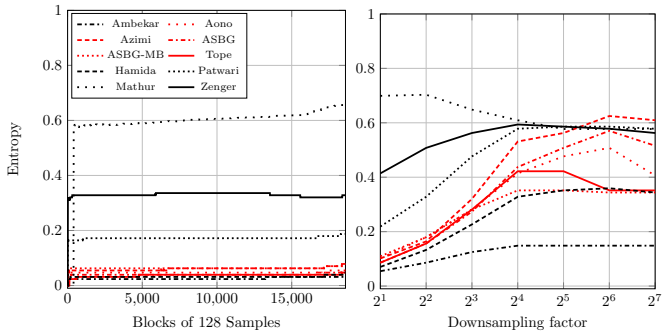


Figure 5: Evaluation results based on the real-world setups $1-12$ of all quantization schemes for (a) estimated min-entropy over time, (b) on-line entropy estimation for different downsampling factors.

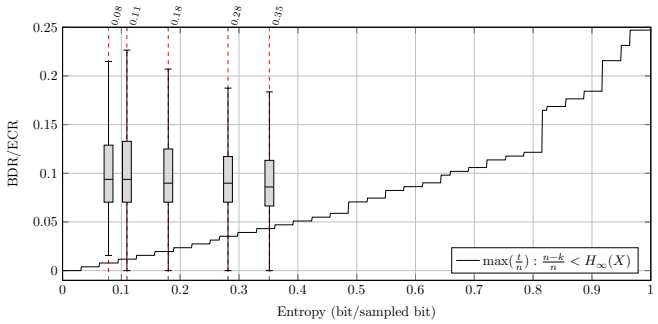


Figure 6: Example of evaluation results of the key material. The *bit disagreement rate* (BDR) distribution of the key material is illustrated as a box plot (Jana et al. [13] for downsampling factors $1, 2, 4, 8, 16$). Its position is based on the result of the estimated entropy. The position identifies the boundary of secure code parameters represented by t/n.

tests is used. Because of the high channel sampling rate r_s of 100 Hz, the key material is highly correlated in time and therefore the estimated entropy is relatively low. Reducing the sampling rate (applying downsampling in our framework) helps to find the optimal sampling rate at the maximum estimated entropy as demonstrated in Figure 5(b). The stagnation of the estimated entropy at the downsampling rate of $\approx 2^4$ might depend on statistical defects of the quantizers.

For demonstration, we apply single-bit quantization by Jana et al. [13] and the information reconciliation scheme by Dodis et al. [6] wiht a $\mathcal{C}$[255,k,d] BCH code. We introduce the *error correction rate* (ECR) as the ratio of correctable errors to the length of the code word: $\frac{t}{n}$, with $t = \lfloor \frac{d-1}{2} \rfloor$. The ECR depends on the chosen code parameter and does not include any security metric. Figure 6 illustrates our evaluation strategy based on the estimated entropy using the draft 800 − 90B of NIST [4]. The highest possible t/n ratio for the worst case of $H_\infty^{WC}(X|Y)$ that fulfills the security requirements of not zeroing the conditional entropy, i.e., $\frac{n-k}{n} < H_\infty(X)$, (please refer to (2) of section 2.2.5) is plotted as a serrated line. In other words: we try to achieve the highest *secure* error correction performance. Applying these boundaries, the system is able to select the remaining subset of secure codes, based on the estimated entropy. Note that these assumptions are applicable to the system independently from the used quantization scheme.

Each of the box plots refers to one downsampling factors and shows two metrics of our example application of the quantization scheme by Jana et al. [13]. The horizontal position represents the estimated entropy value. The box plot itself shows the distribution of the blockwise bit disagreement generated by the quantization scheme. The example shows that for this scheme only a few blocks at the lower extreme are reconcilable securely. However, applying downsampling to address oversampling improves the estimated entropy and therefore allows a higher error correction rate which leads to better performance of the system.

The *channel profiles per secret key rate* (SKR) indicates how many channel profiles are processed on average to generate a key with a 128-bit security level. It is a function depending on the distribution (box plot) of the *bit disagreement rate* (BDR), the estimated entropy, and the chosen code parameter. The decoding may lead to false-positive error correction caused by overly high bit disagreement of the preliminary key material. Therefore, a *key verification fail ratio* (KVFR) is given. We summarize the results in Table 1.

The results of the on-line entropy estimation implies that statistical defects and therefore a point of attack are given if no correct code parameter are applied, which are not treated in previous (off-line) approaches. Further, we propose the use of the highlighted subset of schemes because they do not require additional information exchange, which could lead to security vulnerabilities. Among them, the single bit scheme of Azimi et al. [3] and the multibit scheme by Jana et al. [13] fulfill the security requirements. The duration time on average for Azimi et al.'s scheme to establish a secret key with a security level of 128 bits is 87 s; Jana et al.'s multibit scheme requires 58 s on average.

Table 1: Evaluation results of different quantizations schemes and corresponding code parameters resulting in a maximum SKR for average-case conditional min-entropy.

Quantizer	**BCH**	**SKR**	**KVFR**
Tope et al. [18]	$\mathcal{C}$[255,223,9]	37213	0.0469
Aono et al. [2]	$\mathcal{C}$[255,231,7]	13456	0.0395
Azimi et al. [3]	$\mathcal{C}$[255,87,53]	8692	0
Mathur et al. [14]	$\mathcal{C}$[255,223,9]	5526	0
ASBG [13]	$\mathcal{C}$[255,223,9]	6598	0.0332
ASBG-multibit [13]	$\mathcal{C}$[255,87,53]	5795	0
Hamida et al. [12]	$\mathcal{C}$[255,47,85]	125346	0
Patwari et al. [15]	$\mathcal{C}$[255,47,85]	2676	0
Ambekar et al. [1]	$\mathcal{C}$[255,223,9]	3593	0.0181
Zenger et al. [19]	$\mathcal{C}$[255,45,87]	340225	0

4. CONCLUSION

Prior work has documented the effectiveness of channel-based key extraction systems in improving key generation rates and reducing bit disagreements. This paper extends recent key extraction protocols which typically rely on channel abstractions that are not fully substantiated. In the present paper, we investigate on-line statistical testing for channel-based key extraction which is independent from channel abstractions due to the capability to verify the entropy of the resulting key material on the fly. We point out an important security breach if proper statistical testing is not applied. Finally, we address the common goal of achieving cryptographic keys with a security level of 128 bits on the basis of on-line entropy estimation. Therefore, we performed real-world evaluations and provide performance results of several protocols from the literature.

5. REFERENCES

[1] A. Ambekar, M. Hassan, and H. D. Schotten. Improving channel reciprocity for effective key management systems. In *ISSSE*. IEEE, 2012.

[2] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels. *Antennas and Propagation, IEEE Transactions on*, 53(11):3776–3784, 2005.

[3] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener. Robust key generation from signal envelopes in wireless networks. In P. Ning, S. D. C. di Vimercati, and P. F. Syverson, editors, *Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, Alexandria, Virginia, USA, October 28-31, 2007*, pages 401–410. ACM, 2007.

[4] E. Barker and J. Kelsey. NIST DRAFT Special Publication 800-90b recommendation for the entropy sources used for random bit generation. 2012.

[5] G. Brassard and L. Salvail. Secret-key reconciliation by public discussion. In T. Helleseth, editor, *EUROCRYPT '93, Lofthus, Norway, May 23-27, 1993*, volume 765 of *Lecture Notes in Computer Science*, pages 410–423. Springer, 1993.

[6] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM J. Comput.*, 38(1):97–139, 2008.

[7] S. Eberz, M. Strohmeier, M. Wilhelm, and I. Martinovic. A practical man-in-the-middle attack on signal-based key generation protocols. In S. Foresti, M. Yung, and F. Martinelli, editors, *Computer Security - ESORICS '12, Pisa, Italy, September 10-12, 2012. Proceedings*, volume 7459 of *Lecture Notes in Computer Science*, pages 235–252. Springer, 2012.

[8] M. Edman, A. Kiayias, Q. Tang, and B. Yener. On the security of key extraction from measuring physical quantities. *CoRR*, abs/1311.4591, 2013.

[9] A. Goldsmith. *Wireless communications*. Cambridge university press, 2005.

[10] S. Gopinath, R. Guillaume, P. Duplys, and A. Czylwik. Reciprocity enhancement and decorrelation schemes for PHY-based key generation. In *Globecom 2014 Workshop - TCPLS*, pages 1471–1476, Austin, USA, Dec. 2014.

[11] M. Hamburg, P. Kocher, and M. E. Marson. Analysis of intel's ivy bridge digital random number generator. *Online: http://www. cryptography. com/public/pdf/Intel_TRN G_Report_20120312. pdf*, 2012.

[12] S. T. B. Hamida, J. Pierrot, and C. Castelluccia. An adaptive quantization algorithm for secret key generation using radio channel measurements. In K. A. Agha, M. Badra, and G. B. Newby, editors, *NTMS 2009, Cairo, Egypt*, pages 1–5. IEEE, 2009.

[13] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy. On the effectiveness of secret key extraction from wireless signal strength in real environments. In K. G. Shin, Y. Zhang, R. Bagrodia, and R. Govindan, editors, *MOBICOM 2009, Beijing, China, September 20-25, 2009*, pages 321–332. ACM, 2009.

[14] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik. Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel. In *MobiCom 2008*, pages 128–139. ACM, 2008.

[15] N. Patwari, J. Croft, S. Jana, and S. K. Kasera. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. *IEEE Trans. Mob. Comput.*, 9(1):17–30, 2010.

[16] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, DTIC Document, 2001.

[17] V. B. Suresh, D. Antonioli, and W. P. Burleson. On-chip lightweight implementation of reduced NIST randomness test suite. In *2013 IEEE HOST, Austin, TX, USA, June 2-3, 2013*, pages 93–98. IEEE, 2013.

[18] M. A. Tope and J. C. McEachen. Unconditionally secure communications over fading channels. In *Military Communications Conference, 2001. MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force. IEEE*, volume 1, pages 54–58. IEEE, 2001.

[19] C. T. Zenger, M.-J. Chur, J.-F. Posielek, G. Wunder, and C. Paar. A novel key generating architecture for wireless low-resource devices. In *International Workshop on Secure Internet of Things (SIoT)*, volume 3, pages 74–89.

[20] J. Zhang, S. K. Kasera, and N. Patwari. Mobility assisted secret key generation using wireless link signatures. In *INFOCOM 2010, San Diego, CA, USA*, pages 261–265. IEEE, 2010.