Contents

Chapter 1

Application cases of Secret Key Generation in communication nodes and terminals

François Delaveau, Christiane Kameni Ngassa, Renaud Molière, Taghrid Mazloum, Alain Sibille, Adrian Kotelba, Jani Suomalainen, Sandrine Boumard, Nir Shapira

1.1 Introduction

The main objective of this chapter is to study explicit key extraction techniques and algorithms for the security of radio communication. After some recalls on the main processing steps (Figure 1.1a) and on theoretical results relevant to the radio wiretap model (Figure 1.1b), we detail recent experimental results on randomness properties of real field radio channels. Furthermore we detail a practical implantation of Secret Key Generation (SKG) schemes, based on the Channel Quantization Alternate (CQA) algorithm helped with channel decorrelation techniques, into modern public networks such as WiFi and radio-cells of fourth generation (LTE, Long Term Evolution). Finally, through realistic simulations and real field experiments of radio links, we analyze the security performance of the implemented SKG schemes, and highlight their significant practical results and perspectives for future implantations into existing and next generation radio standards.

The chapter is organized as follows.

Section 1.2 introduces the usage of a shared source of randomness under a reciprocity assumption, explains the particular interest of radio propagation for achieving confidentiality of wireless links in the wiretap channel model, provides security metrics suited to wireless links, and analyses the impact of radio-channel properties from simulated samples.

Section 1.3 provides a complete implementation of a SKG scheme, adapted to Orthogonal Frequency Division Modulated (OFDM) signals such as encountered in modern digital Wireless Access Networks (802.11n/ac and LTE). Then, simulations of SKG into realistic LTE links and practical over-the-air implementation of SKG into WiFi chipsets assess the feasibility proof and provide the practical performance, while computation of entropy and mutual information complete the security analysis.

Section 1.4 points out the potential advantages of these techniques for radio standards. After some recalls on existing vulnerabilities of public radio networks, many potential application cases of SKG are highlighted for enhancing the privacy of sub-

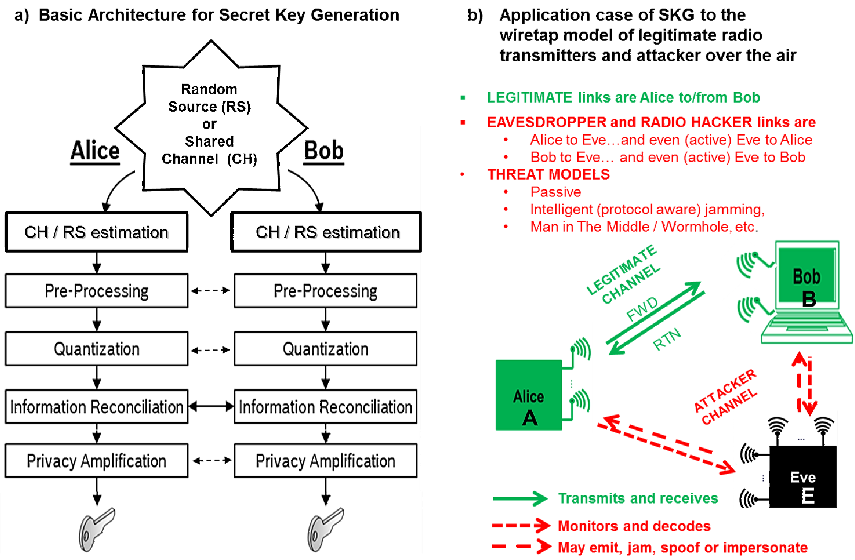

Figure 1.1: Principle of Secret Key Generation - application case to the wiretap radio channel.

scribers and confidentiality of data streams into existing and future wireless standards. Especially, practical tracks are proposed for securing the early stages of radio access protocols where identification and authentication are performed.

1.2 Fundamental aspects of Secret Key Generation

Given a common or highly correlated source of randomness and a public error-free authenticated channel, legitimate users may generate a shared secret key about which an eavesdropper that has an uncorrelated access to the random source would have negligible information [1]. The users extract correlated random sequences from their correlated source of randomness and subsequently agree on the same random key through public communications. Messages exchanged between legitimate users over the public channel do not carry enough information to allow the eavesdropper to recover the same cryptographic key. This secret key generation (SKG) approach was introduced in 1993 [2, 3] and provides information-theoretic security as the eavesdropper is assumed to have unlimited computing power.

1.2.1 Channel based random bit generators

While the first implementations of SKG concerned quantum physics, the propagation channel has also captured very much attention in establishing on-the-fly secure key bits [4, 5, 6, 7, 8]. Indeed, it is possible to create a random bit generator based on

the characteristics of the propagation channel, owing to the stochastic nature of the multipath propagation and to the intrinsic reciprocity of the electromagnetic (EM) transmission media.

A shared source owing to reciprocity

The reciprocity law states that the multipath properties are the same on both directions of a link since EM waves undergo the same physical interactions in both senses of propagation. Such a reciprocity especially holds in Time Division Duplex (TDD) systems , e.g. IEEE 802.11, LTE and next generation (5G) of wireless standards, where both up-link and down-link use the same frequency band. Accordingly and without any feedback, any two entities (e.g. legitimate ones) may share common information extracted from the reciprocal channel, from which identical key bits may be generated.

However, some practical issues disrupt reciprocity. On one hand, in TDD systems the channel must be estimated over a duration smaller than the coherence time, in order to reduce the discrepancies between Alice and Bob. On the other hand, hardware calibration should be performed in order to account for the asymmetric properties of certain electronic components in the transmit and receive communication chains. Briefly speaking, both the non-reciprocity sources and the channel noise limit the number of shared bits that legitimate parties may reliably share [9].

Randomness owing to multipath propagation

Both length and randomness are fundamental properties of a robust cryptographic key. The former is required to avoid any brute force attack while the latter increases the eavesdropper uncertainty. A long key may result from the concatenation of several sub-keys where each one, of a limited number of reliable bits, comes from a single channel sample [9, 10]. Moreover, the channel samples must be statistically decorrelated as much as possible in order to enhance the randomness vs. a single sample.

Owing to multipath propagation, the radio channel is subject to intrinsic stochastic variations in the time (e.g. through terminal movement or people motion in the surrounding area), space (e.g. using multiple antennas systems) or frequency (e.g. using an orthogonal frequency division multiplexing (OFDM) scheme) domains. Indeed, it is shown in [11] that, for multiple-input multiple-output (MIMO) systems, the richer the channel in multipaths, the richer in randomness. Consistently, the authors in [12] proved by the mean of a ray tracing tool that the diffuse scattering components of the channel play an essential role in improving the performance of SKG.

Nonetheless, the challenge resides on how to sample the propagation channel in order to select sufficiently decorrelated realizations. Intuitively, this relies on the transmission medium itself from the point of view of its richness in scattered obstacles as well as on the source domain of randomness (e.g. time, space or frequency domains). As shown in [10, 13], if we consider SKG by investigating either the space, the frequency or the time domains, the performance can be respectively assessed according to the coherence distance, the coherence bandwidth or the coherence time.

For better performance, it is therefore proposed in [10] to jointly exploit both the space and the frequency propagation channel variability and in [13] to jointly exploit both the space and time propagation channel variability.

Confidentiality

The purpose of an information-theoretic framework is to achieve a configuration where the eavesdropper does not have enough information to collapse the key difference between the computation of legitimates and its own computations.

Owing to spatial channel decorrelation of the multipath propagation, Eve may measure decorrelated radio channel with respect to Alice-Bob channel. The key confidentiality is ensured when the correlation coefficient does not exceed a certain threshold that depends on the implemented SKG scheme. The efficiency of such a scheme, described in Section 1.3.1, relies on providing independent keys even from highly correlated channels, however, without disturbing the reliability between Alice and Bob (i.e. obtaining exactly the same key from very highly correlated channels).

Furthermore, the channel correlation, and subsequently the key confidentiality, is impacted by the relative position of Eve to at least one of the legitimate users (for example Bob) as well as to the channel characteristics (for example the coherence distance when considering space diversity).

The worst scenario occurs when Eve and Bob are collocated; they measure the same channel except independent noise which may lead to some discrepancies between the extracted keys. These discrepancies increase when Eve moves away from Bob as the correlation coefficient decreases. Even that, the correlation is still relatively high as they are in the same stationary region where they share the same multipath components. In this case, Eve may employ tools such as ray-tracing, while exploiting further information (e.g. the location of Bob and the environment characteristics), in order to improve her learning about the key. Nevertheless, the correlation is very low when Eve and Bob are not in the same stationary area, where they do not share the same multipath components. In this latter case, the security is ensured.

Experimental results in [13] show that special decorrelation occurs after one half wave length distance in most of dispersive radio-channel configurations encountered in Non Line Of Sight (NLOS) geometry, while a distance of several wavelength (up to 4 wavelengths) is usually required to achieve space decorrelation in more stationary radio channels, such as encountered in Line Of Sight (LOS) geometry.

1.2.2 Metrics for Secret Key Generation assessment

As already shown, the robustness of the key relies on its length, randomness and confidentiality. All these features may be assessed, theoretically, by the secret key rate through mutual information computations. On the other hand, from the practical point of view, the quality of the key resulting from the implementation of the SKG protocol may be assessed in terms of both reliability and confidentiality through the key bit error rate, and also in terms of randomness through statistical tests.

Secret key rate: In an information-theoretic framework, the maximum amount of random information reliably shared between Alice and Bob is measured by the

mutual information between their legitimate channels (i.e. $I_K = I(\hat{\mathbf{h}}_a, \hat{\mathbf{h}}_b)$). Such an amount is entirely secure if Eve experiences channels that are statistically independent from those measured by the legitimate terminals (e.g. Eve is sufficiently far from both Alice and Bob). Otherwise and more generally, the secret key rate is the mutual information between Alice and Bob's channels, given Eve's observations. We note that the mutual information is expressed by the covariance matrices of channel observations if the latter are both marginally and jointly Gaussian distributed. Otherwise, there is no closed-form expression for the mutual information.

Key bit error rate (KBER): More practically, the SKG performance can be assessed after applying the protocol in the whole or part of it. Thus, it is crucial to compare the keys through the evaluation of the key bit error rate (KBER)[1] by computing the ratio of the number of differing bits to the key length. Obviously, when comparing the keys generated by legitimate terminals, the KBER should approach 0 while for the comparison versus the key computed by Eve, it should approach 1/2.

Statistical tests for randomness: The randomness of the key may be assessed by specific statistical tests, among which are notably the National Institute of Standard and Technology (NIST) test suite [14] and the Intel health check test [15]. The NIST test suite is composed of 16 tests, where each attempts to detect if the key bits follow a certain deterministic behaviour resulting from imperfect randomness in the key generation process. Among the 16 tests, selected examples below have used both the 'mono-bit frequency' test and the 'runs' test. The former investigates the occurrence of bit 0 on the entire key bits, while the latter checks whether the transition between bits 0 and 1 is too fast or too slow. Since NIST tests are complex to embed into nodes and terminals, we also employ the Intel health check test, which checks the entropy of the generated keys by evaluating the occurrence of six different bit patterns in a 256-bit sequence.

1.2.3 Impact of channel characteristics

In this section we address some concrete aspects of SKG in relation with the characteristics of the radio channel. We particularly show here the behaviour of I_K when increasing the number of investigated frequency-varying sub-channels. Thus, we build a key from N_u consecutive sub-carriers, even correlated, selected among N_f total sub-carriers in a given bandwidth of an OFDM system. We assume that the power spectral density (PSD) of both the sub-carrier and the noise is constant, with a Signal to Noise Ratio (SNR) of 15 dB.

For the sake of comparison, we consider the following different types of channel data:

a) **A power decay profile model**: We consider a simple dispersive channel model, based on periodic independent multipaths in the delay domain, with an exponentially decreasing mean power. Each path complex amplitude is circularly-symmetric Gaussian distributed.

[1] We choose to evaluate the BER instead of the symbol error rate in order to account for the reconciliation phase which operates at the bit level.

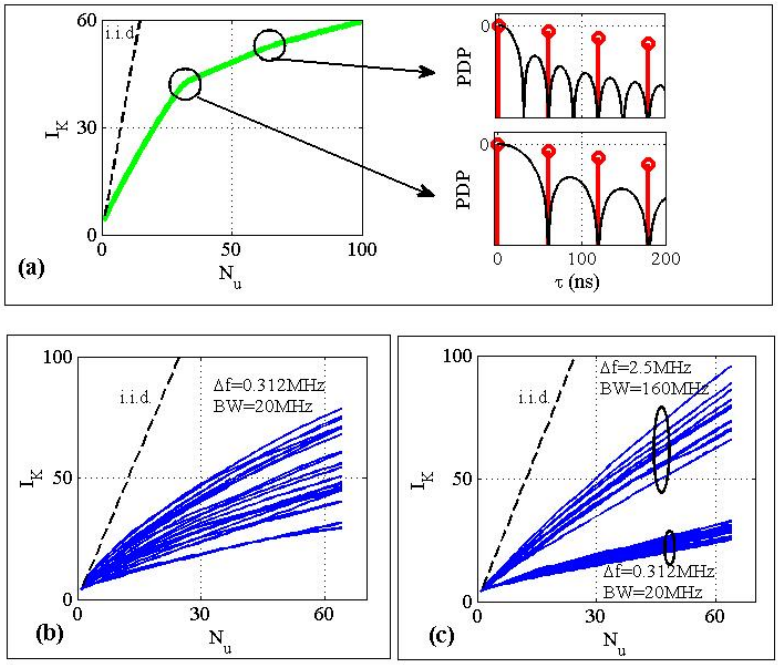

Figure 1.2: I_K with respect to the number of used sub-carriers N_u: (a) Power decay profile model, (b) RT data model, (c) Measured channel data.

b) **A ray-tracing outdoor data**: We exploit deterministic simulations using a commercial ray tracing (RT) tool [16], specially extended by incorporating diffuse scattering, implemented according to the effective roughness approach [17]. We consider an outdoor sub-urban environment located in Paris (i.e. the 'carrousel du Louvre'). Alice is represented by a fixed base station at 48m above the ground level, whereas Bob takes several positions covering the considered area at 1.5m antenna height. I_K is statistically computed for each position of Bob by considering a small scale stationarity region around each RT computed Bob location, where the variability stems from the varying phase for each antenna position and for each path.

c) **Measured indoor channels**: Channel coefficients have been recorded in the 2-6 GHz frequency band using a vector network analyzer, in the premises of Telecom ParisTech [9, 10, 13]. For each position of Bob in either a room, a corridor or a hall, the transmitter representing Alice is spatially scanned over a 11x11 square grid confined to a small area, which allows the evaluation of I_K.

I_K is assessed in the frequency domain by stacking N_u sub-carriers within a single vector. Since the channel model and the RT tool produce channel impulse responses (CIRs), we perform a discrete Fourier transform in order to obtain N_f channel transfer functions within a given bandwidth (BW).

Fig. 1.2 shows the behaviour of I_K with respect to N_u. Obviously, increasing N_u yields an increase in the amount of randomness, which depends on the correlation of the sub-carriers. In fact, a set of N_u sub-carriers is equivalent, in the delay domain, to N_u resolved paths of a gain obtained by using a cardinal sinus filter. When the resolved paths are independent, no more randomness is obtained by increasing N_u, which should yield to a saturation behaviour. However, as shown in Fig. 1.2 (a), beyond the saturation point, I_K still increases with N_u, although slowly. This is explained by the improvement on the SNR per resolved path, owing to the increase in the total transmitted power as N_u increases. Actually, it is shown in [18] that there is an optimal bandwidth that maximizes I_K if the total transmitted power is fixed, rather than the PSD.

Moreover, in Fig. 1.2 (b) and Fig. 1.2 (c), the curves show a sub-linear behaviour, which is more pronounced for the RT data. This is explained by the fact that the rays computed by the RT tool are not evenly distributed over all the delay bins, while measured CIRs turn out to be very dense in multipaths. This requires a much higher BW than 160 MHz in order to exploit the rich degrees of freedom of the channel. Furthermore, we notice that, for a given N_u sub-carriers, I_K values change from one measured location to another one since the channel coherence bandwidth changes according to the richness in multipaths as well as on their spread in the delay domain [12].

As a conclusion of practical interest, as shown in [12], it appears that indoor environments are less prone to SKG from frequency-variant channels, since such environments have naturally large coherence bandwidths, as opposed to outdoor environments where delay spreads are usually longer that implies smaller coherence BW and higher frequency diversity.

When considering spatial-variant channels,

- increasing randomness can be captured into indoor radio-channels, especially with large bandwidth channel sounding, relevant coherence distance is low (half wave length) to medium (usually less than ten wavelengths) depending on the NLOS/LOS configuration.
- Outdoor radio-channel, usually more dispersive than indoor radio-channels, provide native randomness at limited bandwidth channel sounding, relevant coherence distance is usually low (half wavelength), and very low especially in dense urban NLOS geometries.

1.3 Integration of Secret Key Generation into existing Radio Access Technologies

1.3.1 Practical Secret Key Generation scheme

The proposed SKG protocol targets existing and future radio-communication standards, such as Wireless Local Access Networks (WLAN) 802.11n/ac and radio-cells of second, third, fourth and fifth generation.

It is composed of the following steps (as mentioned in Figure 1.1).

Instantaneous channel estimation at the signal frame level: this first step of the SKG scheme computes the Channel Impulse Response (CIR) or the Channel Frequency Response (CFR) for the signal frame.

Spatial decorrelation: the goal of this step is to reduce spatial correlation between channel measurements by using the eigenvectors of the full covariance matrix of the channel estimates [19]. However, this process is computationally expensive and only helpful in Line-Of-Sight (LOS) configurations. Therefore, unless otherwise specified, the spatial decorrelation step is not performed in the remaining of the chapter.

Channel coefficient decorrelation over several frames: this second step optimizes the selection of the randomness material in stationary environments. We apply a selection algorithm to channel coefficients issued from the previous CIRs or CFR, in order to achieve low cross correlation of these coefficients over several frames.

Quantization: this step uses the Channel Quantization Alternate (CQA) algorithm introduced by Wallace to quantize selected channel coefficients [11], that minimizes key mismatch between the legitimate users Alice and Bob.

Information reconciliation: this step corrects the remaining mismatch between Alice and Bob keys. Secure sketches and error correcting codes are employed to allow Bob to recover the same key than Alice. To do so, Alice has to send the secure sketch over the public channel, what possibly leaks a controlled amount of information to the eavesdropper Eve.

Privacy amplification: this step improves the randomness of the secret key and removes the information leaked during the information reconciliation step. To do so, hash functions are used and the key length is reduced if necessary. This final step guarantees that the generated secret key is fully de-correlated from the key computed by the eavesdropper.

Note: in the following, practical implementation of SKG scheme inside communication devices is studied. Hence robust and simple algorithms are considered. For example, simple algebraic Forward Error Correction (FEC) code are employed to reconcile Alice and Bob keys and a classical family of 2-universal hash function is chosen in the privacy amplification step [20].

1.3.1.1 Channel estimation – Application case to OFDM signals

When considering an OFDM (such as defined in WiFi and LTE), the component of the Channel Frequency Response (CFR) H_f in the frequency domain quantifies the fading applying on each subcarrier. In a sampled system, considering a finite response and band, the k^{th} frequency component f_k of the CFR can be calculated as follows:

$$H_f(k) = \frac{Y(f_k)}{X(f_k)} \tag{1.1}$$

where Y is the received signal, and X is the emitted signal (or reference signal). In the time domain, an equivalent Channel Impulse Response (CIR) estimation can be deduced from the CFR by IFFT, as follows:

$$H_{\text{IFFT}} = \text{IFFT}(H_f) \tag{1.2}$$

When considering now Time Division Multiple Access (TDMA) of Code Division Multiple Access (CDMA) waveforms defined in 2G and 3G Radio Access Technologies (RAT), CIR can be computed directly in the time domain by applying filter estimations techniques to reference signal X.

1.3.1.2 Channel decorrelation

Secret key bits should be completely random to keep them unpredictable by Eve. Therefore any deterministic component in the radio propagation channel should be removed. To obtain key bits with equal probability, the quantization algorithm should tamper with channel coefficients as random and decorrelated as possible. The goal of this step is thus to decrease the negative effect of channel correlation by a careful selection of the channel coefficient to be quantized. Channel correlation can be observed in time and frequency domains.

Time correlation is decreased between channel coefficients. To do so, channel coefficients are recorded during a given acquisition time, constituting a frame. Then cross-correlation coefficients are computed between two consecutive frames and finally only frames with low cross-correlation coefficient (above a given threshold T_t) are selected.

Similarly, the frequency correlation is decreased by first computing cross-correlation coefficients between two consecutive frequency carriers. Only frequency carriers for which the cross-correlation coefficient is above a given threshold T_f are selected. In addition, lowest and highest frequency carriers are dropped. Finally, Alice sends to Bob the position of the channel coefficients over the public channel. Hence, Eve also knows which coefficients were dropped and which ones were selected but she does not have any additional information on their value. Therefore there is no information leakage during the channel decorrelation step.

1.3.1.3 Quantization

After measuring the radio channel, Alice and Bob jointly employ an algorithm to quantize the channel taps that they have estimated in order to generate a common sequence of key bits, under reciprocity assumption.

However, due to noise and channel estimation errors, Alice and Bob may disagree on some key bits. Several quantization algorithms employing censoring schemes have been developed to limit this mismatch between Alice and Bob keys.

A typical censoring algorithm defines guard band intervals and discards any channel measurement falling into them [11]; leading to an inefficient exploitation of channel measurements and to a lower number of generated key bits.

Other schemes employ different quantization maps where each one is adapted to the channel observations, e.g. Channel Quantization Alternate (CQA) algorithm [11]. The principle consists in choosing the adaptive quantization map where the

current observation is less sensitive to mismatch. Moreover this method keeps higher number of key bits. Consequently, CQA algorithm is applied on complex channel coefficients to generate secret key bits in remaining of the chapter.

1.3.1.4 Information reconciliation

This step suppresses remaining mismatches between Alice and Bob keys by using secure sketch based on error-correcting codes [21]. The key computed by Alice is considered as the reference secret key that Bob wants to obtain using the key K_b extracted from his channel measurements.

Alice first selects a random codeword c from an error-correcting code $\mathscr{C}$. She then computes the secure sketch $s = K_a \bigoplus c$ and sends s to Bob over the public channel. Bob subtracts s from its computed key K_b : $c_b = K_b \bigoplus s$ $(= K_b \bigoplus K_a \bigoplus c)$, decodes c_b to recover c and gets $\hat{c}$. Finally Bob computes K_a by shifting back and gets $(K_a) = \hat{c} \bigoplus \hat{s}$.

Perfect reconciliation is achieved when Bob perfectly retrieves the random codeword chosen by Alice, meaning that $c = \hat{c}$. As a result, there is no mismatch between Alice and Bob keys ($K_a = K_b$).

The secure sketch s, sent over the public channel, allows the exact recovery of the secret key without revealing the exact value of the key. However, s might leak some information on the secret key over the public channel as Eve can also use the secure sketch to retrieve the secret key K_a. Thus, a final step is then necessary to suppress the leaked information and to improve the quality of the secret key.

1.3.1.5 Privacy amplification

The objective of the privacy amplification step is to erase the information leaked to Eve on the secret key during the information reconciliation step and to improve the randomness of the key. We interpret the secret key K as an element of the Galois Field GF(2^n) and we choose the following two-universal family of hash functions [22] where n is the number of bits of the key K.

For $1 \leq r \leq n$ and for $a \in \mathrm{GF}(2^n)$, the functions $\{0,1\}^n \rightarrow \{0,1\}^r$ assigning to the key K the first r bits of key $aK \in \mathrm{GF}(2^n)$ define a two-universal family of hash functions. r is the final length of the secret key. In practice, at each new key computation, the parameter a is randomly chosen by Alice who sends it to Bob over the public channel. Alice and Bob then compute the product $aK \in \mathrm{GF}(2^n)$.

The hash mechanism spreads any bit error all over the final key $(aK)_{(r \text{ bits})}$ (first r bits of aK), thus when Eve tries to recover the initial key K (at the reconciliation step), any error on K will make the final key $(aK)_{(r \text{ bits})}$ unusable for her. Nevertheless, Bob has to perfectly recover the initial key K (i.e. reconciliation should be perfectly achieved) in order to get the usage of the final key $(aK)_{(r \text{ bits})}$.

1.3.2 Simulation results from single sense recorded signals

In this section we generate keys from real LTE and WiFi signals acquired using the PHYLAWS test bed presented in 1.3 and described in [13]. The test bed emulates

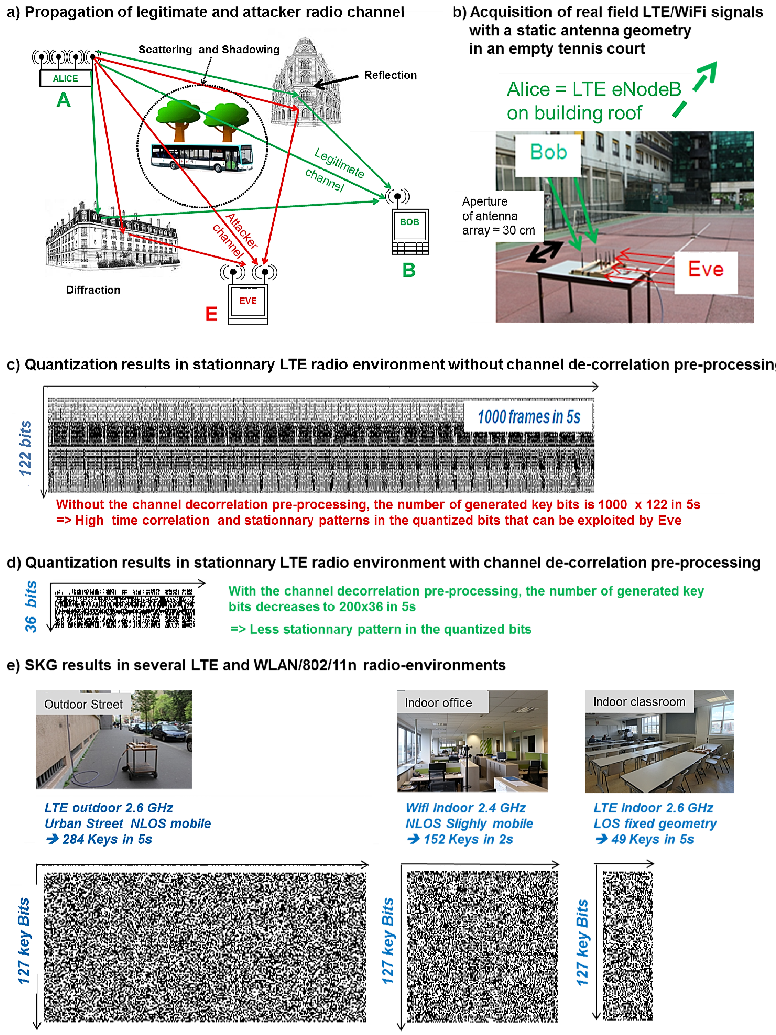

Figure 1.3: SKG principle and results.

Bob and Eve. Bob is considered to have 2 antennas spaced out of 33 cm corresponding to 3λ where λ is the signal's wavelength. Eve is considered to have 4 antennas spaced out of 11 cm corresponding to λ.

1.3.2.1 Impact of the SKG pre-processing step on the randomness of generated keys

Figure 1.3c shows the output of the CQA quantization algorithm applied on LTE signals which were recorded during 5 seconds in a very stationary propagation en-

Table 1.1: NIST test results

	LTE indoor 2.6 GHz		LTE outdoor 2.6 GHz		WiFi LOS 2.4 GHz		WiFi NLOS 2.4 GHz	
NIST test	Frequency	Runs	Frequency	Runs	Frequency	Runs	Frequency	Runs
Quantization	98% (48/49)	27% (13/49)	99% (281/284)	80% (228/284)	87% (132/152)	84% (128/152)	100% (171/171)	99% (169/171)
Amplification	100% (49/49)	100% (49/49)	100% (284/284)	100% (284/284)	99% (151/152)	98% (149/152)	100% (171/171)	99% (170/171)

vironment at 2627.5 MHz with a total bandwidth of 10 MHz. CFR were computed from the Primary Synchronization Signal that occupies only 1.4 MHz.

When using 4 quantization regions, the CQA produces 1000 frames detections and 122 secret bits per frames. However, we can notice a repetitive pattern on the generated keys meaning that CFR coefficients are highly correlated in time and frequency. This high correlation represents a major vulnerability as the generated secret key bits will not be random enough.

Figure 1.3d shows key bits obtained when the channel coefficient decorrelation processing is applied on the same record. The algorithm manages to extract the useful information and remove most of the repetitions of the bit pattern. Hence the number of key bits is reduced at the output of the quantization algorithm but the correlation between obtained bits is significantly decreased both in time and frequency.

1.3.2.2 Evaluation of the randomness of the keys using NIST Statistical tests

In this section, the quality of keys generated from previous records of LTE and WiFi signals is evaluated with two randomness tests defined in the NIST statistical test suite [14].

NIST frequency mono-bit test: the goal of this test is to determine whether the numbers of 0s and 1s in the key are approximately the same, as expected for a truly random sequence. Table 1.1 provides the percentage of keys that passed the frequency mono-bit test for the previous LTE and WiFi signals. As expected, almost all the keys pass the test after quantization since the CQA algorithm intrinsically distributes 0s and 1s in a uniform way.

NIST runs test: the goal of this test is to determine whether the oscillation between 0s and 1s is too fast or too slow compared to what expected for a truly random sequence. The results in table 1.1 shows that after quantization, only 27% of keys generated in the stationary LTE indoor environment pass the runs test whereas a high percentage ($\geq 80\%$) is achieved with keys generated in other environments which are much more dispersive.

The runs test better captures the randomness of a sequence.

As expected, near 100% of generated keys pass NIST tests after privacy amplification step, even in the static indoor environment. This final step of the SKG scheme is therefore crucial for practical application in low dispersive radio environments and narrow band signals.

Table 1.2: Entropy estimates

		Min-entropy estimates					
	Antennas	Bob_1	Bob_2	Eve_1	Eve_2	Eve_3	Eve_4
Min-entropy	LTE LOS 2.6 GHz	19.5%	50%	32.4%	22.6%	28.9%	32.4%
	WiFi NLOS 2.4 GHz	63.1%	65.2%	74%	69.7%	76.2%	74%
		Max mutual information					
	Antennas	Bob_1 - Bob_2	Bob_1 - Eve_1	Bob_2 - Eve_1	Bob_1 - Eve_4	Eve_1 - Eve_2	Eve_3 - Eve_4
Max mutual information	LTE LOS 2.6 GHz	19.7%	16.5%	38.6%	24.9%	84%	73.9%
	WiFi NLOS 2.4 GHz	19.8%	18%	20.6%	19.4%	79.7%	85%

1.3.2.3 Entropy estimation and analysis

The aim of this section is to evaluate the percentage of entropy bits extractable from the radio channel in realistic radio environment. To do so, we estimate the min-entropy of channels, first between Alice and Bob, then between Alice and Eve, at the output of the quantization step of the SKG scheme (without applying the channel decorrelation). The computation uses NIST tests for estimating the min-entropy of non-IID sources described in [23]. We also estimate the joint entropy and the maximum mutual information between pairs of antennas in order to evaluate the percentage of information shared by two distinct antennas. Finally, for a given pair of antennas, the entropy and the mutual information can provide us an experimental insight on the percentage of secure entropy bits.

Table 1.2 provides the entropy estimates for the six antennas of the PHYLAWS test bed shown in Figure 1.3b. The results are provided for two extreme propagation environments. The first one, very stationary, is an empty tennis indoor court surrounded by building on the top of which is an LTE e-nodeB. The configuration is fixed and LOS. The second one, much less stationary is an indoor office where antennas are slightly moving. WiFi signals come from NLOS access point. The results show that there are at least 20% of entropy bits in the first (worse) case and around 70% of entropy bits in second (better) case. In addition, the computed maximum value of the mutual information between pairs of antennas reveals that one antenna on Eve's array shares only few information (around 20%) with one antenna on Bob's array.

1.3.3 Simulation results from dual sense LTE signals

The application of the practical Secret Key Generation scheme to LTE is straightforward as the scheme only needs access to the channel estimates in the frequency domain, which are readily available in the physical layer. In order to assess its performance in a LTE system, Monte-Carlo simulations have been performed using MATLAB.

1.3.3.1 Simulators

For performance assessment, we use the MATLAB-based LTE link-level simulators [24] developed by Technical University of Vienna. The simulators implement standard-compliant LTE downlink and LTE uplink transceivers with their main fea-

tures, i.e., basic channel models, modulation and coding, multiple-antenna transmission and reception, channel estimation, multiple-user scenarios, and scheduling. The LTE link-level simulators include, among other basic channel models, the QuaDRiGa channel model [25], which can model realistic distance-dependant correlation of radio propagation between Alice-Bob, Alice-Eve, and Bob-Eve channels. In the simulations indeed, only the large-scale channels parameters are spatially correlated.

1.3.3.2 Channel coefficient estimates

Estimates of the channel coefficients are computed for each subcarrier carrying known sequences and each transmit and receive antenna pair, then averaged over the sub-frame to provide only one coefficient per sub-frame and per subcarrier per antenna pair. In the downlink, Bob (and Eve) can use the downlink Reference Signals (RS) over the whole bandwidth and the channel estimates are obtained by dividing the received signal at the pilot tones or reference sequence location by the known transmitted signal. In the uplink the situation can be different as the Sounding Reference Signals (SRS) are not mandatory and one cannot rely on them. The De-Modulation Reference Signals (DMRS) are used to estimate the channel at Alice. Alice thus has knowledge of the channel limited to the resource allocated for the uplink transmission for Bob.

The subcarriers in the frequency domain are selected such that they hold estimates in both DownLink (DL) and Uplink (UL) directions. However, in the simulations herein, all the resource blocks are allocated to Bob and the bandwidth limitation is not taken into account.

Considering now the Time Division Duplex (TDD) configuration of LTE RAT, we need to ensure that the reciprocity assumption is still valid. For this, the channel estimates obtained at adjacent downlink and uplink sub-frames should be used, which happens when the system switched from uplink to downlink. The sub-frame indexes at which the channel coefficients are extracted at Alice and Bob/Eve depend on the TDD configuration. We assume here a TDD configuration that allows us to extract two sets of channel coefficients per frame.

1.3.3.3 Simulations scenarios and parameters

The simulations process is such that the QuaDRiGa channel coefficients are created and then used first in the downlink LTE simulator and second in the uplink LTE simulator. At the end of this run, the secret keys generated by Alice, Bob, and Eve are compared. A simulation run is set to last 100 frames.

Alice is a fixed base station. Bob and Eve are mobile and follow the same track at the same speed, which in the simulations is a straight line. The speed depends on the radio environment. Alice uses a 4-antennas spatially-uniform linear array and both Bob and Eve use a 2-antennas array. The signal bandwidth is set to 10 MHz and the carrier frequency is 2.6 GHz. The channel model is block-fading and the channel estimation uses the least-square methods as provided in the LTE simulators. The SNR is defined as the average SNR at Bob for the duration of the simulation.

Several standard radio propagation environments have been tested: A1 indoor office, B1 urban micro-cell, and C2 urban macro-cell [26]. The minimum distance between Bob and Alice has been set to 1, 10, and 50 m, respectively. The mobiles' speed has been set to 1 m/s, 2 m/s and 14 m/s in A1, B1, and C2, respectively. Eve can be placed at various distance from Bob. The radio propagation can either be LOS or NLOS.

The SKG algorithm outputs a fixed key length of 127 bits. Time and frequency decorrelations are always used. After several tests, the de-correlation thresholds T_f and T_f have been set to value 0.5, that achieves a suitable trade-off between the number of extracted keys and their randomness quality.

Results with and without spatial decorrelation are presented. When spatial decorrelation is used in a LOS environment, the LOS component is removed.

The quantization of the real and imaginary part of the pre-processed channel coefficients produces one bit each, i.e., two regions are used. The coding rate of the reconciliation BCH code varies in order to correct the errors between Bob's and Alice's keys. This coding rate needs to be tailored to the SNR on the channel estimates in order to correct errors between Bob's and Alice's keys while preventing Eve from correcting the errors in her keys. In other words, the coding rate is set such that Bob is able to correct the maximum number of errors at each simulation.

For each separation distance between Bob and Eve and each SNR values, 100 channel realizations, corresponding to 100 simulation runs, are processed and statistical distributions of various figure-of-merit over those channel realizations can be extracted.

1.3.3.4 Simulation results

In order for the SKG to work well, Eve should not be able to estimate the key that Alice and Bob have extracted from the channel estimates, Alice and Bob should agree on the same keys, and these keys should have good entropy quality.

When considering the security of the keys, the BER between the keys extracted at Alice and Eve is the main figure-of-merit to be measured. When considering the key agreement, the mismatch between the keys estimated at Alice and Bob will also be measured in order to assess the effect of the channel estimation error, after each step of SKG algorithm: quantization, reconciliation, amplification.

When considering the keys' quality, the intrinsic randomness of the key will also be assessed by using the NIST randomness tests (frequency mono-bit and run tests). These tests are performed on all keys obtained by Bob for a specific SNR value over all channel realizations.

An example of simulation results is shown in figure 1.4 which is relevant to the urban micro-cell environment B1 for Bob and Eve moving on a straight line at 2 m/s. Figure 1.4 represents the cumulative distribution functions (CDF) of the BER of Bob's keys (column 1) and Eve's keys (columns 2 to 4) compared to Alice's keys.

The first column, which shows the results at Bob's side, evaluates the key agreement efficiency. The next columns, which shows the results at Eve's side (for increasing distances between Bob and Eve) evaluate the key security.

The impact of the value of the SNR is represented in each case (4 curves per figure).

The first line shows the results for the LOS scenario with no spatial decorrelation and the second line shows the results for the LOS scenario with spatial decorrelation.

The third and fourth lines replicate the results of the first and second line for the NLOS scenario.

The results of Figure 1.4 above show the following:

- The mismatch between Bob and Alice reduces as the SNR increases.
- In the NLOS case, a separation distance of one wavelength (λ) between Eve and Bob is enough to ensure the key's security against Eve. However in the LOS case, the use of spatial decorrelation might be required to achieve the same security.
- When spatial decorrelation is performed, a higher SNR is needed for Bob to estimate the right key.
- Especially in LOS configuration, the use of channel decorrelation increased the number of keys extracted with correct quality.
- In terms of key quality, more than 99% of the keys passed randomness tests after amplification, with or without spatial decorrelation, and for both LOS and NLOS.

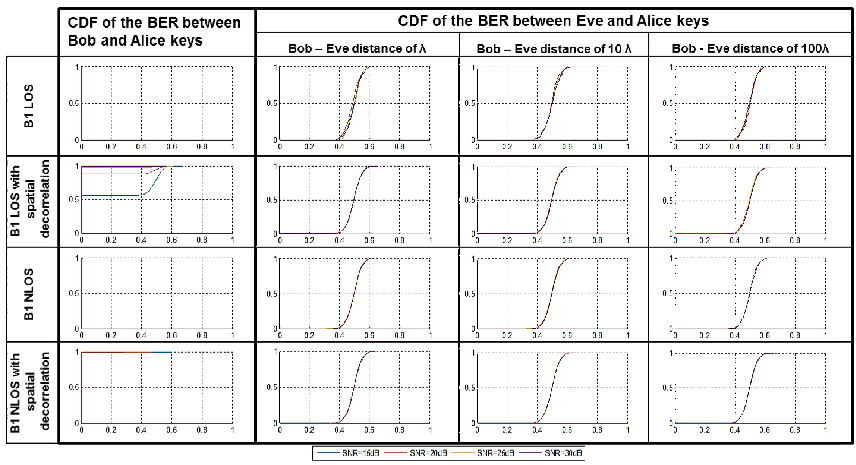

Figure 1.4: BER of Bob and Eve's keys compared to Alice's keys for various environments and SNR values. Movement of Bob and Eve is 2 m/s straight line within the urban micro-cell environment B1.

1.3.3.5 Discussion

The SKG algorithms implemented in the LTE simulator has proven to work well in most of the simulated radio propagation environments. The minimum distance between Bob and Eve in order to protect the keys extracted at Alice and Bob depends on the radio environments (A1, B1, C2), whether there is LOS or NLOS, and on the use of spatial decorrelation.

Especially in A1, and in B1 too, the distance of one wavelength (λ) is enough to prevent Eve from recovering the secret key in both NLOS and LOS cases, when SKG includes spatial decorrelation in LOS cases. This impacts the needed working SNR, as spatial decorrelation needs a higher SNR to lead to the same match between Alice and Bob compared to the situation when it is not used. NLOS leads to more keys and does not require the use of spatial decorrelation.

In LOS cases of C2, the algorithm still does not protect well Alice's and Bob's keys (against Eve's attempts to recover the keys) at a distance between Bob and Eve of 10λ, even when using spatial decorrelation. However, in NLOS, the keys are protected already at a distance of 10λ.

In C2, spatial decorrelation and channel decorrelation pre-processing improve the secrecy Bob's and Alice's keys in both LOS and NLOS cases. In all simulations, the quality of the key was high after amplification, leading to more than 99% of key satisfying the used randomness tests.

1.3.4 Experimental results from dual sense WiFi signals

In this section we generate keys from dual sense real signals emitted and received by WiFi chipsets designed by Celeno Communication Ltd. We then evaluate the randomness and secrecy of generated keys.

1.3.4.1 WiFi Test bed and measurement environment

We use here the Wifi dedictated part of the PHYLAWS's test bed shown in figure 1.5a and described in [13]. Each chipset is based on a Software Defined Radio architecture, using a Digital Signal Processing core that enables to implement algorithms in the physical layer on top a real WiFi system. The test bed supports operation in both 5 GHz and 2.4 GHz bands by using two different chips developed by the fabless semiconductor company Celeno Communications Ltd: the CL2440 is a 4x4 AP chip supporting 5 GHz operation (for up to 80 MHz bandwidth), while the CL2442 is a 4x4 AP chip supporting 2.4 GHz operation (for up to 40 MHz bandwidth). The test bed is also hooked to the local network via Ethernet for control and for data extraction. The antenna spacing on the test bed is always more than half of a wave length (2.7 cm in 5.5 GHz and 6.25 cm in 2.4 GHz) to provide adequate diversity. Experiments are carried out in an testing apartment. The apartment provides a clean testing environment that is relatively interference free. Various indoor NLOS and LOS scenarios can be emulated (figure 1.5).

1.3.4.2 Processing applied for bi-directional sounding exchange

For channel measurements, the testbed is used as both a transmitter and receiver. The transmitting device transmits a channel sounding frame, as defined in the 802.11 standard. This frame, referred to as Non Data Packet (NDP) in Wifi standards, is used in 802.11ac/n for explicit sounding exchange. The channel estimates are therefore a good representation of channels as seen by real WiFi devices, including all implementation and RF impairments.

Alice first sends a sounding frame (at 2462 MHz with a bandwidth of 20 MHz, or at 5180 MHz with a bandwidth of 80 MHz) which is captured by Bob and Eve. Bob sends back to Alice a sounding frame. Alice, Bob and Eve extract 4x4 channel estimates.

CFR estimates are then processed offline: Alice, Bob and Eve first compensate their channel estimation for timing errors and normalize each channel coefficient.

They extract secret key from estimated CFR with the processing described above: channel decorrelation, quantization with CQA algorithm, information reconciliation with BCH codes, privacy amplification with two-universal family of hash functions (and key length reduction , when necessary).

The randomness of generated keys is evaluated using the Intel Health Check [15] applied on keys after quantization step and after privacy amplification steps. The reciprocity is evaluated by computing the mismatch between Alice and Bob's keys. Finally, the secrecy is evaluated by computing the BER between Bob and Eve generated keys.

1.3.4.3 Practical implantation of SKG from bi-directional channel estimates by WiFi chipsets

Figure 1.5a describes the testbed and the experimental testing conditions of the SKG scheme. After channel estimation over real field radio link, an offline Matlab script runs the SKG scheme on three consecutive channel sounding exchanges between Alice and Bob. For her own attempts to recover Alice's and Bob's keys, Eve also captures the signal sent by Alice. The parametrization of the SKG protocol of figure 1.5 is the following.

At Alice's side:

- Pre-processing: if applied, selection of low-decorrelated CFR frames with parameters $T_t = 1$ and $T_f = 0.4$
- Quantization of amplitude and phase of CFR into 4 regions, that provides secret keys of 127 bits length
- Computation of secure sketches used by Bob for information reconciliation using the FEC code BCH $(127, 15, 27)$
- Privacy amplification of the secret keys without key length reduction
- Key concatenation to final length of 256-bits
- Test of the key randomness after quantization and amplification with the Intel Heath Check [15]. All keys should pass the test after privacy amplification since a hash function is used during this step.

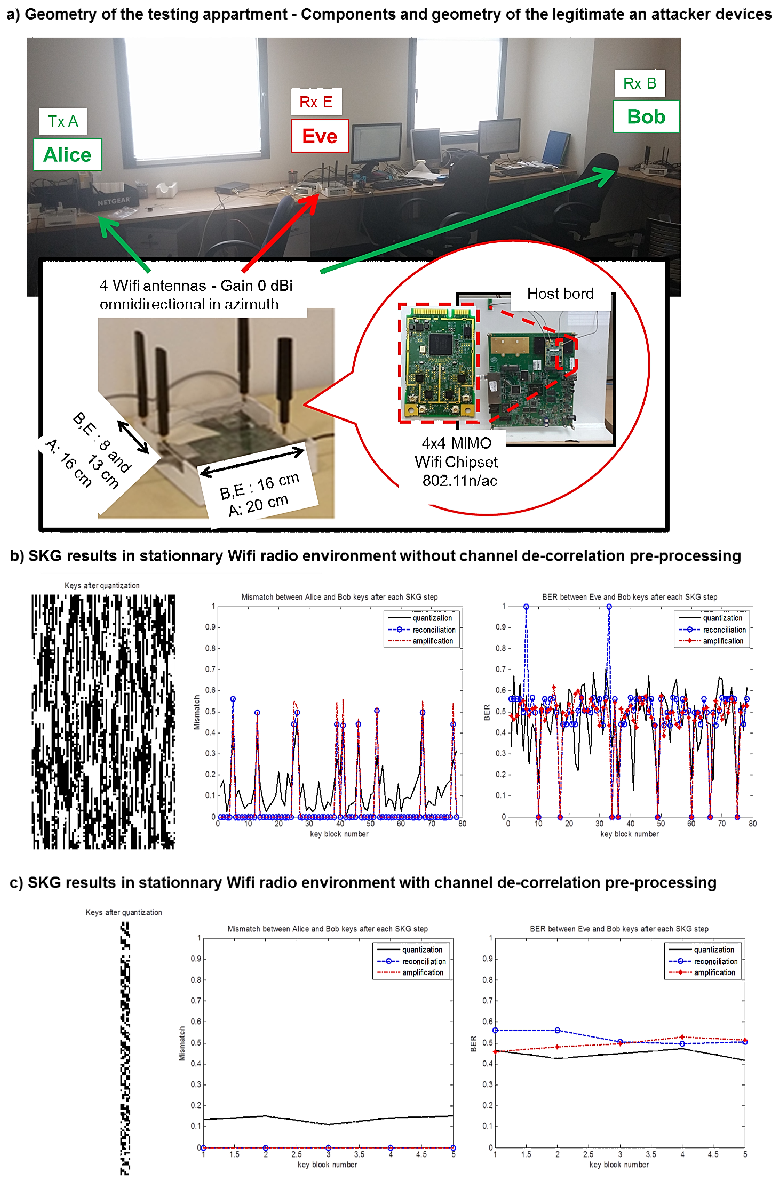

Figure 1.5: SKG experimental testbed and results from dual sense CFR.

- Selection of the 256-bits keys that pass the Intel Health Check after quantization and amplification.
  Final secret keys are the output of the privacy amplification step.

Alice also sends over the public channel a message containing indexes of the selected CFR frames and quantization map, secure sketches, hashing parameters and indexes of successful 256-bit secret keys. Although this message helps Bob's to compute same secret keys than Alice, secure sketches sent for reconciliation might leak some information to Eve as it allows her to correct errors she made on Alice's keys. This leaked information can be mitigated by reducing the length of extracted keys during the privacy amplification step.

Bob's and Eve's side (In our experiments, Eve performs exactly the same SKG steps as Bob):

- Pre-processing: selection of CFR frames according to the indexes sent by Alice.
- Quantization of channel measurements taking into account quantization map indexes sent by Alice.
- Information reconciliation step using secure sketches sent by Alice and using BCH (127,15, 27).
- Privacy amplification of the keys using the hashing parameters sent by Alice. Key concatenation to 256-bits.
- Selection of successful 256-bit secret keys according to the indexes sent by Alice.

1.3.4.4 Results without channel decorrelation processing

Figure 1.5b shows the keys extracted after quantization by Alice from channel measurements when no pre-processing step is performed. 78 keys of length 127-bits were generated but none of them passed the NIST runs test. 38 keys of length 256-bits were obtained by concatenating previous keys and none of them passed the Intel Health Check.

Figure 1.5b also shows the mismatch between Alice and Bob, and the BER between Bob and Eve's keys after each step of the SKG processing: quantization, information reconciliation and privacy amplification.

According to the results, Bob often computes different keys than Alice while Eve manages to recover some of the secret keys: SKG performance is weak in this case.

1.3.4.5 Results with channel decorrelation processing

Figure 1.5c shows the keys extracted after quantization by Alice from channel measurements when the channel decorrelation pre-processing is performed with thresholds values $T_t = 1$ (no selection in time domain in this particular test case, because only 3 time instances were available in the records) and $T_f = 0.4$. Here, 5 keys of length 127-bits were generated and 4 of them passed the NIST runs test. 2 keys of length 256-bits were obtained by concatenating previous keys and both of them passed the Intel health Check.

After privacy amplification, all keys passed both NIST runs test and Intel Health Check.

Using the same representation for figure 1.5b, figure 1.5c also shows the BER be-

tween Alice and Bob (expected to be close to 0 when the processing is successful), and the BER between Bob and Eve's keys (expected to be close to 0.5 when the processing is successful). Here, Bob successfully computes the same keys than Alice while Eve's BER is always very close to 0.5: the SKG perfectly works. This illustrates the importance of the channel de-correlation pre-processing that selects only frames with low cross-correlation, increases the available entropy into the selected frames while decreasing the mutual information between Alice and Eve's channel measurements relevant to these frames, leading at the end to a greater number of secure keys.

1.4 Conclusion: security upgrades opportunities for Radio Access Technologies

1.4.1 Existing vulnerabilities

In the current architectures, no protection is applied on the transmission of several crucial parameters that are exchanged during the first access stages with the network (and during roaming procedures). These parameters are used for performing the authentication with privacy, and setting up the integrity and the confidentiality protections of the user and control planes.

Concerning the authentication procedure, the following crucial messages are exchanged in clear text:

- in 2G: RAND, SRES and TMSI;
- in 3/4G: RAND, RES, AUTN, KSI_{ASME} and TMSI.

Radio access of public networks is managed with identification procedures, involving subscriber and network identification numbers, authentication procedures, involving dual sense exchanges of random input parameters, parallel computation and output check at mobile and at core network. In radio-cell networks and in WLAN networks, this processing is performed very early (before the establishment of ciphering keys).

Several crucial parameters (such as IMSI, IP or MAC address) transmitted over the physical layer are not encrypted during the attach or roaming procedures (especially international roaming).

Furthermore, subscriber's and equipment's parameters are used for performing the authentication, setting up the integrity and the confidentiality protections (of both user and control protocol layers). Unfortunately, they are transmitted in clear text with significant temporization times in their transmission procedures. Finally they are very vulnerable to many kind of attacks such as passive monitoring, active hacking (denial of service, replay attack), man in the middle and spoofing.

Concerning the identification procedure of radio-cells, the following crucial subscriber or equipment parameters are exchanged in clear text.

- In 2G, 3G and 4G radio cellular networks: usually TMSI, and when requested (because of international roaming or failure of conventional TMSI identity check), IMSI, IMEI, IMEISV or GUTI

- In WLAN standards: IP Address, SSID, and even the MAC address in first attach procedures and in many other dedicated procedures.

Concerning the authentication procedure of radio-cells, the following crucial messages are exchanged in clear text

- In 2G radio cellular networks: random parameter RAND, SRES at the input and output of the single terminal authentication check by the network
- In 3/4G radio cellular networks: random parameter RAND, RES, AUTN and KSI_{ASME} at the input and output of the dual sense authentication check.

In general, the interception of identifiers (such as mentioned above) reveals sensitive information such as subscriber identity and location. It thus allows Eve to focus on the monitoring of target messages of given subscribers, to build replay attacks, to spoof and impersonate terminals and nodes, etc. See [13] and [27] for more details.

Moreover, the hacking of long term secret keys K/Ki by cyber attackers have been recently reported (for more details see [13]), Therefore, it then becomes easy for a passive eavesdropper to retrieve the other necessary parameters by monitoring the signaling and access messages. First, Eve can recover authentication and cipher keys, then Eve can break all protections (such as the integrity control and the confidentiality of an on-going communication).

Finally, a major security enhancement of existing and future radio-networks would be achieved by preventing the decoding capability by third parties of sensitive message exchanged at the radio air interface between nodes infrastructure and terminals. In particular, the protection of the identification procedures, authentication protocols and cipher establishment should be reinforced, by removing any capability for Eve to intercept and decode the associated parameters that are today given for free at the radio layer. This would strongly enhance privacy and confidentiality, and this would significantly mitigate the consequences of a leakage of K/Ki keys.

1.4.2 Proposed solutions for securing radio access protocols with Secret Key Generation

As explained above, the principle of SKG is to re-use radio-channel sounding outputs as common random sources of legitimate radio-devices under an assumption of reciprocity, without any shared secret.

For any radio access using a Time Division Duplex protocol (such as defined in WLAN, 4G radiocells and expected 5G networks), the SKG technology thus appears very suitable at early stages. As soon as radio channel measurements are enabled from prior frame and slot synchronization, reception of signaling, transmission and reception of access messages, initialization of equalization and Quality of Services procedures etc., their outputs could be re-used of SKG purposes.

SKG can also apply to Frequency Division Duplex (FDD) if the user equipment and the node have the ability to operate on the same carrier frequencies for the access stages

Moreover, when considering any kind of public radio access protocols, even FDD protocols such as defined in most of 2G and 3G radio cellular, the study carried out in [13] pointed out a key-free secure pairing technology.

This secure pairing procedure is based on dual sense low power self-interfering signals (referred to as tag signals) that allow accurate measurements of Channel Impulse Responses (CIR) and support Interrogation and Acknowledgement Sequences (IAS) between terminals and nodes. Very early in the radio access, IAS provide dual sense paired CIR (which are output by the synchronization and equalization procedures of the dual sense tag signals) at Alice and Bob while they ensure the secure pairing of Alice's and Bob's devices by checking the CIR.

Secret key generation can be input by these paired CIR. Moreover, the exchanges of paired tag signal would offer a native authenticated public channel for exchanging information during the SKG processing: frame index in channel decorrelation preprocessing, plane index in quantization algorithm, secure sketch into reconciliation procedure, etc.

1.4.3 Practical usage of Secret Key Generation into Radio Access Technologies

We finally consider some possible practical usage of SKG.

As seen before, the output keys of 128 or 256 bits, could protect early messages exchanged between Alice and Bob

- as a direct protection of signaling and access messages,
- as a private key (shared only by Alice and Bob) to be used in a traditional cipher scheme applied to sensitive contents of the signaling and access messages.

Keys can be stored in terminal memory and network data base and changed over time when necessary (during on-going communications by using the output or equalization procedures).

Many other potential usages appear for WLAN and radio cellulars are listed below.

- to facilitate new attach procedures and new roaming procedures in idle mode.
- To input and facilitate secure schemes of upper protocols layers during ongoing communication. Some examples relevant to in WLAN and radio cellular network are:
  - protection of the headers of IP packets,
  - protection of control frames,
  - protection of return information messages in explicit artificial Noise and Beam forming schemes defined in some WLAN (802.11n/ac),
  - input of the integrity control and cipher schemes of data stream with non-mathematical random.
  - Usage of generated keys as temporal identifier

  - Usage as integrity control check to prevent intrusion of messages, rogue and man in the middle attacks of on-going communications
  - Detection of intrusion attempts (including false authentication requests): if the node and the terminal receive in parallel similar messages with uncorrelated keys generated from different channel instances.
  - Usage as a pre-shared key or header input in existing ciphering scheme.
  - The use of the secret key to protect ultra low latency transmission expected in the future, where current stream ciphers are too slow.
  - To protect the un-ciphered near field communication.
- To cope with the problem of distribution and management of secret keys with the deployment of massive Internet-of-Things.

1.5 Bibliography

[1] M. Bloch and J. Barros, *Physical-layer security: From information theory to security engineering*. Cambridge University press, 2011.

[2] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. on Inform. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[3] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. i. secret sharing," *IEEE Trans. Inform. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul 1993.

[4] A. Hassan, W. Stark, J. Hershey, and S. Chennakeshu, "Cryptographic key agreement for mobile radio," *Digital Signal Processing*, vol. 6, pp. 207–212, Oct 1996.

[5] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *14th ACM international conference on Mobile computing and networking*, September 2008, pp. 128–139.

[6] S. Jana, S. Premnath, M. Clark, S. Kasera, N. Patwari, and S. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *15th annual international conference on Mobile computing and networking*, September 2009, pp. 321–332.

[7] L. Lai, Y. Liang, and W. Du, "Cooperative key generation in wireless networks," *IEEE JSAC*, vol. 30, no. 8, p. 15781588, 2012.

[8] J. Zhang, R. Woods, T. Duong, A. Marshall, and Y. Ding, "Experimental study on channel reciprocity in wireless key generation," in *IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, July 2016, pp. 1–5.

[9] T. Mazloum, F. Mani, and A. Sibille, "Analysis of secret key robustness in indoor radio channel measurements," in *Proc. 2015 IEEE 81st Vehicular Technology Conference (VTC-Spring)*, May 2015.

[10] T. Mazloum and A. Sibille, "Analysis of secret key randomness exploiting the radio channel variability," *International Journal of Antennas and Propagation (IJAP)*, 2015.

[11] J. Wallace and R. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," *IEEE Trans. Inform. Forensics and Security*, vol. 5, no. 3, pp. 381–392, Sept 2010.

[12] T. Mazloum, "Analysis and modeling of the radio channel for secret key generation," Ph.D. dissertation, Telecom ParisTech, 2016.

[13] "Phylaws," http://www.Phylaws-ict.org.

[14] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, and L. E. Bassham III, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. Information Technology Laboratory, NIST, Gaithersburg, Maryland, Tech. Rep., 2010.

[15] M. Hamburg, P. Kocher, and M. Marson, *Analysis of Intels Ivy Bridge Digital Random Number Generator*, 2012.

[16] "Volcano lab," http://www.siradel.com.

[17] V. Degli-Esposti, F. Fuschini, E. Vitucci, and G. Falciasecca, "Measurement and modelling of scattering from buildings," *IEEE Trans. Antennas and Propagation*, vol. 55, no. 1, pp. 143–153, Jan 2007.

[18] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inform. Forensics and Security*, vol. 2, no. 3, pp. 364–375, Sept 2007.

[19] C. Chen and M. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *Mobile Computing, IEEE Transactions on*, vol. 10, no. 12, pp. 205–215, 2011.

[20] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels .ii. privacy amplification," *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 839–851, April 2003.

[21] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM Journal on Computing*, vol. 38, no. 1, pp. 97–139, 2008.

[22] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1915–1923, Nov 1995.

[23] M. Turan, E. Barker, J. Kelsey, K. McKay, M. Baish, and M. Boyle, *Recommendation for the Entropy Sources Used forRandom Bit Generation*. National Institute of Standards and Technology Special Publication 800-90B, NIST, Gaithersburg, Maryland, Tech. Rep., 2016.

[24] C. Mehlfuehrer, J. C. Ikuno, M. Simko, S. S, M. Wrulich, and M. Rupp, "The vienna lte simulators - enabling reproducibility in wireless communications research," *EURASIP Journal on Advances in Signal Processing*, vol. 21, 2011.

[25] S. Jaeckel, L. Raschkowski, K. Brner, , and L. Thiele, "Quadriga: A 3-d multicell channel model with time evolution for enabling virtual field trials," *IEEE Trans. Antennas Propag*, vol. 62, pp. 3242–3256, 2014.

[26] "Winner II channel models," https://www.ist-winner.org/WINNER2-Deliverables/D1.1.2v1.1.pdf.

[27] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.