COMBINING ARTIFICIAL NOISE BEAM FORMING AND CONCATENATED CODING SCHEMES TO EFFECTIVELY SECURE WIRELESS COMMUNICATIONS

Christiane L. Kameni Ngassa (Thales Communications and Security (TCS), Gennevilliers, France; Christiane.Kameni@thalesgroup.com); Jean-Claude Belfiore (Telecom ParisTech (TPT), Paris, France; jean-claude.belfiore@telecom-paristech.fr); Renaud Molière (TCS; Renaud.Moliere@thalesgroup.com); François Delaveau (TCS; Francois.Delaveau@thalesgroup.com); Nir Shapira (Celeno Communications, Ra'anana, Israel; Nir.Shapira@celeno.com)

ABSTRACT

In this paper we present a new scheme combining Artificial Noise Beam Forming and Secrecy Coding to strengthen the security of existing wireless communication systems. Artificial Noise and Beam Forming guarantees a radio advantage to legitimate users, which makes it possible to apply our Secrecy Coding Scheme to provide reliability and secrecy. This overall security protocol is compliant with existing widespread Radio Access Technologies and it can be considered as key-free add-on to improve security of the physical layer of wireless networks.

1. INTRODUCTION

Most of existing security mechanisms for wireless communication rely on pre-shared cryptographic keys to encrypt exchanged data. However, recent news about public Radio Acces Technologies (RATs) revealed that attackers can have access to these encryption keys by exploiting weakness of SS7 protocol and international roaming [1, 2]. Furthermore, the recent hacking of SIM card manufacturers to get encryption keys proves that the cryptographic key distribution approach can no longer be considered as completely secure [3]. Physical layer security (Physec) appears therefore as a crucial help to strengthen wireless communication security as it leverages inherent properties of the wireless channel to provide secrecy by remaining key-free. Secrecy (or wiretap) Coding is one of the main Physec techniques. Its goal is to provide both reliability and secrecy without using any secret key. This requires a radio advantage for the legitimate nodes and terminals [4]. Nevertheless, secrecy coding has major adavantages:

- SC needs only a guaranteed radio advanatage, no accurate radio-channel measurement. And no radio channel reciprocity are required. Any established and resilient radio protocol that achieves a controlled radio advantage to legitimate users offers the opportunity for Secrecy coding
- SC requires no secured radio link nor authentication
- SC is independent of eavesdropper's computational capability, thus it remains secure from attacks with unlimited computational power.

Nevertheless, the design of a practical wiretap code is very challenging: despite numerous theoretical results, secrecy coding schemes proposed in the literature apply only to ideal wiretap radiochannels and cannot be readily implemented in existing wireless communication networks.

In this paper we propose a practical implantation of secrecy coding schemes helped by Artificial Noise (AN) and Beam Forming (BF), this implantation, which is only slighly suboptimal when compared to theory [4] is derived form the works performed in the Phylaws Project (www-phylaws-ict.org) [5].

In §2, we describe how the Artificial Noise scheme provides a controlled radio advantage to legitimate users, while the Beam Forming allows reliable link to the legitimate terminal. Relevant considerations on the radio constraints are detailed in § 3.

In §4, we show how the concatenation of an "outer" polar code and an "inner" Forward Error Corrector (FEC) code applied to the legitimate messages builds a wiretap coding scheme. The outer polar code provides the link secrecy while the inner FEC code provides the link reliability as usual.

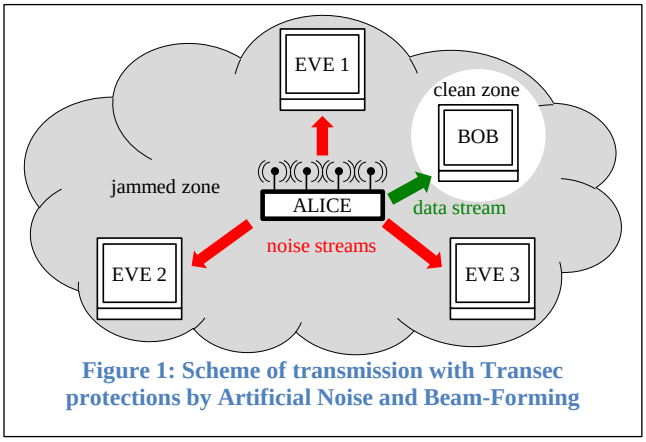

Figure 1: Scheme of transmission with Transec protections by Artificial Noise and Beam-Forming

In § 5, we study one particular example of this scheme with classical "inner" FEC built with LDPC and a "outer" Polar code (PC) or Red-Muller code (RMC) of limited lengths such as encountered in public RATs. We consider a typical scenario where two legitimate users (Alice and Bob) attempt to securely communicate in presence of an eavesdropper (Eve).

Simulation results are provided in § 6 which illustrated the promising performances of our Secrecy Coding Schemes and conclusion in §7 highlights its practical secrecy performance and the implementations perspectives in the next future.

2. ARTIFICIAL NOISE AND BEAM FORMING

2.1. Artificial Noise (AN) and Beam Forming (BF) for achieving radio advantage

Such schemes combine Beam-Forming of data towards the legitimate receiver and emission of interfering signals elsewhere. For AN purpose, the power of the artificial noise is controlled and steered to limit the link budget of eavesdroppers while optimizing the MIMO transmission scheme for legitimate links.

2.2. Artificial Noise processing

Most promising AN schemes studied in the literature proceed as follows [6]:

- Estimation of the legitimate Channel Frequency Response (CFR) or Channel Impulse Response (CIR), from Alice to Bob, and extraction of orthogonal directions of the legitimate CFR or CIR.
- Transmission of noise streams on orthogonal directions. As Eve cannot estimate the legitimate channel matrix, she is thus forced into low Signal to Interference Noise Ratio (SINR) regime and is unable to decode.
- Beam-Forming of the Alice-Bob data stream for Bob to maximize legitimate link budget. Bob extracts Alice's channel and suppresses orthogonal noisy channel directions thanks to Beam Forming. In ideal cases, the Interference at Bob's side completely vanishes and the Signal to Interference Noise Ratio at Bob's side reduces to a Signal to Noise Ratio ($SINR_{Bob}=SNR_{Bob}$).

When Artificial Noise and Beam Forming techniques are established, a better SINR is provided to Bob than to Eve in any case and the SINR at Eve's side is controlled by Alice. The relevant radio advantage $SINR_{Bob}$-$SINR_{Eve}$ is thus guaranteed and it can be further exploited by the legitimate link to compute secrecy codes.

2.3 A.N. and B.F. for initiating Secrecy Coding schemes

The goal of secrecy codes is to ensure reliable communication at the legitimate link and to avoid any information leakage elsewhere.

Secrecy codes conceal the information sent by Alice in the difference of channel capacity between Bob and Eve (difference of SINR in simplest cases such as AWGN channel). Therefore the legitimate receiver should have a better radio link than the eavesdropper. With this radio advantage, the secrecy capacity is positive and driven by the difference $SINR_{Bob}$-$SINR_{Eve}$. Without this permanent radio advantage, secrecy capacity is null.

Moreover, this radio advantage should be controlled: without this control, the secrecy capacity varies and Alice and Bob cannot properly choose and control the protected bits.

3. RADIO CONSIDERATIONS ON A.N.

3.1 Power of the jamming signal

Regarding Frequency Division Multiple Acess (FDMA), Time Division Mulytiple Acess (TDMA) and Code Division Mulytiple Acess (CDMA) RATs and regarding RATs based on Orthogonal Frequency Division Multiplex (OFDM) schemes, one has to consider the limit decoding sensitivity which is required in the standard in term of received Signal to Interfrence + Noise Ratio (SINR). This SINR is noted SRx/(JRx+NRx) and reduces to a Signal to Noise Ratio (SNR=SRx/NRx) when no Interference occur.

When the sources of artificial noise and user data stream are strictly co-located (i.e. same antenna elements at transmitting), Alice has to adjust the Jamming signal JTx to the user transmit signal STx to such a value that Eve has no chance of decoding even in optimal reception.

For RATs based on FDMA, TDMA or OFDM: $(STx/JTx) \leq (SRx/NRx)min$ leading to $JTx \geq STx / (SRx/NRx)min$. Most often, a co-located jamming signal at each orthogonal direction with power roughly equal to the user signal is enough to limit most of eavesdropping risk and a jamming signal 6 dB above the data stream would avoid any eavesdropping risk.

For RATs based on PN/CDMA schemes: $(STx/JTx) \leq (SRx/(JRx+NRx))min$ leading to $JTx \geq STx / (SRx/(JRx+NRx))min$. Example of UMTS: low data rate signals have spreading factors of 256 (24 dB), and $(SRx/(JRx+NRx))min$ is roughly -18 dB. Thus a co-located artificial jamming signal of 18 dB above the data stream would avoid any eavesdropping risk.

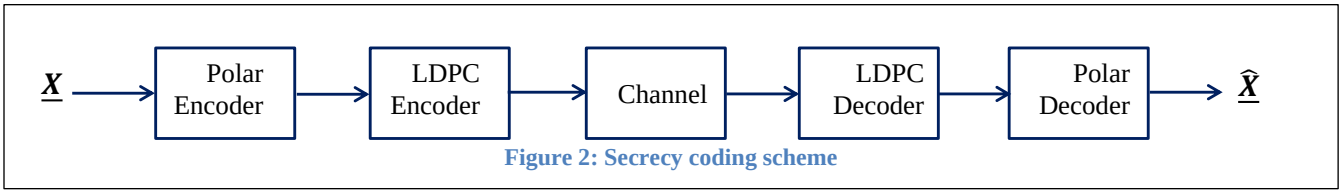

Figure 2: Secrecy coding scheme

3.2 Co-location of antennas transmitting the jamming signal and the user signal

When the sources of artificial noise and user data stream are not strictly co-located (i.e. different antenna or different antenna elements, such as in many scenarios of cooperative jamming), efficiency of artificial noise is highly dependent on the spatial correlation at Bob's side, and of the source separation capabilities at Eve's side.

The channel estimation performed by Bob over dedicated frames sent by Alice may not match perfectly for artificial noise issued from different locations of antenna.

Several questions relevant to Eve's capabilities regarding source separation remain open. Even with a very low distance (lower than a quarter of wave length), several experiments showed that an accurate location of Eve's multiple antennas combined with analog mitigation techniques and digital antenna processing such as power inversion may achieve practical discrimination of the transmitted steam with significant performance.

Nevertheless, even if discrimination of Alice's streams can be performed at Eve's side, recent experiments showed that the building of the legitimate channel by Eve seems always difficult to achieve.

Finally, the most resilient AN-BF schemes would uses co-located and even same antenna elements artificial noise and user data stream.

4. SECRECY CODING SCHEME

The design of secrecy codes for continuous channels is challenging [4]. However since Polar codes provide strong security for discrete channels [7], a first idea is to concatenate them to a capacity approaching code. In this way, the channel between the polar encoder and the polar decoder can be viewed as a Binary Symmetric Channel.

Thus, we propose a scheme which is composed of a LDPC code as inner code and of a polar code as outer code. The inner code can be any FEC codes employed currently for practical wireless communications such as LDPC codes or Turbo codes. The design of the inner code is therefore straightforward as we only follow the requirements defined in those standards.

In this work we consider particularly LDPC codes defined in 802.11 standard (WiFi).

4.1 Construction of the outer code using polar codes

We first consider two nested polar codes of length $N = 2^n$ as the outer code.

The rate of the first polar code is the target rate for Eve denoted R_E and the rate of the second polar code is the target rate for Bob, denoted R_B .

Since we suppose that legitimate users have a radio advantage over Eve, $R_E < R_B$. Therefore Eve can perfectly decode $N.R_E$ bits and Bob $N.R_B$. In order to confuse Eve and to ensure 0.5 error probability at her side, we send random bits over $N.R_E$ perfect bit-channels. In other words, over the bit-channels for which Battacharyya parameters are zeros.

The design strategy of the outer code is then the following.

- Battacharyya parameters are computed for Bob target's error probability at the output of the inner decoder
- Bit-channels are sorted in ascending order of their Battacharyya parameters
- Random bits are sent over the first $N.R_E$ bit-channels.
- Information bits are sent over the following $N(R_B - R_E)$ bit-channels
- Frozen bits (i.e. zeros) are sent over the remaining bit-channels.

4.2 Construction of the outer code using Reed-Muller codes

The constructions of Reed-Muller codes and polar codes are similar. The main difference is the selection of bit-channels over which information bits are sent. Indeed, for polar codes the selection criteria is the Battacharrya parameter while the selection criteria for bit-channels for the Reed-Muller codes is the Hamming weight of rows of the generator matrix. Consequently, for a given code length, the Reed-Muller code usually has a larger minimum distance and better performance than the corresponding polar code for small and moderate code length.

We propose to use Reed-Muller codes as an alternative to polar codes in the design of the outer code [8].

Table 1: Resulting secrecy codes

	Secrecy code 1	Secrecy code 2	Secrecy code 3	Secrecy code 4	Secrecy code 5
Inner code	LDPC code of length 1296 and rate 5/6 defined in the 802.11 standard				
Outer code	Polar code	Polar code	Polar code	Reed-Muller code	Reed-Muller code
Eve's target rate	0.1	0.1	0.1	0.05	0.05
Bob's target rate	0.6	0.5	0.4	0.5	0.4
(R,I,F)	(102, 512, 410)	(102, 409, 513)	(102, 307, 615)	(56, 430, 538)	(56, 330, 638)
Secrecy code rate	0.4	0.33	0.24	0.33	0.25

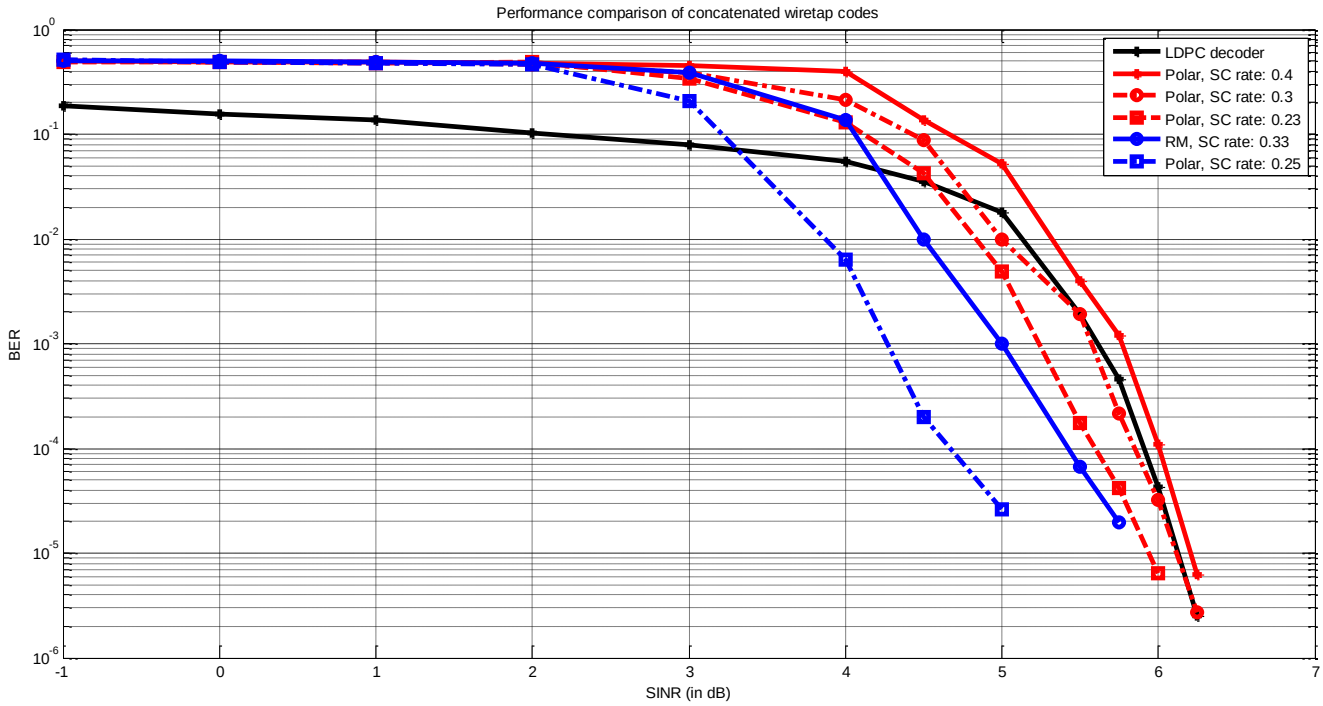

Figure 3: Performance of the designed secrecy codes

The design strategy of the outer code is then modified as follows.

- Hamming weights of generator matrix's rows are computed
- Bit-channels are sorted in ascending order of their Hamming weight
- Random bits are sent over the $N.R_E$ first bit-channels.
- Information bits are sent over the $N(R_B - R_E)$ following bit-channels
- Frozen bits (i.e. zeros) are sent over the remaining bit-channels.

5. EXAMPLES OF SECRECY CODES CONSTRUCTION

We use the LDPC code of length 1296 and rate 5/6 defined in the 802.11 standard as the inner code. The outer code is either a polar code of length 2^{10} = 1024 or a Reed-Muller code of the same length.

For simulation purpose, five outer codes were designed using polar and Reed-Muller codes of different rates.

The parameters of these five secrecy codes are presented in Table 1. Note that R, I and F denote respectively the number of random bits, information bits and frozen bits.

6. SIMULATION RESULTS

Simulations were carried out using MATLAB and messages were sent over an AWGN channel using a QPSK modulation.

6.1 Performance analysis

Figure 3 shows the performance of the designed secrecy codes.

- The black curve represents the Bit Error Rate (BER) at the output of the LDPC decoder

- Red curves represent the BER at the output of secrecy polar decoders
- Blue curves represent the BER at the output of secrecy Reed-Muller decoders

The results show that:

- When SINR $\leq$ 2 dB, the BER at the output of the five secrecy codes is equals to 0.5. Meaning that, all secrecy codes guarantee no information leakage if Eve's SINR is less than 2 dB. Only the polar based secrecy code with rate 0.4 (Secrecy code 1) guarantees no information leakage until 3 dB.
- All Reed-Muller based secrecy codes have better reliability performance than polar based secrecy codes.
- For a target error probability of 5.10^{-5} for Bob, the require radio advantage is only 3 dB to 4 dB.

These simulation results show that Eve cannot retrieve any transmitted information when a slight radio advantage ($<$ 4 dB) is provided to legitimate users. The secrecy is achieved at the cost of a limited increase in coding and decoding complexity.

Figure 4: Original image to be transmitted over the channel

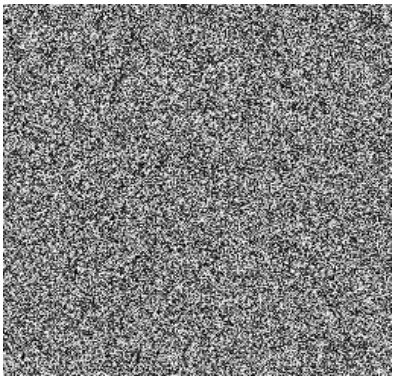

Figure 5: Received image around SINR targeted for Eve

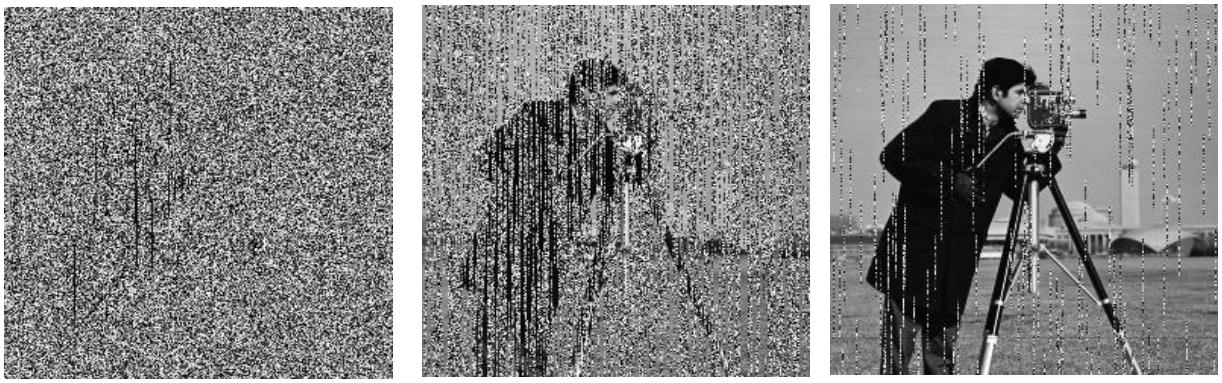

Figure 6: Received image in the transition region

Figure 7: Received image around SINR targeted for Bob

6.2 Performance illustration

To illustrate the performance of our secrecy coding scheme, we simulate the transition of MATLAB cameraman image (Figure 4) over an AWGN channel, for different values of the SINR.

Figure 5 shows the received image when for SINR ≤ 2 dB. No clue on the transmitted image can be deduced from the received image. The BER at the output of the secrecy code is equal to 0.5.

Figure 6 represents the received image when the SINR increases. The BER at the output of the secrecy code for the three images is respectively, 0.46, 0.30 and 0.04. At BER=0.46, the information leakage is insignificant since Eve cannot guess the transmitted image. However, when BER=0.3 Eve manage to successfully decode enough information on the transmitted image. Although 0.3 is a high value for a BER, too many information was leaked. Consequently, Eve's BER should be as close as possible of 0.5 to guarantee no information leakage.

Figure 7 shows the received image at higher SINR values. The BER at the output of the secrecy code for the two images is respectively, 10^{-3} and 10^{-5}. A few errors remain in the first image and no error is detected for the second image. Meaning that Bob can perfectly receive the transmitted information when his SINR is high enough ($>$ 5 dB to 6 dB depending on designed secrecy code).

6.3 Tuning of the radio advantage

Therefore the proposed secrecy coding scheme ensure no information leakage when the SINR is lower than 2 dB for all designed secrecy codes and lower than 3 dB for the secrecy code 1. These values of the SINR can thus be considered as maximum SINR tolerated for Eve.

Consequently, only a few dB of radio advantage (typically 3 dB to 4 dB) is required to provide reliability and secrecy to legitimate users. These reasonable values ensure the compatibility of SC schemes with exiting AN-BF schemes.

Our simulation results show, as expected, that the Bit Error Rate at the output of the polar decoder is 0.5 up to a given "attacker threshold" of the Signal to Interference + Noise Ratio ($SINR_{Eve}$), depending on the modulation and of concatenated coding scheme, that ensures no information leakage. When the $SINR_{Bob}$ grows at Bob's side, as expected, the bit error rate at the output of the polar decoder vanishes. When $SINR_{Bob}$ is high enough (meaning greater than a "user threshold" $SINR_{user}$) the bit error rate at the output of the polar decoder approaches zero. Thus the artificial noise intensity I_{AN} should be tuned in order to achieve suitable $SINR_{Bob}$ at Bob's side thanks to the BF capabilities and un-practicable $SINR_{Eve}$ at Eve's side who cannot apply BF.

Finally, it appears that two basic radio parameters are necessary to tune the radio advantage, which mainly drives the efficiency of the secrecy scheme:

- A "minimum SNR_{user}" for the legitimated link, which is relevant to the performance of the Beam-Forming modulation and coding schemes at Bob's receiver. This depends on the Channel estimation and on the energy budget of the legitimate link, all these parameters being part of the equalization processing and of the Quality of Service Management.
- A "SINR Security gap" that represents the lower bound of the radio advantage to be provided at legitimate link by improving the interference at Eve's side (using artificial noise as interference power I_{AN}), on the efficiency of the BF efficiency being controlled by Alice and Bob in the established AN scheme, the SINR Security gap drives the tuning of the Artificial Noise power by the Node to ensure the radio advantage at any Eve's location.

7. CONCLUSION

To the best of our knowledge, this is the first work on a full secrecy coding scheme with proposal of practical outer and inner codes and complete simulation of the scheme with theoretical and real field channel models. Our promising results are evidence that the proposed secrecy coding schemes are efficient as soon as light radio advantage is achieved. Even if it remains sub-optimal when compared to theoretical results in ideal case (that have no constraints on code lengths and operated in non-realistic radio channels), the provided secrecy capacity is significant (as shown table 1).

Moreover, it should be quite easy to implement in existing wireless MIMO or MISO communication systems that propose AN-BF services (such as in many emerging WLAN, 4G and 5G standards): the AN-BF scheme being activated, only minor modifications of the software architecture of the nodes and terminals are required for the implementation of the secrecy coding scheme. These modifications are located at the coding stage only and remain transparent for upper protocol layers.

8. REFERENCES

[1] ZEIT, "Wie Merkels Handy abgehört werden konnte," 18 12 2014. [Online]. Available: http://www.zeit.de/digital/datenschutz/2014-12/umts-verschluesselung-umgehen-angela-merkel-handy.

[2] Metronews, "Une énorme faille de sécurité permet d'écouter vos appels et de lire vos SMS," 22 12 2014. [Online]. Available: http://www.metronews.fr/high-tech/une-enorme-

faille-de-securite-permet-d-ecouter-vos-appels-et-de-lire-vos-sms/mnlv!YnqDbOgrtHFYk/.

[3] T. Intercept, «The Great SIM Heist. How Spies Stole the Keys to the Encryption Castle,» 2015. [En ligne]. Available: https://theintercept.com/2015/02/19/great-sim-heist/.

[4] M. Bloch and J. Barros, Physical-Layer Security, Cambridge University Press, 2011.

[5] PHYLAWS, «www.Phylaws-ict.org,» [En ligne].

[6] N. Romero-Zurita, M. Ghogho and D. McLernon, "Physical layer security of MIMO-OFDM systems by beamforming and artificial noise generation," *PHYCOM: Physical Communication*, vol. 4, no. 4, pp. 313-321, 2011.

[7] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6428-6443, 2011.

[8] E. Arikan, «A performance comparison of polar codes and Reed-Muller codes,» *Communications Letters, IEEE*, vol. 12, n° %16, pp. 447-449, 2008.