Implementation pratique des codes polaires Wiretap

Khaled Taleb, Meryem Benammar
ISAE-SUPAERO, Université de Toulouse, France
{khaled.taleb,meryem.benammar} (at) isae-supaero.fr

***Résumé*—La construction de codes polaires wiretap, pour des longueurs de blocs petites à moyennes, est un défi. Elle nécessite de choisir des paramètres initiaux spécifiques pour chaque canal. Dans ce papier, nous considérons un code polaire wiretap de longueur de bloc finie, nous rappelons leur construction pour les canaux d'entrée binaires typiques, nous montrons l'effet des paramètres clés de construction sur le débit du code et cette fuite d'information. Enfin, nous présentons une mise en œuvre réelle de ces codes polaires wiretap, en montrant comment un espion est incapable de bien décoder en raison de sa distance plus grande par rapport à l'émetteur [1].**

I. Introduction

Le codage du canal wiretap, présenté dans [1] , est l'une des principales techniques de sécurité de la couche physique pour communiquer en toute sécurité sur des canaux bruités. Cette technique s'appuie sur les qualités asymétriques du canal entre le récepteur légitime (Bob) et l'espion (Eve) pour infliger artificiellement de mauvaises capacités de décodage à l'espion tout en permettant au récepteur légitime de décoder de manière fiable le message critique transmis U^k. Récemment, une preuve de concept d'une construction de code de canal wiretap réussie a été permise par les codes dits polaires (introduits dans [2]). En effet, les auteurs en [3] ont proposé deux constructions de *codes polaires wiretap* qui atteignent chacune des capacités de *securité forte* et *sécurité faible* pour tous les canaux symétriques à entrée binaire. Hof et Shamai [4] et Andersson et al. [5] prouvent indépendamment que ce schéma de codage atteint la région entière de débit-équivoquation [6]. Cela fait des codes polaires les meilleurs candidats connus à ce jour pour la contruction de codes wiretap pratiques. Cependant, l'analyse de [3] étant asymptotique dans la longueur de bloc, elle ne spécifie pas exactement comment choisir certains paramètres clés de la conception, en particulier pour les longueurs de bloc finies. Dans ce travail, en plus de spécifier analytiquement le choix des dits paramètres de construction, nous fournissons une mise en œuvre pratique et une évaluation des performances des codes polaires wiretap suggérés. Enfin, nous implémentons le code polaire de wiretap obtenu dans un banc d'essai bassés sur de la radio logicielle, qui consiste à communiquer une image de manière sécurisée à travers un lien radiofréquence (RF) entre un émetteur USRP (Alice) et un récepteur USRP (Bob) en présence d'un espion équipé d'un USRP (Eve). Nous montrons comment construire des estimateurs des paramètres de canal nécessaires à la construction du code polaire wiretap, et prouvons que le code obtenu permet de communiquer de manière fiable au récepteur légitime, tout en gardant l'image secrète vis à vis de l'espion.

1. Ce travail fait partie d'un article soumis au journal TIFS

II. Problème de codage du canal wiretap

Nous présentons le canal wiretap, la construction, l'encodage et le décodage des codes polaires, ainsi que la construction des codes polaires wiretap.

A. Canaux symétriques binaires de base

Nous rappelons maintenant trois canaux symétriques à entrée binaire qui seront utilisés tout au long de ce travail.

- Le canal binaire symétrique (BSC) avec probabilité de croisement p est défini par

$$Y = X \oplus W \text{ with } W \sim \text{Bern}(p). \tag{1}$$

- Le canal binaire à effacement (BEC) avec probabilité d'effacement e est défini par

$$Y = (1 - W)X + W.E \text{ with } W \sim \text{Bern}(e). \tag{2}$$

- Le canal gaussien à bruit blanc additif à entrée binaire (BI-AWGN) avec une variance de σ^2.

$$Y = (2X - 1) + W \text{ avec } W \sim \mathcal{N}(0, \sigma^2). \tag{3}$$

B. Problème du codage du canal wiretap

Le problème du codage par canal wiretap, tel qu'introduit par Wyner dans [1] , consiste en un message de k bits u^k supposé être uniformément distribué, et un encodeur du côté d'Alice, $f_e^N : \{0,1\}^k \to \mathcal{X}^N$, qui transforme le message u^k en une séquence de N symboles $x^N = f_e^N(u^k)$. La séquence obtenue x^N est ensuite transmise aux deux récepteurs (Bob et Eve) par un canal sans mémoire $\mathcal{W}$ donné par la distribution conjointe $P_{Y^N Z^N|X^N}(y^N, z^N|x^N)$ qui vérifie

$$P_{Y^N,Z^N|X^N}(y^N, z^N|x^N) = \prod_{i=1}^{N} P_{Y,Z|X}(y_i, z_i|x_i). \tag{4}$$

Du côté de Bob, un décodeur $f_d^N : \mathcal{Y}^N \to \{0,1\}^k$ attribue à chaque séquence reçue y^n un message estimé $\hat{u}^k$.

Le problème du codage du canal wiretap vise à fournir une communication fiable à Bob, en termes de probabilité d'erreur P_e définie comme $P_e = \mathbb{P}(U^k \neq \hat{U}^k)$, tout en assurant une sécurité par rapport à Eve, défini soit par le débit d'équivoquation $\frac{1}{N}H(U^k|Z^N)$, soit par la fuite d'information $I(U^k; Z^n)$.

C. Codes polaires wiretap : encodage et décodage

Dans [3], les auteurs ont introduit deux constructions pour les codes polaires wiretap, l'une qui atteint la sécurité faible, c'est-à-dire, $\frac{1}{N}I(U^k;Z^N)\to 0$, et l'autre qui atteint la sécurité fort, c'est-à-dire, $I(U^k;Z^N)\to 0$. Dans ce travail, nous nous concentrons sur le schéma de secret forte et détaillons dans ce qui suit son principe et ses paramètres de conception.

Nous allons partitionner les N bits $[1:N]$ en trois ensembles : $\mathcal{I}$ pour les bits d'information, $\mathcal{F}$ pour les bits fixés à 0 (dits *gelés*), et $\mathcal{R}$ pour les bits aléatoires. Pour un message de k bits U^k, l'encodage est effectué en utilisant

$$X^N = V^N\cdot\mathbf{G}, \tag{5}$$

où $\mathbf{G}=\mathbf{B}\cdot\mathbf{T}_2^{\otimes\log_2(N)}$, et $\mathbf{T}_2=\begin{pmatrix}1&0\\1&1\end{pmatrix}$ est le noyau d'Arıkan et $\mathbf{B}$ est connue comme la matrice *bit-reversal*, et en définissant V^N comme suit :

$$V_{\mathcal{I}}^N=U^k,\qquad V_{\mathcal{R}}^N=C^r,\qquad V_{\mathcal{F}}^N=\mathbf{0}^{N-k-r}. \tag{6}$$

où C^r sont r bits aléatoires indépendants de U^k.

Du côté du décodeur, Bob, les bits aléatoires et d'information sont décodés conjointement à l'aide du décodage par annulation successive (SCD). Cependant, du côté d'Eve, il a été démontré dans [3] que l'introduction de ces bits aléatoires C^r, aux positions précises des bits $\mathcal{R}$, est crucial pour assurer une équivoquation complète (ou une fuite d'information minimale) .

Donnons maintenant plus de détails sur la répartition des bits de l'ensemble $[1:N]$ en ensembles $\mathcal{I}$, $\mathcal{R}$, et $\mathcal{F}$.

D. Codes polaires : partitionnement des bits

Soit W_e (resp. W_b) le canal d'Eve (resp. le canal de Bob) défini par $P_{Z|X}$ (resp. $P_{Y|X}$). Les codes polaires classiques (non wiretap) [2] réalisent la polarisation du canal grâce à l'encodage dans (5) qui transforme N bits observant tous le même canal, disons W_b, en N bits observant chacun un canal binaire $W_b^{(i)}, i\in[1:N]$, avec des probabilités d'erreur inégales. Les bits dans $[1:N]$ peuvent alors être divisés en bits d'information ou en bits frozen, sur la base du paramètre de Bhattacharyya ou de l'information mutuelle de leur canal binaire $W_b^{(i)}$. Dans ce qui suit, nous décrivons le partitionnement des bits dans le cas d'un code polaire wiretap, atteignant une sécurité forte.

Definition 1. Bons, mauvais et *pauvres* canaux binaires [3]
Soit $\beta\in[0:0.5[$. Les *bons* et mauvais canaux binaires de Bob, ainsi que ceux pauvres pour Eve sont donnés par :

$$\mathcal{G}(W_b,\beta)\stackrel{\text{def}}{=}\left\{i\in[1:N]:Z(W_b^{(i)})<2^{-N^\beta}\right\}, \tag{7}$$

$$\mathcal{F}(W_b,\beta)\stackrel{\text{def}}{=}\left\{i\in[1:N]:Z(W_b^{(i)})\geq 2^{-N^\beta}\right\}, \tag{8}$$

$$\mathcal{P}(W_e,\beta)\stackrel{\text{def}}{=}\left\{i\in[1:N]:I(W_e^{(i)})\leq 2^{-N^\beta}\right\}, \tag{9}$$

où, on definit le Bhattacharyya d'un canal binaire par :

$$Z(W^{(i)})\stackrel{\text{def}}{=}\sum_{(y^n,u^{i-1})}\left[W(y^n,u^{i-1}|U_i=0)W(y^n,u^{i-1}|U_i=1)\right]^{\frac{1}{2}},$$

et l'information mutuelle d'un canal binaire par :

$$\begin{aligned}I(W^{(i)}) &\stackrel{\text{def}}{=} I(U_i;Y_1,\dots,Y_n|U_1^{i-1})\\ &= 1-\mathbb{E}_{Y^n,U^{i-1}}H_2(P(U_i=0|Y^n,U^{i-1})).\end{aligned}\quad\square$$

Les auteurs dans [3] montrent que le choix suivant des ensembles $\mathcal{I}$, $\mathcal{R}$, and $\mathcal{F}$

$$\mathcal{I}=\mathcal{G}(W_b,\beta)\cap\mathcal{P}(W_e,\beta), \tag{10}$$

$$\mathcal{F}=\mathcal{F}(W_b,\beta)\cap\mathcal{P}(W_e,\beta), \tag{11}$$

$$\mathcal{R}=[1:N]\setminus\mathcal{P}(W_e,\beta). \tag{12}$$

permet d'atteindre la capacité de sécurité forte.

III. Le choix du paramètre β

Dans la preuve théorique et asymptotique (en N) de l'optimalité des codes polaires wiretap [3], il a été montré qu'il suffisait de considérer n'importe quelle valeur de $\beta\in[0:0.5[$ afin d'atteindre la forte capacité de secret. Cependant, pour des blocs finis $N\ll\infty$, nous montrons dans ce qui suit que la valeur de β est déterminante pour le couple débit-équivoquation ou débit-fuite obtenu par le code polaire wiretap construit. À cette fin, considérons un code polaire construit suivant (10)-(12) et définissons les notations suivantes :

$$R(\beta)\stackrel{\text{def}}{=}\frac{|\,\mathcal{G}(W_b,\beta)\cap\mathcal{P}(W_e,\beta)\,|}{N}, \tag{13}$$

$$L(\beta)\stackrel{\text{def}}{=}\frac{1}{N}I(U^k;Z^N),\text{ and }R_e(\beta)\stackrel{\text{def}}{=}\frac{1}{N}H(U^k|Z). \tag{14}$$

Dans ce cas, $R(\beta)$ désigne le débit d'information utile fournie à Bob, tandis que $L(\beta)$ et $R_e(\beta)$ sont, respectivement, le débit de fuite d'information et le débit d'équivoquation induits chez Eve. Dans ce qui suit, nous cherchons à caractériser la région de fuite d'information $\{(R(\beta),L(\beta)),\beta\in[0:0.5[\}$ ou, de manière équivalente, la région d'équivoquation $\{(R(\beta),R_e(\beta)),\beta\in[0:0.5[\}$.

Le théorème suivant donne une première caractérisation .

Theorem 1. *$L(\beta)$ ainsi que $R(\beta)$, sont décroissants en β.*

Démonstration. Soient $0\leq\beta_1\leq\beta_2<0,5$ deux paramètres de construction possibles. Prouvons que $R(\beta_2)\leq R(\beta_1)$. D'abord, par définition, nous pouvons montrer du côté de Bob que $\mathcal{G}(W_b,\beta_2)\subseteq\mathcal{G}(W_b,\beta_1)$. Ensuite, du côté d'Eve, nous pouvons aussi écrire $\mathcal{P}(W_e,\beta_2)\subseteq\mathcal{P}(W_e,\beta_1)$. Donc,

$$\mathcal{G}(W_b,\beta_2)\cap\mathcal{P}(W_e,\beta_2)\subseteq\mathcal{G}(W_b,\beta_1)\cap\mathcal{P}(W_e,\beta_1), \tag{15}$$

ce qui, combiné à (13), donne que $R(\beta_2)\leq R(\beta_1)$.

Prouvons maintenant que, de manière similaire, $L(\beta_2)\leq L(\beta_1)$. Soit $k_1=NR(\beta_1)$ et $k_2=NR(\beta_2)$, et soit U^{k_1} et U^{k_2} le vecteur des bits d'information sélectionnés pour chaque β. Comme nous l'avons déduit dans le paragraphe précédent, nous avons que $R(\beta_1)>R(\beta_2)$, donc $k_1>k_2$. De plus, puisque $\mathcal{G}(W_b,\beta_2)\subseteq\mathcal{G}(W_b,\beta_1)$, cela signifie que les bits d'information U^{k_2} sont contenus dans les bits d'information U^{k_1}. On peut alors écrire que

$$\underbrace{I(U^{k_1};Z^N)}_{\Rightarrow L(\beta_1)}=\underbrace{I(U^{k_2};Z^N)}_{\Rightarrow L(\beta_2)}+\underbrace{I(U^{k_1};Z^N|U^{k_2})}_{\geq 0}, \tag{16}$$

ce qui, avec (14), implique que $L(\beta_2) < L(\beta_1)$. □

Remark 1. Notez que le résultat du théorème 1 s'applique à tout canal à entrée binaire (BEC, BSC, et BI-AWGN).

Le théorème 1 implique qu'il n'existe pas de choix optimal de β, et que, selon la valeur choisie lors de la construction, le débit d'information délivrée et le débit de fuite pourraient varier. Nous devons donc caractériser davantage les points extrêmes $(R(\beta), L(\beta))$ atteints par les choix possibles de β.

Theorem 2. *Le code polaire wiretap atteint, pour N suffisamment grand, les deux points extrêmes suivants sur les régions de débit de fuite et de débit-équivoquation :*

$$\beta = 0,5 \implies R(\beta) = 0, R_e(\beta) = 0, \textit{ et } L(\beta) = 0 \quad (17)$$
$$\beta = 0 \implies R(\beta) = C_s, R_e(\beta) = C_s, \textit{ et } L(\beta) = 0. \quad (18)$$

où C_s est la capacité de securité. Ces deux points appartiennent aux régions théoriques de débit d'équivoquation (resp. de débit de fuite).

Démonstration. Soit $\beta = 0,5$. Nous savons, d'après la définition de l'exposant d'erreur du code polaire [7, Définition 10], que pour tout $i \in [1 : N]$, $Pr\left[Z(W^{(i)} > \frac{1}{2}\right] = 1$, i.e., $\mid \mathcal{G}(W_b, \beta) \mid = 0$ ce qui donne $R(\beta) = 0$ et $L(\beta) = 0$.

Soit $\beta = 0$. Nous pouvons d'abord montrer que les constructions de Bhattacharyya et d'information mutuelle sont toutes deux équivalentes, c'est-à-dire que $Z(W^{(i)}) > 0,5 \Leftrightarrow I(W^{(i)}) \leq 0.5$ pour une taille suffisante de N. Par conséquent, les définitions des bits pauvres ainsi que mauvais sont équivalentes $\mathcal{G}(W_e, \beta) = \mathcal{P}(W_e, \beta)$. De plus, lorsque la polarisation est complète, $|\mathcal{G}(W_b, \beta)| \approx NI(X;Y)$ et $|\mathcal{G}(W_e, \beta)| \approx NI(X;Z)$. Ensuite, en notant que les canaux sont dégradés, on a que $\mathcal{G}(W_e, \beta) \subseteq \mathcal{G}(W_b, \beta)$, ce qui donne

$$|\mathcal{G}(W_b, \beta) \cap \mathcal{P}(W_e, \beta)| = |\mathcal{G}(W_e, \beta)| - |\mathcal{G}(W_b, \beta)|. \quad (19)$$

Donc, $R(\beta) = I(X;Y) - I(X;Z)$. □

IV. Implementation Hardware

Nous présentons le banc d'essai expérimental qui met en œuvre un code polaire pratique.

A. Banc experimental

Le banc expérimental est composé de trois périphériques radio logiciels universels (USRP B200), un pour l'émetteur (Alice), un pour le récepteur légitime (Bob) et un pour l'espion (Eve). Le récepteur de Bob est placé près de l'émetteur, ce qui lui permet d'avoir un rapport signal/bruit (SNR) plus élevé, tandis que celui d'Eve est placé plus loin, ce qui rend le SNR assez faible pour qu'il ne puisse pas décoder.

L'émetteur (Alice) consiste en une transmission monoporteuse d'une modulation QPSK et à antenne unique d'une image en noir et blanc, décrite comme suit. Une image en noir et blanc est convertie en un flux binaire U^k, puis brouillée (scrambled) à l'aide d'un registre à décalage linéaire (LFSR). U^k est ensuite mappée à travers le code polaire wiretap en utilisant la fonction d'encodage $f_e^N(\cdot)$ en une séquence binaire X^N. X^N est convertie en une séquence de symboles QPSK $S^{N'}$ de $N' = \frac{N}{2}$. La séquence de symboles QPSK $S^{N'}$ est ensuite mise en forme à l'aide d'un filtre racine de cosinus surélevé (SRRC) avec un facteur de dépassement de bande λ et à un débit symbole R_s, en un signal en bande de base $s(t)$. Le signal en bande de base $s(t)$ est ensuite transposé autour d'une fréquence porteuse f_c à l'aide d'un USRP B200, en un signal RF $s_{RF}(t)$.

Du côté du récepteur, soit Bob ou Eve, la chaîne de réception qui traite le signal RF reçu $r_{RF}(t)$ est décrite comme suit. Le récepteur USRP B200 effectue une première démodulation de fréquence pour produire un signal en bande de base non synchronisé. Un filtrage de réception, à travers un filtre SRRC adapté, est ensuite effectué sur le signal synchronisé pour produire le signal en bande de base $r(t)$. On effectue ensuite des opérations de synchronisation (synchronisation symboel et trame, récupération de fréquence et de phase, et contrôle de gain) pour compenser toutes les dégradations du canal à l'exception du bruit, puis on échantillonne au débit de symboles R_s pour récupérer l'ensemble des symboles QPSK en bande de base $R^{N'}$. Les symboles QPSK $R^{N'}$ sont ensuite démodulés de manière "soft" pour produire des LLR d'entrée pour le décodeur polaire (SCD). Le SCD produit une séquence de bits estimés $\hat{u}^k$, en utilisant la fonction de décodage $f_d^N(\cdot)$, qui sont ensuite désembrouillés (descrambled) et mis en correspondance avec une image.

Les structures de l'émetteur et du récepteur sont illustrées dans les Fig. 2 et 3 ci-dessous, et les valeurs numériques utilisées dans l'implémentation sont données en tableau 1c.

B. Estimation des paramètres du canal

Afin d'estimer le SNR de transmission, modélisons le canal résultant entre le signal transmis en bande de base et le signal reçu comme suit :

$$R^{N'} = \alpha S^{N'} + W^{N'}, \quad (20)$$

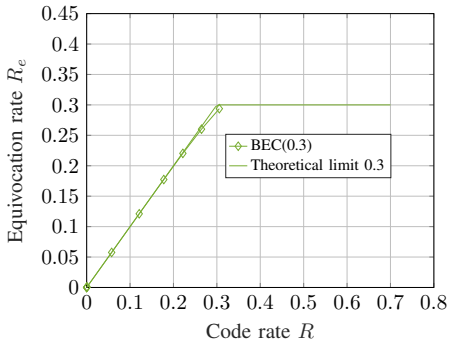
où $R^{N'}$ est le signal reçu en bande de base en temps discret à valeurs complexes après synchronisation, filtrage de réception et échantillonnage du débit de symboles, tandis que $S^{N'}$ est le signal transmis en temps discret appartenant à une constellation QPSK, et $W^{N'}$ est un bruit gaussien additif circulaire supposé être blanc $W^{N'} \sim \mathcal{CN}(0, 2\sigma^2 I_{N'})$, et α est un facteur positif à valeur réelle qui caractérise l'atténuation du signal (perte sur le trajet, pertes de couplage, gains d'antenne, etc.). Le modèle de canal AWGN dans (20) est obtenu par le fait que la synchronisation, le filtrage de réception et l'échantillonnage du débit de symboles sont supposés être suffisamment précis pour ne produire qu'un bruit additif résiduel.

Remark 2. On peut montrer que le modèle de canal dans (20) est équivalent à un BI-AWGN sans mémoire.

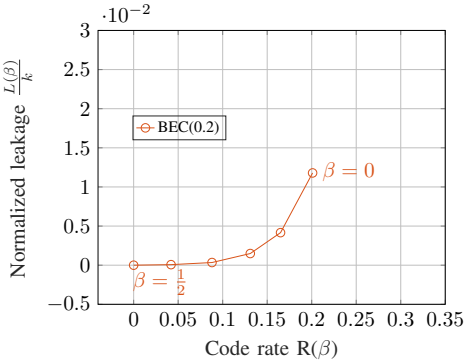
$$Y^N = \alpha(2X^N - 1) + W^N, \quad (21)$$

où $N = 2N'$ et où W^N est un bruit gaussien additif à valeur réelle, avec $W^N \sim \mathcal{N}(0, \sigma^2 I_N)$.. □

Afin de construire le code polaire pour ce canal BI-AWGN, nous devons estimer le rapport signal/bruit (SNR) γ que



(a) La région débit-equivocation pour un canal BEC



(b) La région débit-fuite pour un canal BEC

Débit de symboles (R_s)	200 KBaud
Fréquence d'échantillonnage (F_s)	400 KHz
Fréquence centrale	434 MHz
Facteur d'amortissement	0.5
Longueur de bloc (N)	2048
Longueur du message (k)	640
beta (β)	0.2

(c) Paramètres utilisés pour l'implémentation

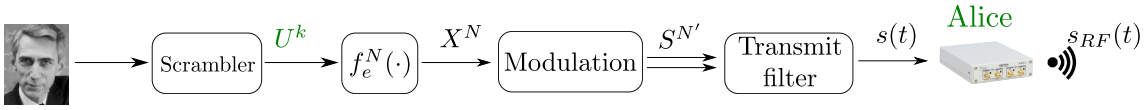


FIGURE 2 – Le côté de l'émetteur de l'expérience

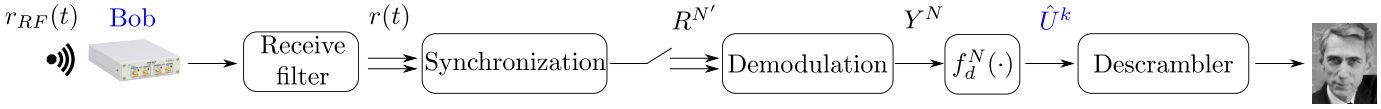


FIGURE 3 – Le côté du récepteur de l'expérience

nous définissons comme $\text{SNR} = \frac{\alpha^2}{\sigma^2}$, pour chacun des canaux de Bob et Eve. À cette fin, nous avons recours à une séquence pilote connue X^N, donc des symboles $S^{N'}$ connus, et construisons des estimateurs de α et de σ au moyen de méthodes d'estimation de la variance. À cette fin, on désigne par Q_q pour $q \in [1:4]$ les quatre symboles QPSK transmis de la forme $(\pm 1 \pm j)/\sqrt{2}$, et on partitionne l'ensemble des indices $[1:N']$ en quatre sous-ensembles,

$$[1:N'] = I_1 \cup I_2 \cup I_3 \cup I_4, \text{ où } I_q = \{i \in [1:N'] S_i = Q_q\}. \quad (22)$$

où chaque sous-ensemble I_q, pour $q \in [1:4]$, correspond aux indices dans lesquels un symbole Q_q est rencontré dans $S^{N'}$.

Lemma 1. Un estimateur d'atténuation, ainsi que la variance du bruit σ^2 peuvent être définis par :

$$\hat{\alpha} = \frac{1}{4}\sum_{q=1}^{4}\left|\sum_{j\in I_q}^{|I_q|} R_j\right| \quad \text{and} \quad \hat{\sigma}^2 = \sum_{i=1}^{N'}\frac{|R_i - \hat{\alpha}S_i|^2}{N'-1}. \quad (23)$$

où $|I_q|$ est le cardinal de l'ensemble I_q. Une estimation du SNR peut donc être donnée par

$$\hat{\text{SNR}}_1 = \frac{\hat{\alpha}^2}{\hat{\sigma}^2}. \quad (24)$$

C. Transmission sécurisée des images

Pour les tests, nous utilisons une photo en noir et blanc de *Shannon*, et l'envoyons aux deux parties. Nous avons effectué des tests, sans code wiretap, afin de nous assurer que Bob et Eve peuvent effectivement décoder l'image, même avec le bruit ambiant. D'autres tests ont été effectués en utilisant un code polaire wiretap, et ces tests aboutissent au comportement prévu : Bob reçoit et décode l'image, tandis que Eve reçoit un signal bruité, et est incapable de récupérer l'image complète. Ceci est illustré dans la Fig. 4.

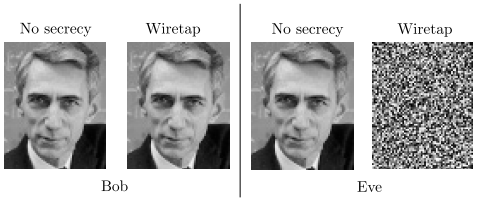


FIGURE 4 – Image reçue avec et sans code wiretap

RÉFÉRENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] E. Arikan, "Channel polarization : A method for constructing capacity-achieving codes," in *2008 IEEE International Symposium on Information Theory*. IEEE, 2008, pp. 1173–1177.

[3] 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.

[4] E. Hof and S. Shamai, "Secrecy-achieving polar-coding," in *2010 IEEE Information Theory Workshop*, 2010, pp. 1–5.

[5] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, "Nested polar codes for wiretap and relay channels," *IEEE Communications Letters*, vol. 14, no. 8, pp. 752–754, 2010.

[6] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5g wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, 2018.

[7] S. B. Korada, E. Şaşoğlu, and R. Urbanke, "Polar codes : Characterization of exponent, bounds, and constructions," *IEEE Transactions on Information Theory*, vol. 56, no. 12, pp. 6253–6264, 2010.