IMPLEMENTATION DU PROTOCOLE DE CRYPTOGRAPHIE QUANTIQUE « BB84 » PAR MODULATION QPSK UTILISANT DES MODULATEURS MACH-ZEHNDER A DEUX ELECTRODES

Sébastien AGNOLINI, Philippe GALLION
Ecole Nationale Supérieure des Télécommunications
GET, Telecom Paris et CNRS UMR 5141
46, rue Barrault – 75634 Paris Cedex 13
sebastien.agnolini@enst.fr, philippe.gallion@enst.fr

RESUME

L'utilisation de modulateurs Mach-Zehnder (MZ) à deux électrodes est proposée pour une implémentation originale du protocole de distribution quantique de clé cryptographique de Bennett et Brassard élaboré en 1984. L'implémentation proposée permet de générer des signaux QPSK satisfaisant à des choix de base et de symbole indépendants sous la contrainte de signaux à enveloppe constante.

MOTS CLES :
Cryptographie Quantique, Distribution Quantique de Clé, QPSK, modulateur Mach-Zehnder.

1. INTRODUCTION

Le protocole de cryptographie quantique de Bennett et Brassard (BB84) utilise la polarisation (spin des photons) et l'impossibilité d'une mesure informative dans une base conjuguée [1]. La nécessité de maintenir ou de contrôler la polarisation est un handicap à son implémentation sur des liaisons à fibre optique [2].
L'utilisation de la phase optique réputée très vulnérable aux non-linéarités est envisageable dès lors que des signaux très faibles et/ou d'enveloppe constante sont transmis et qu'une réception sensible à la phase utilisée. Cette dernière peut être réalisée par interférométrie au prix de la réalisation et de la stabilisation d'un interféromètre pour une démodulation cohérente [3]. Les contraintes de polarisation, qui n'est plus porteuse de l'information, sont alors relaxées.
L'utilisation de modulateurs Mach-Zehnder (MZ) à deux électrodes et l'utilisation de la phase d'une modulation par sous-porteuse ont donné lieu à une démonstration convaincante au prix de circuits et d'une synchronisation radio fréquence complexes [4] [5]. L'utilisation de ce type de modulateur pour une implémentation directe sur la phase optique ne permet pas, sous la contrainte de signaux à enveloppe constante, l'affectation d'une électrode au choix de base et de l'autre au choix de symbole. Nous proposons une implémentation originale supportant ces choix sous cette contrainte en utilisant un simple additionneur radio électrique.

2. PROTOCOLE BB84

La distribution quantique de clé (Quantum Key Distribution) permet l'échange de clés de chiffrement entre un émetteur (nommé Alice) et un récepteur (Bob). Toute personne (appelée Eve) qui tenterait d'écouter le canal de transmission en mesurant l'état quantique des photons perturbera irrémédiablement la transmission en signalant sa présence par l'introduction d'erreurs facilement détectables.
Le protocole d'échange BB84 nécessite 4 états quantiques constituant 2 bases notées A_1 et A_2 contenant chacune deux symboles notés 0 et 1 [1]. Les bases A_1 et A_2 sont dites conjuguées, i.e. toute mesure effectuée dans la base A_2 d'un photon émis dans la base A_1 donne un résultat complètement aléatoire et entraînant la perte définitive de son information.
Alice transmet une séquence, résultat d'une suite de choix aléatoires indépendants de la base et des symboles. Elle encode cette séquence sur un photon. Bob mesure l'état quantique du photon sur une des deux bases qu'il choisit aléatoirement. Puis sur un canal classique, Alice et Bob échangent publiquement leur choix de base. Lorsqu'il y a coïncidence, ils conservent alors les symboles correspondants, constituant ainsi une clé de chiffrement commune.

3. ENCODAGE DES CHOIX DE BASE ET DE SYMBOLE D'ALICE

La figure 1 présente l'encodeur proposé pour une implémentation du protocole BB84 utilisant des signaux QPSK. Alice transmet ses choix de base et symbole en modulant la phase d'une onde optique au moyen d'un modulateur MZ à deux

électrodes qui permet de contrôler indépendamment les déphasages optiques introduits sur chaque bras (figure 1).
L'onde optique incidente sur le modulateur, de fréquence angulaire ω_0, est caractérisée par son champ électrique $E_0(t)$ (1).

$$E_0(t) = E_0.\exp(jw_0 t) \tag{1}$$

L'onde émergente, après application des déphasages ϕ_1 et ϕ_2, est :

$$E_1(t) = E_0(t).\sqrt{2}.\cos\left(\frac{f_1 - f_2}{2}\right).\exp\left(j\frac{f_1 + f_2}{2}\right) \tag{2}$$

Le champs électrique $E_1(t)$ comporte une modulation simultanée en amplitude et en phase. Quelques soient les valeurs des déphasages introduites par Alice, le terme de modulation d'amplitude ne peut varier. En effet cette variation, détectée par Eve, constituerait une information exploitable. La contrainte d'une enveloppe constante impose le choix d'une différence $f_1 - f_2 = \pm\frac{p}{2}$. La modulation de phase $\frac{f_1 + f_2}{2} = f_{Alice}$ doit permettre à elle seule l'encodage des choix de base et de symbole.
Le protocole BB84 impose, par définition, l'existence de quatre états quantiques distincts correspondant à quatre valeurs distinctes de ϕ_{Alice}.
Le respect de ces contraintes et des choix de valeurs de ϕ_1 et ϕ_2 (tableau 1) permettent d'écrire :

$$E_1(t) = E_0(t).\exp\left(j\frac{f_1 + f_2}{2}\right) \; avec \; \frac{f_1 + f_2}{2} \in \left\{-\frac{p}{4}, \frac{p}{4}, \frac{3p}{4}, \frac{5p}{4}\right\} \tag{3}$$

(3) correspond à un signal numérique modulé en phase à 4 états (QPSK) d'équation caractéristique :

$$E_{out}(t) = E_{in}(t).\exp\left(j\frac{2p}{M}(m-1)\right).\exp\left(j\frac{p}{4}\right) \; avec \; m \in \{1,2,3,4\} \; et \; M = 4 \tag{4}$$

La partie gauche du tableau 1 établit la correspondance entre les déphasages optiques introduits par Alice (ϕ_1 et ϕ_2) et ses choix de bases (A_1 ou A_2) et de symboles (0 ou 1). L'implémentation consiste donc à encoder le choix de base par le signe de la tension quart d'onde appliquée à la première électrode. La seconde est commandée par le même signal auquel s'ajoute une tension demi-onde selon le symbole. L'additionneur correspond à un coupleur radiofréquence à fort isolement entre ces deux entrées.

Alice					Bob			
base	bit	f_1	f_2	f_{Alice}	base	f_3	$f_{Alice}+f_{Bob}$	bit retenu
A_1	0	0	$\frac{p}{2}$	$\frac{p}{4}$	B_1	$-\pi/2$	0	0
					B_2	$\pi/2$	$\pi/2$	?
	1	p	$\frac{3p}{2}$	$\frac{5p}{4}$	B_1	$-\pi/2$	p	1
					B_2	$\pi/2$	$-\pi/2$	?
A_2	0	0	$-\frac{p}{2}$	$-\frac{p}{4}$	B_1	$-\pi/2$	$-\pi/2$	?
					B_2	$\pi/2$	0	0
	1	p	$\frac{p}{2}$	$\frac{3p}{4}$	B_1	$-\pi/2$	$\pi/2$	?
					B_2	$\pi/2$	p	1

Tableau 1: Implémentation du protocole BB84 par codage de phase en utilisant un modulateur MZ à 2 électrodes.

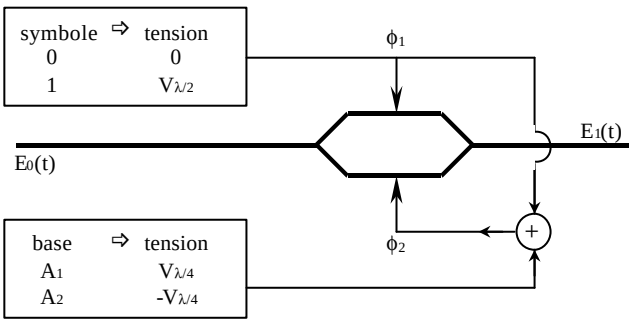

Figure 1 : Module d'encodage de Alice

4. ENCODAGE DU CHOIX DE BASE ET DETECTION DE BOB

Bob encode son propre choix de base au moyen d'un modulateur MZ à deux électrodes en introduisant un unique déphasage $f_3 = \pm\frac{p}{2}$. En ne tenant pas compte des effets de dispersion et de biréfringence de la fibre optique, l'onde optique incidente au modulateur de Bob est identique à celle sortant du modulateur MZ d'Alice. En sortie du modulateur MZ de Bob, le champ électrique de l'onde optique s'écrit :

$$E_2(t) = E_1(t).\sqrt{2}.\cos\left(\frac{f_3}{2}\right).\exp\left(j\frac{f_3}{2}\right) \tag{5}$$

La seconde électrode du modulateur de Bob est susceptible d'être utilisée pour l'implantation d'un asservissement en

phase. Nous supposerons ici, pour simplifier, $f_4 = 0$ .En posant $\frac{f_3}{2} = f_{Bob}$, (5) s'écrit :

$$E_2(t) = E_0(t).\sqrt{2}.\cos(f_{Bob}).\exp\left(j(f_{Alice} + f_{Bob})\right) \quad (6)$$

Lorsqu'il y a coïncidence des bases, le déphasage $\phi_{Alice} + \phi_{Bob}$ prend une des deux valeurs antipodales que Bob est capable de mesurer. Dans le cas de non coïncidence, Bob reçoit des valeurs orthogonales aux états propres de son détecteur. La mesure alors réalisée n'étant pas informative est écartée. La partie droite du tableau 1 établit la correspondance entre déphasage optique et symbole retenu pour la synthèse de la clé.
Bob effectue une détection cohérente, de type interférométrie ou hétérodyne. Cette dernière consiste à détecter le battement de l'onde signal par rapport à une onde de référence. L'avantage majeur de ce mode de photo-détection est de pouvoir mesurer des puissances signal très faibles et transférer les mesures de phase dans le domaine radioélectrique.

5. ERREURS CLASSIQUES / ERREURS QUANTIQUES

Pour un nombre de photon par bit n>>1 et l'approximation du bruit optique par un bruit additif gaussien de densité spectrale $\frac{hn}{2}$ [5], la réception est celle d'une modulation PSK à deux états antipodaux.

La décision entre les deux signaux antipodaux de la base choisie est prise en faveur de celui sur lequel le signal reçu a une plus grande projection.
Pour une coïncidence des bases, le taux d'erreur binaire classique est [6] :

$$BER = \frac{1}{2} erfc\sqrt{2n} \quad (7)$$

Pour une anti-coïncidence des bases, le taux d'erreur est voisin de $\frac{1}{2}$ et la décision non-informative.

Pour un photon unique, le résultat des mesures coïncide nécessairement avec ses valeurs propres.
La robustesse à une attaque résulte selon les implémentations, du caractère irréversible d'une mesure (Quantum Demolition) ou, pour des variables continues, de l'utilisation de protocoles adaptés [7].

6. CONCLUSION

L'implémentation proposée permet de générer des signaux QPSK satisfaisant à des choix de base et de symbole indépendants sous la contrainte de signaux à enveloppe constante. Ce système original possède l'avantage de ne pas utiliser de sous-porteuse électrique. Sa réalisation expérimentale est en cours.

REFERENCES

[1] C.H. Bennet, G. Brassard. « Quantum cryptography : Public key distribution and coin tossing », Proceedings of IEEE International Conference on Computers, Systems, and Signals Processing, 1984, pp. 175-179.

[2] D. S. Bethune, W. P. Risk, « An Autocompensating Fiber-Optic Quantum Cryptography System Based on polarization Splitting of Light », IEEE Journal of Quantum Electronics, v. 36, n.3, 2000.

[3] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, N. Gisin : « Plug and play systems for quantum cryptography », Appl. Phys. Lett., p. 793, 17 février 1997.

[4] J-M. Mérolla, Y. Mazurenko , J-P. Goedgebuer, H. Porte, W. T. Rhodes : « Phase-modulation transmission system for quantum cryptography », Optics Letters, vol. 24, n. 2, p. 104, 1999.

[5] L. Duraffourg, J-M. Merolla, J-P. Goedgebuer, Y. Mazurenko, W. T. Rhodes : « Compact transmission system using single-sideband modulation of light for quantum cryptography », Optics Letters, vol. 26, n. 18, p. 1427, sept. 2001.

[6] P. Gallion : « Basics of Digital Optical Communication », Undersea Fiber Systems, edited by J. Chesnoy, p. 51-93, Academic Press New York, 2002.

[7] J. G. Proakis : « Digital Communications », 4 ed., p. 266-272, McGraw-Hill , 2001.

[8] F. Grosshans, P. Grangier, « Continuous Variable Quantum Cryptography Using Coherent States », Phys. Rev. Lett., v. 88, n. 5, 4 février 2002.