SMARTQUAMTUM

Révolutionne la sécurité des fibres optiques

Les réseaux de fibres optiques constituent le cœur des infrastructures modernes de notre monde de télécommunication dont le trafic ne cesse de croître tant en terme de voix, de données que d'images. Mais, contrairement à l'idée la plus répandue, les infrastructures des liaisons haut-débit sont extrêmement vulnérables. A tel point, que n'importe qui peut s'amuser à intercepter des informations confidentielles transmises sur les réseaux optiques….et sans être détecté. Il suffit tout simplement d'acheter un système d'écoute disponible dans le commerce et de le brancher sur le réseau de fibre d'optique de son choix pour obtenir des données circulant sur la bande passante. Ceci est très simple, notamment aux Etats-Unis où les trappes d'accès aux réseaux haut-débit sont signalées par des bornes et très facilement accessibles.

Conscient de ce problème, les informations issues des secteurs sensibles comme la défense, la recherche, la finance ou l'industrie sont souvent cryptées à l'aide d'une clé, c'est-à-dire transformées en charabia inintelligible chiffré. Et, lorsque la clé de décryptage circule sur le réseau le pirate peut intercepter l'algorithme de cryptographie et le déchiffrer.

C'est à ce stade qu'intervient la société SmartQuamtum. Cette jeune pousse se positionne sur un marché en plein développement, celui des solutions de sécurité pour les réseaux haut-débit. La société conçoit et commercialise des produits de sécurisation des réseaux de très haut niveau en utilisant deux technologies clés : la cryptographie numérique et la cryptographie quantique (lire encadré ci-dessous) qui permettent d'assurer de manière hautement sécurisée l'échange de données sur les réseaux de fibre optique. Les équipes de SmartQuantum ont ainsi mis au point une clé inviolable.

Et tout laisse à croire que la société est à la tête d'une technologie qui va révolutionner le cryptage des données.

Car la société canadienne Dawavesys (www.dawavesys.com) devrait d'ici à 2010 annoncer la sortie d'un ordinateur utilisant la technologie quantique et capable de déchiffrer les algorithmes les plus complexes. En clair, cette ordinateur pourra décrypter toutes les clés, sauf celles basées sur la cryptographie quantique (lire en cadré ci-dessous).

SmartQuantum a vite compris le potentiel qui s'offrait à elle. Pour cela elle a développé des solutions simples en phase avec les besoins du marché et des clients, qui ne nécessitent pas de surcoûts.

Ce n'est pas le cas de ses concurrents les plus proches : l'un suisse et l'autre américain, ont essayé de développer un produit de cryptographie quantique, mais leur solution nécessite des changements importants et coûteux au niveau de l'infrastructure réseau des clients alors qu'avec SQBox Defender, le produit vedette de Smartquantum, le réseau existant n'est pas changé.

SQBox Defender

Pour commercialiser ses produits la société s'appuie sur trois axes :

- la vente en direct au gouvernement et au secteur de la défense qui souhaitent, pour des raisons de confidentialité, traiter uniquement en direct,
- la vente par intermédiaires auprès d'intégrateur de sécurité qui reçoivent des appels d'offres.
- La vente de licences auprès d'opérateurs téléphoniques

Son Président, Frédéric Fabre, nous a indiqué que plusieurs contrats et partenariats seront annoncés dans les mois à venir, et ce dès le mois d'avril.

Du coup la direction table pour 2009 et 2010 sur un résultat net respectivement de 907.005 euros et de 4.513.679 euros, faisant ressortir un PER (ratio cours sur bénéfices) de 12,73 et 2,55. Mais avant d'en arriver là, la société a du chemin à faire car l'exercice clos le 31 décembre 2007 devrait se solder par une perte et un chiffre d'affaires de 351.000 euros.

La société a déjà réalisé une augmentation de capital en décembre 2007, ce qui lui assure de valider son implantation aux Etats-Unis et lui permet de travailler sereinement au développement présenté lors de son introduction en Bourse. L'entreprise bénéficie en effet, grâce à ses caractéristiques de JEI, de nombreuses possibilités d'aides. Par ailleurs, afin de répondre aux opportunités de croissances qui pourraient se présenter et d'une manière complémentaire à son Besoin en fonds de roulement (BFR), la société pourra toujours faire appel au Marché, celle-ci n'ayant pas, à ce jour, exploité l'ensemble des

autorisations validées par l'AGE des actionnaires. Cette opération étant de plus éligible aux nouvelles déductions d'ISF (75% de la somme et maximum de 50.000 euros par opération).
Les actionnaires actuels désirant participer à l'opération, n'ont pas intérêt à céder leurs titres sur le marché, car Frédéric Fabre que nous avons tout récemment rencontré à Lannion, nous a clairement indiqué que le prix de souscription se fera au-dessus de 3,01 euros. Un prix entre les cours actuels proche de 4 euros et 3,01 euros, nous semble un bon compromis.
Nous conseillons de participer à l'augmentation de capital réservée aux investisseurs qualifiés tout en prenant en compte que l'achat d'actions se résume à une opération de capital risque plutôt qu'un investissement de bon père de famille.

Notre avis

Participer à la prochaine augmentation de capital

Fiche technique

Code Isin :	FR0010557793
Mnémotechnique :	MLSAM
Cours (€) :	4,00
Capitalisation (M€) :	11,55
Nombre de titres :	2 887 367
Degré de risque :	☑ ☑ ☑

Exercice	2006	2005
Clôture	31-dec	
Durée exercice	12 mois	
Devise	EUR	
Nbre d'actions (1) :	2 741 791 (1)	
Comptes	Consolidés	
Chiffre d'affaires (K €)	119	-
Rés. Expl. (K €)	-209	-
Marge d'exploitation	-	-
Résultat net (K €)	-71	-
Marge nette	-	-
Dette nette par action (€)	0,08	-
Div. / action	0	-
Rendement	-	-

(1) le nombre d'actions a été porté à 2.887.367 le 7 janvier 2008

La cryptographie quantique

La cryptographie quantique n'est pas un algorithme de chiffrement à proprement parler : elle permet simplement de mettre en œuvre un algorithme de cryptographie classique, et même ancien, qui est le seul démontré sans failles : le "masque jetable". Cet algorithme, bien que parfaitement sûr, est peu utilisé car il nécessite un échange de clé de longueur aussi grande que le message à transmettre. Cet échange de clé pose des problèmes de sécurité aussi importants que la transmission du message en lui-même, ce qui limite le domaine d'applicabilité de cet algorithme.

Cependant, la cryptographie quantique permet à deux interlocuteurs de s'échanger une clé en toute sécurité ; en effet, cette méthode permet non seulement de démasquer toute tentative d'espionnage grâce aux propriétés de la mécanique quantique, mais également de réduire la quantité d'information détenue par un éventuel espion à un niveau arbitrairement bas et ce grâce à des algorithmes classiques (« privacy amplification »). La cryptographie quantique constitue donc un outil précieux pour des systèmes de cryptographie symétrique où les deux interlocuteurs doivent impérativement posséder la même clé et ce en toute confidentialité.

Mais pourquoi utiliser le système de cryptographie quantique pour communiquer une clé, et non le message en lui-même ? Pour deux raisons essentielles :

· Les bits d'informations communiqués par les mécanismes de la cryptographie quantique ne peuvent être qu'aléatoires. Ceci ne convient pas pour un message, mais convient parfaitement bien à une clé qui, dans le cas du "masque jetable" peut (et même doit) être aléatoire.

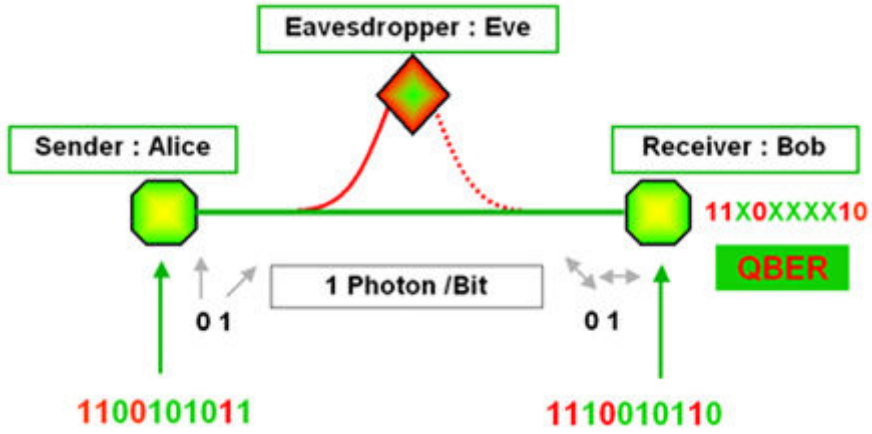
· Même si le mécanisme de la cryptographie quantique garantit que l'espionnage de la communication est détectée, il est possible que des bits d'informations entrent en possession de l'espion avant que celui-ci ne soit détecté. Ceci est inacceptable pour un message, mais sans importance pour une clé aléatoire qui peut être simplement jetée en cas d'interception.

Les fondements de la cryptographie quantique ont été établis, entre autres, par les travaux de 1984 de Charles H. Bennett et Gilles Brassard. Les premières idées ont été posées par Stephen Wiesner dans les années 1960, mais, chose que l'on peut considérer surprenante, leur publication avait été rejetée.

Source : Wikepedia

Introduction à la cryptographie quantique

La cryptographie consiste à brouiller les informations afin de les rendre inintelligibles à quiconque ne possède pas la clé secrète pour les décoder. Jusqu'à présent, les systèmes cryptographiques distribuent ces clés via des solutions logicielles reposant sur des principes mathématiques. Les verrous mathématiques sont cependant vulnérables, un intrus peut en effet copier une clé, décoder et accéder à des données sans laisser trace de son piratage.
La cryptographie quantique résout définitivement le problème de la distribution de clés. Cette technologie de rupture protège de manière absolue les communications voix, données, images. Au lieu de transmettre les clés, ce procédé révolutionnaire les forgent de manière dynamique grâce aux principes universels de la physique quantique. Pour la première fois dans l'histoire de la cryptographie, les clés ainsi obtenues sont invulnérables.
La nette différence avec la cryptographie quantique réside dans le fait que l'émetteur transmet au récepteur une chaîne continue de bits véhiculés par des grains de lumière appelés photons. Si un intrus essaie de les intercepter, leur état changera de manière irréparable. L'émetteur et le récepteur détecteront la tentative d'espionnage. La chaîne corrompue est alors rejetée. Aucun de ces bits douteux ne sera utilisé pour établir une clé. Seuls les photons intègres fournissant une information sans risque participent à la génération de clés secrètes.



En cryptographie numérique, le risque d'une attaque par intrusion reste indétectable. Les pirates réalisent alors une copie des messages transmis et procèdent ensuite à leur cryptanalyse en vue de briser les codes secrets. Ce type d'espionnage est indécelable et les crypto systèmes actuels n'offrent aucune résistance contre de telles interceptions.
En revanche, la cryptographie quantique détecte systématiquement les intrusions et supprime le risque d'espionnage. Si un intrus tente de cloner les informations transportées par les photons envoyés sur la fibre optique reliant deux interlocuteurs, la mécanique quantique garantit que cette attaque entraînera une perturbation détectable. Les utilisateurs légitimes de la ligne retarderont alors l'envoi d'informations sensibles jusqu'à ce que la sécurité du lien soit de nouveau assurée.
Pour la toute première fois dans l'histoire de la cryptographie, la sécurité absolue des communications via liaisons optiques est rendue possible grâce aux lois de la physique quantique.

Source : SmartQuantum