Contre la menace quantique : la compatibilité sélective

L'usurpation d'identité est un problème sérieux en informatique et facilite d'innombrables autres fraudes. Un article de 2019 de l'*ISACA® Journal* intitulé "Chaos to the Rescue"[1] a expliqué comment gérer le vol d'identité en informatique. L'article proposait cinq hypothèses fondamentales sur la manière de prévenir la fraude, dont la cinquième est une conséquence des quatre précédentes :

H1. Aujourd'hui, personne n'a besoin d'un nom ou d'un numéro pour être reconnu par un ordinateur.

H2. Deux objets ne peuvent pas être entièrement identiques au niveau du micromètre.

H3. Pour devenir plus sûre, l'informatique doit obéir à de nouvelles lois et à une nouvelle logique.

H4. Les systèmes d'information peuvent protéger les personnes en se protégeant eux-mêmes.

H5. Il est désormais possible, sur la base des hypothèses précédentes, de concevoir des systèmes d'information avec une compatibilité limitée (c'est-à-dire qu'il peut être impossible pour deux ordinateurs de communiquer s'il n'y a pas eu, préalablement,

d'interaction « physique » [à distance ou non] entre ces derniers.[2]

Après cette publication, plusieurs objections ont été soulevées, notamment à propos de la cinquième hypothèse. Certains lecteurs ont eu l'impression que l'article revenait en arrière et ramenait les ordinateurs à l'époque du terminal, quand ceux-ci ne pouvaient afficher que les résultats du serveur central avec lequel seuls des techniciens formés pouvaient communiquer via une console, des codes incompréhensibles et un écran vert. Il restait à savoir : ce retour en arrière sera-t-il toujours possible ou même nécessaire ?

Pour répondre à cette question, on doit comprendre l'évolution de la cybernétique, la science des communications et de la régulation des êtres

JEAN JACQUES RAPHAEL | CISA, CISM, AZURE SECURITY ENGINEER, CEH, CNDA, ISO 27001 LI

Is a lead implementer of IT security at OctoSafes Inc. He is a gold ISACA® member and belongs to the ISACA Quebec City (Canada) Chapter. He can be reached at *jean.j.raphael@octosafes.com*.

JEAN CLAUDE CÉLESTIN | COMPTIA A+

Manages practical work at the University of Ottawa (Canada). He can be reached at *jcele091@uottawa.ca*.

ERIC ROMUALD DJIETHIEU | CDPSE

Is an IT security and telecommunication architect at Desjardins. He is also a cofounder of OctoSafes Inc. He can be reached at *eric.romuald.djiethieu@octosafes.com*.

vivants et des machines,[3] au cours des 30 dernières années. A une certaine époque, les puces d'origine qui équipaient les ordinateurs Commodore ont été reléguées à la poubelle. Bien sûr, les commandes de base d'origine étaient toujours utilisées, mais pour répondre à la marche du progrès, les ordinateurs personnels (PC) devaient devenir compatibles entre eux. Le label IBM Compatible permettait aux ordinateurs de communiquer entre eux. C'est grâce à cette compatibilité que le système d'exploitation sur disque (DOS) s'est développé et est devenu l'outil de prédilection de ceux qui commençaient à entrevoir le formidable destin de l'information automatique (l'informatique). Cette compatibilité généralisée a rendu de grands services à la cybernétique, comme l'entrée des ordinateurs dans les foyers. La compatibilité a rendu, et rend encore en ces temps de télétravail, de grands services pour le traitement de l'information. Les utilisateurs savent qu'ils peuvent utiliser leur ordinateur pour leurs besoins quotidiens sans avoir à se demander si les programmes fonctionneront, et ils n'ont pas besoin d'être des programmeurs ou des techniciens pour obtenir des états financiers, des graphiques statistiques, des rapports médicaux ou des analyses stratégiques. Mais qu'en est-il de la sécurité ? Au fur et à mesure que les PC sont devenus plus populaires et utiles, des individus aux intentions malveillantes se sont donné pour mission d'essayer de découvrir des moyens d'en bénéficier de façon frauduleuse d'une manière ou d'une autre. Ainsi, l'hypothèse posant les avantages de la compatibilité sélective peut être la seule option pour éliminer définitivement la menace en établissant infailliblement le besoin de confidentialité dont les systèmes d'information ont désespérément besoin.

"Le chaos à la rescousse", a décrit la carte numérique à quatre dimensions (4D),[4] qui est le substrat de la compatibilité sélective. C'est un PC qui est connecté à un serveur d'authentification (AS). Seuls les gouvernements démocratiques peuvent collecter les données (par exemple, la biométrie) qui sont échangées et stockées entre ces deux systèmes en raison de leur nature très sensible. Les données sur la naissance, le décès, les noms, l'ADN et les caractéristiques physiques d'une personne sont collectées à partir de la carte. Ces informations sont associées aux méthodes de cryptage actuellement utilisées pour rendre inviolables les transactions effectuées par la carte. Il s'agit à la fois d'une carte d'identité et d'un passeport qui contient les dossiers médicaux, universitaires et autres actifs du propriétaire. Les données biométriques enregistrées à la fois sur la carte et sur l'AS sont confirmées à chaque utilisation par le véritable propriétaire par des scans de rétine et d'empreintes palmaires pour éviter toute usurpation d'identité.

La recherche d'un minimum d'intimité a été prise en compte lors de la conception de la carte 4D. Sans un minimum de confidentialité (c'est-à-dire si certaines caractéristiques n'étaient pas uniques à la carte ou aux données telles que les données génétiques ou biométriques et conservées uniquement dans des serveurs ultra-sécurisés par les autorités gouvernementales), il serait facile pour quiconque de commettre un crime en volant la carte.[5]

Depuis sa création, cette carte aura effectué des milliers d'échanges indéchiffrables par l'intelligence humaine, mais aussi incassables par un compilateur quantique en raison de paramètres uniques comprenant le nom du bébé, le numéro de sécurité sociale (SSN), la biométrie et les données génétiques ; la disposition schématique unique du circuit de la carte et la numérisation de la surface de la carte par un microlaser ; et l'emplacement (c'est-à-dire les données du système de positionnement global [GPS]), la date et l'heure calculées à la milliseconde près. L'interaction initiale rejoint les exigences d'une autre hypothèse dans « Le chaos à la rescousse », qui stipule que la machine peut se protéger. Selon cette hypothèse, les deux machines ne pourront déterminer les protocoles de cryptage et de communication qu'au début de chaque transaction. Les protocoles seront uniques et aléatoires lors de chaque connexion. Il sera impossible pour un intermédiaire de retrouver certains « patterns » en analysant un très grand nombre de données échangées lors de ces connexions.[6]

L'émergence de l'informatique quantique

Depuis quelques décennies, les cybernéticiens ont vu venir le danger de la menace quantique et ont tenté en vain de la contrecarrer. Même lorsqu,on a tenté de gérer le besoin de confidentialité à l'aide de mots de passe complexes et d'une authentification multifacteur (MFA), les chevaux de Troie prennent toujours le dessus grâce à des méthodes de contournement telles que le phishing. Pendant ce temps, la menace quantique se rapproche.

L'ordinateur quantique est :

> *[Une] machine qui s'appuie sur les lois de la mécanique quantique pour stocker et manipuler des informations. Contrairement à un ordinateur classique qui manipule des bits d'information (0 ou 1), un ordinateur quantique manipule ce qu'on appelle des bits quantiques - ou qubits. Ceux-ci peuvent être à l'état 0 ou 1 mais aussi dans une superposition de ces états.*[7]

Mais quel impact cela aura-t-il sur les systèmes d'information de sécurité actuels ?

Parce que le compilateur quantique peut augmenter de manière exponentielle la puissance de calcul de l'ordinateur quantique, il est à craindre que la factorisation de certains nombres premiers jusqu'alors impossible pour les ordinateurs classiques ne devienne monnaie courante pour l'ordinateur quantique. Le rôle que joue cette factorisation dans l'algorithme RSA illustre le danger potentiel qu'aurait le compilateur quantique sur les systèmes bancaires et même sur le décodage des clés des missiles balistiques. Avec le compilateur quantique, tout devient théoriquement déchiffrable.

L'espoir des experts de la sécurité est que ces menaces restent « théoriques » le plus longtemps possible. Cela peut être possible si les principes de compatibilité sélective sont mis en pratique pour aider à contrecarrer le décryptage quantique.

Les enjeux sont si importants que le National Institute of Standards and Technology (NIST) des États-Unis étudie le problème depuis 2016.[8]

La Compatibilité sélective

La compatibilité sélective est un ensemble d'outils techniques, de processus et de protocoles permettant une connexion conditionnelle entre plusieurs systèmes d'information (par exemple, la carte 4D, l'AS et le système d'information tiers). Contrairement aux modes de connexion actuellement utilisés, la communication implique de nouveaux paramètres tels que :

- Les caractéristiques physiques uniques de la carte
- Les caractéristiques biométriques et génétiques uniques de l'utilisateur
- Un système d'information tiers avec lequel l'utilisateur a certaines relations spécifiques (par exemple, sa banque, son université, sa clinique médicale)

À titre d'exemple extrême, prenons le cas du président des États-Unis. Le jour de son investiture, sa carte 4D le met en contact avec toutes les institutions stratégiques du pays : le Pentagone, le Congrès américain et la National Aeronautics and Space Administration (NASA) américaine. Son niveau d'accréditation est le plus élevé; les autres fonctionnaires ayant accès à l'une de ces institutions n'ont que des accès correspondant à leur rang. Ce système d'information sera tellement segmenté qu'il est impossible pour un pirate d'accéder à des informations aussi sensibles.

Parmi les autres innovations de la technologie moderne qui peuvent faciliter et renforcer la mise en œuvre de cette compatibilité sélective, citons :

- L'intégration croissante de processus chaotiques dans notre quotidien
- La multiplication du nombre d'interconnexions et l'augmentation phénoménale de la vitesse de circulation des informations grâce à la communication 5G
- Les récents progrès réalisés en intelligence artificielle
- L'émergence de nouveaux types de codage remplaçant les symboles (0, 1) du langage binaire par d'autres symboles tels que ceux que l'on trouve dans l'ADN
- Les avancées de plus en plus pertinentes vers la création du premier compilateur quantique

Les nouvelles directions de la cybernétique

L'évolution de la technologie ces dernières années repose sur trois concepts fondamentaux :

1. La logique booléenne - Basée sur le calcul binaire, l'algèbre booléenne est à la base de la création de l'informatique.[9]
2. La machine de Turing - C'est une machine conceptuelle assez simple imaginée par Alan Turing par laquelle il a expliqué comment les ordinateurs devraient fonctionner.[10]

3. La théorie de la compilation de Von Neumann - A travers cette théorie, Von Neumann a introduit la notion d'automatisme, grâce à laquelle l'ordinateur est devenu plus qu'une calculatrice.[11]

Les ordinateurs conventionnels d'aujourd'hui sont plus rapides et peuvent stocker plus de données sur des disques durs de plus petits volumes que jamais auparavant, mais ils obéissent toujours à ces trois concepts. C'est ce qui rendra vaine toute tentative future de résoudre les problèmes complexes de sécurisation des systèmes d'information. Le fait qu'à l'origine ces 3 concepts visaient avant tout le fonctionnement optimal de l'ordinateur et que les problèmes de sécurité ne se posaient pas encore, cela a rendu encore plus difficile l'intégration des mécanismes de sécurité par la suite.

Les pirates parviennent toujours à contourner les contrôles et à trouver des failles. Par conséquent, les systèmes d'information ne seront jamais fiables s'ils continuent encore à reposer sur ces trois concepts fondamentaux. C'est là qu'intervient la notion de compatibilité sélective. Lorsqu'une faille de sécurité aura été découverte, la compatibilité sélective sera utilisée pour contenir cette faille et l'empêcher de se propager.

Le principe d'exclusion de Pauli et la compatibilité sélective

Pour mettre en œuvre la compatibilité sélective, il est utile de saisir d'abord l'interprétation classique que nous avons donnée à la théorie quantique connue sous le nom de principe d'exclusion de Pauli.[12] Notre interprétation reste classique du fait que le principe d'interposition, qui veut qu'un qbit puisse avoir à la fois les valeurs 0 et 1,[13] n'est pas pris en compte. Par exemple, selon notre interprétation, si un électron est dans une orbite de la bande de conduction pendant un intervalle de temps, cela représente le bit 1.[14] L'intervalle de temps pendant lequel cet électron quitte cette orbite ou niveau d'énergie représente le bit 0.

Pour vous aider à mieux comprendre le comportement de ce courant électronique au sein de l'atome de silicium, nous nous référons au concept de liaisons covalentes trouvé au chapitre 2 (p.30-33) du livre d'Albert Paul Malvino et David J. Bates : « Principes d'électronique ».

D'après Bates et Malvino, chaque atome d'un élément du tableau périodique est constitué d'un noyau positif composé d'un certain nombre de protons et de neutrons autour duquel se trouvent une ou plusieurs couches d'électrons (e-) tournant autour du noyau suivant des orbites bien définies. Les métaux sont de bons conducteurs du courant électrique car lorsqu'un fil métallique est soumis à une tension, les électrons, dans la couche de valence, passent instantanément à une couche supérieure, la couche de conduction. Pour l'élément silicium (SI), l'orbite la plus externe contient 4 e-, c'est l'orbite de valence qui selon certaines conditions de température et de dopage deviendra la bande de conduction.[15, 16]

Comme le montre la **figure 1**, en ce qui concerne les éléments semi-conducteurs tels que le germanium (Ge) ou le silicium (Si), ce passage vers la couche de conduction est plus ou moins facilité par des éléments dopants tels que le phosphore (à cinq électrons e- de valence) ou aluminium (avec trois e- de valence).

N.B.Notre interprétation repose sur le SI, mais d'autres alliages de semi-conducteurs peuvent aussi bien être utilisés.

Basé sur le principe d'exclusion de Pauli, il existe une interprétation complètement nouvelle et plus précise de l'interprétation classique de la bande de conduction. Selon Pauli, deux particules fermioniques ne se retrouvent jamais dans le même état quantique, il faut donc considérer qu'il n'y a pas qu'une seule bande de conduction, mais que le courant électronique est le résultat de plusieurs bandes de conduction.

FIGURE 1

Semi-conducteur de type N

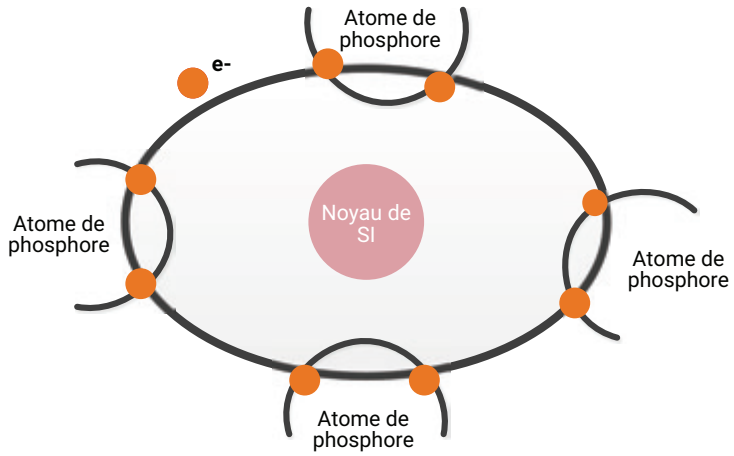


Figure 3 Représentation des bandes de conduction suivant le Principe d'exclusion de Pauli

Les théoriciens classiques ne croyaient pas nécessaire de considérer ces subdivisions de la bande de conduction en des sous-bandes, contenant chacune un électron à un niveau d'énergie spécifique (ou état quantique). Selon Pauli, chaque électron est à un niveau d'énergie distinct des autres niveaux. Chaque niveau d'énergie est déterminé par quatre nombres quantiques désignés par les lettres n, l, m, s (n, l, m et s sont uniques pour chaque électron).[17] Ainsi, comme à aucun moment deux électrons orbitant autour du noyau atomique ne peuvent posséder les mêmes lettres (n, l, m, s), il est tout à fait possible de concevoir un autre comportement du courant électronique. En maintenant cette interprétation dans le contexte de la technologie, un problème important en cybernétique est résolu : empêcher le compilateur quantique de casser les clés de chiffrement actuellement utilisées pour sécuriser les informations sensibles enregistrées dans les systèmes d'information actuels. Parce que certaines données doivent rester confidentielles quel que soit le compilateur utilisé, cette adaptation classique d'une théorie quantique reste le seul moyen de protéger les informations chiffrées de la menace quantique.

Interprétation classique basée sur le principe d'exclusion de Pauli

A partir des 4 électrons de valence du SI, l'électronique classique en a déduit qu'il y a, théoriquement, 16 états possibles (2^4) allant de 0000 (4 trous) à 1111 (4 électrons).

Cependant, en intégrant les exigences du principe d'exclusion de Pauli dans le modèle classique, nous obtenons (avec les huit électrons (1) ou les huit trous (0) du modèle de Pauli) : 256 (2^8) états initiaux pour un même atome (c'est-à-dire des valeurs binaires variant de 00000000 à 11111111).

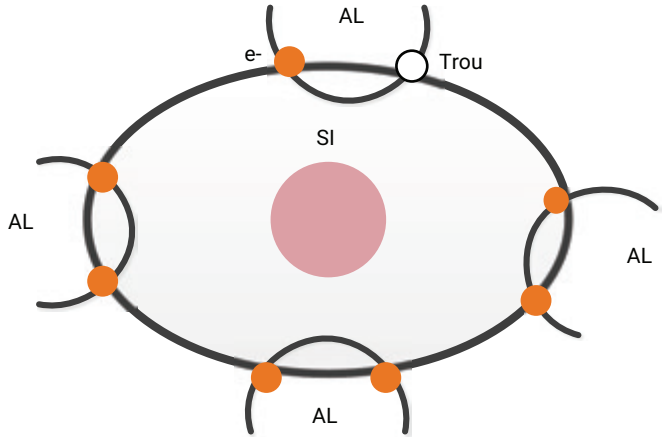
Après avoir examiné les immenses services que les 16 états initiaux rendent actuellement en termes de cryptage et de hachage, il existe de nombreuses autres ressources qui pourraient être tirées avec 256 états initiaux pour sécuriser les données actuelles.

L'algorithme des bits colorés

Un modèle de bit coloré peut être utilisé pour expliquer comment fonctionneront les nouveaux

FIGURE 2

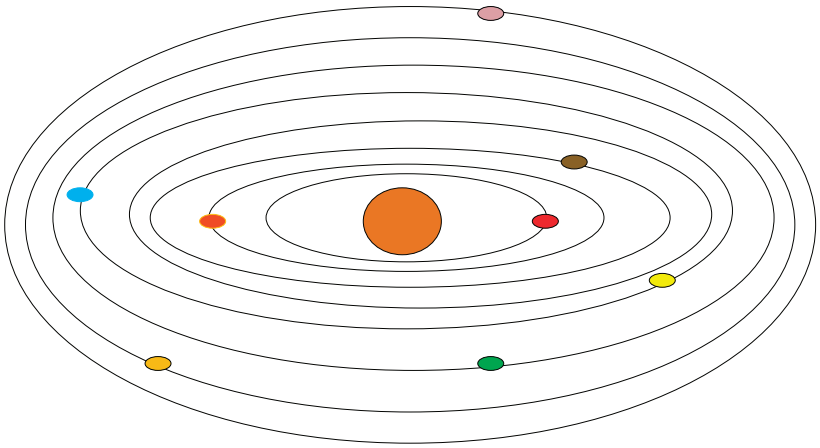
Semi-conducteur de type P



Notre interprétation repose sur le SI, mais d'autres alliages de semi-conducteurs peuvent aussi bien être utilisés.

FIGURE 3

Représentation des bandes de conduction suivant le Principle d'exclusion de Pauli



circuits électroniques construits pour simuler la théorie du niveau d'énergie de Pauli. Il est important de noter que chaque couleur représente un électron à un niveau d'énergie spécifique.

La **figure 3** représente les liaisons covalentes pour les semi-conducteurs de type N selon la théorie des niveaux d'énergie de Pauli. Une représentation théorique des applications de cette nouvelle interprétation du modèle électronique est présentée. Cette approche n'est pas nouvelle. Par exemple, les théoriciens ont dû concevoir "l'effet transistor",[18] avant que ce composant ne soit produit avec succès, en laboratoire. Donc, il convient de noter que ces

FIGURE 4

// Algorithme du Bit coloré

```
//Déclaration
β: Booléen  // Peut prendre la valeur 0 (Trou)
ou 1 (électron)
t: réel  // Temps en microseconde de type float
∑: états[7]  /* Tableau représentant  les sous-couches
allant de 0 à 7
indiquant l'état de β à  l'instant t  avec 0 :Noir; 1
:Marron; 2 :Rouge;
3 :Orange;  4 :Jaune; 5 :Vert; 6 :Bleu; 7 :Violet*/
/*(À noter que les couleurs n'ont rien à voir avec le
codage électronique utilisé par exemple pour déterminer
la valeur des résistances. Chaque couleur représente une
fréquence admise, un niveau d'énergie) */
C: canaux[7]  /* Array of 8 elements representing the
monochrome bits (0 and 1) β0 to β7 as traditionally
represented on the Internet */
A: Authentification[3]  /* Array  representing the bits from
β0 to β2 addressed to the Authentication server with
Black: Physical data of the 4D card; Brown: User biometric
data; Red: GPS location data */
M : Message[4]  /* Représente les bits de β3 à
β7  adressés au destinataire avec Orange : Clés de
chiffrement du message;  Jaune : Données concernant
par exemple la Direction générale; Vert: Données
concernant par exemple la Direction des RH; Bleu :
Données concernant par exemple la Direction des
Finances ; Violet : Données concernant par exemple la
Direction informatique*/
Begin //Émission
Initialisation
 t=0.00
β reçoit β
β reçoit β
β reçoit β
β reçoit β
β reçoit β
β reçoit β
β reçoit β
β reçoit β

Afficher : états
∑= [β, β, β, β, β, β, β, β]
Pour t allant de 0.00 à n.nn on a :
∑= [β, β, β, β, β, β, β, β]
Next
Fin Next
//Transmission des signaux émis à travers les
canaux de l'Internet
β recoit β0
β recoit β1
β recoit β2
β recoit β3
β recoit β4
β recoit β5
β recoit β6
β recoit β7
Affichez canaux
c=[β0, β1, β2, β3, β4, β5, β6, β7]
End //Émission

Begin //Réception
Initialisation
c=[β0, β1, β2, β3, β4, β5, β6, β7]
//Filtrage des canaux et dispatching
Authentification // Bits adressés au serveur
d'authentification
Avec :
β0 reçoit β
β1 reçoit β
β2 reçoit β
Afficher: Authentification
A= [β, β, β]
End Authentification
Message // Bits adressés à l'entreprise avec la
clé de chiffrement
Avec
β3 reçoit β
β4 reçoit β
β5 reçoit β
β6 reçoit β
β7 reçoit β
Afficher: Message
M= [β, β, β, β, β]
End Réception
End
/* Le présent programme suppose que la propagation
des bits se réalise de façon parallèle. Il n'empêche
que les circuits peuvent être modifiés afin que la
propagation se fasse en série de sorte qu'on ait les trains
d'impulsion suivants : */
β reçoit β5
β reçoit β6
β reçoit β7
β reçoit β0
β reçoit β1
β reçoit β2
β reçoit β3
β reçoit β4
/*Dans le canal contenant par exemple les données
biométriques de l'utilisateur. Ou encore : */
β reçoit β6
β reçoit β2
β reçoit β3
β reçoit β4
β reçoit β7
β reçoit β0
β reçoit β1
β reçoit β5
/* adressés à la Direction des Technologies de
l'Information. Ce pour augmenter l'inviolabilité des
informations transmises */
```

concepts doivent être testés au laboratoire afin qu'on puisse se prononcer sur leur faisabilité.

Le circuit électronique, découlant de l'algorithme du bit coloré, est représenté à la **figure 4**. Ce circuit devrait constituer le point de départ à la réalisation d'autres circuits logiques élémentaires capables de simuler le fonctionnement tout à fait "classique" du principe d'exclusion de Pauli.

Exemple de transactions possibles avec des bits colorés

La notion de bit coloré est une manière symbolique de représenter une réalité mathématique. En fait, chaque couleur représente le niveau d'énergie dans lequel se trouve le bit.

Les bits colorés ne seront plus les mêmes pour chaque transaction (cela signifie par exemple si quelqu'un fait 5 retraits sur son compte bancaire le même jour chaque transaction sera exécutée par une gamme différente de bits colorés). Par exemple, un bit rouge utilisé dans un canal pour une transaction bancaire peut devenir vert pour la prochaine transaction adressée à la même banque le même jour. Le bit peut redevenir rouge plus tard, mais ce sera lorsque le propriétaire de la carte communiquera avec son médecin ou son université, par exemple.

Le besoin de confidentialité est déjà largement appliqué par l'utilisation de mots de passe. Cependant, les mots de passe échouent car il s'agit d'une mesure qui se produit longtemps après que la menace s'est installée et parce que cette mesure utilise les mêmes processus et la même logique que la menace. Que ce soit pour protéger ou pour attaquer les systèmes d'information, les mêmes outils sont utilisés : les mêmes machines booléennes avec les mêmes compilateurs qui obéissent aux mêmes règles de langage formel.

Fonctionnement d'un afficheur sept lignes selon l'algorithme des bits colorés

En plus de l'algorithme du bit coloré, l'étape suivante consiste à créer une matrice de diodes pour matérialiser la notion de commutation issue de l'algorithme du bit coloré (**figure 5**). Ce réseau de diodes est généralement un exercice de laboratoire de base qui permet aux étudiants débutants de comprendre le fonctionnement d'un circuit de commutation de base. La matrice de diodes traditionnelle est représentée telle qu'elle fonctionne actuellement, puis elle est légèrement modifiée pour répondre aux exigences de l'algorithme de bit coloré et de notre interprétation du principe de Pauli.

Cette matrice permet aux interrupteurs d'afficher les chiffres de 0 à 9 ou certaines lettres comme A, C ou E. Elle est composée d'interrupteurs , de résistances , de diodes et de diodes électroluminescentes (LED).

Variantes adaptées au principe des niveaux d'énergie

La **figure 6** et la **figure 7** représentent quelques modifications de la matrice de diodes présentées précédemment. Pour les besoins de notre démonstration nous avons remplacé les interrupteurs par des condensateurs fixes (**figure 6**) puis par des condensateurs variables (**figure 7**). Ces variations ont été conçues par nous.[19]

Un exemple de scénario

Pour bien comprendre comment fonctionne ce nouveau type de multiplexage de l'information, prenons l'exemple de trois employés travaillant dans une banque : l'un au service financier, le deuxième aux ressources humaines (RH) et le troisième à l'informatique.

FIGURE 5

Matrice de diodes traditionnelle

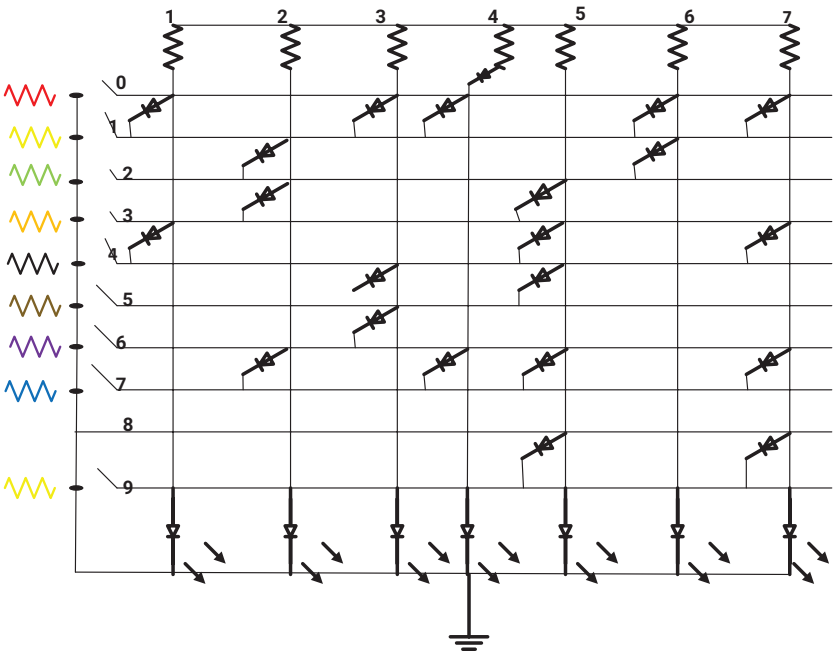


FIGURE 6

Afficheurs à sept branches avec trains d'impulsions fixes

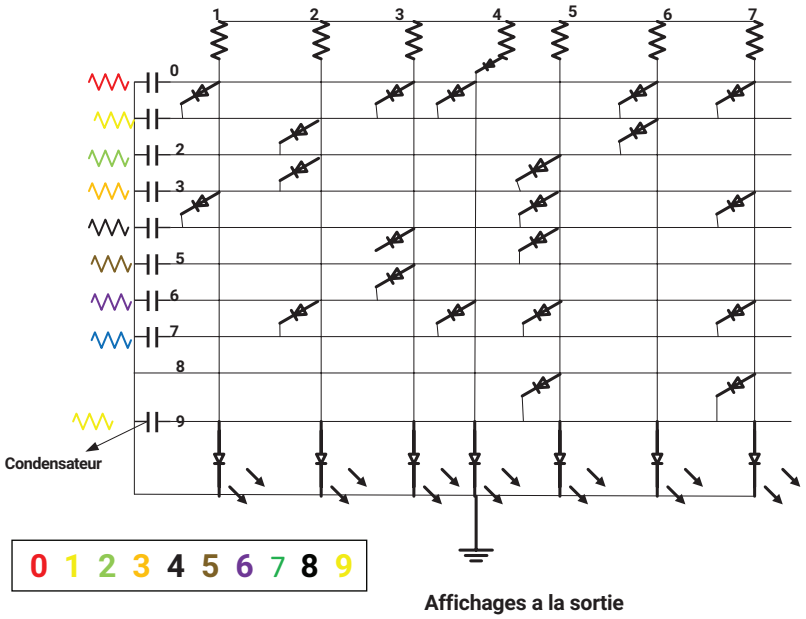
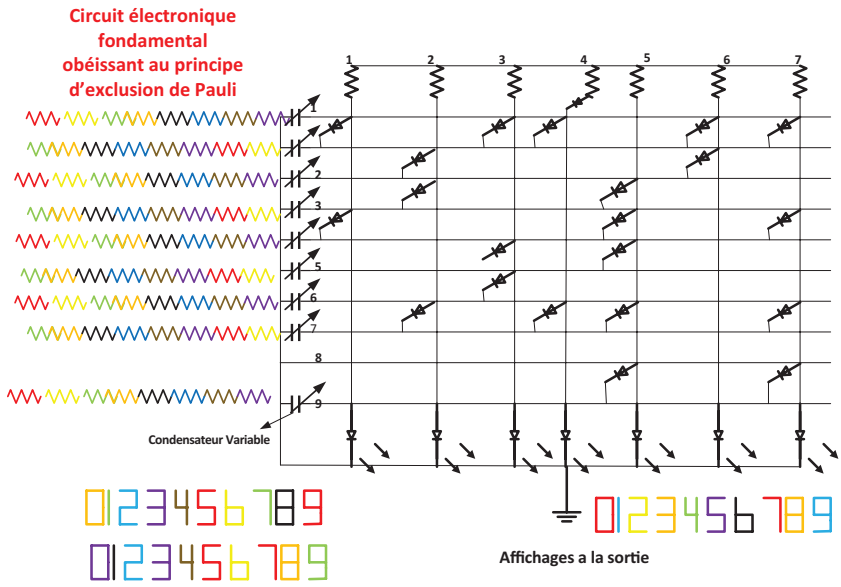


FIGURE 7

Afficheurs à sept branches avec trains d'impulsions variables



Ces 3 salariés travaillent à domicile et utilisent leur carte 4D pour effectuer leurs tâches quotidiennes et autres activités nécessitant ou non une authentification stricte. Par exemple, le premier salarié utilise sa connexion pour travailler et consulter son dossier universitaire, le deuxième salarié utilise sa carte 4D pour faire son travail, mais en même temps pour discuter avec ses amis sur l'internet sans avoir besoin de s'authentifier, et le troisième salarié envoie plusieurs rapports relatifs aux départements TI, RH et finance.

Grâce à ce nouveau mode de commutation, les scénarios suivants deviennent possibles en fonction du jour, de l'heure et de la destination :

- Pour le premier employé, le serveur d'authentification ainsi que les données de la carte 4D décident que pour chaque destination, un certain nombre de fréquences (c'est-à-dire des couleurs) seront utilisées. Par exemple, en plus des fréquences relatives aux caractéristiques physiques de la carte et aux données biométriques de l'utilisateur, les couleurs vert, rouge et bleu seront utilisées pour les données bancaires et les couleurs orange, jaune et rouge seront utilisées pour la communication avec l'université.
- Pour le deuxième employé, la fonction de clavardage s'effectue selon les modes de connexion traditionnels et seules les données concernant la banque sont traitées par des bits de couleur.
- Pour le troisième employé, les bits de couleur sont parfois distincts et parfois similaires durant le même intervalle de temps, permettant à l'employé de communiquer avec les trois services différents.

Comment est-ce possible? Chacun de ces protocoles est programmé lors des différents points de contact physiques que le serveur d'authentification a avec les différentes cartes 4D. Ces points de contact permettent au serveur d'authentification et à la carte 4D de déterminer quel filtre sera utilisé de bout en bout pour chaque communication. Pendant ce temps, un man-in-the-middle ne verra qu'un certain nombre de bits monochromes (0 ou 1), que le système soit équipé d'un compilateur classique ou quantique. Toutes les données qui quittent la banque pour passer par Internet forment une séquence de bits indiscernables qui sont complètement chaotiques pour tout système non concerné par la communication proprement dite. De plus, comme indiqué dans "Le chaos à la rescousse", les bits colorés se trouvent à la couche 1, ou la couche physique du modèle OSI en charge du courant électronique et de la bande passante. Les autres méthodes traditionnelles de cryptage et de hachage sont associées aux bits colorés pour rendre impossible tout processus de décryptage frauduleux.

Ces bits colorés fournissent un nouveau type de périmètre de sécurité virtuel. Tout en participant au chiffrement et à la factorisation, les bits colorés doivent d'abord être considérés comme un « sauf-conduit », sans lequel aucun intrus ne peut entrer dans un système d'information car il ne peut faire une demande d'autorisation exacte. Ainsi, un man-in-the-middle perdra son temps à essayer de déchiffrer un ensemble de bits inutiles qui ne sont, en définitve, qu'une déformation physique de la structure interne de la carte.

Conclusion

Avec la prolifération des applications dans le dark web, les faussaires sur Internet ont de nombreuses possibilités pour commettre des actes répréhensibles. Ce n'est pas une hypothèse farfelue que les méthodes d'authentification qui sont fiables aujourd'hui deviendront accessibles aux manipulations à l'avenir. Il est probable que des attaques auront lieu lorsque les cybercriminels seront équipés de compilateurs quantiques et pourront violer les protections des systèmes d'information les plus critiques. Dans ce monde à venir, la véracité et l'authenticité des informations peuvent devenir un véritable défi. C'est dans cette quête d'authenticité que réside la compatibilité sélective.

Cette recherche présente tous les aspects qui doivent être mis en œuvre pour atteindre la sécurité des systèmes d'information tout en veillant à ce que les données critiques des citoyens ne se retrouvent pas entre les mains de ceux qui pourraient les utiliser à des fins malveillantes. Elle propose une nouvelle approche pour faire face à la menace quantique en utilisant une solution intermédiaire basée sur l'algorithme du bit coloré. Cette solution expérimentale est principalement basée sur l'algorithme du bit coloré mais aussi sur de nouveaux circuits électroniques fondamentaux représentant une matérialisation de cet algorithme.

Cette recherche vise également à établir une imputabilité irréfutable en matière de sécurité de l'information. En ce 21e siècle, l'imputabilité et l'authenticité doivent toujours être incontournables.

Endnotes

1 Raphael, J. J.; J. C. Célestin; E. R. Dijethieu; "Chaos to the Rescue," *ISACA® Journal*, vol. 4, 2019, *https://www.isaca.org/archives*
2 *Ibid*.
3 Dico en ligne Le Robert, "Cybernétique," *https://dictionnaire.lerobert.com/definition/cybernetique*
4 *Op cit* Raphael *et al*.
5 Nobody could steal information inside the card because of the chaotic encryption processes in place.
6 *Op cit* Raphael *et al*.
7 Collège de France "The Quantum Computing Ecosystem Is Emerging," 31 May 2021, *www.college-de-france.fr/site/frederic-magniez/Lecosysteme-de-linformatique-quantique-est-en-train-de-naitre.htm*
8 Calik, C.; M. Sonmez Turan; R. C. Peralta; "Boolean Functions With Multiplicative Complexity 3 and 4," *Cryptography and Communication*, vol. 12, 18 July 2020, *https://doi.org/10.1007/s12095-020-00445-z*
9 ScienceDirect, "Boolean Logic," *https://www.sciencedirect.com/topics/computer-science/boolean-logic*
10 Université de Toulon (La Valette-du-Var, France), *https://www.univ-tln.fr/*
11 Futura Sciences, "John Von Neumann," *https://www.futura-sciences.com/sciences/personnalites/matiere-john-von-neumann-256/*
12 Encyclopaedia Britannica, "Pauli Exclusion Principle," *https://www.britannica.com/science/Pauli-exclusion-principle*
13 Techno-Science, "Quantum Superposition Principle: Definition and Explanations," *https://www.techno-science.net/definition/8048.html*
14 Malvino, A. P.; D. J. Bates; *Electronic Principles*, McGraw Hill, USA, 2006
15 Georgia State University, Atlanta, Georgia, USA, "Pauli Exclusion Principle," *http://hyperphysics.phy-astr.gsu.edu/hbase/pauli.html*
16 Georgia State University, Atlanta, Georgia, USA, "Covalent Bonds," *http://hyperphysics.phy-astr.gsu.edu/hbase/Chemical/bond.html#c2*
17 Lobo, C.; "The Philosophical Meaning of the Pauli Exclusion Principle or the Position of the Problem of Individuation in Quantum Mechanics," Rue Descartes, 2020, *https://www.cairn.info/revue-rue-descartes-2020-2-page-166.htm*
18 Cité des Télécoms, "Invention of the Transistor and Integrated Circuit," *https://www.cite-telecoms.com/blog/histoire/200-ans-de-telecoms/les-temps-modernes/du-transistor-au-circuit-integre/*
19 *Op cit* Raphael *et al.*