

L'ORDINATEUR QUANTIQUE EST-IL L'AVENIR DE L'INFORMATIQUE ?

SOMMAIRE

SOMMAIRE	2
AVANT-PROPOS	3
INFOGRAPHIE	
▪ QU'EST-CE QUE L'INFORMATIQUE QUANTIQUE ?	4
INTERVIEW	
▪ ORDINATEUR QUANTIQUE : APPLICATIONS DANS L'INDUSTRIE DU FUTUR	5
DE PETITES AVANCÉES EN PETITES AVANCÉES...	
▪ LE PING-PONG QUANTIQUE, UN BOND EN AVANT POUR L'INFORMATIQUE QUANTIQUE	11
CRYPTOGRAPHIE QUANTIQUE	
▪ VERS DES SYSTÈMES DE CRYPTOGRAPHIE QUANTIQUE PLUS SÛRS	12
ATTAQUES QUANTIQUES	
▪ LA SÉCURITÉ DU WEB FACE À L'INFORMATIQUE QUANTIQUE	14
EN VIDÉO	
▪ VULGARISER LA PHYSIQUE QUANTIQUE : TOUT UN ART	15



AVANT-PROPOS

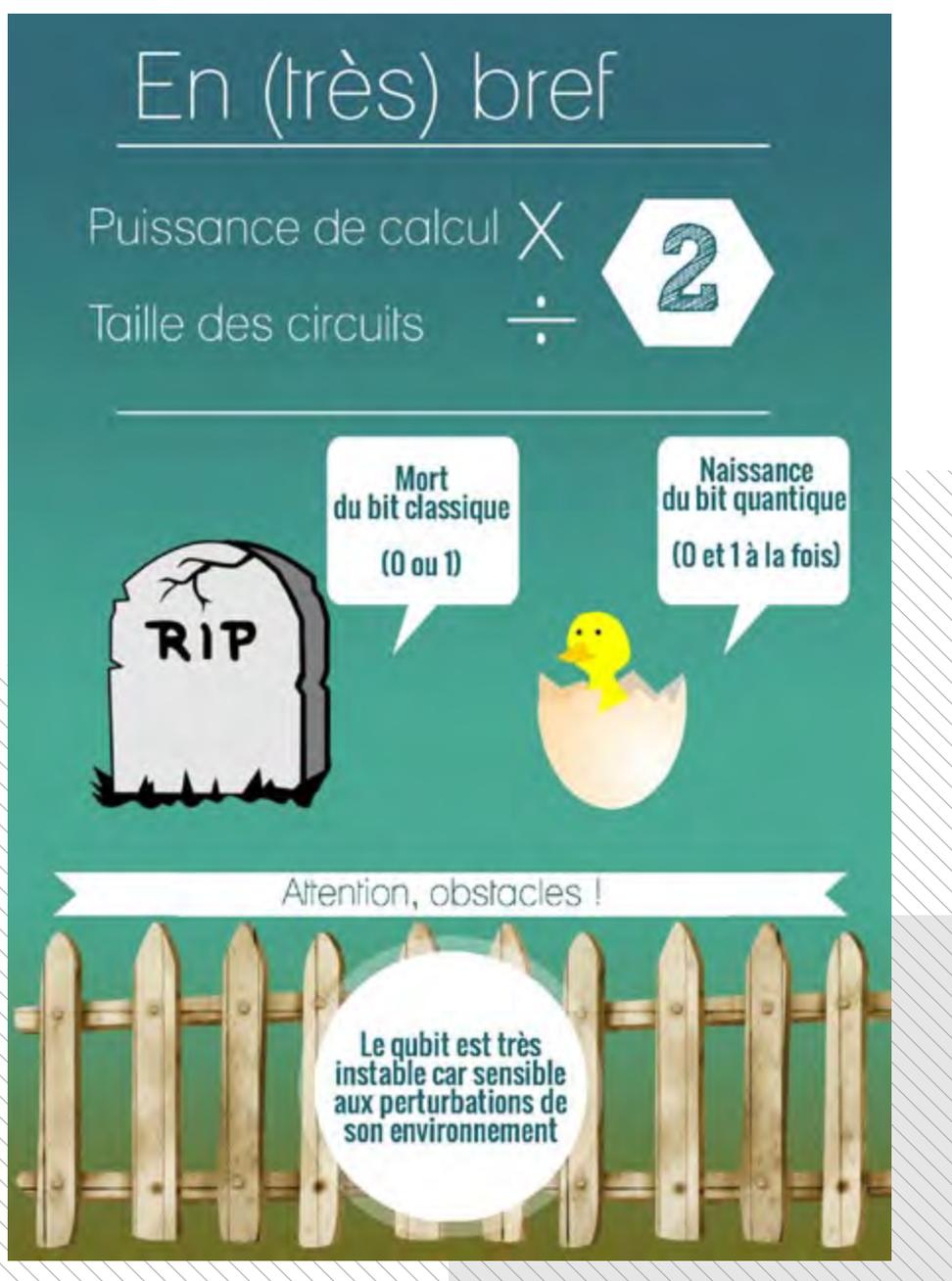
Il fait rêver bien des scientifiques. Plus rapide, plus performant, il pourrait réaliser des opérations jusqu'à présent impossibles et dépasser les plus puissants supercalculateurs. Oui, mais il reste des obstacles non négligeables à franchir : les qubits sont capricieux, ils ne cessent de bouger !

Les industriels rivalisent d'ingéniosité pour s'emparer du premier spécimen viable. Google a monté une équipe de chercheurs entièrement dédiée à ce projet. Créer le tout premier ordinateur quantique lui conférerait non seulement une aura indescriptible mais lui assurerait surtout une place de choix dans le monde technologique de demain.

Les applications ne manquent pas : chimie moléculaire, big data, machine learning, cryptographie... Celui qui posséderait l'ordinateur quantique serait à même de déchiffrer tous les codes. La rédaction de Techniques de l'Ingénieur vous propose de partir à la découverte de ce mystérieux ordinateur...

INFOGRAPHIE

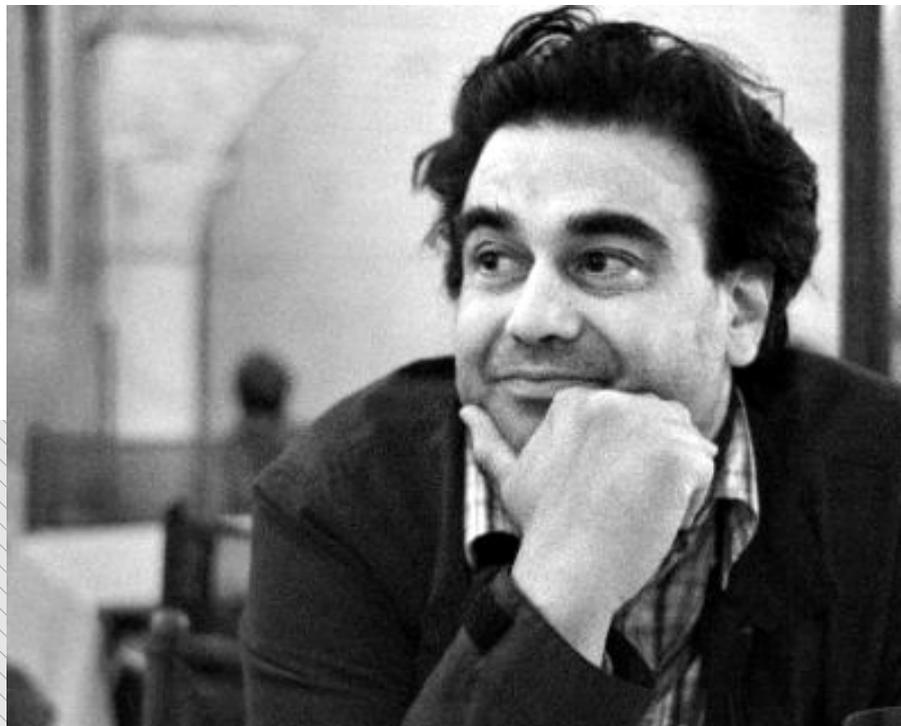
QU'EST-CE QUE L'INFORMATIQUE QUANTIQUE ?



INTERVIEW

ORDINATEUR QUANTIQUE : APPLICATIONS DANS L'INDUSTRIE DU FUTUR

On entend souvent que l'ordinateur quantique est l'avenir de l'informatique : puissance de calcul démultipliée, microprocesseurs de la taille d'un atome, applications dans le big data, la chimie moléculaire, le machine learning et la cryptographie... Cela laisse rêveur. Mais qu'en est-il vraiment ? Quelles sont les réelles possibilités ? Les défis à relever ? Et quand découvrirons-nous enfin le premier ordinateur quantique ? Nous avons posé ces questions à Laurent Saminadayar, chercheur à l'Institut Néel au département des nanosciences et spécialisé en physique mésoscopique.



Techniques de l'Ingénieur : M. Saminadayar, vous êtes professeur à l'Université de Grenoble et chercheur à l'Institut Néel au département des nanosciences, c'est bien ça ? Quel est votre champ d'études ?

Laurent Saminadayar : Oui, je travaille depuis 15 ans sur ce qu'on appelle la physique mésoscopique, c'est un des champs dans lesquels ont émergé les ordinateurs quantiques et tout ce qui concerne la cohérence quantique.

Selon vous, qu'est-ce qui différencie un ordinateur quantique d'un ordinateur classique ?

C'est un problème fondamental. C'est tout l'intérêt de l'ordinateur quantique.

Avec un ordinateur classique, vous effectuez des opérations avec des bits qui seront 0 ou 1. L'ordinateur quantique s'inscrit quant à lui dans un système où le bit se trouve dans un état qui est une superposition de 0 ou 1. Donc au lieu d'avoir 0 ou 1, vous avez une proportion de 0 et de 1.

Quel est l'intérêt ? Ce n'est pas simplement un jeu d'écriture ! Quand votre système est une superposition d'états, c'est un petit peu comme si vous faisiez des calculs parallèles, donc vous allez beaucoup plus vite sur certains calculs. S'il n'y avait que cela, ce ne serait pas vraiment très intéressant.

Donc pourquoi est-ce que cela a suscité autant d'engouement ? Parce que cela vous donne la possibilité de changer

complètement certains algorithmes, c'est-à-dire la façon même d'effectuer certains calculs.

En informatique, il existe des problèmes dits « NP complets ». Comment se caractérisent-ils ? Imaginons que vous vouliez faire une opération sur un nombre, par exemple factoriser un nombre en produits de facteurs premiers. Ce problème peut paraître très simple, nous avons tous réalisé des exercices de ce type au collège. Pourtant, pour un ordinateur classique, ce problème est délicat. Pourquoi ? Simplement parce que le nombre d'opérations qu'il lui faudra faire va croître exponentiellement avec la taille du nombre à factoriser. Donc, pour factoriser un grand nombre, c'est long... Et c'est là le principe de la cryptographie, qui permet de coder nos échanges (numéros de cartes de crédit ou données encore plus sensibles...).

Supposons que je veuille vous envoyer un nombre a . Je le multiplie par un nombre premier b , et je vous envoie le résultat c . Mais vous, vous avez la clef, c'est à dire le nombre b ; quand vous recevez c , vous le divisez par b (votre clef), et voilà, vous avez le nombre a que je voulais vous transmettre en toute sécurité. Si je suis un pirate malveillant, j'intercepte le nombre c que vous envoyez ; mais comme je suis un pirate malveillant, je n'ai pas la clef, c'est à dire le nombre b . Donc je demande à mon ordinateur (classique) de factoriser c en produits de nombres premiers, pour récupérer a et b . Si a et b sont des nombres assez grands... je n'arriverai pas à casser le code en un temps... raisonnable.

La sécurité du cryptage est entièrement basée sur cet aspect du problème.

L'ordinateur quantique, lui, n'aurait besoin que de beaucoup moins d'opérations élémentaires pour factoriser mon nombre c en produit de facteurs premiers (en fait, guère plus qu'il ne vous en faudra à vous qui avez la clef, pour diviser le nombre c par votre clef, le nombre b). Là, ça devient très intéressant, car plus besoin de clef pour voir ce que vous avez voulu envoyer ! Donc, dit un peu brutalement :

"Quelqu'un qui sait créer un ordinateur quantique sait créer à peu près tous les codes qui existent actuellement"

On considère donc qu'il existe un seul modèle d'ordinateur quantique ? Ou plusieurs modèles sont possibles ?

Il y a des variantes autour des algorithmes mais la grande différence intervient au moment où vous passez des bits de 0 et 1 à cette superposition de 0 ou 1.

Il y a des problèmes que les ordinateurs ne peuvent pas résoudre, comme le fameux problème du « voyageur de commerce ». Je suis un voyageur de commerce, je dois passer pour mon travail par un certain nombre de villes. Je me demande donc comment passer par toutes ces villes mais en faisant un minimum de kilomètres ; c'est ce qu'on appelle un problème d'optimisation. C'est un problème difficile à résoudre pour un ordinateur classique car quand vous augmentez le nombre de villes, le nombre de calculs élémentaires nécessaires à la résolution du problème croît exponentiellement. Grossièrement, on peut dire qu'il essaie tous les chemins et qu'il regarde quel est le plus court, car il n'y a pas d'autre façon de faire.

Ce qui a vraiment motivé la communauté scientifique, c'est la factorisation en produits de nombres premiers. Des sommes d'argent énormes ont été investies par les industriels et l'armée qui s'y sont évidemment intéressés de très près car s'ils peuvent factoriser en produits de nombres premiers en un temps « polynomial », ils peuvent casser tous les codes. Au niveau de la cryptographie, si vous savez faire cela, il n'y a plus aucun code qui tient, vous pouvez casser tous les codes, tels qu'ils sont conçus actuellement en tout cas, il faudrait en concevoir d'autres. Actuellement, casser un code est une opération très longue à réaliser. Si vous la rendez beaucoup plus courte, c'est gagné.

Un autre aspect fondamental du problème repose sur la sécurité de la transmission de l'information elle-même. Si vous utilisez un système quantique pour coder et transmettre une information, on peut voir très facilement si votre transmission a été interceptée. C'est le principe même de la mécanique quantique : si je regarde un objet je le modifie, j'agis sur lui... Et je laisse donc ma signature !

Il n'y a aucun moyen de le voir sur un ordinateur classique ?

Non, si votre transmission est vue, vous ne le savez pas.

Avec l'ordinateur quantique si quelqu'un nous espionne, on le voit tout de suite ! C'est donc très intéressant au niveau de la sécurité des transmissions...

Que peut nous apporter un ordinateur quantique en dehors de la cryptographie ?

Pour nous, en tant que particuliers, je pense que cela ne nous apportera rien. Parce qu'on n'a aucun algorithme qu'on ne peut pas faire avec un ordinateur classique. En revanche, pour la communication et la cryptographie, c'est vital. Donc cela va plutôt intéresser les gros systèmes, comme l'armée et les banques.

Est-ce que cela pourrait remplacer des supercalculateurs ?

Pour la plupart des problèmes, un ordinateur quantique n'apporterait aucun avantage par rapport aux supercalculateurs actuels.

**"La question importante est :
qu'est-ce que vous ne savez pas faire
avec un ordinateur classique et que
vous pourriez faire avec
un ordinateur quantique ?"**

Pour les chercheurs, dans certains domaines très spécifiques, un ordinateur quantique peut se révéler intéressant : en effet, il existe certains systèmes physiques très compliqués à simuler avec des ordinateurs classiques, alors que ce serait beaucoup plus efficace avec des algorithmes quantiques.

Mais de façon générale, je pense que si des ordinateurs quantiques voient le jour, ce sera pour répondre à des besoins très spécifiques qui concerneront la recherche, l'armée, les banques, mais sans doute pas les particuliers...

Même s'il y a une plus grande puissance, une plus grande capacité de calcul ?

Pour faire des calculs classiques, il n'ira pas plus vite qu'un ordinateur classique. Il y a des problèmes qu'il sait résoudre qu'un ordinateur classique ne sait pas résoudre. Mais sur les problèmes standards qu'un ordinateur sait parfaitement bien gérer, il ne saura pas faire grand-chose de plus...

L'ordinateur quantique est basé sur un principe de probabilité, c'est bien ça ? Comment peut-on faire confiance à un ordinateur basé sur quelque chose de probable ?

On répète l'expérience. On le fait plusieurs fois en parallèle pour en sortir les probabilités. Donc cela fonctionne bien, ce n'est pas un gros problème. Mais ce qui est important, c'est que le support de codage que vous utilisez, le fameux « bit quantique », ne soit pas altéré trop vite. Au départ, on crée une superposition de 0 et de 1. Mais malheureusement, ce genre d'objet quantique n'a qu'une envie, c'est de redevenir un bête 0 ou 1 : c'est ce qu'on appelle la décohérence. Il faut donc que notre superposition dure assez longtemps, que son « temps de cohérence » soit assez long, pour qu'on ait le temps de faire les calculs souhaités... et ça, c'est un problème très compliqué.

Il faut sans cesse vérifier que votre système reste dans le même état quantique, qu'il n'a pas été perturbé ! Parce que le problème, c'est qu'il faut qu'il reste dans cet état quantique suffisamment longtemps pour qu'on ait le temps de faire le calcul et c'est un énorme problème actuellement. On ne sait pas le faire.

Parce que cela bouge tout le temps ?

Disons que la moindre perturbation extérieure transforme votre superposition initiale en un simple 0 ou 1. Imaginons qu'on commence un calcul, tout se passe bien ; et puis, par exemple, votre q-bit va être heurté par un photon (une particule de lumière). Pour lui, c'est un grand coup sur la tête. Au beau milieu du jeu, votre superposition de 0 et de 1 devient un simple 0 ou un simple 1. Le carrosse se trans-

forme en citrouille, le calcul ne peut plus se faire, c'est perdu.

C'est le problème contre lequel tout le monde lutte actuellement et que personne n'arrive à résoudre.

Pour être plus précis, il existe différentes sortes de q-bits. D'une part, vous avez des q-bits réalisés (presque) de la même façon que les circuits intégrés actuels. Donc, on sait en faire un très grand nombre sur une toute petite surface, et on peut aisément envisager de les utiliser dans un ordinateur. Mais voilà, ce sont aussi les plus sensibles aux perturbations extérieures, disons que leur temps de cohérence est de l'ordre de la micro-seconde, et il semble difficile de résoudre ce problème. Et puis il y a des systèmes plus « exotiques », comme des ions piégés dans des « pièges optiques ». Ces systèmes sont beaucoup moins sensibles aux perturbations extérieures, ce qui est un gros avantage. Mais voilà, le problème est qu'ils ne sont pas très pratiques à manipuler : mettre 5 q-bits ensemble prend une pièce entière, alors des millions... Bref, des deux côtés, l'affaire semble buter sur des problèmes sérieux...

Qu'est-ce que le temps de cohérence exactement ?

C'est simplement le temps où le système va rester dans un état de superposition entre 0 et 1. En général, vous n'avez pas le temps de finir votre opération qu'il va se mettre dans un bête état de 0 ou 1. Cela limite énormément les possibilités de ces systèmes-là.

Donc l'optique et le solide sont deux sortes d'ordinateurs quantiques ?

Oui tout à fait, mais « ordinateur », c'est un grand mot, là on parle de 3 ou 4 q-bits... Un ordinateur classique actuel, ce sont des millions de bits... Et dans le cas de l'ordinateur quantique, on a déjà du mal à faire marcher ces 3 ou 4 q-bits ensemble...

Et il en faudrait combien pour que cela fasse un ordinateur ?

Je dirais... des dizaines pour que cela commence à être intéressant. En tous cas, plus que 2...

Parce que là, avec 2 ou 3, les performances sont très limitées ?

Non... vous savez le mieux qui a été réalisé de mieux, avec des q-bits faits d'ions piégés, a été de factoriser 15 en 3×5 . C'est une preuve de principe, cela fonctionne. On peut dire que c'est un début...

Ce qui est intéressant en revanche, et très mystérieux, c'est ce qu'on appelle le projet D-Wave de Google. Ils prétendent que cela fonctionne. Le seul problème, c'est que personne n'a le droit de voir ce qu'il y a dedans. Ils n'apportent pas de preuve définitive qu'il s'agit bien d'un ordinateur quantique. Il y a des gens qui pensent que c'est uniquement une opération marketing. On vous montre une belle voiture, on vous dit que le moteur est révolutionnaire, mais on n'a pas le droit de soulever le capot pour voir ce qu'il y a dedans. Donc on peut avoir de très sérieux doutes. En laboratoire, on ne parvient pas à faire marcher 3 q-bits et eux prétendent en faire marcher 500 ? Soit ils ont réussi là où tout le monde a échoué, à savoir résoudre ce fameux problème de la décohérence, soit il s'agit d'une immense opération d'intox....

Ce sont les seuls qui sont en train de développer un ordinateur quantique actuellement ?

Oui, ce sont les seuls au niveau industriel. Sinon, c'est dans les laboratoires. Après, vous avez toujours des effets d'annonce. IBM avait annoncé qu'ils développaient un ordinateur quantique, on n'a encore jamais rien vu. C'est un peu du business, pour prendre position sur tel ou tel domaine.

Vous avez dit que cela avait surtout un intérêt pour les chercheurs et les banques, quel serait l'intérêt pour Google de développer un ordinateur quantique ?

S'ils sont les seuls à savoir le faire, on sera tous obligés de passer par eux.

"Celui qui sait créer un ordinateur quantique a tiré le jackpot."

Pourrait-on un jour imaginer une application au niveau des particuliers ?

Non actuellement je ne connais personne qui imagine une application au niveau des particuliers. On reste au niveau des grands organismes, banque, armée... Le marché est énorme et comme, en plus, il y a un aspect militaire c'est stratégique. C'est ce qui fait couler beaucoup d'encre... On a réalisé ce que cela représentait, même si la probabilité que cela marche est extrêmement faible. Mais si jamais cela marche, les conséquences sont énormes.

Mais qu'est-ce qui nous bloque actuellement ?

Le principal obstacle, c'est que ces systèmes de bits quantiques ne restent pas cohérents assez longtemps. Il y a 10 ans, les gens disaient : il n'y a aucune raison que cela ne dure pas plus longtemps. Ils ont raison sur le principe ! Mais dans la réalité personne n'y arrive, pourquoi ? On ne sait pas...

Ils sont trop perméables à ce qui se passe à l'extérieur ?

Oui ils sont trop perméables à l'environnement, donc on essaie de fabriquer un joli bit quantique, d'assurer la superposition de 0 et de 1 et puis, à un moment, vous avez quelque chose qui va rompre cet équilibre. Imaginez que vous faites un château de cartes : si quelqu'un ouvre la fenêtre et qu'il y a du vent, tout se casse la figure. C'est trop fragile. Ce sont des constructions qui ne sont pas stables. Et actuellement, elles tiennent debout seulement quelques microsecondes. Il y en a qui se sont lancés dans des calculs savants pour savoir le temps de cohérence minimal qu'il faudrait atteindre pour que le système soit utilisable, éventuellement en incluant des systèmes de corrections d'erreur etc. Mais on est encore loin du compte !

Mais par quoi est-ce perturbé ?

Par la chaleur, le rayonnement électromagnétique, et aussi un facteur important qu'on ne sait pas trop quantifier : il y

a des charges électrostatiques qui se promènent dans les puces. Il faut savoir qu'il y a toujours des petites charges qui bougent à la surface, ces charges créent un champ électrique qui perturbe énormément le système. Donc de nombreux chercheurs travaillent là-dessus dans le but d'éliminer toutes les charges en surface... C'est une des hypothèses pour expliquer que cela ne marche pas pour le moment.

On pourrait envisager un ordinateur quantique d'ici combien de temps ?

Je crois que maintenant plus personne ne fixe de délais... Nous sommes vraiment sur un os. Donc arriverons-nous à le surmonter ou pas ?

En fait, je comparerais un peu le système aux débuts de l'ordinateur. A l'origine, les ordinateurs étaient dans de grandes armoires qui prenaient énormément de place. Et un jour, on a créé le circuit intégré. Si on n'avait pas créé le circuit intégré, et qu'on n'avait pas eu la possibilité de graver tout cela sur une puce de 2 cm, on n'aurait jamais eu l'évolution qu'on connaît car cela aurait été ingérable. Cela a vraiment été une révolution.

Pour l'instant, on en est à une preuve de principe. Tant qu'on n'aura pas trouvé la solution pour garder un temps de cohérence suffisamment long, cela n'ira pas plus loin. Actuellement, on ne connaît pas la solution, mais peut être qu'elle sortira un jour... Au niveau de la cryptographie, cela aurait des conséquences énormes car dans nos sociétés où tout est codé : communications bancaires, commerciales, mots de passe sur ordinateur, etc. si quelqu'un était capable d'intercepter tous les codes... Une armée qui communique à distance c'est toujours codé...

L'ordinateur quantique permettrait un énorme saut. Ce ne serait pas une amélioration, mais un saut !

Il faudra trouver une façon complètement différente de crypter. Pour le moment, on n'a aucune idée de la façon dont on pourrait crypter. Car tous les cryptages actuels sont plus ou moins compliqués mais ils sont tous basés sur le même principe. Si ce principe ne fonctionne plus, vous ne savez plus coder.

Donc l'ordinateur quantique pourrait être dangereux...

C'est justement pour cette raison que cela intéresse les gens...

Actuellement, si vous envoyez un code et qu'il faut dix jours pour le décoder, ce n'est pas forcément intéressant. S'il faut dix minutes, là c'est autre chose ! C'est ce qui est en jeu. Si on peut faire cela, cela changera énormément de choses au niveau mondial, militaire, etc.

Je pense que les milliards qui ont été engloutis là-dedans, ce n'est pas pour rien. Derrière, les enjeux sont faramineux. Et c'est pour ces enjeux que les gens sont prêts à payer énormément. Même s'il y a une chance infime que ça marche, comment passer à côté de cela ?

C'est vraiment stratégique au niveau de tous les domaines importants de notre société : défense et banques notamment. Actuellement, quand vous envoyez un ordre à une armée, le problème n'est pas tant d'intercepter le message mais plutôt de le décoder.

Le tournant de la guerre du Pacifique, cela a été le moment où les alliés ont réussi à décoder les messages des Allemands. C'était fini, on savait où étaient les sous-marins. Là nous sommes un petit peu dans le même enjeu.

"Si vous avez un ordinateur quantique, c'est comme si vous possédiez la machine Enigma, vous savez tout décoder."

Actuellement, on sait décoder bien sûr, mais on se heurte toujours au même problème : c'est long, car factoriser en produits de nombres premiers est quelque chose d'intrinsèquement long, on ne sait pas faire autrement avec un ordinateur classique. Si vous avez un outil qui réalise cela beaucoup beaucoup vite, vous avez gagné. Et là c'est évident que ça intéresse tout le monde...

Propos recueillis par Iris Trahin

DE PETITES AVANCÉES EN PETITES AVANCÉES...

LE PING-PONG QUANTIQUE, UN BOND EN AVANT POUR L'INFORMATIQUE QUANTIQUE

Une équipe de chercheurs anglais est parvenue à se rendre maître de la trajectoire d'un électron, parvenant même à jouer virtuellement au ping-pong avec l'un d'entre eux. Cet impressionnant degré de contrôle pourrait bien s'avérer crucial en informatique quantique.

Une équipe de scientifiques du prestigieux laboratoire Cavendish, le département de physique de l'université anglaise de Cambridge, a réalisé une petite prouesse : déplacer un seul électron le long d'un fil, lui faisant faire une soixantaine d'allers-retours. Ce jeu de ping-pong virtuel où l'électron devient la balle, illustre un degré de contrôle de l'électron sans précédent.

Les électrons transportant un courant le long d'un fil ne vont pas directement d'un bout à l'autre de celui-ci, mais suivent un chemin plus complexe. Cela peut devenir problématique lorsque l'électron transporte une information, car il est plus à même de l'oublier, ou plus scientifiquement, son état quantique est plus à même de perdre sa cohérence.

Ici, un électron peut être confiné dans un petit puits de potentiel, une boîte quantique, juste à la surface d'une feuille d'arséniure de gallium (GaAs). Un chemin, dont l'énergie est plus élevée que les électrons, mène à une autre boîte quantique, vide, et se trouvant à une distance de 4 microns. Un son très bref (quelques milliardièmes de secondes) est alors envoyé à la surface, créant une

« vague », un potentiel électrique qui emmène l'électron, surfant littéralement vers l'autre boîte, où il se retrouve capturé. En reproduisant le son, mais cette fois-ci dirigé dans l'autre sens, l'électron recommence son voyage, dans le sens opposé et ainsi de suite, comme au ping-pong, accomplissant ainsi une soixantaine d'allers retours.

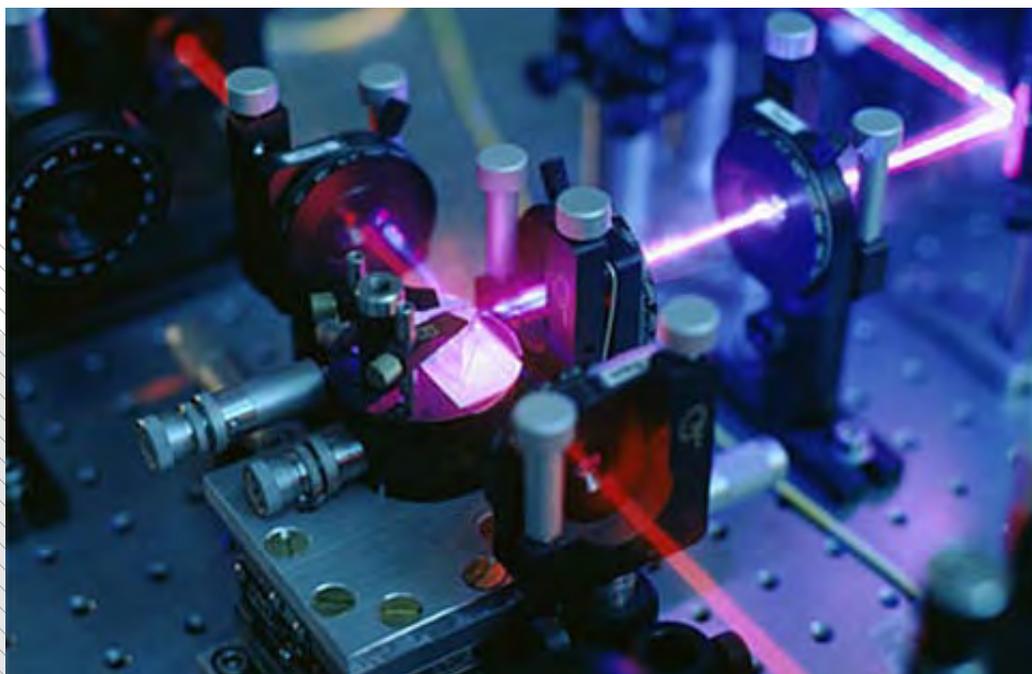
« Cette prouesse est pleine de promesses pour nos ordinateurs quantiques », explique Chris Ford, qui a dirigé l'équipe responsable de la découverte, et dont le travail a été publié dans la revue Nature. « Ces calculateurs pourraient bien aider à résoudre certains problèmes complexes plus rapidement que les ordinateurs traditionnels. Des efforts sont d'ores et déjà fournis pour connecter entre eux différents composants, tel le processeur et la mémoire. Bien que notre expérience ne montre pas que l'électron se souvienne de son état quantique, c'est pourtant plus que probable » poursuit-il. « Cette méthode de transfert des qubits [bits quantiques] pourrait bien être celle choisie, au sein même d'un ordinateur quantique. »



par Rahman Moonzur

CRYPTOGRAPHIE QUANTIQUE

VERS DES SYSTÈMES DE CRYPTOGRAPHIE QUANTIQUE PLUS SÛRS



Des chercheurs de l'Université libre de Bruxelles et de l'Institut des Sciences Photoniques de Barcelone ont prouvé pour la première fois il y a quatre ans que les nouveaux systèmes de cryptographie quantique sont plus sûrs que les systèmes actuels, et avec des taux de génération de clés similaires.

La cryptographie quantique permet de sécuriser la transmission de données en utilisant des clés générées et échangées à l'aide de particules quantiques, les photons. Comme la mécanique quantique stipule que toute observation de l'état quantique d'une particule modifie cet état, toute tentative d'interception de la clé par un espion peut en principe être repérée par les utilisateurs. La sécurité des protocoles de cryptographie quantique est donc absolue et garantie par les lois mêmes de la physique. En théorie oui, mais en pratique ?

La sécurité d'un protocole de cryptographie quantique repose sur le fait que les appareils quantiques mesurent

bien les bonnes propriétés physiques des photons, celles qui permettent de détecter un espion éventuel. Or, des défauts d'implémentation ou des failles du système peuvent compromettre la sécurité d'un système de cryptographie quantique sans laisser de trace visible aux utilisateurs. De tels défauts d'implémentation (corrigés depuis) ont été exploités l'année dernière par des « hackers quantiques » pour casser complètement les principaux systèmes de cryptographie quantique actuellement commercialisés.

Depuis quelques années, suivant une approche initiée par Jonathan Barrett alors postdoc à l'Université libre de Bruxelles (ULB), les chercheurs s'intéressent à des pro-

toques de cryptographie quantique dont la sécurité, si elle se base toujours bien sur les lois de la physique quantique, ne repose en revanche sur aucune hypothèse sur le fonctionnement interne des appareils quantiques.

PREMIÈRE PREUVE COMPLÈTE DE SÉCURITÉ DE NOUVEAUX SYSTÈMES DE CRYPTOGRAPHIE

Les appareils quantiques sont décrits comme des « boîtes noires » qui reçoivent des données à l'entrée et produisent en réponse des données à la sortie. Pourvu que les deux utilisateurs observent certaines corrélations particulières entre les données produites par leurs boîtes noires respectives, le caractère secret des clefs générées par les appareils quantiques est garanti indépendamment de toute hypothèse sur leur fonctionnement interne. En principe, les appareils quantiques pourraient même avoir été conçus par l'espion lui-même.

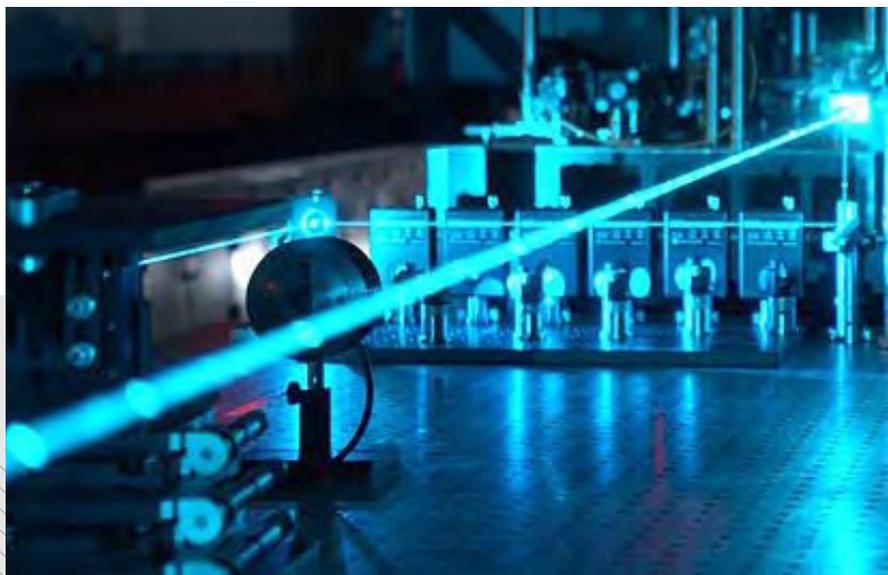
En dehors de son intérêt pratique, qui rend toute tentative d'attaque du système futile, cette approche représente sur un plan plus conceptuel, le niveau ultime de sécurité permis par nos connaissances physiques actuelles. Il restait cependant encore à prouver que cette nouvelle approche était en effet sûre, ceci n'avait été fait jusqu'à présent que pour certaines attaques restreintes. Il fallait aussi montrer que cette nouvelle approche permettait de générer des clefs à un taux raisonnable.

C'est ce qu'ont démontré Stefano Pironio de la Faculté des Sciences de l'ULB et Lluís Masanes et Antonio Acín de l'Institut des Sciences Photoniques à Barcelone qui, dans un article paru le 16 mars 2011 dans la revue *Nature Communications*, établissent la première preuve complète de sécurité de ces nouveaux systèmes de cryptographie pour des taux de génération de clefs comparables à ceux des systèmes actuels. Bien que leur preuve de sécurité repose sur une petite hypothèse sur le fonctionnement des appareils quantiques, qui peut se justifier dans certaines implémentations, leurs résultats démontrent que cette nouvelle approche est en principe possible et représentent une avancée vers des systèmes de cryptographie quantique plus sûrs.

ATTAQUES QUANTIQUES

LA SÉCURITÉ DU WEB FACE À L'INFORMATIQUE QUANTIQUE

En permettant de réaliser des calculs jusqu'ici impossibles, les ordinateurs quantiques pourraient briser les systèmes asymétriques de chiffrement. Les chercheurs tentent de trouver une parade à ces "attaques quantiques", qui menacent la sécurité du Web.



L'avenir de l'informatique est-il dans les ordinateurs quantiques ? En s'appuyant sur les propriétés quantiques de la matière, ces machines hypothétiques permettraient de réaliser des calculs combinatoires complexes, irréalisables avec les machines actuelles.

A la différence du système numérique classique, qui repose sur des données codées en chiffres binaires, le calcul quantique utilise le "bit quantique", ou "qubit" - la plus petite unité de stockage d'information quantique. Contrairement au "bit", qui prend soit la valeur d'un 0, soit la valeur d'un 1, le "qubit" est une combinaison linéaire. Il peut prendre la valeur 0 ou 1, mais aussi les deux ensemble - selon le principe de la superposition d'états quantiques, comme illustré dans l'expérience du chat de Schrödinger, où un atome peut être à la fois intact et désintégré.

Cette technologie, qui devrait permettre de démultiplier le potentiel de calcul, est l'un des chevaux de bataille de Google, qui tente, avec l'université de Santa Barbara, de concevoir un ordinateur quantique. Avec la NASA, la firme a aussi créé la " Quantum A.I. Lab Team", avec pour objectif de développer une intelligence artificielle grâce à l'informatique quantique.

LA FIN DU CHIFFREMENT ASYMÉTRIQUE ?

L'informatique quantique devrait aussi bouleverser le Web actuel, avec des conséquences plus ou moins négatives. Car cette nouvelle technologie permettra, selon l'expert Renaud Lifchitz, de briser le chiffrement asymétrique et les algorithmes RSA, utilisés dans presque tous les domaines touchant la sécurité de la Toile.

“D’ici 25 ans, tous les systèmes asymétriques vont tomber. Il faudra donc trouver une solution alternative”, avait-t-il expliqué en novembre dernier lors de la No Such Conference 2014, à Paris. Le chiffrement RSA repose sur la difficulté de factoriser les grands nombres en nombres premiers, mais avec des calculs quantiques, il deviendrait possible de casser l’algorithme asymétrique.

Pour être la première à profiter de ce type “d’attaques quantiques”, la NSA investit massivement dans un projet baptisé “Penetrating Hard Targets”, destiné à concevoir un ordinateur capable de “briser qui pourrait briser presque tous les types de chiffrements utilisés pour protéger les banques, les transactions en ligne, les entreprises et les documents gouvernementaux dans le monde entier”, indique le Washington Post.

CODE DU SAC À DOS ET CHIFFREMENT QUANTIQUE

Face à ces menaces, deux mathématiciens, Nathan Hamlin et William Webb, effectuent des recherches en “cryptographie quantique”. Ils auraient conçu un code de chiffrement capable de résister aux piratages reposant sur des ordinateurs quantiques. Pour cela, ils ont modifié un algorithme remontant aux années 1970 - le “knapsack code”.

Ce problème d’optimisation combinatoire (en français, le “problème du sac à dos”), très difficile à résoudre, “fut un temps envisagé comme un outil de chiffrement, mais cette idée fut abandonnée quand la clé publique créée fut cassée”, explique William Webb, à la Washington State University. Les chercheurs ont “réalisé des corrections dans la base du code”, comblant de nombreux “points faibles”, jusqu’à concevoir un nouvel algorithme, qui n’utilise que des clés publiques, et qui serait capable, affirment-ils, de déjouer les attaques quantiques.

D’ici à la validation du code de Hamlin et Webb par leurs pairs, le chiffrement quantique permet, d’ores et déjà, d’échanger en toute sécurité des clés privées. Il utilise les propriétés de la physique quantique pour établir des protocoles de chiffrement - par exemple, dans le cas du Protocole BB84, en envoyant des photons polarisés par fibre optique. Seul hic : si cette technologie, déjà utilisée par de nombreuses entreprises, est très efficace, elle reste difficilement applicable au Web, en raison des distances de transmission quantique des clés de chiffrement - pour l’instant, la distance record est de 67 kilomètres.

Par Fabien Soyez

EN VIDÉO

VULGARISER LA PHYSIQUE QUANTIQUE : TOUT UN ART



La physique quantique est une théorie complexe qui peut, d'une certaine façon, défier la logique. Julien Bobroff, physicien, Laboratoire de Physique des Solides à l'Université Paris Sud, a donné il y a quelques mois une conférence - voir la quantique ? - pour mieux appréhender un sujet qui passionne mais rebute par sa complexité.

L'Espace des Sciences est un centre de culture scientifique technique et industrielle. Cette association organise "Les Mardis de l'Espace des sciences", une série de conférences autour de sujets scientifiques, avec un souci de vulgarisation. **Voir le quantique ?**, présenté par **Julien Bobroff**, physicien, revient sur les théories qui font la physique quantique pour les relier à la science du macro que nous connaissons mieux.

Chats de Schrödingers, lévitation, téléportation, effet tunnel... La **physique quantique** est étrange, paradoxale, invisible et insaisissable. Julien Bobroff présente pourtant quelques-unes des astuces qu'ont trouvées les physiciens pour « voir » ces étrangetés du monde quantique et même les filmer en direct !

Il montre aussi comment, en collaborant avec des designers, des graphistes et des artistes, son groupe a développé de nouvelles façons de vous aider à imaginer ce qu'est vraiment la physique quantique.

TECHNIQUES DE L'INGÉNIEUR

QUI SOMMES-NOUS ?

Fondées en 1946 et membres du groupe Weka depuis 1996, les Éditions T.I. sont un leader incontesté de l'information scientifique et technique. Intégrées depuis leur création au paysage mondial de la documentation francophone, elles se déclinent aujourd'hui en deux grandes activités :

- La publication de ressources documentaires de référence (Dossiers fondamentaux, Fiches et outils pratiques », Services associés, articles de Veille & Actualités, etc.)
- Un service de conseil en ingénierie technologique : « Conseil et Formation »

TECHNIQUES DE L'INGÉNIEUR C'EST :

- La plus importante collection documentaire technique et scientifique en langue française,
- Un département dédié à la formation, externe et interne,
- Un acteur majeur du conseil pour l'industrie française et la recherche,
- Le partenaire de référence qui accompagne les industriels français dans leurs projets depuis 60 ans.

TECHNIQUES DE L'INGÉNIEUR EN QUELQUES CHIFFRES :

- Une référence pour les ingénieurs depuis plus de 60 ans,
- Plus de 400 bases documentaires,
- Un réseau de 3 500 experts,
- Plus de 8 000 articles de base documentaire (ou scientifiques), dont 3 000 articles d'archives,
- Près de 2 000 articles d'actualité,
- Plus de 700 fiches de mise en application pratique,
- Un bouquet de 9 services,
- Plus de 300 000 utilisateurs,
- Plus d'un million de pages vues chaque mois sur www.techniques-ingenieur.fr.

LES THÉMATIQUES COUVERTES :

Sciences fondamentales | Génie industriel | Procédés Chimie Agro Bio | Mesures Analyse
Matériaux | Mécanique | Énergies | Électronique Photonique | Technologies de l'information
Construction | Innovation | Environnement

EDITIONS TECHNIQUES DE L'INGÉNIEUR (E.T.I.)

IMMEUBLE PLEYAD 1 – 39, BOULEVARD ORNANO 93200 SAINT-DENIS CEDEX
TÉL. : 01 53 35 20 20 – FAX : 01 53 26 79 18 – TECHNIQUES-INGENIEUR.FR
SAS AU CAPITAL DE 1 375 000 € – RCS BOBIGNY B 380 985 937
SIRET 380 985 937 00032 – NAF 5811 Z



L'expertise technique et scientifique de référence

Techniques de l'Ingénieur vous apporte une information précise et fiable pour l'étude et la réalisation de vos projets. Actualisées en permanence, les **ressources documentaires** profitent aujourd'hui à plus de **300 000 utilisateurs** et sont la référence pour tout ingénieur, bureau d'études, direction technique et centre de documentation.

Depuis près de 70 ans, **3 500 experts** contribuent quotidiennement à développer, enrichir et mettre à jour cette documentation professionnelle unique en son genre.

L'intégralité de ces ressources représente plus de **9 000 articles**, répartis dans plus de **430 bases documentaires**, accessibles sur internet, en téléchargement PDF, et sur tablette.

4 BONNES RAISONS DE CHOISIR TECHNIQUES DE L'INGÉNIEUR

- Une **actualisation permanente** du fonds documentaire
- Un **comité d'experts** scientifiques et techniques reconnus
- Une **collection scientifique et technique incontournable** sur le marché francophone
- L'espace actualité pour suivre les **tendances et innovations** de vos secteurs



DES SERVICES ASSOCIÉS À CHAQUE ABONNEMENT

- **Service de questions-réponses** ⁽¹⁾⁽²⁾ : interrogez les plus grands spécialistes des domaines couverts par vos bases documentaires. Votre abonnement vous permet en effet de poser des questions techniques ou scientifiques.
- **Les articles Découverte** : un article vous intéresse, mais ne fait pas partie de votre abonnement ? Techniques de l'Ingénieur vous offre la possibilité de l'ajouter.
- **Le Dictionnaire technique multilingue** : 45 000 termes scientifiques et techniques – avec illustrations et légendes – en français, anglais, espagnol, allemand.
- **Les Archives** : vos bases documentaires s'enrichissent et sont mises à jour en ligne en permanence. Les Archives conservent la mémoire de ces évolutions et vous permettent d'accéder aux versions antérieures de vos articles, ainsi qu'à ceux qui traitent des technologies plus anciennes.

Profitez également de l'impression à la demande ⁽¹⁾, pour commander une ou plusieurs éditions papier supplémentaires de vos bases documentaires (sur devis).

(1) Disponible pour la France, le Luxembourg, la Belgique, la Suisse et Monaco.

(2) Non disponible pour les établissements scolaires, écoles, universités et autres organismes de formation.

ILS NOUS FONT CONFIANCE :

SAGEMCOM



SAFRAN
AEROSPACE DEFENCE SECURITY



ARKEMA

groParisTech

3M

SIEMENS

ROLEX

CCS

DASSAULT
AVIATION

EADS

L'ORÉAL

SAINT-GOBAIN



Schneider
Electric

THALES





Pour disposer d'un panorama complet sur une thématique
DÉCOUVREZ
les offres de packs !

LES + DES OFFRES PACK

- Un large choix de **+ de 60 thématiques** pour des besoins de contenu plus larges
- Des **tarifs préférentiels sur mesure** adaptés à vos besoins

LES UNIVERS DOCUMENTAIRES

- Plus de 430 bases documentaires et plus de 9 000 articles en 14 univers

- Sciences fondamentales
- Environnement - Sécurité
- Énergies
- Technologies de l'information
- Mécanique
- Innovations
- Génie industriel
- Biomédical - Pharma
- Procédés Chimie -Bio - Agro
- Matériaux
- Mesures - Analyses
- Électronique - automatique
- Construction
- Transports



POUR EN SAVOIR PLUS SUR LES OFFRES DE PACKS...

... contactez le service Relation Clientèle
qui se chargera de vous rediriger vers un chargé d'affaires :

Tél : +33 (0)1 53 35 20 20

Email : infos.clients@teching.com
www.techniques-ingenieur.fr

LES AVANTAGES **TECHNIQUES DE L'INGÉNIEUR**

Le droit d'accès, annuel ou pluriannuel, permet une consultation illimitée des ressources documentaires sélectionnées, ainsi que le téléchargement des versions PDF des articles de référence ou fiches pratiques inclus dans ces ressources. Les droits d'accès sont proposés en monoposte ou multiposte.

▪ ACTUALISATION PERMANENTE

Mises à jour permanentes, publication de **nouveaux articles** de références et fiches pratique : un contenu complet sur le sujet qui vous intéresse, des alertes par email.

▪ DES SERVICES INCLUS

En plus de l'accès aux ressources documentaires, chaque souscription offre un **accès privilégié** à un **ensemble de services**.

▪ MOBILITÉ



Votre abonnement étant **100 % web**, vous pouvez le consulter à tout moment, sur n'importe quel ordinateur ou sur nos versions **iPad et Android**.



Pour accompagner vos équipes et projets,
CHOISISSEZ
les offres de formation et conseil

MONTEZ EN COMPETENCE

- Des formations personnalisées, réalisées au sein de votre établissement et à vos dates
- Un accompagnement à la mise en conformité réglementaire
- Des missions d'audit et de recommandations techniques

LES ENGAGEMENTS **TECHNIQUES DE L'INGÉNIEUR**

- Un réseau d'experts reconnus pour vous conseiller
- Une veille scientifique et technique pour mieux décider
- Les dernières obligations HSE pour être en règle
- Les clés en management des hommes et des projets pour gagner en efficacité

Consultez l'intégralité
des programmes sur le site
de Techniques de l'Ingénieur,
espaces **FORMATION** et **CONSEIL**
www.techniques-ingenieur.fr



RESSOURCES
DOCUMENTAIRES



FORMATION



CONSEIL