Une parade contre les hackers quantiques

Autor(en): **Saraga, Daniel**

Objekttyp: **Article**

Zeitschrift: **Horizons : le magazine suisse de la recherche scientifique**

Band (Jahr): **24 (2012)**

Heft 93

PDF erstellt am: **29.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-970894

Nutzungsbedingungen

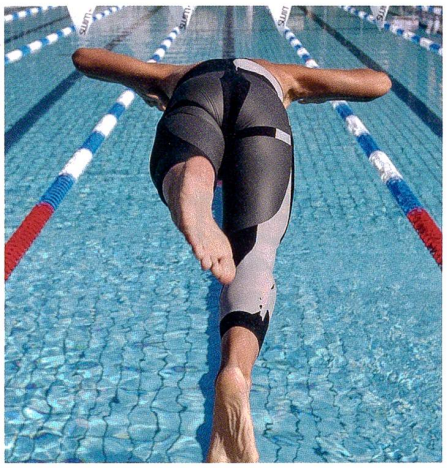
Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch



Patrick B. Kraemer/Keystone

L'entraînement des nageurs pourrait être amélioré grâce à l'intégration de capteurs dans leurs combinaisons.

Des capteurs high-tech pour nager plus vite

Dans une compétition de natation, chaque dixième de seconde compte, et les coaches ne doivent rien laisser au hasard lorsqu'ils entraînent les athlètes. Un capteur high-tech est de nature à les aider. Intégré dans les combinaisons des nageurs, le système « Physiolog® III » comporte des accéléromètres et des gyroscopes dont les signaux, une fois traités, fournissent en quelques minutes des informations essentielles comme la vitesse et la coordination des mouvements.

L'idée est astucieuse. Les chercheurs du Laboratoire de mesure et d'analyse des mouvements (LMAM) de l'EPFL et de l'Université de Lausanne qui l'ont développée ont toutefois dû relever quelques défis. Le principal tient au fait que « dans l'eau, il n'y a pas de phase d'appui ; les modèles utilisés pour la locomotion au sol n'ont donc pas pu être utilisés, note Kamiar Aminian, directeur du LMAM. Il fallait aussi tenir compte de la spécificité biomécanique de la nage ». Testé sur l'équipe du Lausanne Natation, « dont les nageurs et les entraîneurs ont été très coopératifs », ce système va encore faire l'objet de recherches avant son industrialisation éventuelle. Il pourra alors se révéler utile pour l'entraînement en natation, mais aussi dans le domaine clinique, où il est susceptible d'aider à la rééducation dans l'eau. **Elisabeth Gordon** ■

Une parade contre les hackers quantiques

La cryptographie quantique se targuait d'être inviolable. Hélas ! En 2010, une équipe norvégienne a réussi l'impensable : déjouer deux dispositifs commerciaux, dont un vendu par la start-up genevoise ID Quantique. L'astuce ? Les scientifiques ont exploité une faiblesse pour obtenir des informations supplémentaires et percer ainsi la clé de chiffrement secrète, à l'instar d'un voleur qui devinerait votre PIN bancaire grâce au bruit fait par vos doigts sur le clavier d'un distributeur de billets.

« La cryptographie quantique est sûre à 100 %, mais seulement de manière théorique avec des appareils idéaux, explique Renato Renner, de l'EPFZ. En pratique, ce n'est jamais le cas. Les chercheurs norvégiens ont profité du fait que les détecteurs de photons utilisés ne sont pas parfaits. En les aveuglant à l'aide d'un laser, ils sont parvenus à s'immiscer incognito entre l'émetteur et le récepteur de la clé secrète. »

En janvier 2012, Renato Renner a lancé une contre-attaque théorique dans la revue *Nature Communications* et a démontré, grâce à une preuve élégante, qu'un système de cryptographie pouvait retrouver sa fiabilité. « Il suffit que les détecteurs dépassent un niveau d'efficacité donné, fait valoir le physicien. Dans ce cas, on sera certain que le système est sûr, même sans connaître tous les autres détails des appareils. » L'un des auteurs de l'article, Nicolas Gisin, professeur et chercheur à l'Université de Genève, est particulièrement motivé à améliorer ces détecteurs. C'est lui qui, en 2001, a lancé la start-up ID Quantique ! **Daniel Saraga** ■

Eric Martin/Le Figaro Magazine/Dukas

Les troncs des kauris parlent aux climatologues grâce à leurs cernes caractéristiques qui enregistrent les conditions climatiques régionales.

Des arbres sacrés témoins du climat

Le kauri est le plus grand arbre de Nouvelle-Zélande. Le tronc de certains spécimens atteint un diamètre de 5 mètres, voire plus. Les Maoris vénèrent ces géants de la forêt, parfois vieux de plusieurs millénaires. Mais les kauris racontent aussi des histoires particulièrement intéressantes aux climatologues, car ils présentent des cernes caractéristiques et enregistrent avec exactitude les conditions climatiques régionales. Cela permet de reconstruire des calendriers de plusieurs siècles, avec le détail des variations climatiques.

Une équipe internationale de chercheurs, dont faisait aussi partie Jan Wunder, spécialiste en écologie forestière à l'EPFZ, a étudié ces données consignées naturellement en les mettant en rapport avec le phénomène El Niño. Ce système de circulation de l'océan et de l'atmosphère du Pacifique – El Niño/Southern Oscillation (ENSO) – n'a fait pour l'instant l'objet que d'un décryptage fragmentaire. Il induit un changement presque cyclique à l'échelle du climat, et peut avoir un impact local dévastateur : sécheresses avec chutes des récoltes et feux de forêt, tornades et inondations.

On suppose que le changement climatique renforce le phénomène ENSO, mais il était presque impossible, jusqu'ici, d'en apporter la preuve. Les informations fournies par les troncs de kauri permettent de conclure qu'au cours des cinq cents dernières années, c'est au XXe siècle qu'ENSO a été le plus actif. Les données montrent aussi que l'on doit s'attendre à une augmentation de cette activité si les températures continuent à grimper. **Roland Fischer** ■