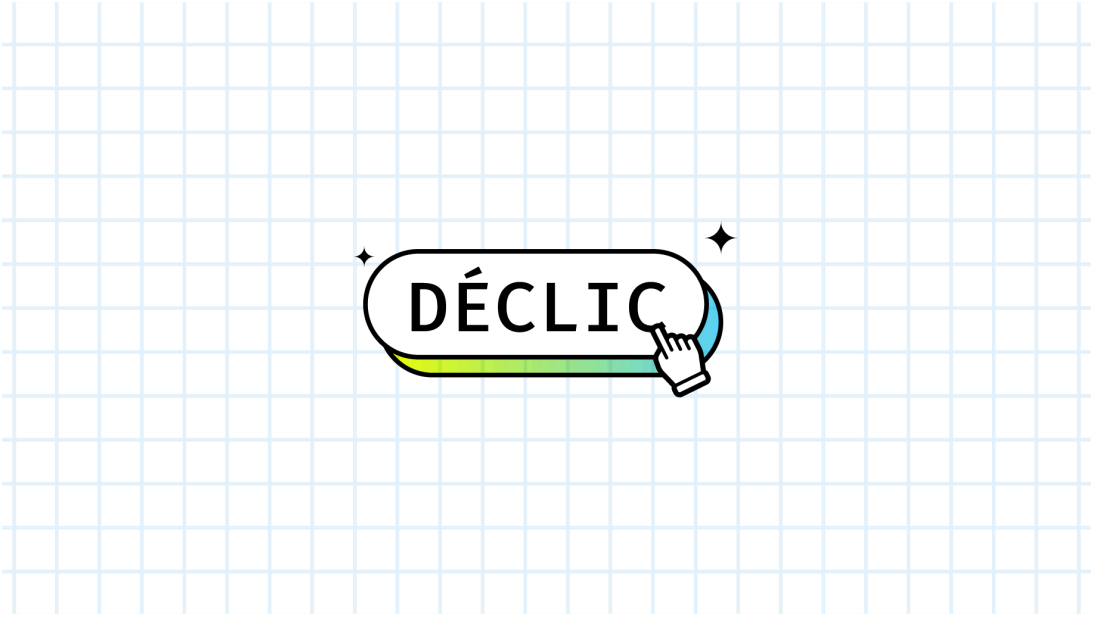
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Inria

Transcripción de la voz en off

DÉCLIC - La criptografía postcuántica



La computación cuántica promete cálculos ultrarrápidos. Pero ¿qué cambiará en términos de seguridad?

Un computador cuántico a plena potencia podría resolver en pocos segundos problemas matemáticos que a los computadores clásicos les tomaría millones de años.Y es por eso que actuamos ahora mismo con la criptografía post-cuántica.

Esto se debe a que la mayoría de los sistemas de seguridad que utilizamos hoy para proteger nuestros datos se basan en métodos eficaces, pero que no fueron diseñados para resistir a la potencia de la cuántica. Los sistemas de seguridad actuales podrían volverse obsoletos.

La buena noticia: ¡existen soluciones!

La criptografía postcuántica es un conjunto de nuevas herramientas creadas para mantenerse fuertes y proteger nuestros datos, incluso frente a las capacidades de los computadores cuánticos. Los desafíos son muchos: inventar nuevos algoritmos, testearlos, y hacer que se puedan usar a gran escala. ¡Y eso toma tiempo!

En Inria, al igual que en otras instituciones, los investigadores en ciencias digitales ya están trabajando en esta transición. Su misión: asegurar la seguridad del futuro, sin esperar a que sea demasiado tarde.

Anticiparse a la cuántica es una cuestión de confianza. Y eso empieza... ¡Hoy mismo!

Encuentra todos los episodios de DÉCLIC en nuestro canal de YouTube, en Inria.cl y en nuestras redes sociales.