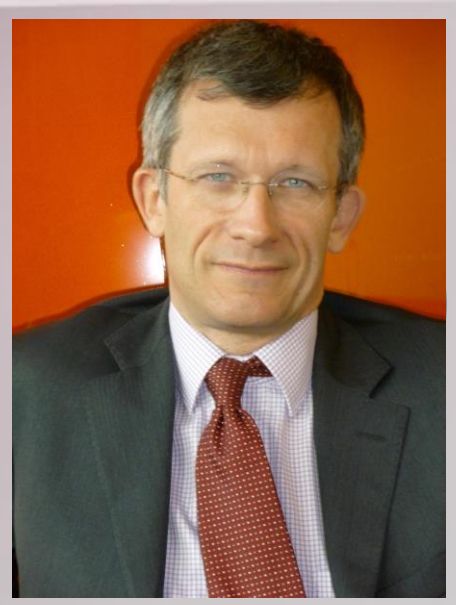
Technologies quantiques et souveraineté

EVIDEN



Philippe Duluc
CTO big data & sécurité

EVIDEN

La révolution de la cryptographie asymétrique (ou à clés publiques)

➔ « non-secret encryption » : Ellis, Cocks, and Williamson (GCHQ), 1969, révélé en 1997

➔ DH76 : Diffie, Helmann, Merkle, 1976 (breveté par Stanford de 1980 à 2000)

➔ RSA77 : Rivest, Shamir, Adelman, 1977 (breveté par MIT de 1980 à 2000)

La (seconde) révolution quantique

➔ cryptographie quantique : sécurité absolue des communications, QKD
protocole BB84 : Gilles Brassard et Charles Bennet en 1984
protocole E91 : Artur Ekert en 1991

➔ calcul quantique : superposition et intrication, qubits, accélération exponentielle
Peter Shor en 1994, décryptement RSA et DH

Exponential speedup explains cyber-threat against asymmetric cryptography in post-quantum world

EVIDEN

PAST & TODAY (pre-quantum)

- after **RSA768** in 2010, **RSA795** in 2019, **RSA829** is the factorization world record (2700 years of cores on tens of thousands powerful machines running CADO-NFS, in 2020)

21403246502407449612644230728393335630086147151447550177977549208814180234471401366433455190958046796109928518724709145876873962619215573630474547705208051190564931066876915900197594056934574522305893259766974716817380693648946998715784949759374979377

=

64135289477071580278790190170577389084825014742943447208116859632024532344630238623598752668347708737661925585694639798853367

×

33372027594978156556226010605355114227940760344767554666784520987023841729210037080257448673296881877565718986258036932062711

- classical CADO-NFS algorithm: **exponential time**
- complexity[**RSA1024**] ≅ complexity[**RSA829**] x 10^{57}

This exponential complexity is the keystone of security of RSA crypto algorithm: standard is evolving today from RSA1024 to RSA2048

TOMORROW (post-quantum)

- quantum Shor algorithm (1994): **polynomial time**
- **RSA829**: almost instantaneous broken by using a quantum computer with several thousands Qubits
- complexity[**RSA1024**] < complexity[**RSA829**] x 2

Critical risk (very high impact, very low probability today) for IT security everywhere, because asymmetric cryptography is everywhere to secure internet and e-commerce

Cas d'usage souverains

EVIDEN

Cryptographie quantique

QKD

communications ultra-protégées bas-débit, haut-débit

Cryptographie post-quantique, mise en oeuvre dans produits cybersécurité Eviden

Capteurs quantiques

gravimètre à atomes froids, horloges atomiques

systèmes de navigation inertielle hyper-stables

détection de sous-marins et d'avions furtifs : capteurs magnétiques (centres NV, SQUID)

guerre électronique: capteurs électromagnétiques

Calcul quantique

émulation (offre Qaptiva d'Eviden), premiers QPU (avec supériorité quantique)

décryptement : vs systèmes asymétriques (Shor), vs systèmes symétriques (Grover)

simulation physique nucléaire, simulation de matériaux critiques

optimisation combinatoire : planification de mission, gestion de ressources

simulation électromagnétique (conception de radars) : résolution équations linéaires (HHL)

quantum RADAR and LIDAR

What is the Penetrating Hard Targets program? (p. 1)

U) RESEARCH & TECHNOLOGY (U) PENETRATING HARD TARGETS

What if a large-scale quantum computer cannot be built? (p. 1)

/SI//REL TO USA, FVEY) Conduct basic research in quantum physics and architecture/engineering studies to determine if, and how, a cryptologically useful quantum computer can be built.

One small step (p. 2)

(TS//SI//REL TO USA, FVEY) Demonstrate dynamical decoupling and complete quantum control on two semiconductor qubits. A qubit is the basic "building block" of a quantum computer. This will enable initial scaling towards large systems in related and follow-on efforts. [CCP_0127]

What is "Owning the Net"? (p. 2)

) RESEARCH & TECHNOLOGY

(U) OWNING THE NET

escription

S//SI//REL TO USA, FVEY) Continue research of quantum communications technology to support the development of novel Quantum Key Distribution (QKD) attacks and assess the security of new QKD system designs.

TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

EVIDEN

Une priorité de la NSA dès 2011

Source : E. Snowden dans le Washington Post, dévoilé en 2014

- **Penetrating hard target (QC) 80m$**
- **Owning the net (QKD)**

Contrôle à l’exportation

Armes de guerres (CIEEMG, SGDSN)
Moyens de cryptologie (double contrôle ANSSI et SBDU)
Biens et technologies à double usage (CIBDU, DGE/SBDU) qui regroupe plusieurs traités

- Catégorie 0 Matières, installations et équipements nucléaires
- Catégorie 1 Matières spéciales et équipements apparentés
- Catégorie 2 Traitement des matériaux
- Catégorie 3 Électronique
- Catégorie 4 Calculateurs
- Catégorie 5 Télécommunications et "sécurité de l’information"
- Catégorie 6 Capteurs et lasers
- Catégorie 7 Navigation et aéro-électronique
- Catégorie 8 Marine
- Catégorie 9 Aérospatiale et propulsion

➔ *« calculateurs numériques" ayant une "performance de crête corrigée" (PCC) dépassant 0,75 Teraflops pondérés (TP); »*
➔ *« conçus ou modifiés pour utiliser la "cryptographie quantique »*

Arrêté du 2 février 2024 relatif aux exportations vers les pays tiers de biens et technologies associés à l'ordinateur quantique et à ses technologies habilitantes et d'équipements de conception, développement, production, test et inspection de composants électroniques avancés

➔ *« 1. Ordinateurs quantiques supportant 34 ou plus, mais moins de 100, ‘qubits physiques’ ‘entièrement contrôlés’, ‘connectés’ et ‘fonctionnels’, et ayant une ‘erreur C-NOT’ inférieure ou égale à 10^{-4} »*

Souveraineté financière

2021 : 2,2 milliards € d'investissement privé dans les startups de calcul quantique dans le monde

- ➔ **1,7 milliards € aux Etats-Unis (Rigetti, PsiQuantum et IonQ)**
- ➔ **50 millions € en France (Quandela, C12, Pasqal)**

Nécessité de plans quantiques nationaux pour pallier le manque de capacités d'investissement privé en Europe

- ➔ **plan quantique France 2021 : 1,8 milliards sur 4 ans (1 md Etat, 550 m privé, 250 m EU)**