Cryptographie post-quantique

Stéphane Bortzmeyer
stephane+pses@bortzmeyer.org

Pas Sage en Seine, 29 juin 2018

L'orateur

- Ne connait rien en crypto.
- Et pas grand'chose en quantique.
- Ce qui en fait la personne idéale pour se mettre à la place de la majorité des gens qui vont devoir décider s'ils jettent RSA, ECDSA et EdDSA...

Crypto classique

- Toute la sécurité de l'Internet en dépend.
- Si on casse RSA, on n'a plus de sécurité.
- RSA repose sur le problème de la décomposition en facteurs premiers.
- ECDSA et EdDSA (les courbes elliptiques) reposent sur le problème du logarithme discret.
- Ne pas oublier les algorithmes de chiffrement symétriques (AES) et ceux de condensation (SHA).

Quantique

- Branche de la physique qui traite de phénomènes en général limités aux trucs très petits.
- D'habitude, peu de manifestation dans le monde « macroscopique » (mais il y en a, comme le laser).
- Des prédictions hautement non-intuitives **mais très bien vérifiées**.
- « Si vous croyez comprendre la quantique, c'est que vous ne comprenez pas la quantique. » (Richard Feynman) « *If quantum physics sounds challenging to you, you are not alone.* » (documentation du calculateur quantique d'IBM).

La quantique amusante

- Le qubit, équivalent quantique du bit.
- 0, 1 ou peut-être un peu des deux (superposition), tant qu'on ne mesure pas (chat de Schrödinger). Si vous voyez 0 écrit |0>, c'est un qubit. a$|0\rangle$+b$|1\rangle$ est une superposition.
- Impossibilité du clonage, vous ne pouvez pas copier des qubits sans les mesurer (et donc les réduire à des bits classiques).
- Intrication, dans certains cas, des qubits ont leur sort lié : la mesure de l'un réduit l'autre à un bit. « Individuellement aléatoires, mais corrélés entre eux »
- Décohérence, quand ça cesse d'être quantique.
- Fort potentiel de pipeautage, commercial ou New Age pseudo-écolo.

Ordinateur quantique

- Un ordinateur qui utilise des concepts purement quantiques.
- Première (?) idée par Richard Feynman en 1982.
- Ce n'est pas un ordinateur général.
- Le concept est un tel succès que certaines boîtes annoncent avoir des ordinateurs quantiques. . . qui n'en sont pas.

Calculateur théorique

- Ada Lovelace avait écrit des tas de programmes. . . pour un ordinateur qui n'existait pas (et qui n'a jamais été construit).
- En 1994, Shor met au point le premier programme utile pour un ordinateur quantique. . . qui n'existait pas.
- L'algorithme de Shor permet de décomposer un nombre en ses facteurs premiers (et donc de casser RSA).
- Depuis, des ordinateurs quantiques expérimentaux ont été réalisés.
- Le plus grand nombre décomposé par cet algorithme est 21.
- Difficile de prévoir le rythme des progrès (pas de loi de Moore).

Petit détour : la QKD

- Distribution quantique de clés. (Branche de la cryptographie quantique.)
- Si un espion copie la clé, cela se voit (contrairement au numérique classique). Conséquence de l'intrication. « Sécurité physique et non plus algorithmique ».
- Permet de distribuer des clés de manière sûre.
- **Absolument rien à voir avec le calcul quantique**, et donc avec la crypto post-quantique.
- Le soi-disant « Internet quantique » chinois, ou le pipeau de Schrödinger. « *allows perfectly secure, unhackable communication* » (Équivalent européen *Quantum Internet Alliance*.)
- Pourquoi la QKD n'a guère d'intérêt : pas d'authentification et, de toute façon, elle ne sécurise que le maillon déjà le plus

Prévoir le futur

C'est bien joli, mais comment construire un qubit ? Et N qubits ?
« *The question of when a large-scale quantum computer will be built is a complicated one* » (NIST)

- Si on a un ordinateur quantique sérieux, on peut casser RSA, ECDSA et EdDSA (*cryptapocalypse* ?) et ébranler certains algorithmes symétriques.
- Les ordinateurs quantiques existants et connus publiquement sont des prototypes.La décohérence est un problème sérieux.
- Quand est-ce que Dell nous vendra un ordinateur quantique ?
- Rappel : on est plus proche de la recherche fondamentale que de l'ingéniérie. Difficile de prévoir les progrès. « *Breakthrough might be imminent, but then again it might not.* »

Écoutons ceux qui savent

- En août 2015, la NSA publiait un communiqué (retiré de leur site Web depuis) disant en substance :
- « Si vous n'avez pas encore migré de RSA vers les courbes elliptiques, ce n'est pas la peine : les ordinateurs quantiques arriveront avant. »
- Curieusement, certaines personnes ne font pas confiance à la NSA.
- « *A Riddle Wrapped in an Enigma* » disait un des nombreux articles d'exégèse.

L'algorithme de Shor en action

Comme je n'ai pas d'ordinateur quantique, j'ai utilisé un émulateur

```
% ./shor 42
N = 42, 31 qubits required
Random seed: 41
Measured 1024 (0.500000), fractional approximation is 1/2.
Possible period is 2.
Unable to determine factors, try again.

% ./shor 42
N = 42, 31 qubits required
Random seed: 37
Measured 682 (0.333008), fractional approximation is 345/1036.
Possible period is 1036.
42 = 2 * 21
```


Émulateurs de calculateurs quantiques

Pour jouer en attendant.

- libquantum `http://www.libquantum.de/`. Inclus un exemple Grover et Shor (ci-dessus).
- Quintuple `https://www.github.com/corbett/QuantumComputing`
- Vous vous souvenez des fermes de compilation de SourceForge ? Vous pouvez accéder à un vrai ordinateur quantique `https://quantumexperience.ng.bluemix.net/qx/experience` (cinq qubits).
- Déjà beaucoup de questions sur StackOverflow.

Qu'est-ce qu'un algorithme post-quantique

- Un algorithme de chiffrement pour lequel on ne connait pas **actuellement** d'algorithme quantique de cassage.
- Ce n'est pas une propriété intrinsèque : on découvrira peut-être un tel algo plus tard.
- Exemples : McEliece (théorie des codes), réseaux euclidiens (*lattice*).
- Souvent des clés très longues.
- Peu testés au feu.

État du logiciel post-quantique

- Rien dans OpenSSL ou GnuTLS (version git).
- codecrypt `http://e-x-a.org/codecrypt`
- libbqcrypto `https://libpqcrypto.org/`
- libPQP `https://github.com/grocid/libPQP` (expérimental)
- liboqs `https://openquantumsafe.org/`
- Et bien d'autres (par exemple les soumissions au NIST pour leur projet post-quantique).

Exemple Codecrypt

McEliece trapdoor running on quasi-dyadic Goppa codes

```
% ccr -g help
available algorithms: ([S]ig., [E]nc., sym. [C]ipher, [H]ash)
...
 E MCEQCMDPC128FO-CUBE256-ARCFOUR
 E MCEQCMDPC128FO-CUBE256-CHACHA20
 E MCEQCMDPC128FO-CUBE256-XSYND
...

% ccr -g    MCEQCMDPC128FO-CUBE256-CHACHA20 --name pq1
Seeding done, generating the key...

% ccr -k
pubkey MCEQCMDPC128FO-CUBE256-CHACHA20 @4d8b428e05... pq1

% ccr -e --name pq1 --in /etc/motd --out motd.encrypted

% ccr -d --in motd.encrypted
```


Normes

- Rien de normalisé à l'heure actuelle. C'est une sérieuse limite pour les réseaux (pensez à TLS).
- NIST et autres : rien de concret pour l'instant, mais un projet est en cours. Pas mal de soumissions dont Classic McEliece, NewHope. . .. Pas de résultat attendu avant des années.
- IETF : commencez par le brouillon qui pose le problème, `draft-hoffman-c2pq`. Certains trichent en appelant post-quantiques des mécanismes à clé secrète pré-partagée `draft-ietf-ipsecme-qr-ikev2`. Également le groupe de recherche QIRG sur la QKD.

Conclusion

- La situation reste confuse et peu prédictible.
- On ne sait pas tout (la NSA a un ordinateur quantique installé par les extra-terrestres dans la zone 51).
- Cela ressemble aux problèmes où on invoque le principe de précaution : décider en situation d'incertitude.
- Mon pari : il n'y a pas urgence à se précipiter vers la crypto post-quantique.
- Il faut poursuivre les recherches (implémenter, tester et normaliser des algorithmes post-quantiques).
- Il y a une probabilité non nulle de m'être totalement trompé ici.