Cryptographie post-quantique : le défi technologique français

L'enjeu de la révolution quantique est de taille. La bonne nouvelle, c'est que la France peut compter sur le savoir-faire de ses industriels pour s'y préparer dès aujourd'hui.

 # PAIEMENT
 # CONNECTIVITÉ
 # IDENTITÉ

POSTÉ LE 21.12.21

Le Président de la République l'a annoncé : la révolution quantique est en marche.[1] En faisant le choix d'investir près de deux milliards d'euros dans le domaine quantique pour accompagner la transformation de l'industrie française, le gouvernement a démontré son ambition de voir la France occuper une place sur le podium mondial des technologies quantiques. Cet acte fondateur est une nouvelle satisfaisante, car derrière ce défi mondial, la question de la souveraineté numérique est en jeu. La bonne nouvelle, c'est que la France peut compter sur le savoir-faire de ses industriels pour préparer dès aujourd'hui la réalité de demain.

Marc BERTIN, CTO SET chez IDEMIA

Ceci n'est pas une fiction.

Mots de passe, codes de cartes bancaires, signatures numériques, dossiers médicaux, matériel militaire, véhicule autonome, ou encore communications électroniques… d'une manière générale, une faille de sécurité peut avoir de graves conséquences, non seulement pour les particuliers, mais aussi et surtout pour les entreprises et l'État qui traitent, chaque jour, des données sensibles.

La révolution quantique, dont l'existence a été révélée il y a plus de vingt ans, vient décupler ce risque. Imaginez un ordinateur permettant de déjouer les algorithmes en exploitant les systèmes quantiques pour trouver rapidement les clés secrètes, habituellement incassables. Il ne s'agit pas de fiction, mais d'une projection inévitable dans les années à venir, et à laquelle les industriels de la sécurité se préparent ardument. L'ordinateur quantique viendra en effet perturber tout ce qui est aujourd'hui presque infaillible, notamment notre cryptographie actuelle. **L'enjeu est de taille car la cryptographie est au cœur de toute solution de sécurité** : authentifier les données, les dispositifs et les utilisateurs, sécuriser les communications et les transactions (numériques), garantir le respect de la vie privée… toutes

ces choses dont nous avons cruellement besoin dans le monde numérique dans lequel nous vivons.

Si l'expression « cryptographie post quantique » a des allures d'expression futuriste, elle désigne pourtant une réalité bien concrète, derrière laquelle se joue la souveraineté nationale et le rayonnement de la France à travers le monde.

La nécessité d'installer la France sur le podium mondial

Les différents acteurs, au premier rang desquels les industriels, doivent anticiper cette transition vers de nouveaux protocoles de chiffrement dont les enjeux sont éminemment stratégiques. Il en va de la souveraineté technologique de la France. Le rapport rendu par la députée Paula Forteza[2] à ce sujet pointe du doigt l'enjeu principal : « *face à la rapidité et à l'incertitude de ces évolutions, seuls les pays qui auront osé prendre des risques trouveront une place dans ce nouveau tournant technologique et pourront donc garantir leur souveraineté. Il y a urgence à agir* ».

Et demain se prépare dès aujourd'hui. Même si les ordinateurs quantiques ne sont pas dimensionnés pour menacer la cryptographie dans l'immédiat ou dans un avenir proche, **la cryptographie post-quantique doit être conçue et construite dès à présent**. La conception d'algorithmes sécurisés, leur normalisation, leur développement, leur déploiement à grande échelle peuvent prendre des années. Très concrètement, la technique consiste à intégrer dans une carte à puce traditionnelle, un algorithme post-quantique qui crée une signature infalsifiable et donc une authentification renforcée. Pour atteindre des performances acceptables pour ce type d'usage (paiement sans contact, passage au frontière…), **la communauté de la sécurité doit travailler sur des optimisations à tous les niveaux** : le logiciel (software) bien sûr, mais aussi le matériel (hardware).

S'agissant plus particulièrement des applications gouvernementales ou militaires, qui intéressent directement les États, les données cryptées d'aujourd'hui doivent pouvoir rester confidentielles pendant plusieurs décennies. Par conséquent, **pour être en sécurité dans un avenir lointain**, ces données sensibles doivent être protégées par des techniques de sécurité post-quantique dès que possible.

À l'heure où la crise sanitaire a mis en évidence la nécessité plus globale de **réindustrialiser la France**, il est important de rappeler qu'il existe aujourd'hui sur le territoire national des industriels disposant d'un **savoir-faire technologique d'excellence**, pleinement mobilisés et capables de répondre aux grands défis de demain.

Le discours de Saclay est l'acte fondateur d'une véritable ambition étatique pour laquelle les industriels français seront au rendez-vous.

La version originale en français de cet article a été publiée dans latribune.fr le 12 mai 2021.

---

[1] Stratégie nationale sur les technologies quantiques, discours du 21 janvier 2021 à Saclay
[2] Quantique : le virage technologique que la France ne ratera pas

---