IDEMIA

France's hi-tech challenge: post-quantum cryptography

Quantum computers will be fast, powerful, and easily able to crack today's impenetrable encryption technology. There is a lot at stake.

PAYMENT
CONNECTIVITY
IDENTITY

POSTED ON 12.21.21



President Emmanuel Macron has said, "The quantum revolution is underway".[1] By committing to invest nearly two billion euros into quantum to boost transformation in French manufacturing, the Government has shown it wants France to lead the way in the world of quantum tech. This first call to action is a step in the right direction because this global challenge involves France's digital sovereignty. The good news is that France can count on the expertise of its manufacturers to be ready for tomorrow's world.

Marc BERTIN, CTO SET at IDEMIA

This is not science fiction

Passwords, payment card PINs, digital signatures, medical records, military equipment, driverless cars, emails and more—generally a security flaw can lead to very serious consequences not only for individuals but also, and most of all, for companies and governments that handle confidential data every day.

The quantum revolution, which first came to people's attention more than 20 years ago, will soon magnify that risk. Imagine a computer that can run quantum system-based algorithms so as to instantly find out secret codes that under current technology would be watertight. This is not science fiction, it's an inevitable reality in the next few years, and security firms are working diligently to ensure their defences are in order. Yes, **the quantum computer is on the way to penetrating everything that now is practically impenetrable**; including today's encryption. There is a lot at stake because encryption underpins all electronic security including data authentication, software and users, communication and digital transaction security, data privacy security and so on. In fact, everything that we rely on in the modern digital world.

While the phrase "post-quantum cryptography" smacks of futuristic science fiction, it is today's reality—and it will

protect France's sovereignty and national secrets around the world.

France needs to lead the world

Led by manufacturers, the various parties involved must anticipate the coming switch towards new encryption protocols. This is clearly a national strategic issue given that France's tech sovereignty is at stake. Member of Parliament Paula Forteza[2]'s report on this issue explains: "*Given that these developments are happening so fast and causing such uncertainty, only countries that dare to take risks will emerge unscathed from this latest tech upheaval and so will be able to safeguard their sovereignty. We've got to take action now*".

Forteza's dire warning is not hyperbole; even if quantum computers do not have the scale or power to threaten encryption right now or in the near future, **development of post-quantum cryptography must start now**. Writing, setting standards for, developing and rolling out secured algorithms may take years. Specifically, the technique consists of adding in a post-quantum algorithm, which creates a fraud-proof signature, to a standard microchip card, thereby beefing up authentication. In order to attain acceptable performance for purposes like contactless payments, crossing borders and so on, the security community must work on **improving both software and hardware**.

With specific regard to government or military applications, in which governments have a vital interest, today's encrypted **data must stay confidential for decades**. To be on the safe side when considering a far-flung future, such highly confidential data should be protected by post-quantum security techniques as soon as possible.

At a time when the pandemic has highlighted the general need to bring back manufacturing to France, it is important not to forget that **France has manufacturing companies backed by world-class hi-tech know-how** that are ready and able to take up tomorrow's great challenges.

Macron's Saclay speech was the first call to action for a goal that French manufacturers will not fail to heed.

This article was originally published in the French language in latribune.fr on May, 12, 2021

---

[1] Quantum technologies national strategy; January 21, 2021; Saclay, France
[2] Quantum: the tech turning point that France won't miss
