*** 北米連携センター定期報告***

2014 年 9 月 3 日

●一般向け量子暗号技術の開発目指すロスアラモス国立研究所

【Nextgov, 2014/09/03】
エネルギー省のロスアラモス国立研究所は、アライド・マインズ子会社のホワイトウッド・エンクリプション・システムズと一般向け量子暗号技術の開発で協力。ロスアラモス創設以来、最大となる 21 件の知的財産をホワイトウッドにライセンス提供する。
現在使われている暗号技術は、スーパーコンピュータの進化で解読可能になり、その目的のために量子コンピュータ開発を進めている国もあるといわれている。
量子コンピュータは、従来のコンピュータよりも高速な演算ができるが、量子暗号技術も同様に暗号鍵を高速に生成可能。暗号化されたメッセージが傍受された場合、その形跡が明確に残り、情報は破壊されることになる。
ロスアラモスは、一般市民や企業の使用を想定した暗号ツールの開発を目指しており、暗号化のための機器は USB ドライブほどの大きさで、安価に販売されるようになるだろうとしている。
しかし、量子暗号の実用にあたっては、通信者間を結ぶ専用の光ケーブルが必要という点が大きな課題となる。

（参考）本件報道資料
Energy Races to Build Quantum Encryption – for Citizens
By Aliya Sternstein

The Energy Department's Los Alamos National Laboratory and a Boston startup are joining efforts in a marathon to build uncrackable encryption for citizens who are increasingly concerned about snoops and government eavesdropping.

Supercomputers are expected to be able to break today's encryption formulas, as they grow exponentially faster. Foreign adversaries are believed to be at work on such “quantum computers” for that very purpose. Meanwhile, technology outfits -- and some federal agencies -- are countering the threat with "quantum encryption."

The deal between Los Alamos and Allied Minds subsidiary Whitewood Encryption Systems marks the lab's largest transfer of intellectual property.

"The company has licensed more than 21 separate pieces of intellectual property, making it the largest single licensing of its type" in Los Alamos' history, Energy spokesman James E. Rickman said in an email. The exact dollar amounts are proprietary, but will amount to a certain percentage of profits made by the Boston-based company.

Their tools have been under development for 20 years, according to officials at Los Alamos, a national security lab.

Quantum computers will be able to unravel algorithms at lightning speed, but quantum encryption can create cryptographic "keys" with lightning speed, backers say. The technique relies on physics, using unique particles of light -- called photons -- to physically move secret messages between two individuals. Today's encryption uses random-number generation based on mathematical formulas to make and break codes.

Any attempt to intercept messages secured with quantum encryption is detected because eavesdropping alters the properties of the key.

"If nobody tries to cut that letter open, it stays intact. If anybody tries to cut the envelope, what quantum physics tells us is, they'll actually change the information, so they'll destroy that information," said Matthew Green, a cryptography researcher at the Johns Hopkins Information Security Institute.

Los Alamos' designs are tailored to the needs of ordinary Americans and businesses. Lab officials claim the equipment can be as small as a computer thumb drive and could be produced very inexpensively to sell on the shelves of a consumer electronics store.

"If implemented on a wide scale," the technology "could ensure truly secure commerce, banking, communications and data transfer," officials said in a statement.

One drawback to quantum encryption is the amount and type of infrastructure

involved. It requires running dedicated fiber optic cables between correspondents, potentially across continents and oceans. "The problem is that it's a real hassle to use," Green said.

This is not the government's first foray into quantum encryption. Energy awarded Qubitekk $3 million to create tamper-proof coding to fend off power grid cyberattacks, the San Diego firm announced last week. Under that arrangement, Qubitekk will be collaborating with several other U.S. national laboratories and Pacific Gas & Electric.

Meanwhile, other parts of the government are working on the opposite side of the crypto equation. There is speculation that the National Security Agency is making steady progress on “a cryptologically useful quantum computer" for code breaking, according to The Washington Post.

Most estimates on how close any organization is to truly achieving such a machine are at least a decade out.

As for Energy's code-making endeavor, Green said, "If the government's helping make things more secure, then that's good for everybody."

Source:
http://www.nextgov.com/cybersecurity/2014/09/energy-races-build-quantum-encryption-citizens/93038/

以　上