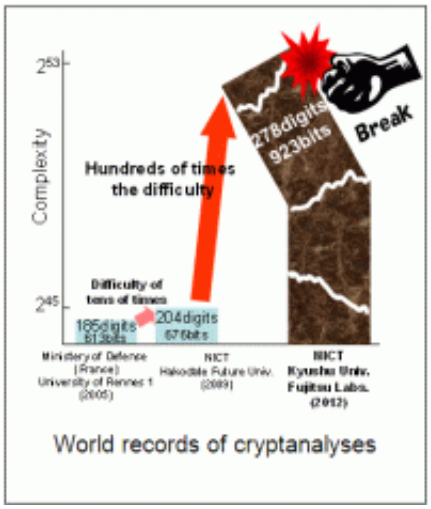
Japanese researchers achieve world record cryptanalysis of next-generation cryptography

June 18 2012



Fujitsu Laboratories, National Institute of Information and Communications Technology and Kyushu University jointly broke a world cryptography record with the successful cryptanalysis of a 278-digit (923-bit)-long pairing-based cryptography, which is now becoming the next generation cryptography standard.

Until now, cryptanalysis of pairing-based cryptography of this length was thought impossible as it was estimated to take several hundred thousand years to break. Indeed, despite numerous efforts to use and spread this

cryptography at the development stage, it wasn't until this new way of approaching the problem was applied that it was proven that pairing-based cryptography of this length was fragile and could actually be broken in 148.2 days. This result is used as the basis of selecting secure encryption technology, and is proving useful in the standardization of next-generation cryptography in electronic government systems in Japan and international standardization organizations.

Many cryptography systems are used from the viewpoint of information security on a modern information system. Recently, much attention has been paid to the new "pairing-based" cryptography system, which is being standardized as a next-generation encryption system. The technology is attractive as it can be used for various useful applications such as "Identity-based encryption", "keyword searchable encryption", and "functional encryption", which were impossible using previous public key cryptography.

As cryptanalytic techniques and computers become more advanced, cryptanalytic speed accelerates, and conversely, cryptographic security decreases. Therefore, it is important to evaluate how long the cryptographic technology can be securely used. On the other hand, pairing-based cryptography has not advanced, so it was premature to evaluate its security against a new attack method.

As for a security evaluation of cryptographies, we succeeded with the cryptanalysis of the pairing-based cryptography of 278 digits (923 bits) by using 21 personal computers (252 cores) in 148.2 days. The cryptanalysis is the equivalent to spoofing the authority of the information system administrator. As a result, for the first time in the world we proved that the cryptography of the parameter was vulnerable and could be broken in a realistic amount of time.

This was an extremely challenging problem as it required several

hundred times computational power compared with the previous world record of 204 digits (676 bits). We were able to overcome this problem by making good use of various new technologies, that is, a technique optimizing parameter setting that uses computer algebra, a two dimensional search algorithm extended from the linear search, and by using our efficient programing techniques to calculate a solution of an equation from a huge number of data, as well as the parallel programming technology that maximizes computer power.

This result is not just a new world record of cryptanalysis, it also means the acquisition of valuable data that forms a technical foundation on which to estimate selection of secure encryption technology or the appropriate timing to exchange a key length. We will continue to move forward on research that pushes the boundary of the secure use of cryptography.

Source: Fujitsu