［Press Release］

June 18, 2012
Kyushu University
National Institute of Information and Communications Technology
Fujitsu Laboratories LTD.

Kyushu University, NICT and Fujitsu Laboratories Achieve World Record Cryptanalysis of Next-Generation Cryptography

Establishes security of pairing-based cryptography and contributes to its standardization as the next-generation cryptography

Kyushu University[*1], The National Institute of Information and Communications Technology (NICT)[*2], and Fujitsu Laboratories Limited[*3] jointly broke a world cryptography record with the successful cryptanalysis of a 278-digit (923-bit)-long pairing-based cryptography,[*4] which is now becoming the next generation cryptography standard.

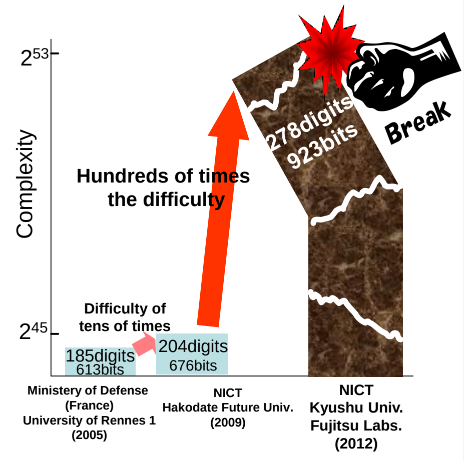
Until now, cryptanalysis of pairing-based cryptography of this length was thought impossible as it was estimated to take several hundred thousand years to break. Indeed, despite numerous efforts to use and spread this cryptography at the development stage, it wasn't until this new way of approaching 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.

Background

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[*5]", "keyword searchable encryption[*6]", and "functional encryption[*7]", which were impossible using previous public key cryptography [*8].

Technological Issues

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.



World records of cryptanalyses

New Achievements

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.

Future Prospects

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.

Glossary and Notes

*1 Kyushu University, President: Dr. Setsuo Arikawa

*2 National Institute of Information and Communications Technology, President: Dr. Hideo Miyahara

*3 Fujitsu Laboratories Limited, President: Tatsuo Tomita (Headquarters: Kawasaki, Kanagawa Prefecture)

*4 Pairing-based cryptography: A next-generation cryptography (proposed in 2001) based on a map called pairing, which offers many useful functionalities that could not be achieved by previous public-key cryptography. The security of pairing-based cryptography is based on the intractability of discrete logarithm problem (DLP). DLP is a problem to compute *d* such that $a = g^d$ for given *g* and *a*

*5 Identity-based encryption：A type of public-key encryption in which the public key of a user is some unique information about the identity of the user (e.g. a user's email address). It does not require authentication of public keys unlike former public-key cryptosystems.

*6 Keyword searchable encryption：An encryption scheme which enables searching keywords on encrypted data.

*7 Functional encryption：An encryption scheme where an author of a document can specify access control info in a predicate logic using attributes and embed it into an encrypted document.

*8 Public-key cryptography：A cryptographic system requiring two separate keys, one to encrypt the plaintext, and one to decrypt the ciphertext. One of these keys is public and the other is kept private. Introduced by Diffie and Hellman in 1976. RSA and Elliptic curve cryptography (ECC) are typical examples.

Technical Contacts

Kyushu University
Institute of Mathematics for Industry
Professor Tsuyoshi Takagi
Tel： 092-802-4456　 E-mail： takagi@imi.kyushu-u.ac.jp

Fujitsu Laboratories Limited
Software Systems Laboratories Secure Computing Laboratory,
Takeshi Shimoyama, Ph.D.
Tel： 044-754-2681　E-mail： dlp-query@ml.labs.fujitsu.com

National Institute of Information and Communications Technology
Network Security Research Institute, Security Fundamentals Laboratory,
Naoyuki Shinohara, Ph.D.
Tel： 042-327-5343　E-mail： dlp-query@ml.nict.go.jp

Press Contacts

Kyushu University, Public Relations Office
Tel：092-642-2106　E-mail：koho@jimu.kyushu-u.ac.jp

Fujitsu Limited
Public and Investor Relations Division
Inquiries: https://www-s.fujitsu.com/global/news/contacts/inquiries/index.html

National Institute of Information and Communications Technology,　Public Relations Department
Tel：042-327-6923　E-mail：publicity@nict.go.jp

About Kyushu University

Kyushu University is a national, comprehensive and one of the top research universities in Japan. The university is located in Fukuoka, the largest and most active business center in Kyushu Island. Founded in 1911, Kyushu University has established itself as a leader in education and research not only in Japan but throughout the world. Celebrated its centennial in 2011, today we have 11 undergraduate schools, 18 graduate schools and more than 50 research institutes and centers. And the university consists of roughly 2,300 academic staff, 2,700 non-academic staff and 19,000 students on 6 campuses.
For more information, please visit www.kyushu-u.ac.jp

About Fujitsu
Fujitsu is the leading Japanese information and communication technology (ICT) company offering a full range of technology products, solutions and services. Over 170,000 Fujitsu people support customers in more than 100 countries. We use our experience and the power of ICT to shape the future of society with our customers. Fujitsu Limited (TSE:6702) reported consolidated revenues of 4.5 trillion yen (US$54 billion) for the fiscal year ended March 31, 2012. For more information, please see http://www.fujitsu.com.

About Fujitsu Laboratories
Founded in 1968 as a wholly owned subsidiary of Fujitsu Limited, Fujitsu Laboratories Limited is one of the premier research centers in the world. With a global network of laboratories in Japan, China, the United States and Europe, the organization conducts a wide range of basic and applied research in the areas of Next-generation Services, Computer Servers, Networks, Electronic Devices and Advanced Materials. For more information, please see: http://jp.fujitsu.com/labs/en.

About NICT

The National Institute of Information and Communications Technology (NICT) is the independent administrative agency of ICT in Japan. NICT promotes the full spectrum of research and development from basic to applied research with an integrated perspective, and thus promotes the advancement of Japan as an intellectual nation that leads the international community. Moreover, NICT forms close ties with the academic and business communities in Japan as well as with research institutes overseas and returns its R&D findings to society in a broad range of fields. For more information, please visit www.nict.go.jp/en/index/html

Reference Materials

Implication of our joint research:

Modern information systems have numerous applications using confidential information, such as for internet shopping, internet banking, and electronic submissions to public agencies. In order to securely use these services, we need to ensure their information security using cryptographic technology.

From the recent research and development in cryptography, “pairing-based encryption” can accomplish many novel and flexible services such as “ID-based encryption”, “searchable encryption”, and “functional encryption”, which have not been achieved by conventional public-key cryptography. On the other hand, pairing-based encryption does not have a long history in cryptography, and its security has not yet been well studied. In order to securely use this cryptography we have to correctly estimate the secure term of its usage by considering the advances of computational speed. The security of paring-based cryptography is based on the difficulty of solving the “discrete logarithm problem”. It is required to accurately evaluate the computation resources and time of breaking the discrete logarithm problem from the viewpoints of both theory and practices, and then we are eventually able to know the precise security of pairing-based cryptography.

Our joint project has succeeded in breaking pairing-based cryptography of 278 digits (923 bits), which had been considered impossible to break. There are already several implementations in practical systems. From our cryptanalysis, we have determined that a key length of 278 digits has become vulnerable and thus longer key lengths have become necessary. However it is possible to accurately estimate the required computational resources and time from our cryptanalysis of pairing-based cryptography, namely we have at last obtained important cryptanalysis data for selecting secure key-lengths used in the future. We will continue to investigate key-lengths by considering the advances of computational speed.

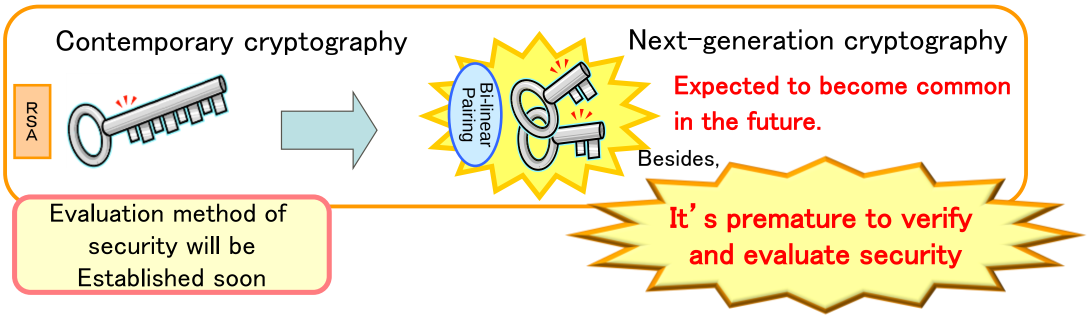

Contemporary cryptography
RSA
Next−generation cryptography
Bi-linear Pairing
Expected to become common in the future.
Besides,
It’s premature to verify and evaluate security
Evaluation method of security will be Established soon

Fig. 1 The security comparison of conventional and new cryptographic technology

The details of our experiment:

In our experiment of breaking the pairing-based cryptography, we used the “function field sieve” which is currently the fastest algorithm for solving the discrete logarithm problem. We have succeeded the cryptanalysis by improving the fastest algorithm and optimizing it in the computational architectures used in our experiment. The appealing points of our development are in the following.

1. Optimizing the initial parameters by mathematical formulas

We proposed several mathematical formulas with which we can estimate the required computational powers of our experiment in advance, and then we have selected the initial parameter of the smallest computational power from the theoretically possible ones.

2. Data searching technology using two-dimensional space

Our cryptanalysis has to search the seed of the solution from the huge data base. The previous world-top record used the “line sieve” for this data search, but we extended it to the two-dimensional space called “lattice sieve”, and then its speed was accelerated dozens of times by using our own modification.

3. Computing the solution of equations of massive numerical data

We applied the “Lanczos method” for computing the solution of huge systems of equations obtained from massive numerical data. We improved the computational speed several times by optimizing the program for our computational environments.

4. Parallel programming for maximal usage of our computational power

Our programming code achieved the maximal potential of our computational resources by using the SIMD operation equipped in the recent general-purpose computers. This optimization made our cryptanalysis several time faster.

We have succeeded in breaking the pairing-based cryptography for 148.2 days in total using the computers of 21 servers (252 CPU cores) at Kyushu University, NICT and Fujitsu Laboratories. This computational cost is equivalent to the total time of computing Intel Xeon processor of 1 CPU core for 102 years.

Comparison with the previous results:

Many research groups have attempted to solve the discrete logarithms problem of large scales. The figure below presents our new world-top record and the previously two world-top records by “Ministry of Defense in France and Rennes Institute of Mathematics” and “NICT and Future University Hakodate”. The vertical line is the estimated time of solving the target problems. Our new record of 278 digits (923 bits) is significantly larger than the previous record of 204 digits (676 bits), namely our target is about several hundred times harder.

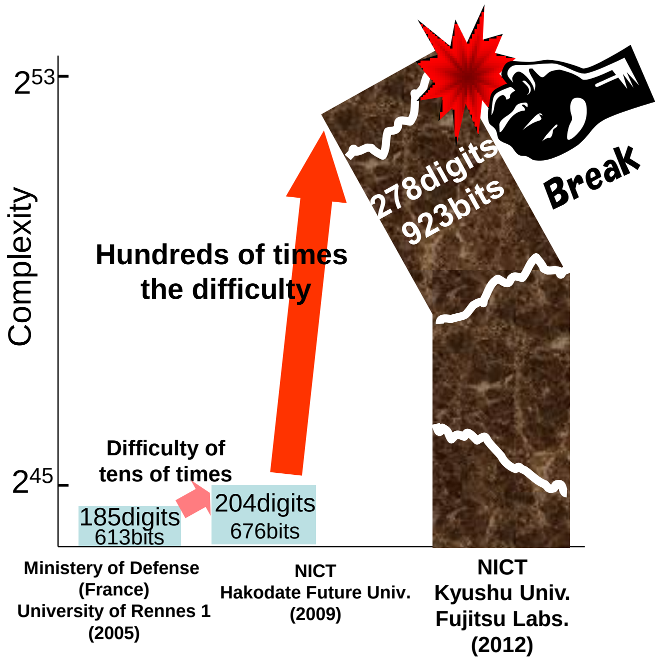


Fig 2. World records of cryptanalyses

Target problem and the solution:

We set the target problem in the following. We first represent finite field $GF(3^{97})$ by $GF(3)[x]/(x^{97}+x^{16}+2)$, and then the discrete logarithm problem over super singular curve $E(GF(3^{97}))\ y^2 = x^3 - x + 1$ is converted that over finite field $GF(3^{582})$ using the η_T pairing. Next let $Int(\pi)$ and $Int(e)$ be the circle constant $\pi = 3.14159...$ and the Napier's constant $e = 2.71828...$, respecitevely. We then select two points $Q_\pi = (Int(\pi)+4, y_\pi)$ and $Q_e = (Int(e)+15, y_e)$ on the elliptic curve as the nearest 3-adic number of $Int(\pi)$ and $Int(e)$, respectively. In this way the target problem can be chosen independently from the biased selection (out of our cotroll for chosing a potentially easy target problem).

By computing the η_T pairing from the above two points, we generate the following discrete logarithm problem:

$$\eta_T(Q_\pi, Q_e)^d = \eta_T(Q_\pi, Q_\pi).$$

On April 24th, 2012 we finally obtained the following solution of this target problem using 21 general-purpose computers of 252 CPU cores after the computation of 148.2 days.

$$d = 1752799584850668137730207306198131424550967300$$

Main roles of the organizations:

The main roles of the organizations are as follows.

1. Kyushu University : Management of project promotion, programming, administration of the computers, execution of the computer experiment

2. NICT : Establishment of a theory of reducing the computing time, optimization of the parameter of the attacking algorithms, preparation of computers

3. Fujitsu Laboratories : Design of algorithms, parallelization of the program, management of the promotion of execution of the computer experiment

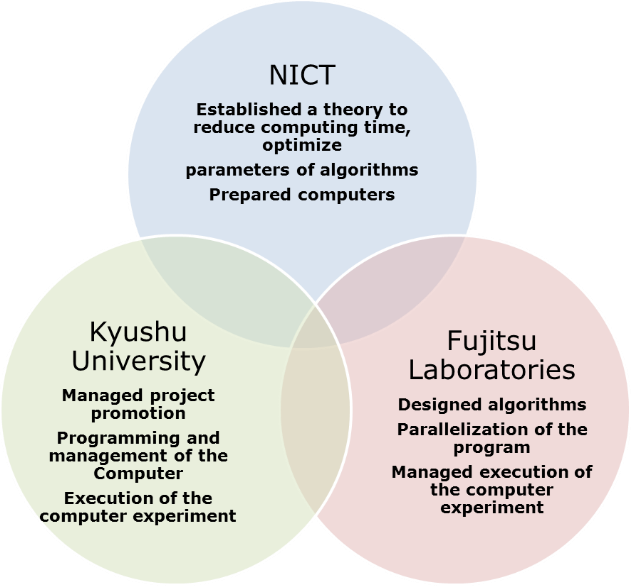

NICT
Established a theory to reduce computing time, optimize
parameters of algorithms
Prepared computers
Kyushu University
Managed project promotion
Programming and management of the Computer
Execution of the computer experiment
Fujitsu Laboratories
Designed algorithms
Parallelization of the program
Managed execution of the computer experiment

Fig 3. The main roles of each organization

(Industry-university-government cooperation)