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.

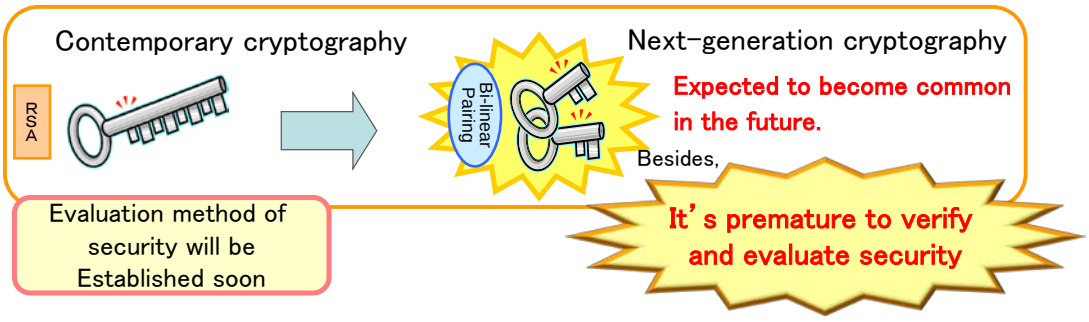

Fig. 1 The security comparison of conventional and new cryptographic technology

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 NICT, Kyushu University 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.

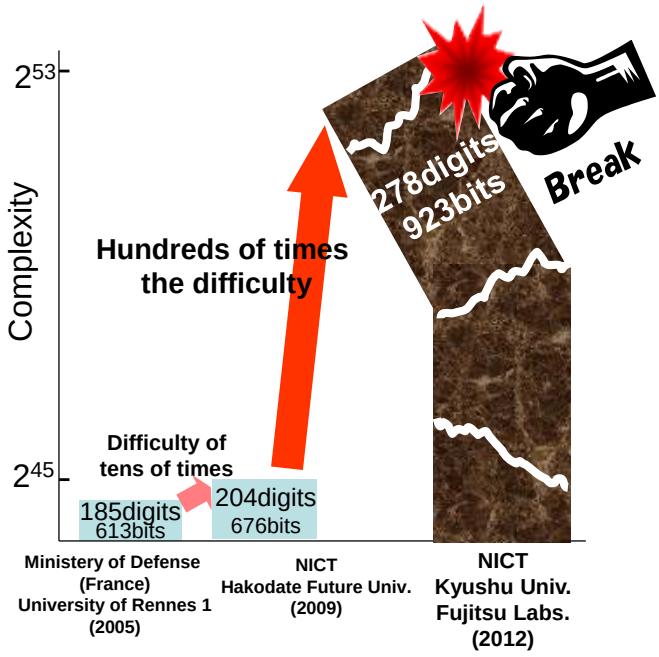

Fig 2. World records of cryptanalyses

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.

$$d=17527995848506681377302073061981314245509673 00$$

Main roles of the organizations:

The main roles of the organizations are as follows.

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

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

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

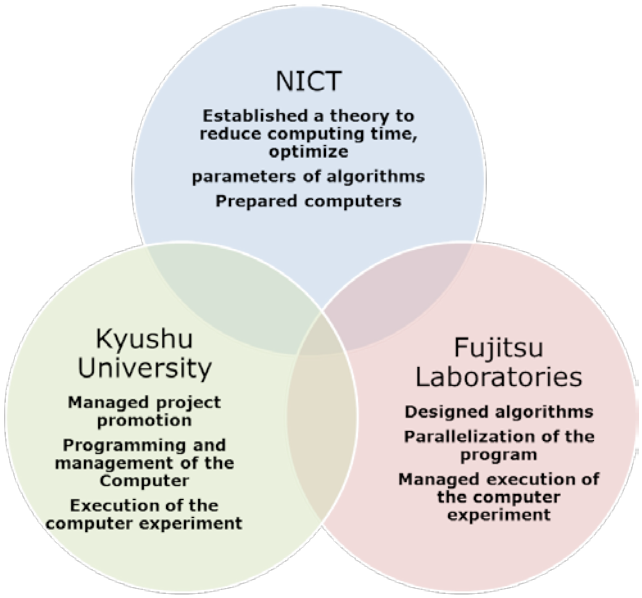

Fig 3. The main roles of each organization
(Industry-university-government cooperation)