NEWS RELEASE

NTT

May 21, 2007

New World Record for "Integer Factorization" Used to Verify Security of Public Key Cryptography

- Encryption-key security verification based on integer factorization of special-type composite number exceeding 1000 bits -

Nippon Telegraph and Telephone Corporation (hereafter NTT, headquarters: Chiyoda-ku, Tokyo, President and CEO: Norio Wada) through collaborative research with the University of Bonn, and the Ecole Polytechnique Fédérale de Lausanne (hereafter EPFL) in a large-number integer-factorization experiment developed as a worldwide challenge and as a means to grasp the security and strength of RSA [*1], a famous scheme in public key cryptography [*2], achieved for the first time in the world integer factorization of a special-type composite number exceeding 1000 bits using the special number field sieve method [*3].

In light of the integer factorization problem [*4] where even for a difference of a small number of bits a significant increase in the number of calculations is required, the current experimental results show the completion of integer factorization for an epoch-making world record of a 1017 bit composite number, which is a substantial increase over the special number field sieve method world record (911 bits).

The experimental results show the factorization for "(2^1039-1)/5080711" a special type composite number. The analysis target is 1017 bits, and we anticipate that the difficulty is equivalent to the general composite number target for the general number field sieve method [*5] of approximately 700 bits.

It is said that difficulty in the integer factorization problem is the foundation of security and in regard to RSA encryption using the current 1024 bit encryption key as the mainstream, the establishing of the new world record carries an extremely important meaning in that the effectiveness of the security and strength can be more precisely estimated.

<Background and Significance of Research>

Accompanying the fundamental spread of the Internet, e-businesses and Internet banks etc. that put networking into practical use providing convenient services have become familiar, and exchanging secret information over the Internet has increased to a large scale.

Encryption technology is a core technology that guarantees information security. Currently, RSA encryption, which is implemented in digital signatures [*6], is a de facto standard, and is incorporated into the encrypted communication protocol SSL [*7] in almost all web browsing software.

The reason for the high evaluation of RSA encryption security is that the difficulty in the integer factorization problem is the foundation of security. In other words, we have

yet to find the key to highly efficient integer factorization, and in order to factor a large number into prime numbers, even using any kind of high performance computer we will still require an enormous amount of time. These ideas form the mathematical basis when performing the calculations.
By estimating to how large a composite number the factorization is possible, based on the current integer factorization technology and calculation power, the potential for cryptanalysis to reach an estimate accurately becomes possible. From these results the period for updating the RSA encryption key length can be appropriately set and in the future we can provide a safe and strong encryption system.

<Contents of Research>

(1) Selecting Analysis Candidates

At the NTT Information Sharing Platform Laboratories [*8] (hereafter NTT Research Laboratories), using the elliptic curve method we tried to confirm whether or not there is a small factor for an analysis target. The results showed that there is less than a 3.4% probability that a factor of less than 65 digits is overlooked and less than a 53.2% probability that a factor of less than 70 digits is overlooked. For this confirmation, the calculation load equivalent to 127.5 years of operation on an AMD Opteron 248 [*9] was required.

(2) Sieve Processing

We employed the sieve program developed at the University of Bonn. The NTT Research Laboratories, EPFL, and the University of Bonn respectively provided 84.1%, 8.3%, and 7.6% of the calculation resources, and the calculation amount equivalent to 95 years of operation on a Pentium D [3 GHz] was required.

(3) Linear Algebra

PC clusters established at the NTT Research Laboratories and EPFL comprising 110 and 36 PCs, respectively, were run in parallel for a little longer than two months for the calculations. The results were 47 non-trivial solutions of the simultaneous equations defined by an approximate 70,000,000 X 70,000,000 large sparse linear matrix.

(4) Square Root

Based on the few hours of operation provided to us on the PC cluster at the University of Bonn, we were able to complete the prime factorization below (factored to 80 digits and 227 digits)

(2^1039-1)/5080711

=

55853666619936291260749204658315944968646527018488637648010052346319853288374753

X

20758181946442382764570481370359469516293970800739520988120838703792729090324679382343143884144834882534053344769112223028158327696525376091410189105241993899334109711624358962065972167481161749004803659735573409253205425523689

<Future Outlook>

The information security industry is anticipated to grow substantially in the twenty-first century. The NTT Research Laboratories will use the fruits of this experiment and, while continuously evaluating the current de facto RSA security, will hereafter be a driving force in a wide range of areas in security research from cipher theory to social influences of security issues.

<Glossary>

*1 RSA
RSA, which comes from the first letter of each developer Rivest, Shamir, and Adleman, is a public key encryption and digital signature scheme that was released in 1978. RSA is currently the most widely used digital signature scheme. Until now, various improvements have been implemented, and several of these improvements are included in digital signature method guidelines and the E-government recommended encryption list. The security of RSA is dependent on the parameter called "modulus," and the larger it is the more secure but the processing capability decreases. Currently, the modulus of 1024 bits is widely used.

*2 Public key cryptography
This concept was proposed by Diffie and Hellman in 1976. The RSA encryption scheme is the most famous application instance of this concept. While the conventional encryption scheme keeps the key used for both encryption and decryption secret, the key for encryption can be disclosed for public key cryptography, and only the decryption key needs to be kept secret.

*3 Special number field sieve
This is an integer factorization algorithm that is effective for composite numbers in a special form such as a^b±1. In the latter half of the 1980s, J.M. Pollard developed a prototype and A.K. Lenstra *et al*. completed the algorithm. Since then, this algorithm has been expanded to the general number field sieve (GNFS) method, which can even factor general form composite numbers.

*4 Integer factorization problem
This problem involves solving composite numbers into the multiplication of prime numbers. While a small composite number can be factored into prime numbers in a short time, the calculations for a large number cannot be completed in a realistic amount of time. However, for a case with a moderately large prime factor, we can use the elliptic curve method to obtain the prime factor. For the factorization of the product of two large prime factors that comprise a composite number used in the RSA method, we utilize the number field sieve method. Currently, the general number field sieve method is the fastest method for the composite numbers used in the RSA method.

*5 General number field sieve (GNFS) method
In the first half of the 1990s, A.K. Lenstra *et al*. completed this integer factorization algorithm. The well-known GNFS is asymptotically the fastest algorithm for a general-type composite number prime factorization algorithm used in RSA. While the run time for the so-called trial division, which employs division by 2, 3, 5, 7, etc., is the exponential time, the GNFS is evaluated to be completed in the subexponential time. However, since the evaluation of the currently known run time is the upper bound of

the average, we must compile calculation experiment data in order to estimate accurately a definitive run time for practical numbers.

*6 Digital signature
This technology is used to implement seals and signature functions. In Japan in 2001, the so-called digital signature was established with legal effectiveness.

*7 SSL (Secure Socket Layer)
This technology enables secure encrypted communications when browsing the web and is incorporated into commonly-used web browsing software. RSA encryption is used as a component technology to implement SSL.

*8 NTT Information Sharing Platform Laboratories
In order for customers to enjoy secure, safe, and convenient service, the NTT Information Sharing Platform Laboratories have been the driving force in research and development from world top class encryption technology, security, FMC, Internet and IP communications, to basic information processing technology such as computer architecture to form the platform for a broadband and ubiquitous era.

*9 Opteron 248
This is a CPU based on the AMD developed 64-bit architecture AMD64. The Opteron 248 has a clock frequency of 2.2 GHz and is a member of the Opteron family. Intel developed EM64T, which is an AMD64 compatible architecture, and CPUs such as the Pentium D and Core2 Duo.

For more information, contact:
NTT Information Sharing Laboratory Group
(Information Sharing Platform Laboratories)
Planning Dept. Public Relations Contact Person
Chizuka, and Yamagata
Tel: 0422-59-3663
E-mail:islg-pr@lab.ntt.co.jp