Security of $N = P^2Q$ in ESIGN

January 28, 2002

Abstract

ESIGN signature scheme uses a particular modulus with a square factor. Each factor has the same number of bits. The goal of this study is to evaluate the security of this kind of modulus. Its security against known algorithms and other attacks which exploit its characteristics or not is studied.

1 Introduction

In this report, we study all potential weaknesses of the ESIGN modulus. The particularity of ESIGN modulus $n = p^2q$ is to have a square factor and to be made of prime factors of same length. In the beginning of this study, we consider the factoring algorithms (more precisely, the two algorithms who are the most efficient against ESIGN modulus). In a second part, we consider close problems induced by the special form of ESIGN modulus. Afterwards, we briefly comment the efficiency of attack based on lattice theory. Before the conclusion and a last remark, we give formulas for the extrapolation of factorization records which can be used to specify the size of ESIGN modulus now and in the future.

2 Factoring Algorithms

The difficulty of factoring number $n = p^2q$ where p and q are prime integers is an element of the security of the ESIGN signature scheme. In the recent years, the limits of the best factorization algorithms have been extended greatly. Now, you can easily factorize 100-decimal digit numbers and it is feasible to factor numbers of 155 decimal digits (512 bits). But, there is no known deterministic or randomized polynomial-time[1] algorithm for finding a factor of a given composite integer n.

There are two classes of algorithms for finding a nontrivial factor f of a composite integer n. The algorithms in which the run time depends mainly of the size of n: Lehman's [Leh74], Continued Fraction [MB75], Multiple Polynomial Quadratic Sieve [Pom84][Sil87], Number Field Sieve [LLMP90][LLMP90],...

[1]The expected running time should be a polynomial in the length of the input, i.e. $O((\log n)^c)$ for some constant c.

And the algorithms in which the run time depends mainly on the size of f: Trial Division, Pollard "rho" [Pol75], Elliptic Curve Method [Len87],...

In this section, we study the best efficient algorithm in each category, i.e. the Number Field Sieve algorithm and the Elliptic Curve Method, and their application to the ESIGN modulus. Let

$$L_n[s,\, c] = e^{(c+o(1))\log^s(n)\log\log^{1-s}(n)} \tag{1}$$

2.1 Number Field Sieve

The number field sieve algorithm [Len94] is the fastest algorithm known. Its efficiency depends on the size of the integer n to factorize. Its expected running time is $L_n[1/3, (64/9)^{1/3}]$. The NFS algorithm does not run faster if a factor of n is small and could not exploit the special form of the ESIGN modulus as far as we know.

At present, the largest number factorized with NFS is the RSA-155 number which is a 155-digit or 512-bit number. This factorization was completed on August 22, 1999, and the amount of computing was about 8400 MIPS years[2][CDL+00]. The size of the modulus in ESIGN is more than 960-bit. Consequently, it is out of the range of NFS algorithm.

2.2 Elliptic Curve Method

The Elliptic Curve Method uses groups defined by pseudo-random elliptic curves over GF(p), where $p > 3$ is the prime factor you hope to find. Since p is not known in advance, computation is performed in the ring Z/nZ of integers modulo n rather than in GF(p). The Elliptic Curve Method could be considered as a generalization of Pollard's $p-1$ algorithm where the group $\mathbb{Z}_p^\star$ is replaced by a random elliptic curve group over $\mathbb{Z}_p$. If the order of group chosen has no large prime factors, i.e. is smooth with respect to some pre-selected bound, the ECM will find a non-trivial factor of n with a high probability. Else the ECM will fail with this particular elliptic curve but another one can be chosen and the process be repeated. As the algorithm tends to find small factors first, the efficiency of the Elliptic Curve Method [Len87] depends on the size of the shortest prime factor of n. If $p < q$ then the expected running time is $L_p[1/2,\, 2^{1/2}]$.

The ECM could be speeded by the addition of a second phase when the first phase described above fails with a particular elliptic curve. This second phase could find a non-trivial factor of n if the cyclic group generated by the group element given when the first phase terminates is reasonably small. There are several implementations of the second phase and some of them could exploit the special form of the ESIGN modulus.

Peralta and Okamoto [PO96] proposed a factoring algorithm based on the elliptic curve method against the number of the form p^2q which is a little bit faster than the original elliptic curve method. Pollard and later Bleichenbacher

[2]One MIPS year is the equivalent of a computation during one full year at a sustained speed of one Million Instruction Per Second.

suggested improvements leading to the algorithm in [Per01]. This algorithm is just several times faster than the traditional ECM. More precisely, the speedup given in [Per01] is slightly larger than $O(\log Q)$ with $n = p^2q$. It is not enough to threaten security of ESIGN with the size of parameters currently recommended.

At this moment, the largest factor found by the elliptic curve factoring method has 55-digit, i.e. 183-bit. It was found by Izumi Miyamoto on 6 October 2001 [Bre]. In the ESIGN modulus, the shortest factor has more than 320-bit. Consequently, the ESIGN modulus is out of range of ECM.

Remarks

- As the efficiency depends on the size of the shortest prime factor of n and n has three factors, the ECM algorithm is much more efficient on the ESIGN modulus than on a RSA modulus of the same size.

- At present, if we consider the two factorization records, the ESIGN modulus must be greater than $55 * 3 = 165$-digit to avoid ECM factorization and greater than 155-digit to avoid NFS factorization. But, due to a best asymptotic running time, only the NFS efficiency will be to consider in the future to define the size of the ESIGN modulus if no new factoring algorithm or new ways to speed up existing ones are discovered (see Section 5).

3 Close problems

3.1 Squarefree part

For an input $n \in \mathbb{N}$, it is an open problem in number theoretic complexity to find, in polynomial time, p and q such that $n = p^2q$ where q is squarefree. This computational problem is labeled C7 in [AM94] and the corresponding open problems are O7a and O7b. In the same paper, Adleman and McCurley note that if the computational problem C13, called quadratic signature[3], could be solved in polynomial time then n could be partially factored assuming the extended Riemann hypothesis. This result requires a signature of length $O(log^2 n)$ to determine q and uses the fact that for any a with $\gcd(a, n) = 1$ we have $\left(\frac{a}{n}\right) = \left(\frac{a}{q}\right)$ where $\left(\ \right)$ denotes the Jacobi symbol. Since the article of Adleman and McCurley [AM94] in 1994, no new results have been published.

3.2 Largest square factor

In [Len94], Lenstra presents a result due to Chistov [Chi89]: *under deterministic polynomial time reductions, the problem of determining the ring of integers for*

[3]For an input $\sigma \in \{-1, 1\}^\star$, output the least prime p such that for all i with $1 \leq i \leq |\sigma|$, $\left(\frac{p_i}{p}\right) = \epsilon_i$, where $|\sigma|$, the length of σ, is the number of symbols in σ, p_i is the i^{th} prime, and ϵ_i is the i^{th} symbol of σ.

a given algebraic number field is equivalent to the problem of finding the largest square factor of a given positive integer [Len94, Theorem 4.4].

4 Lattice attacks

4.1 Factoring $N = p^r q$ for large r

Boneh, Durfee and Howgrave-Graham presented at Crypto'99 [BDH99] an algorithm based on the LLL algorithm for factoring integers of the form $N = p^r q$. Their algorithm is efficient when the size of r is greater than $\log p$. Consequently, this algorithm could not be used to factor the modulus of ESIGN.

4.2 Approximate Integer Common Division

Howgrave-Graham gives a lattice-based solution to the problem of approximate common divisor in [How01]. He claims that from the public information, i.e. $n = p^2 q$ and $s^e = r + tpq \pmod{n}$, he can obtain in polynomial time a non-trivial divisor of n when $r < \frac{1}{2}\sqrt{pq}$. As r is randomly and uniformly chosen in $(\mathbb{Z}/pq\mathbb{Z})\backslash p(Z)$, the probability of success of his attack is $1/2\sqrt{pq}$ (hence is negligible).

5 Factorization: extrapolation

Let D be the number of decimal digits in the largest number factored at a given date Y. By considering historical data and assuming Moore's law[4], Brent gives formulas [Bre00] to extrapolate the factorization records with:

- Elliptic Curve Method with a number D like ESIGN modulus:

$$Y = 9.3\sqrt{\frac{D}{3}} + 1932.3 \tag{2}$$

- Number Field Sieve:

$$Y = 13.24D^{\frac{1}{3}} + 1928.6 \tag{3}$$

An ESIGN modulus of 698-bit, i.e. $D = 210$ would be factorized in $Y = 2010$ with the Elliptic Curve Method and in $Y = 2007$ with the Number Field Sieve. A number of 1024-bit, i.e $D = 309$, would be factorized in $Y = 2026$ with ECM and in $Y = 2018$ with NFS. More pessimistic previsions can be found in the article of Lenstra and Verheul [LV99][LV01].

[4]Moore's law predicts that circuit densities will double every 18 months or so.

6 Miscellaneous

In [MS01], the authors note that if $\gcd(p, q-1) \neq 1$ then one can obtain a non-trivial divisor of n. But this property is never satisfied with ESIGN since p and q have the same size.

7 Conclusion

The specificity of the ESIGN modulus does not seem to be a particular problem for the security of the scheme. Even if the Elliptic Curve Method for factoring could be accelerated by exploiting the special form of the modulus, the best way of factoring an ESIGN modulus is still to use the Number Field Sieve algorithm. But, with the size of ESIGN modulus that is now recommended the NFS is inefficient.

We have presented close problems in the number theoretic complexity which permit to evaluate differently the security of ESIGN modulus. We have also briefly presented recent results based on the lattice theory and their impacts on the security of ESIGN modulus. Finally, the extrapolation formulas given in the last part on the factorization records could be used to extrapolate the size of the ESIGN modulus in the future.

References

[AM94] L.M. Adleman and K.S. McCurley. Open Problems in Number-Theoretic Complexity, II. In *Proceedings of ANTS-1*, volume 877 of *Lecture Notes in Computer Science*, 1994.

[BDH99] D. Boneh, G. Durfee, and N. Howgrave-Graham. Factoring $n = p^r q$ for large r. In *Advances in Cryptology - Crypto'99*, volume 1666 of *Lectures Notes in Computer Science*, pages 326–337, 1999.

[Bre] R. Brent. Large Factors Found By ECM. ftp://ftp.comlab.ox.ac.uk/pub/Documents/techpapers/Richard.Brent/champs.txt.

[Bre00] R. Brent. Recent Progress and Prospects for Integer Factorisation Algorithms. In *COCOON 2000*, volume 1858 of *Lectures Notes in Computer Science*, pages 3–22. Springer Verlag, 2000.

[CDL+00] S. Cavallar, B. Dodson, A. K. Lenstra, W. Lionen, P. L. Montgomery, B. Murphy, H. te Riele, K. Aardal, J. Gilchrist, G. Guillerm, P. Leyland, J. Marchand, F. Morain, A. Muffett, C. Putnam, C. Putnam, and P. Zimmermann. Factorization of a 512-bit RSA Modulus. In *Advances in Cryptology - Eurocrypt 2000*, volume 1807 of *Lectures Notes in Computer Science*, pages 1–18. Springer Verlag, 2000.

[Chi89] A.L. Chistov. The Complexity of Constructing the Ring of Integers of a Global Field. *Dokl. Akad. Nauk SSSR*, 306:1063–1067, 1989. English transl.: Soviet Math. Dokl. **39** (1989), 597–600.

[How01] N. Howgrave-Graham. Approximate Integer Common Divisors. In *CaLC 2001*, volume 2146 of *Lectures Notes in Computer Science*, pages 51–66. Springer Verlag, 2001.

[Leh74] R.S. Lehman. Factoring Large Integers. *Mathematics of Computation*, 28:637–646, 1974.

[Len87] H.W. Lenstra Jr. Factoring Integers with Elliptic Curves. *Annals of Mathematics*, 126:649–673, 1987.

[Len94] H.W. Lenstra Jr. Algorithms in Algebraic Number Theory. *Bulletin of the American Mathematical Society*, 26(2):211–244, 1994.

[LLMP90] A.K. Lenstra, H.W. Lenstra Jr, M.S. Manasse, and J.M. Pollard. The Number Field Sieve. In *Proceeding of 22nd Annual ACM Conference on Theory of Computing*, pages 564–572, May 1990.

[LV99] A. Lenstra and E. Verheul. Selecting Cryptographic Key Sizes. Presented at PKC 2000. Available at http://www.cryptosavvy.com, October 1999.

[LV01] A. Lenstra and E.R. Verheul. Selecting Cryptographic Key Sizes. *Journal of Cryptology*, 14:255–293, 2001.

[MB75] M.A. Morrison and J. Brillhart. A Method of Factorisation and the Factorisation of F_7. *Mathematics of Computation*, 29:183–205, 1975.

[MS01] E. El Mahassni and I. Shparlinski. On Some Uniformity of Distribution Properties of ESIGN. In INRIA, editor, *Proc. Intern. Workshop on Coding and Cryptography*, pages 189–196, Paris, 2001.

[Per01] R. Peralta. Elliptic Curve Factorization Using a "Partially Oblivious" Function, 2001. to appear.

[PO96] R. Peralta and E. Okamoto. Faster Factoring of Integers of a Special Form. *IEICE Transactions on Fundamentals of Electronics*, E79-A(4):489–493, 1996.

[Pol75] J. M. Pollard. A Monte Carlo Method for Factorization. 15(3):331–334, 1975.

[Pom84] C. Pomerance. The Quadratic Sieve Factoring Algorithm. In *Advances in Cryptology - Eurocrypt '84*, volume 209 of *Lectures Notes in Computer Science*, pages 169–182. Springer Verlag, 1984.

[Sil87] R.D. Silverman. The Multiple Polynomial Quadratic Sieve. *Mathematics of Computation*, 48:329–339, 1987.