Self-Evaluation of ESIGN Identification

1 Introduction

This document details security assessment and performance on ESIGN identification scheme.

2 Security of ESIGN Identification

2.1 Secure Identification Scheme

We describe here a definition of a secure identification scheme, following the standard definition by Feige, Fiat, and Shamir [12].

Definition 2.1 *Let (A, B) be an identification protocol between a prover A and a verifier B. Let $\mathcal{G}$ be a key-generator for an identification scheme and let (w, x) be a pair of secret and public keys generated by $\mathcal{G}$. We denote by $(A(w), B)(x)$ an experiment of an identification scheme between A and B with regards to (w, x), where x is inputted to both A and B and w is inputted only to A. An identification scheme, (A, B), is secure if the following conditions hold:*

1. *For any constant c, for sufficiently large k,*

$$\Pr[(A(w), B)(x) = \text{`accept'}] > 1 - 1/k^c.$$

2. *There exists no adversary* Adv *such that, for any constants, c, c', for sufficiently large k,*

$$\Pr[(\mathrm{Adv}, B)(x) = \text{`accept'}] > 1/k^c,$$

after $k^{c'}$-times execution of $(A(w), \mathrm{Adv})(x)$.

Here the probabilities above are taken over the coin tosses of $A, B,$ Adv *and $\mathcal{G}$.*

2.2 Security of ESIGN Identification

We convert ESIGN signature scheme into an identification scheme in a standard way. The following result is then well-known.

Theorem 2.2 *Suppose that there exists a digital signature scheme that is existentially unforgeable against adaptive chosen message attacks. Then there exists a secure identification scheme.*

It leads the next theorem.

Theorem 2.3 *ESIGN identification scheme is secure under the approximate e-th root assumption in the random oracle model.*

2.3 Security of ESIGN signature

The security for a digital signature scheme is modeled as the infeasibility of any adversary in winning the following game [16]: First a key-generation algorithm generates a public-key and a secret-key for the digital signature scheme. The adversary then takes the public-key and have access to the signature oracle to get a signature on a message in the adaptively-chosen manner. The adversary will win the game if she can forge a signature on a message other than one for which she asked for a signature. For more details, the reader is referred to [16].

We compare here in Table 1 the security of ESIGN, RSA based schemes (e.g., PSS or FDH-RSA), and elliptic-curve based schemes (e.g., EC-Schnorr).

Table 1: Comparison of security

Scheme	Security against CMA	Number-theoretical assumption	Random function assumption
ESIGN	Secure	AER	Random
PSS or FDH-RSA	Secure	RSA	Random
EC-Schnorr	Secure	EC Discrete Log.	Random

2.4 Theoretical Result

ESIGN signature scheme can be proven secure in the random oracle model under a non-standard but reasonable assumption. The non-standard assumption is called the approximate e-th root (AER) assumption. AER

Problem is analogous to the RSA problem. The RSA problem is to find x, given n, e, y, such that $x^e = y \pmod{n}$; The AER problem is to find x, given n, e, y, such that a part ($1/3|n|$-most significant bit) of $x^e \bmod n$ equals the corresponding part of y, i.e., $[x^e \bmod n]^{1/3|n|} = [y]^{1/3|n|}$. We describe here statements of the problem and the assumption.

Definition 2.4 (AER Problem) *Let $\mathcal{G}$ be the key-generator of ESIGN. The approximate e-th root problem (AERP) is, for given (n, e, k) and given $(k-1)$-bit random string y, to find $x \in (\mathbb{Z}/n\mathbb{Z})\backslash p\mathbb{Z}$ such that $0||y = [x^e \bmod n]^{pLen}$, where the distribution of (n, e, k) follows that of $\mathcal{G}$ ($|n| = 3k$).*

Definition 2.5 (AER Assumption) *The approximate e-th root problem (AERP) is intractable, if for any non-uniform probabilistic polynomial time algorithm* Adv*, for any constant c, for sufficiently large k,*

$$\Pr[\mathrm{Adv}(k, n, e, y) = x] < 1/k^c,$$

where $0||y = [x^e \bmod n]^k$ The probability is taken over the coin flips of $\mathcal{G}$ and Adv*.*

Here we describe the theoretical result of ESIGN in terms of security.

Theorem 2.6 *ESIGN is existentially unforgeable against adaptive chosen message attacks in the random oracle model under AER assumption.*

Proof is shown in [15].

Remark:

[Factoring $n = p^2q$] Although it is not known whether $n = p^2q$ is easier to factor than $n = pq$, some special algorithms to factor $n = p^2q$ have been studied [21, 22, 23, 2]. However, such techniques are specific to the elliptic curve factoring method (ECM), and the fastest algorithm for factoring both $n = pq$ and $n = p^2q$ is the number field sieve (NFS) method, whose running time depends only on the composite size, $|n|$. (Even these algorithms based on the ECM [21, 22, 23] are just several times faster than the traditional ECM.)

Recently Boneh et al. presented an algorithm for factoring $n = p^rq$ with large r, using the LLL algorithm (lattice reduction) [6]. Their algorithm, however, is only effective for the case where r is large (at least $(\log p)^{1/2}$). If r is constant (or small), the running time of their algorithm is exponential in $|n|$. Hence, as for $n = p^2q$, their algorithm is less efficient than the ECM and NFS methods.

Therefore, currently the size of $n = p^2q$ can be the same as $n = pq$ if n is sufficiently large (e.g., $|n|$ is at least 1024). Actually, according to the evaluation equations in [10], the ECM method for $n = p^2q$ (i.e., the sizes of primes of n are 1/3 of $|n|$) with 1024 bits is less efficient than the NFS method for n (both for $n = p^2q$ and $n = pq$) with 1024 bits.

Remark:

[AER Problem] The square degree version of ESIGN was proposed in 1985 [20], was broken by Brickell and DeLaurentis in the same year [7, 8]. In other words, they showed an efficient algorithm to solve the approximate*square* root problem (AERP with $e = 2$). They also presented an efficient algorithm to solve the cubic version, AERP with $e = 3$.

In the late 1980's, French mathematicians, Girault, Toffin and Vallée, extensively studied various types of the approximate e-th root modulo n problems, by using lattice base reduction [13, 26, 27]. (Brickell and DeLaurentis's attack is a special case of their lattice base reduction attack.) However, they could find no efficient solution to AERP with $e \geq 4$.

Since lattice base reduction is currently the only effective tool to solve such approximate e-th root modulo n problems, we have no way to efficiently solve AERP with $e \geq 4$. (Note that lattice base reduction is a very powerful tool to solve various problems: for example, almost all knapsack public-key cryptosystems were broken by lattice base reduction.)

We have the following conjecture on AERP:

Conjecture: Problem A is expected polynomial-time reducible to problem B.

Problem A**:** Given three positive integers, M and n, and e, solve s that satisfies

$$s^e \equiv M \pmod{n}.$$

Problem B**:** Given four positive integers, M, n, δ, and e, and positive real number ε such that

$$|\delta| = (\frac{e-1}{e} - \varepsilon)|n|,$$

solve s that satisfies

$$M \leq s^e \bmod n < M + \delta.$$

If the following conjecture is true, AERP is as intractable as RSA inversion or Rabin inversion. In particular, when e is even (e.g., 8, 16, ...),

which we recommend, the conjecture implies that AERP is as intractable as factoring n.

Remark:

The original ESIGN, based on the same problem as TSH-ESIGN, has been already adopted by ISO/IEC 14888-3 (digital signatures with appendix). (TSH-ESIGN is a provably secure variant of the original ESIGN.)

Both problems, factoring $n = p^2q$ and approximate e-th root problem (AERP), were explicitly raised by us in 1985. For the last 14 years the both problems have been extensively investigated by many excellent researchers such as Adleman, Bleichenbacher, Brickell, DeLaurentis, Girault, McCurley, Odlyzko, Peralta, Pollard, Shamir, Toffin, Vallée. The authors have also communicated with Lenstra and Buchmann on these problems.

The fact that no efficient algorithms on both problems have been found since they were raised more than 14 years implies that these problems can be considered to be almost as intractable as factoring $n = pq$ and the RSA problem.

3 Performance as Implemented

3.1 Performance in Hardware

- **Process:**
  Cell base.
- **Design environment:**
  Verilog-XL + DesignCompiler
- **Resource:**
  About 25.6KG(@ 2NAND areal equality) + Memory(13312bit)
  Structure: [Random logic+Multiplier×2+Adder] + [Memory(13312bit)]
- **Speed:**
  Evaluation speed in 30MHz clock. (Measured by simulator)

ESIGN	
Proof (Sig.)	9.8 ms
Verification	2.5 ms

(Key length = 1152 bit.)

3.2 Performance in Software

- **Platform:**
  CPU: Pentium III 700MHz
  OS: FreeBSD4.0R
  Memory: 131060K bytes

- **Language:**
  C Language (gcc version 2.8.1)

- **Memory size(Code size):**

ESIGN	
Proof (Sig.)	81859 bytes
Verification	80028 bytes

- **Memory size(Work size):**

ESIGN	
Proof (Sig.)	1112 KB
Verification	1064 KB

- **Process speed:**

ESIGN	
Proof (Sig.)	3.401 ms
Verification	0.404 ms

  (Key length = 1152 bit.)

- **Data size:**

Size of n	1152 bits
Value of e	1024 (10 bits)
$hLen$	160 bits
$gLen$	160 bits
Size of plaintext	128 bits
Size of public key file	329 bytes
Size of secret key file	206 bytes
Size of signature file	290 bytes

- **Optimize level:**
  We use compile option "gcc -O3."

Remark:

In this evaluation, we use the simplest modular inversion algorithm for signature generation. If we use a more sophisticated modular inversion algorithm like Lehmer's method, the signature generation speed will be several times faster than that in this evaluation.

4 Comparison of Computation Amount

In this section, we explain the efficiency of ESIGN Identification. We compare the processing speeds of ESIGN Identification, elliptic curve version of Schnorr Identification scheme, and Fiat-Shamir scheme. For each scheme we estimate the amount of work needed for identification generation and verification by calculating the amount of required modular operations in terms of the number of 1152 bit modular multiplications.

Here, we estimate the performance based on standard techniques such as the (extended) binary method for modular exponentiation and the Chinese Remainder Theorem.

We assume that the modulus n for ESIGN and Fiat-Shamir schemes are 1152 bits, and the modulus for EC-Schnorr scheme is 160 bits. We assume public exponent $e = 2^5$ for ESIGN. We assume the number of moves between the prover and the verifier is 30 for Fiat-Shamir scheme.

The next table shows the evaluation.

Table 2: Comparison of computation amount

Schemes	*Proof (Sig.) (M(1152))*	*Verification (M(1152))*	*# of Moves*
ESIGN	9	5	2
EC-Schnorr	41	48	3
Fiat-Shamir	45	45	30

Here, $M(b)$ ($I(b)$) denotes the amount of work for one b-bit modular multiplication (inversion). We assume $M(b_1) = M(b_2)(b_1/b_2)^2$, $I(b_1) = I(b_2)(b_1/b_2)^2$, and $I(b)/M(b) \approx 4$.

References

[1] Abdalla, M., Bellare, M. and Rogaway, P.: DHES: An Encryption Scheme Based on the Diffie-Hellman Problem, Submission to IEEE P1363a (1998, August).

[2] Adleman, L.M. and McCurley, K.S.: Open Problems in Number Theoretic Complexity,II (open problems: C7, O7a and O7b), Proc. of ANTS-I, LNCS 877, Springer-Verlag, pp.291-322 (1995).

[3] Bellare, M. and Rogaway, P.: Random Oracles are Practical: A Paradigm for Designing Efficient Protocols, Proc. of the First ACM Conference on Computer and Communications Security, pp.62–73 (1993).

[4] Bellare, M. and Rogaway, P. : Optimal Asymmetric Encryption, Proc. of Eurocrypt'94, LNCS 950, Springer-Verlag pp.92-111 (1995).

[5] Bellare, M. and Rogaway, P.: The Exact Security of Digital Signatures – How to Sign with RSA and Rabin, Proc. of Eurocrypt'96, LNCS 1070, Springer-Verlag, pp.399-416 (1996).

[6] Boneh, D., Durfee, G. and Howgrave-Graham, N.: Factoring $N = p^r q$ for Large r, Proc. of Crypto'99, LNCS 1666, Springer-Verlag, pp.326-337 (1999)

[7] Brickell, E. and DeLaurentis, J.: An Attack on a Signature Scheme Proposed by Okamoto and Shiraishi, Proc. of Crypto'85, LNCS 218, Springer-Verlag, pp.28-32 (1986)

[8] Brickell, E. and Odlyzko: Cryptanalysis: A Survey of Recent Results, Chap.10, Contemporary Cryptology, Simmons (Ed.), IEEE Press, pp.501–540 (1991).

[9] Canetti, R., Goldreich, O. and Halevi, S.: The Random Oracle Methodology, Revisited, Proc. of STOC, ACM Press, pp.209–218 (1998).

[10] Cryptography Using Compaq MultiPrime Technology in a Parallel Processing Environment, Enterprise Security Solutions, Electronic Commerce Technical Brief, Compaq Computer Corporation, http://www6.compaq.com/solutions/security/ (2000)

[11] Damgård, I., Landrock, P., and Pomerance, C., "Average Case Error Estimates for the Strong Probable Prime Test", Mathematics of Computation 61(1993), pp.177–194.

[12] Feige, U., Fiat, A. and Shamir, A.: Zero-Knowledge Proofs of Identity, Journal of Cryptology, 1, 2, pp.77-94 (1988)

[13] Girault, M., Toffin, P. and Vallée, B.: Computation of Approximate L-th Roots Modulo n and Application to Cryptography, Proc. of Crypto'88, LNCS 403, Springer-Verlag, pp.100-117 (1990)

[14] IEEE P1363 Draft (D9), http://grouper.ieee.org/groups/1363/P1363/draft.html (1999).

[15] Fujisaki, E. and Okamoto, T.: Security of Efficient Digital Signature Scheme TSH-ESIGN, manuscript (1998 November).

[16] S. Goldwasser, S. Micali and R. Rivest, "A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks," SIAM J. on Computing, 17, pp.281–308, 1988.

[17] Menezes, A., van Oorschot, P., and Vanstone, S., "Handbook of Applied Cryptography", CRC Press, Boca Raton, Florida 1996.

[18] Okamoto, T.: A Fast Signature Scheme Based on Congruential Polynomial Operations, IEEE Trans. on Inform. Theory, IT-36, 1, pp.47-53 (1990).

[19] Okamoto, T., Fujisaki, E. and Morita, H.: TSH-ESIGN: Efficient Digital Signature Scheme Using Trisection Size Hash, submission to P1363a (1998).

[20] Okamoto, T. and Shiraishi, A.: A Fast Signature Scheme Based on Quadratic Inequalities, Proc. of the ACM Symposium on Security and Privacy, ACM Press (1985).

[21] Peralta, R.: Bleichenbacher's improvement for factoring numbers of the form $N = PQ^2$ (private communication) (1997).

[22] Peralta, R. and Okamoto, E.: Faster Factoring of Integers of a Special Form, IEICE Trans. Fundamentals, E79-A, 4, pp.489-493 (1996).

[23] Pollard, J.L.: Manuscript (1997).

[24] Silverman, R.D.,: A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths, Bulletin number13, RSA Laboratories, April 2000.

[25] FIPS 180-1 "Secure Hash Standard", Federal Information Processing Standards Publication 180-1, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, April 17 1995.

[26] Vallée, B., Girault, M. and Toffin, P.: How to Break Okamoto's Cryptosystem by Reducing Lattice Bases, Proc. of Eurocrypt'88, LNCS 330, Springer-Verlag, pp.281-291 (1988)

[27] Vallée, B., Girault, M. and Toffin, P.: How to Guess L-th Roots Modulo n by Reducing Lattice Bases, Proc. of Conference of ISSAC-88 and AAECC-6, (1988)