Weak Composite Diffie-Hellman*

Kooshiar Azimian[1], Javad Mohajeri[2], and Mahmoud Salmasizadeh[3]
(Corresponding author: Kooshiar Azimian)
Electronic Research Centre, Sharif University of Technology[1,2,3]
Department of Computer Engineering, Sharif University of Technology[1]
P. O. Box 11155-8639, Azadi Avenue, 14588 Tehran, Iran
(Email: azimian@ce.sharif.edu, {mohajeri, salmasi}@sharif.edu)
(Received Dec. 24, 2005; revised and accepted Feb. 20, 2006)

Abstract

In1985, Shmuley proposed a theorem about intractability of Composite Diffie-Hellman. The theorem of Shmuley may be paraphrased as saying that if there exist a probabilistic polynomial time oracle machine which solves the Diffie-Hellman modulo an RSA-number with odd-order bases then there exist a probabilistic algorithm which factors the modulo. In the other hand Shmuely proved the theorem only for odd-order bases and left the even-order case as an open problem. In this paper we show that the theorem is also true for even-order bases. Precisely speaking we prove that even if there exist a probabilistic polynomial time oracle machine which can solve the problem only for even-order bases still a probabilistic algorithm can be constructed which factors the modulo in polynomial time for more than 98% of RSA-numbers.

Keywords: Computational number theory, cryptography foundation, Diffie-Hellman problem, factoring, public key cryptography

1 Introduction

The first public key cryptosystem was proposed by Diffie and Hellman in 1976 [9]. After that, plenty of public-key cryptosystems have been proposed. The mostly used public-key encryption scheme throughout the world is RSA that invented by Ronald Rivest, Adi Shamir and Leonard Adleman in 1977. After that, many cryptographers tried to combine these two cryptosystems to obtain more security.

The main idea of Composite Diffie-Hellman was first proposed by Shmuley and McCurley [8, 10]. Shmuley proved that breaking Composite Diffie-Hellman with odd-order base is at least as hard as factoring. In 1988, K. S. McCurley proposed a new cryptosystem based on the idea of Shmuley and proved it is provably secure based on intractability of factoring [8]. After that in 1999 Eli Biham, Dan Boneh and Omer Reingold proved that breaking Generalize Diffie-Hellman is also at least as hard as factoring [2]. As will be discussed in more detail in Section 3, both Shmuley and also Biham, Boneh and Reingold only proved that breaking Composite Diffie-Hellman with odd-order base is implied by factoring not breaking Composite Diffie-Hellman in general case.

Paper plan: In Section 2 we list definitions representing the various types of problems we deal with in this paper. In Section 3 we consider the theorem of Shmuley and that of Biham, Boneh and Reingold. After that, we propose our main theorem and prove it comes true modulo special RSA-numbers in Section 4. In Section 5, we will prove that special RSA-numbers introduced in Section 4 have a density more than 98%.

2 Preliminary Definitions

In this section we state definitions used in other sections. In the remainder of this paper, we use the following notations:

- $p|'x$ denotes x is not divisible by p.
- $p\|x$ denotes x is divisible by p but not by p^2.
- $gcd(x, y)$ denotes the greatest common divisor of x and y.
- $lcm[x, y]$ denotes the least common multiple of x and y.
- $ord_N(x)$ denotes the smallest positive integer d such that $x^d = 1(\mathrm{mod}N)$.
- λ denotes the Carmichael Function (also called the least universal exponent function) [4]. For any integer N, $\lambda(N)$ is defined as the smallest integer such that $x^{\lambda(N)} \equiv 1(\mathrm{mod}N)$ for all x relatively prime to N. Note that according to [5], Section 4 for any RSA-number $N = pq$, $\lambda(N) \equiv lcm[p-1, q-1]$.

*The first version in the Electronic Colloquium on Computational Complexity (ECCC) (047): (2005), and the second version in ePrint Archive (eprint.iacr.org) Report 2005/111, April 2005

- $log(x)$ denotes the logarithm function with base 2.
- ϕ denotes the Euler-totient function.

Definition 1. *(FIG) The Factoring-instance-generator, FIG is a probabilistic polynomial time algorithm such that on input 1^n its output, $N = P \cdot Q$ is distributed over $2n-$ bit integers, where P and Qq are two n-bit primes (Such N is known as a RSA-number).*

A natural way to define FIG is to let $FIG(1^n)$ be uniformly distributed over $2n-$ bit RSA-numbers.

Definition 2. *(The function DH) Let N be any possible output of $FIG(1^n)$, let g be any element in Z_N^*. Define the function $DH_{N,g}(g^x, g^y)$ with domain $D = (g) \times (g)$ such that,*

$$DH_{N,g}(g^x, g^y) = g^{xy} \bmod N.$$

g is called the base of the function $DH_{N,g}$, and g^x, g^y are called two inputs of the function.

Definition 3. *(ε-solving the DH-Problem) Let A be a probabilistic oracle machine and $\varepsilon = \varepsilon(n)$ a real-valued function.A ε-solves the DH-Problem if for infinitely n's*

$$Pr(A^{DH_{N,g}}(N, g) = DH(1^n)) \geq \varepsilon(n).$$

Definition 4. *(ε-solving the Hard DH-Problem) Let A be a probabilistic oracle machine and $\varepsilon = \varepsilon(n)$ a real-valued function. A ε-solves the Hard DH-Problem if it ε-solves the DH-Problem for odd-order bases ($ord_N(g)$ is an odd number).*

Definition 5. *(ε-solving the Weak DH-Problem) Let A be a probabilistic oracle machine and $\varepsilon = \varepsilon(n)$ a real-valued function. A ε-solves the Weak DH-Problem if it ε-solves the DH-Problem for even-order bases ($ord_N(g)$ is an even number).*

Although the names selected for these two problems - Hard-DH problem and Weak-DH problem- do not make any difference in what we are looking for, here we show intuitively that the hard-DH problem appear to be harder than Weak-DH problem.

Definition 6. *Let N be any possible output of $FIG(1^n)$. Let g and g' be two integers such that $ord_N(g)$ is an odd number, $ord_N(g')$ is an even number and $g = g'^{2^k} \bmod N$. If g^x, g^y are two possible inputs for $DH_{N,g}$, then we have the followings: (all equations are modulo N)*

$$\begin{aligned} DH_{N,g'}(g^x, g^y) &= DH_{N,g'}(g'^{2^k}, g'^{2^k y}) = g'^{2^k xy} \\ &= g^{2^k xy} = (DH_{N,g}(g^x, g^y))^{2^k}. \end{aligned}$$

Therefore $DH_{N,g'}(g^x, g^y)$ can be obtained if we can compute $DH_{N,g}(g^x, g^y)$. We should remember that we don't want to prove that hard DH-problem is not weaker than weak DH-problem. We only want to show that why we select these names.

Definition 7. *(ε-factoring) Let A be a probabilistic Turing-machine and $\varepsilon = \varepsilon(n)$ a real-valued function. A ε-solves the Factoring-Problem if for infinitely n's*

$$Pr[A(P \cdot Q) \in \{P, Q\} \geq \varepsilon(n)$$

where the distribution of $N = P \cdot Q$ is $FIG(1^n)$.

3 Previous Works

In 1985, Shmuley proved that the following theorem [10]:

Theorem 1. ***Shmuley's Theorem**: If there exist a probabilistic polynomial time oracle machine which ε-solves the Hard DH-Problem modulo an RSA-number N. Then we can construct a probabilistic algorithm which can ε-factor the module in polynomial time.*

In 1988, K. S. McCurley proposed a new key distribution system based on the concept of Diffie-Hellman modulo a composite and proved that breaking that scheme is at least as hard as factoring [8, 10]. In 1999 Eli Biham, Dan Bone and Omer Reingold proposed a theorem like that of Shmuley for Generalize Diffie-Hellman (Diffie-Hellman for more than two parties).

The Shmuley's theorem is restricted in the case where base g is an odd-order element in Z_N^*. The theorem of Biham, Boneh and Reingold is also restricted in the case that N is a Blum-integer and g is a quadratic-residue. It is clear that g will be an odd-order element in those circumstances. It is clear that theorem of Biham, Boneh and Reingold for two parties is a special case of that of Shmuley. Consequently, so far, there is no theorem concerning intractability of breaking Composite Diffie-Hellman in the case which g is an even-order element. In the other hand, there is no fact about intractability of Weak DH-Problem.

4 The Reduction

In this section, we state our main theorem. First we propose some elementary lemma used in our proof, and then we propose our main theorem.

Definition 8. *A $2n$-bit RSA-number, $N = PQ$ is said to be a good RSA-number if $p \parallel \lambda(N)$, for some prime $p < log(N)$.*

Lemma 1. *If N is a good RSA-number, p is a prime such that $p \parallel \lambda(N)$ and $x = y^p (\bmod N)$ for some integer y then $ord(x)$ is not divisible by p.*

Lemma 2. *Let $N = PQ$ be a good RSA-number, s be a prime such that $p \parallel \lambda(N)$ and x and y be two integers chosen randomly from Z_N^*, such that $x^s = y^s (\bmod N)$ then $gcd(x - y, N)$ yields a non-trivial factor of N with probability $1 - (1/s)$.*

The generalized form of this lemma was proposed in [6].

Theorem 2. *If there exists a probabilistic polynomial-time oracle machine which ε-solves the Weak DH-Problem modulo a good RSA-number N, there exists a poly-time algorithm which ε-factors the module N.*

Proof. Assume that A is a probabilistic polynomial time oracle machine, which ε-solves the weak DH-problem modulo a good RSA-number N. Let $p < log(N)$ be an odd-prime such that $p \parallel \lambda(N)$. Note that since N is a good RSA-number such prime exists. To propose the main idea of the proof we first suppose that we know such p. Knowing p we can do the following for factoring the module N:

1) Sample δ uniformly at random in Z_N^* and compute $g = \delta^{p^2}$.
2) Select two random integers a and b.
3) Invoke A and let $x = DH_{N,g}(g^{a+1/p}, g^{b+1/p})$. Let $d = ord_N(g)$. Note that by lemma 1 d is not divisible by p so $(1/p \bmod d)$ exist and is unique. Therefore $g^{1/p}$ will exist and will be unique. In addition we know that $(\delta^p)^p = g$ and $\delta^p \in \langle g \rangle$ so $g^{1/p} = \delta^p$. Let $\sigma = \delta^p$.
4) Let $u = \frac{x}{\sigma^{pab+a+b}} (\mathrm{mod} N)$. We know that: $x = g^{(a+1/p)(b+1/p)} (\mathrm{mod} N)$ and $\sigma = g^{1/p}$. So we have $u = g^{1/p^2}$.
5) Compute $gcd(u - \delta, N)$.

It is easy to see that $u^p = \delta^p (\mathrm{mod} p$ so by lemma 4.2 $gcd(u-\delta, p)$ will yield a non-trivial factor of N with probability $1 - 1/p$. In the other hand we can say that since $u \in \langle g \rangle$ but the probability that $\delta \in \langle g \rangle$ is $1/p$ so the probability of success is equal to $1 - 1/p$.

Note that in general case we do not know such p so we must somehow look for it. For achieving that goal, we do the following:

1) Sample v uniformly at random in Z_N^*.
2) Let $p = \{p_1, p_2, \ldots, p_k\}$ be the set of all odd-primes less than $log(N)$.
3) Compute $w = \prod_{1 \le t \le k} {p_t}^2$ and $g = v^w (\mathrm{mod} N)$.
4) For each $1 \le i \le k$ do the following:
   a. Compute $w = \prod_{1 \le t \le k \& t \ne i} {p_t}^2$.
   b. Let $\delta_i = v^{w_i} (\mathrm{mod} N)$ and $\sigma_i = \delta_i^{p_i} (\mathrm{mod} N)$. If $p_i \parallel \lambda(N)$ then d is not divisible by p_i (according to lemma 1), so $(1/p_i) \bmod d$ exist and is unique. Therefore g^{1/p_i} will exist and will be unique. In addition we know that $(\delta_i^{p_i})^{p_i} = g$ and $\delta_i^{p_i} \in \langle g \rangle$ so $g^{1/p_i} = \delta^{p_i}$. Let $\sigma_i = \delta_i^p$.
   c. Select two random integers a and b.
   d. Invoke A and let $x = DH_{N,g}(g^a \sigma_i, g^b \sigma_i)$. It is clear that $x = DH_{N,g}(g^{a+1/p_i}, g^{b+1/p_i})$.
   e. Set $u = \frac{x}{\delta_i^{p_i ab+(a+b)}}$.
   f. Compute $gcd(u - \delta_i, N)$.

As discussed in the first part of the proof if $p_i < log(N)$ is an odd-prime such that $p_i \parallel \lambda(N)$ the algorithm yields a non-trivial factor of N in the $i'th$ iteration of step 4 with probability at least $(1 - 1/p_i) \cdot \varepsilon$. And in the theorem we suppose that such p_i exist so the algorithm ε'-solves the factoring and $\varepsilon' > \varepsilon/2$. Since the number of iterations is less than $log(N)$ and each operation can be done in poly-time so the algorithm can be accomplished in poly-time. □

5 The Distribution of Good RSA-numbers

In Section 4 we proved the hardness of weak composite Diffie-Hellman modulo good RSA-numbers. Now, it is very important for us to determine the density of good RSA-numbers. For doing so in this section we discuss natural density of good RSA-numbers and prove that the density is more than 98%. At the end of this section we propose some practical result about distribution of good RSA-numbers.

Lemma 3. *For any integer k:*
$d = lim_{n \to \infty} \frac{\sharp\{p; pisan-bitprime, k | p-1\}}{\sharp\{p; pisan-bitprime\}} = \frac{1}{\varphi(k)}$.

This lemma can be obtained by Chebotarev theorem [7] as indicated in [3]. The complete proof is in Appendix A.

Corollary 1. *For any prime s:*
$lim_{n \to \infty} \frac{\sharp\{p; pisan-bitprime, s \| p-1\}}{\sharp\{p; pisan-bitprime\}} = \frac{1}{\varphi(s)} - \frac{1}{\varphi(s^2)} = \frac{1}{s}$.

Definition 9. *For any prime s, we define the function ψ as follows:* $\psi(s) = lim_{n \to \infty} \frac{\sharp\{N; Nisa2n-bitRSA-numbr, s \| \lambda(N)\}}{\sharp\{N; Nisa2n-bitRSA-numbr\}}$.

Lemma 4. *Let s be a prime:* $\psi(s) = \frac{1}{s^2} + \frac{2}{s} \times \frac{s-2}{s-1}$.
The proof is in Appendix B.

Following table show some data collected by computing function ψ for some value s.

S	3	5	7	11	13
$\psi(s)$	0.444	0.339	0.258	0.171	0.146

Definition 10. *Define the function $\xi(c)$ as follows:*
$lim_{n \to \infty} \frac{\sharp\{N; Nisa2n-bitRSA-number, s \| \lambda(N) for some primes < c\}}{\sharp\{n; Nisa2n-bitRSA-number\}}$.
It is obvious that the natural density of good RSA-numbers is equal to $lim_{c \to \infty} \xi(c)$.

Lemma 5. *Let p_i be the $i'th$ and p_{i+1} be the $i+1'th$ odd-prime. We have $\xi(p_{i+1}) = \xi(p_i) + (1 - \xi(p_{i+1})) \cdot \psi(p_{i+1})$.*

Following table show some data collected by computing the recursive functions ξ for some values c:

C	3	5	10	100	1000	10000
$\xi(c)$	0.444	0.633	0.728	0.924	0.965	0.980

Corollary 2. *The natural density of good RSA-numbers is more than 98%. Therefore our main theorem comes true for more than 98% of RSA-numbers.*

The following table shows some experimental result collected about distribution of good RSA-numbers. Our experiments confirm that for any integer n, the density of 2n-bit good RSA-numbers is approximately equal to $\xi(n)$. According to experimental result our theorem about intractability of composite Diffie-Hellman with even-order bases comes true for approximately 97% of 1000-bit RSA-numbers.

n	50	500	5000
$2n$	100	1000	10000
Density of good RSA-numbers	94%	97%	99%
The number of RSA-numbers tested in the experiment	1000	1000	100

6 Conclusion and Future Works

In this paper, we showed that not only Composite Diffie-Hellman with odd-order bases yields factoring but also solving that problem for even-order bases will yield factoring. As a future work, the following conjecture can be shown:

Conjecture 1. *If there exist a probabilistic polynomial-time oracle machine which ε-solves the Weak DH-Problem modulo an RSA-number N and there exist a prime p less than $log(N)$, such that $p \mid \lambda(N)$ not necessarily $p \parallel \lambda(N)$ then still there exist a poly-time algorithm which ε-factors the module N.*

A possible line for further research is the study of the theorem in the case where $ord_N(g) = \lambda(N)$. It is clear that both the new theorem and that of Shmuley does not say anything about this. That is if g is a maximum-order element we cannot say anything about intractability of Composite Diffie-Hellman with base g.

References

[1] A. Selberg, "An elementary proof of dirichlet's theorem about primes in an arithmetic progression," *The Annals of Mathematics*, vol. 50, no. 2, pp. 297-304, Apr. 1949.

[2] E. Biham, D. Boneh, and O. Reingold, "Generalized Diffie-Hellman modulo a composite is not weaker than factoring," *Cryptology ePrint Archive: Report 1997/014*, 1997.

[3] H. W. Lenstra, and P. Stevenhangen, "Chebotarev and his density theorem," *Mathematics Intelligencer*, vol. 18, no. 2, pp. 26–37, 1995.

[4] H. Riesel, *Carmichael's Function, Prime Numbers and Computer Methods for Factorization*, 2nd edition, Boston, MA: Birkhäuser, pp. 273-275, 1994.

[5] J. M. Alfred, C. V. O. Paul, and A. V. Scott, *Handbook of Applied Cryptography*, CRC Press, 1996.

[6] M. A. Leonard, and S. M. Kevin, "Open problems in number theoretic complexity, II," in *Proceeding of ANTS-I*, LNCS 877, pp. 291-322, Springer-Verlag, 1995.

[7] N. G. Chebotarev, "Die bestimmung der dichtigkeit einer menge von primzahlen, welche zu einer gegebenen substitutionsklasse gehören," *Mathematische Annalen*, vol. 95, pp. 191-228, 1926.

[8] S. M. Kevin, "A key distribution system equivalent to factoring," *Journal of Cryptology*, vol. 1, pp. 85-105, 1988.

[9] W. Diffie, and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, IT-22, pp. 644-654, 1976.

[10] Z. Shmuely, *Composite Diffie-Hellman Public-Key Generating Systems Are Hard to Break*, Technical Report, no. 356, Computer Science Department, Technion, Israel, 1985.

Appendix A

Lemma 3. *For any integer k:*

$$d = lim_{n\to\infty} \frac{\sharp\{p; pisan - bitprime, k \mid p-1\}}{\sharp\{p; pisan - bitprime\}} = \frac{1}{\varphi(k)}. \quad (1)$$

Proof. We know from [3, 1] that:

$$d = lim_{n\to\infty} \frac{\sharp\{p; pisax - bitprimewherex < n, k \mid p-1\}}{\sharp\{p; pisanx - bitprimewherex < n\}} = \frac{1}{\varphi(k)}. \quad (2)$$

The Equation (2) is a special form of the Chebotarev theorem [7].

Let:

$$\begin{aligned} a_i &= \sharp\{p; pisan - bitprime, k \mid p-1\} \\ b_i &= \sharp\{p; pisan - bitprime\}, \\ A_i &= \sum_{j=1}^{i} a_j, \quad B_i = \sum_{j=1}^{i} b_j. \end{aligned}$$

$r_i = \frac{a_i}{b_i}$, and $s_i = \frac{A_i}{B_i}$.

The Equation (2) means that:

$$lim_{i\to\infty} s_i = \frac{1}{\varphi(k)}. \quad (3)$$

According to the distribution of prime numbers we know that there is a positive real number α such that:

$$\forall i \in N : b_{i+1} > \alpha B_i.$$

According to elementary calculus, from Equations (3) and (4) we can conclude the lemma. □

Appendix B

Lemma 4. *Let S be a prime:* $\psi(s) = \frac{1}{s^2} + \frac{2}{s} \times \frac{s-2}{s-1}$

Proof. Let N_n denotes the set of all 2n-bit RSA-numbers and P_n denotes the set of all n-bit primes. From Definition 9 we have:

$$\begin{aligned}
\psi(s) &= lim_{n\to\infty} \frac{\sharp\{x; x \in N_n, s \parallel \lambda(x)\}}{\sharp\{x; x \in N_n\}} \\
&= lim_{n\to\infty} \frac{\sharp\{x, y \in P_n; W_1 \text{ or } W_2 \text{ or } W_3\}}{\sharp\{x, y \in P_n\}} \\
&= \frac{1}{s^2} + \frac{2}{s} \times \frac{s-2}{s-1} \\
W_1 &= (s \parallel \lambda(x) \& s \parallel \lambda(y)) \\
W_2 &= (s \parallel \lambda(x) \& s \mid' \lambda(x) \& s \mid' \lambda(y)) \\
W_3 &= (s \mid' \lambda(x) \& s \parallel \lambda(y)).
\end{aligned}$$

□

Kooshiar Azimian got his B. Sc. from Sharif University of Technology, Iran in 2005. Currently he is Ph. D. student in Rutgers University. He is interested in various aspects of theoretical computer science and discrete mathematics like computational complexity, cryptography and computational number theory.

Javad Mohajeri received his B. Sc. in Mathematics from Isfahan University, Isfahan, Iran in 1986 and his M. S. in Mathematics from Sharif University of Technology, Tehran, Iran in 1990. He is a lecturer in the electronic research center of Sharif University of Technology. Javad Mohajeri has published 31 papers in refereed journals and conferences. He is a member of founding committee of Iranian Society of Cryptology. He was the chairman of the technical program committee of the 2nd Iranian society of cryptology conference on cryptology communications and computer security. His research interests include design and analysis of cryptographic algorithms, data security, secret sharing schemes and PKI.

Mahmoud Salmasizadeh received the B. S. and M. S. degrees in Electrical Engineering from Sharif University of Technology in Iran, in 1972 and 1989, respectively. He also received the Ph. D. degree in Information Technology from Queensland University of Technology in Australia, in 1997. Currently he is an assistant professor in Electronic Research Center and adjunct assistant professor in Electrical Engineering Department at Sharif University of Technology, Tehran, Iran. His research interests include cryptology and network security. He is the founding member and the head of scientific committee of Iranian Society of Cryptology.