Weak Composite Diffie-Hellman is not Weaker than Factoring

Kooshiar Azimian[1,2]
azimian@ce.sharif.edu

Javad Mohajeri[1]
mohajeri@sharif.edu

Mahmoud Salmasizadeh[1]
salmasi@sharif.edu

[1] Electronic Research Centre, Sharif University of Technology

[2] Department of Computer Engineering, Sharif University of Technology

Abstract

In1985, Shmuley proposed a theorem about intractability of Composite Diffie-Hellman [Sh85]. The Theorem of Shmuley may be paraphrased as saying that if there exist a probabilistic poly-time oracle machine which solves the Diffie-Hellman modulo an RSA-number with odd-order base then there exist a probabilistic algorithm which factors the modulo. In the other hand factorization of the module obtained only if we can solve the Diffie-Hellman with odd-order base. In this paper we show that even if there exist a probabilistic poly-time oracle machine which solves the problem only for even-order base and abstain answering the problem for odd-order bases still a probabilistic algorithm can be constructed which factors the modulo in poly-time for more than 98% of RSA-numbers.

Keywords. Cryptography, Computational Complexity, Public-Key Cryptography, Diffie-Hellman, Factoring

1 Introduction

The first public key cryptosystem was proposed by Diffie and Hellman in 1976 [DH76]. 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 [Sh85, Mc88]. 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 [Mc88]. 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 [BBM99]. 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. In this paper, we show that if we have a probabilistic poly-time oracle machine, which solves the Composite Diffie-Hellman even only for even-order bases, i.e. it abstains answering Composite Diffie-Hellman with odd-order base we still can factor large integers in poly-time.

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 prove our two main theorems in Section 4 and at the end, some ideas for future works will be proposed.

2 Preliminary Definitions

We state some definitions and notations that we use in another section. We use the notations of [BBM99] in this section.

Definition 2.1 (FIG) *The Factoring-instance-generator, FIG is a probabilistic polynomial time algorithm such that on input* 1^n *its output, N = pq is distributed over* $2n-bit$ *integers, where p and q are two n-bit primes (Such N is known as a RSA-number).*

Definition 2.2 (DH) *Let N be any possible output of* $FIG(1^n)$*, let g be any odd-order element in* Z_N^**. Define the function* $DH_{N,g}(g^x, g^y)$ *with domain* $D = \langle g \rangle \times \langle g \rangle$ *such that,*

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

Definition 2.4 (ε-solving the DH-Problem) *Let A be a probabilistic Turing-machine and ε=ε(n) a real-valued function. A ε-solves the DH-Problem if for infinitely N's*

$$\Pr\left(A^{DH_{N,g}}(N,g) = DH(D)\right) \geq \varepsilon(n)$$

Definition 2.4 (ε-solving the Weak DH-Problem) *Let A be a probabilistic Turing-machine and ε=ε(n) a real-valued function. A ε-solves the DH-Problem if it ε-solves the DH-Problem for even-order bases and it abstains solving DH-problem for odd-order base.*

Definition 2.5 (ε-solving the Factoring-Problem) *Let A be a probabilistic Turing-machine and ε=ε(N) a real-valued function. A ε-solves the Factoring-Problem if for infinitely N's*

$$\Pr(A(N,c) \geq \varepsilon(n)$$

3 Previous Work

In 1985, Shmuley proved that the DH-assumption is implied by Factoring-assumption. In 1988, K.S.McCurley proposed a new key distribution system based on

the idea of Shmuley and proved that breaking that scheme is at least as hard as factoring [Mc88]. In 1999 Eli Biham, Dan Bone and Omer Reingold proposed a theorem like that of Shmuley for Generalize Diffie-Hellman in the case that N is a Blum-integer [BBM99].

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 odd-order element in that case. That is theorem of Biham, Boneh and Reingold for two parties is a special case of that of Shmuley. Consequently, so far, there is not any 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 Reduction

In this section, we state the two main theorems. In the remainder of this paper, we use the following notations:

- $p \nmid x$ 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 $x^d = 1 \pmod N$.
- *Cyclic-Order(N)* denotes the order of maximum-size cyclic subgroup of Z_N^*. Note that according to [MOV96, Section 4] for any RSA-number $N=pq$, $Cyclic - Order(N) = lcm[p-1, q-1]$.
- $\log(x)$ denotes the logarithm function with base 2.

Lemma 4.1 *If N is a composite number, p is a prime such that* $p \| Cyclic - Order(N)$ *and* $x = y^p \pmod N$ *for some integer y then* $ord(x)$ *is not divisible by p.*

Lemma 4.2 *Let N be an RSA number, s be any prime factor of* $Cyclic - Order(N)$ *and x and y be two integers chosen randomly from* Z_N^*, *such that* $x^s = y^s \pmod N$ *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 [AM94].

Theorem 4.1 *If there exist a probabilistic polynomial-time oracle machine which* ε*-solves the Weak DH-Problem module N and there exist a prime p less than* $\log(N)$, *such that* $p \| cyclic - order(N)$ *then there exist a poly-time algorithm which* ε*-factors the module N.*

Proof. Assume that A is a probabilistic poly-time oracle machine, which ε-solves the Diffie-Hellman module N only for even-order bases. Let $p < \log(N)$ be an odd-prime such that $p \| Cyclic - Order(N)$ according to the assumptions of the theorem such a prime exist (Note that p is not a prime factor of N). Knowing p one can do the following for factoring the module N:

1. Sample *v* uniformly at random in Z_N^* and compute $g = v^{p^2}$
2. Select two random integers *a* and *b*.
3. Invoke *A* and set $x = DH_N(g, g^{a+1/p}, g^{b+1/p})$. Let $d = ord_N(g)$. Note that by lemma 4.1 d is not divisible by p so $(1/s) \bmod d$ exist and is unique. Therefore $g^{1/p}$ will exist and will be unique. In addition we know that $(v^p)^p = g$ and $v^p \in \langle g \rangle$ so $g^{1/p} = v^p$.
4. Set $u = \frac{x}{v^{pab+a+b}} (\bmod N)$. We have $u = g^{1/p^2}$.
5. Compute $X = \gcd(u - v, N)$

It is easy to see that $u^p = v^p (\bmod p)$ so by lemma 4.2 $\gcd(u - v, p)$ 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 $v \in \langle g \rangle$ 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 find it. For achieving that goal, we do the following:

1. Sample v uniformly at random in Z_N^*
2. Let $P = \{p_1, p_2, ..., p_k\}$ be the set of odd-primes less than $\log(N)$.
3. Compute $w = \prod_{1 \le t \le k} p_t^{\,2}$ and $g = v^w (\bmod N)$
4. For each $1 \le i \le k$ do the following:
   4.1 Compute $w_i = \prod_{1 \le t \le k \ \& \ t \ne i} p_t^{\,2}$
   4.2 Let $\delta_i = v^{w_i} (\bmod N)$ and $\sigma_i = \delta^{p_i} (\bmod N)$. Note that $\delta_i = g^{1/p_i^2} (\bmod N)$. Note that if $d = ord_N(g)$ is divisible by p_i then g^{1/p_i} will exist and as discussed later $g^{1/p_i} = \sigma_i$. If *d* is not divisible by p_i the remainder of sub-procedure (4.3-4.7) is not important for us.
   4.3 Select two random integers *a* and *b*.
   4.4 Invoke *A* and let $x = DH_{N,g}(g^a \sigma, g^b \sigma)$. It is clear that
   $$x = DH_{N,g}(g^{a+1/p_i}, g^{b+1/p_i})$$
   4.5 Set $u = \frac{x}{\delta_i^{\,p_i ab + (a+b)}}$.
   4.6 Compute $X = \gcd(u - \delta, N)$.
   4.7 If $X \ne 1 \ \& \ X \ne N$ return X.

As discussed in the first part of proof if $p_i < \log(N)$ is an odd-prime such that $p_i \,||\, Cyclic - Order(N)$ the algorithm yields a non-trivial factor of *N* in the *i'th* iteration of step 4 with probability at least $(1 - 1/p).\varepsilon$. And in the theorem we suppose that such *p* 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.

Lemma 4.3 Let s and $p > s$ be two primes. We have $\Pr(s \parallel p-1) = 1/s$.

Proof. Note that since p is prime and $p>s$ so $s \in Z_N^*$.

$$\Pr(s \parallel p-1) = \Pr(s \mid p-1) - \Pr(s^2 \mid p-1)$$

$$= \frac{1}{s-1} - \frac{1}{s(s-1)} = \frac{1}{s}$$

Lemma 4.4 *Let s be a prime and* $N = pq$ *be an RSA number* $(N > s^2)$. *We have*

$$\Pr(s \parallel Cyclic-Order(N)) = \frac{1}{s^2} + \frac{2(s-2)}{s(s-1)}$$

Proof. From [MOV96, Sec 4] we know that $Cyclic-Order(N) = lcm[p-1, q-1]$. In the following proof $x \mid' y$ denotes y is not divisible by x.

$$\Pr(s \parallel Cyclic-Order(N))$$

$$= \Pr(s \mid Cyclic-Order(N) \;\&\; s^2 \mid' Cyclic-Order(N))$$

$$= \Pr((s \parallel p-1) \;\&\; (s \parallel q-1)) + \Pr(s \parallel p-1 \;\&\; s \mid' q-1) + \Pr(s \mid' p-1 \;\&\; s \parallel q-1))$$

$$= \frac{1}{s^2} + \frac{1}{s} \times \frac{s-2}{s-1} + \frac{1}{s} \times \frac{s-2}{s-1}$$

After this we show $\Pr(s \parallel Cyclic-Order(N))$ by $\psi(s, N)$, and define the function $\xi(c, N)$ to be the probability of $s \parallel Cyclic-Order(N)$ for some prime $s<c$ where $N > c^2$. Following table show some date collected by computing function ψ for some values s (suppose that N is large sufficient).

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

Lemma 4.5 *Let* p_i *be the i'th and* p_{i+1} *be the i+1'th odd-prime and N be a sufficient large RSA-number*($N>p_{i+1}^2$). *We have*

$$\xi(p_{i+1}, N) = \xi(p_i, N) + (1 - \xi(p_{i+1}, N)) . \psi(p_{i+1})$$

Following table show some date collected by computing the recursive functions ξ for some values c (suppose that N is large sufficient):

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

Theorem 4.2 *If there exist a probabilistic polynomial-time oracle machine which* ε*-solves the Weak DH-Problem modulo a 2n-bit (n>1000) RSA-number N, then*

there exist a poly-time algorithm which ε-factors the module N for at least 98% of such N.

Since $n > 1000$ so $\log(N) > 1000$, Therefore $\xi(c, N) > \xi(1000, N)$. It is easy to see that as n become larger, this probability will become more than *98%.*

5 Conclusion and Future Works

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

Conjecture 5.1 *If there exist a probabilistic polynomial-time oracle machine which ε-solves the Weak DH-Problem module N and there exist a prime p less than* $\log(N)$*, such that $p \mid \varphi(N)$ not necessarily $p \| \varphi(N)$ 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 $ord_N(g) = Cyclic - Order(N)$. 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:

[AM94] Leonard M. Adleman, Kevin S. McCurley: Open problems in number theoretic complexity, II. Proc. of ANTS-I, LNCS 877, Springer-Verlag, pp.291-322 (1995).

[DH76] W. Diffie and M. Hellman: New directions in cryptography, *IEEE Trans. Inf. Theory, IT-22*, 1976, pp.644-654.

[Mc88] Kevin S. McCurley: A key distribution system equivalent to factoring, *Journal of Cryptology*, vol. 1, pp.85-105, 1988.

[MOV96] Alfred J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone: *Handbook of Applied Cryptography*. CRC Press, 1996.

[R79] M. O. Rabin, Digitalized signatures and public-key functions as intractable as factorization: Technical Report, TR-212, MIT Laboratory for Computer Science, 1979.

[SH85] Z. Shmuely: Composite Diffie-Hellman public-key generating systems are hard to break, Technical Report No. 356, Computer Science Department, Technion, Israel , 1985.