Breaking Diffie-Hellman is no Easier than Root Finding

Kooshiar Azimian
Electronic Research Centre, Sharif University of Technology
Azimian@ce.sharif.edu
http://ce.sharif.edu/~azimian

Abstract. In this paper we compare hardness of two well known problems: the Diffie-Hellman problem and the root finding problem. We prove that in any cyclic group computing Diffie-Hellman is not weaker than root finding if certain circumstances are met. As will be discussed in the paper this theorem can affect many branches of public-key cryptography especially on proving the security of cryptographic protocols in hidden-order groups. For examples of such effects we discuss effects of the new theorem on:

1. Proving the security of cryptosystems based on class groups of imaginary quadratic orders (IQ-cryptosystems),
2. Proving the hardness of the Composite Diffie-Hellman problem and security of its related cryptosystems.

In the concept of IQ-cryptography, root finding is supposed to be a hard problem, but there is no significant argument about the hardness of Diffie-Hellman. By applying the new theorem we prove the hardness of computing Diffie-Hellman in class groups of imaginary quadratic orders, and then we construct a new IQ-cryptosystem and prove that it is hard to break.

There are two significant theorems about intractability of the composite Diffie-Hellman. One of them was proved by Shmuely in 1985 and the other, which is stronger, by Azimian, Mohajeri, and Salmasizadeh in 2005. As will be shown in this paper, both of theorems can be driven by applying the new theorem. We also construct a new public-key scheme based on the composite Diffie-Hellman and prove that it is provably secure based on intractability of factoring.

Keywords: Cryptography foundations, computational number theory, public-key cryptography, Diffie-Hellman problem, root finding problem.

1 Introduction

In 1976 Diffie and Hellman proposed the first public key cryptosystem [DH76]. After that several public key schemes were introduced. The security of each of them is based on intractability of a well-known computational problem [MOV96], [G95], [AM95]. The security of commonly used cryptographic schemes is essentially based on a version of one of these three classes of problems:

1. Computing a certain root of a given element of any group, RSA problem or factoring problem. There are many reductions between these three problems. RSA problem is a special case of root finding. We know that root finding and factoring is computationally equivalent if certain circumstances are met [AM95].
2. Computing the well-known problem Diffie-Hellman or Discrete Logarithm in certain groups. These two problems are supposed to be equivalent in many groups [M94], [MW99], moreover it is clear that discrete logarithm problem is no weaker than Diffie-Hellman in any group.
3. Computing Diffie-Hellman or Discrete Logarithm in Elliptic Curve groups [KMOV91]. This class of problems is different from the second class but they appear to have many similar properties [MOV93].

The set of schemes using the first problem includes RSA and Rabin [RSA78], [R79], while the set of schemes using the second problem includes Diffie-Hellman key agreement and ElGammal [DH76], [E85]. There are also many cryptosystems based on the third class of problems.

In many cases the third class can be seen as a version of the second class. Therefore comparing the hardness of the first two problems plays an important role in proving security of public key schemes. In this paper we prove a basic theorem which compares hardness of those these problems.

In section 2 we firstly define these two problems precisely then we prove the main theorem: if certain circumstances are met the second problem is not weaker than the first one in any abelian group. In section 3 we study applications of the new theorem in IQ-cryptography and show how to prove hardness of computing Diffie-Hellman in class groups. As a result we design a new IQ-related public-key scheme in 3.2 and prove the security of it. In section 4 we discuss influences of the new theorem on the concept of the composite Diffie-Hellman. We first show that the both theorems of Shmuely and the author [AMS05], [Sh85] can be driven by applying the new theorem, then propose a new scheme and prove that it is secure based on intractability of factoring problem.

2 The Main Theorem

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

- $p \mid x$ denotes x is not divisible by p.
- $p \mid' x$ denotes x is not divisible by p.
- $p \mid\mid x$ 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.
- $ord(x)$ denotes the order of a given element x in a group G.
- $ord(G)$ denotes the order of a given group G.
- $U(Z/NZ)$ denotes the multiplicative group of units in Z/NZ.
- $\langle g \rangle$ denotes the cyclic subgroup generated by g.
- $ord_N(x)$ denotes the smallest positive integer d such that $x^d = 1 \pmod N$.
- λ denotes the Carmichael Function (also called the least universal exponent function) [R94]. For any integer N, $\lambda(N)$ is defined as the smallest integer such that $x^{\lambda(N)} \equiv 1 \pmod N$ for all x relatively prime

Definition 2.1 (The R function) *Let* G *be an additive abelian group,* $P \in G$ *and* e *be an integer. Define the function* $R_{G,e}(P)$ *such that,*

$$e.R_{G,e}(P) = P$$

Definition 2.2 (The DH function) *Let G be an additive abelian group, P be an element of G. Define the function* $DH_{G,P}(xP, yP)$ *for some integers* x *and* y *, with domain* $D = \langle P \rangle \times \langle P \rangle$ *such that,*

$$DH_{G,P}(xP, yP) = xyP$$

Main theorem. *Let* G *be an additive abelian group,* $Q \in G$ *and* e *be an integer such that* $\gcd(e, ord(Q)) = 1$*, and let* $P = eQ$*. If there exists a polytime oracle machine which computes the function* $DH_{G,P}$ *, then we can construct a polytime algorithm which can compute the* $R_{G,e}(Q)$*.*

Proof. Having such oracle machine, *we do the following* for computing $R_{G,e}(Q)$:

1. Select two integers *a*, *b* randomly.
2. Let $S = DH_{G,P}(aP + Q, bP + Q)$. Since $\gcd(e, ord(Q)) = 1$, $Q \in \langle P \rangle$, thus both $aP + Q$ and $aP + Q$ are admissible inputs for $DH_{G,P}$
3. Set $T = S - (eab + a + b)Q$

We know $Q = (1/e)P$ so $S = (a + 1/e)(b + 1/e)P$. Therefore $eT = Q$.

Roughly speaking we can say that computing the well-known function DH is not weaker than finding root in any abelian group. This is a computational result, but as will be discussed in the later sections, if it is applied to cryptography, it helps us to prove the security of many cryptography schemes.

3 Applications of the New Theorem in IQ-cryptography

As an example of applications of the new theorem in cryptography, we discuss security of IQ-cryptographic schemes [BW88], [H04], [HD05], [SBW94] in this section.
We first study IQ-cryptography and its related problem briefly in 3.1, then in 3.2 we introduce a new IQ-related public-key scheme and we prove security of it.

3.1 Security of IQ-related Schemes

The term IQ cryptography (IQC) refers to cryptography based on class groups of imaginary quadratic orders. IQC has been invented in 1988 [BW88]. Many public-key schemes were developed concerning the concept of IQC [BW88], [SBW94], [BH01], [HM00], [JSW01], [H05]. In the paper we ignore the details of class groups of imaginary quadratic orders and IQ-cryptography. We only discuss hardness of the related problems briefly.

There are four basic computational problems which security of all IQ-cryptosystems relies on them. These computational problems were addressed in HD05 explicitly. Let $Cl(\Delta)$ be a class group of imaginary quadratic orders, we define:

Discrete logarithm problem (IQ-DLP): given $a, b \in Cl(\Delta)$, find the smallest positive integer x, if any, such that $b = a^z$.

Order problem (IQ-OP): given $a \in Cl(\Delta)$, compute the order $|\langle a \rangle|$ of a in $Cl(\Delta)$.

Root problem (IQ-RP): given $a \in Cl(\Delta)$ and an integer $x > 1$, compute b, if any, such that $b^x = a$.

Diffie-Hellman problem (IQ-DHP): given $a, b, g \in Cl(\Delta)$ with $a = g^{\alpha}$ and $b = g^{\beta}$ for some unknown integers α and β, compute $g^{\alpha\beta}$.
We know from JSW01, BH03 and H05 that

$$IQ - RP \leq_P IQ - OP \leq_P IQ - DLP \quad \text{(I)}$$
$$Factoring \leq_P IQ - OP \quad \text{(II)}$$

IQ-DLP, IQ-OP and IQ-RP all appear to be hard problems [H05], [BH03], [JSW01] but we do not know significant fact about hardness of IQ-DHP. We only know the trivial fact $IQ - DHP \leq_P IQ - DLP$ and it is clear that it can not help us to show hardness of IQ-DHP. Beside the security of many IQC-related cryptosystems is based on intractability of IQ-DHP.

The new theorem can ensure the security of those systems in some ways. We introduce a new scheme based on IQ-DHP in 3.2 and prove breaking that system is not weaker than solving IQ-RP.

3.2 A New IQ-related Cryptosystem

We want to design a new scheme based on IQ-DHP and prove breaking that
system is not weaker than solving IQ-RP but if we use pure version of Diffie-Hellman in class groups of imaginary quadratic orders we can not use the main theorem directly. So we use a modified version of the Diffie-Hellman problem to construct this scheme. For generating keys for the new scheme we do the following:

1. Select a small prime *s*.
2. Construct a class group $Cl(\Delta)$ such that $\gcd(s^2, ord(Cl(\Delta))) = s$. We know from Y70, U70, H05 and Y86 that this can be done in polynomial time. We ignore the details of constructing such group in this paper.
3. Select $u \in Cl(\Delta)$ such that $s \mid ord(u)$. From CL84 and C95 we know that we can find such u efficiently and also we know that with high probability $\langle u \rangle$ is a very large subgroup.
4. Set $w = u^s$.

Now the public key is the triple $(Cl(\Delta), w, s)$, while u is private. Two parties *A* and *B* can compute $g = w^s$, select two secret keys *x* and *y* respectively and communicate each other using the secret g^{xy}. It is clear that computing g^{xy} is simple for both *A* and *B*.

Note that $\gcd(ord(u), s^2) = s$, so $\gcd(ord(w), s) = 1$. So according to the main theorem if one can break the scheme (Compute the function $DH_{G,g}$) she can compute $R_{G,s}(w)$.

4 The New Theorem and the Composite Diffie-Hellman

The main idea of the composite Diffie-Hellman was first proposed by Shmuely. This concept has been used in many cryptographic applications. In 1988 Kevin S. McCurley proposed a key distribution system equivalent to factoring based on the Composite Diffie-Hellman. After that in 1997, Boneh, Biham, and Reingold proved that Generalized Diffie-Hellman modulo a composite (Composite Diffie-Hellman for more than two parties) is secure, based on intractability of factoring. Their theorem for two parties is a special case of Shmuely's theorem. A stronger reduction than that of Shmuely was proved in 2005 by the author, Mohajeri and Salmasizadeh.

4.1 Already Proven Theorems

In the following section we briefly show that the Shmuely's theorem can be driven simply from our new theorem. We ignore the details in the following proof.

Shmuely's Theorem: *Let* N *be an RSA-number,* $G = U(Z/NZ)$ *and* g *be an odd-order element in* G. *Then if there exists a probabilistic polytime oracle machine which can compute* $DH_{G,g}$, *we can construct a probabilistic algorithm which can factor the module in polytime* [Sh85].

Proof. Having an algorithm for computing DH we do the following for factoring the module:

1. Select $u \in G$ randomly.
2. Let $v = u^2$ and $g = u^4$.
3. Extract $w = R_{G,2}(v)$. Note that according to Sh85 with high probability v is an odd-order element [See Sh85: corollary 4]. Suppose that v is an odd-order element. Now since $\gcd(2, ord(v)) = 1$, according to the main theorem if one can compute $DH_{G,g}$, she can extract $w = R_{G,2}(v)$
4. Compute $\gcd(w-u, N)$.
5. If $\gcd(w-u, N)$ is equal to 1 or N, return back to the step 1.

It is easy to see that for each odd-order v we can factor the module by computing $\gcd(w-u, N)$ with probability $1/2$. In addition according to Sh85 the probability that v is an odd-order element is high, so the algorithm can extract a non-trivial factor of the module in polynomial time.

In 2005 the author, Mohajeri and Salmasizadeh proved a stronger reduction about intractability of composite Diffie-Hellman [AMS05]. They showed that even if we can compute the DH function only for even-order elements we still can factor the module for more than 98% of RSA-numbers. As will be discussed in the appendix A their theorem also can be derived from our main theorem.

4.2 A New Key Agreement Scheme Equivalent to Factoring

In this section we introduce a new key agreement protocol like that of McCurley [Mc88]. We use the idea which had been used in 3.2 for constructing this scheme. By applying the main theorem we directly prove that our scheme is provably secure based on intractability of factoring problem. For generating keys for the new scheme we do the following:

1. Select a small prime *s*.
2. Select an RSA-number $N = pq$, such that $\gcd(s^2, p-1) = s$ and $\gcd(s, q-1) = 1$.
3. Select a maximum-order element $u \in U(Z/NZ)$. Note that $ord(u) = lcm(p-1, q-1)$ [C95], [MOV96].
4. Compute $g = u^{s^2}$.

Now the public key is the triple (N, u, s). Two parties *A* and *B* can compute $g = u^{s^2} \pmod N$, select two secret keys *x* and *y* respectively and communicate each other using the secret $g^{xy} \pmod N$. It is clear that computing $g^{xy} \pmod N$ is simple for both *A* and *B*. Notice that even if we use (N, g) instead of (N, u, s) as public key still the system works but selecting (N, u, s) as public key help us to prove the security of the scheme more easily.

Note that $\gcd(ord(u), s^2) = s$, so $\gcd(ord(u^s), s) = 1$. Thus according to the main theorem if one can break the scheme she can compute $x = R_{G,s}(u^s)$. It is clear that $x \neq u \pmod N$ because u is a maximum-order element while $x \in \langle g \rangle$ so it can not be a maximum-order. Therefore according to [AM95] she can factor the module *N* with computing $\gcd(x-u, N)$.

5 Conclusion and Future Works

In this paper we proved that the well-known problem Diffie-Hellman is not weaker than root finding problem in certain criteria. In the paper we showed that this theorem could be applied in many branches of cryptography.

In section 3 and 4 we discussed IC-cryptography and Composite Diffie-Hellman and studied applications of the new theorem in them. In section 3, we showed that the well-known problem Diffie-Hellman in class groups of imaginary quadratic orders is hard and proposed a new secure key agreement scheme using it. We proved the security of the scheme by applying our new theorem. In section 4, we showed that all already proven theorems about intractability of the Composite Diffie-Hellman can be driven from our new theorem simply. We also introduced a new key agreement based on Composite Diffie-Hellman in 4.2 and by applying the new theorem; we showed it is provably secure based on intractability of factoring.

As a future work we can extend the scheme proposed in section 3 and increase the efficiency and security of it. The possible ways for efficient key generation for that scheme also can be discussed.

Another possible line for further research is the study of the theorem's applications in the other hidden order groups and their usage in zero knowledge [BCM05] or digital signature protocols. Also applications of the new theorem in Elliptic Curve cryptography can be discussed.

References:

[AM95] 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).

[AMS05] Kooshiar Azimian, Javad Mohajeri and Mahmoud Salmasizadeh, Weak Composite Diffie-Hellman is not weaker than factoring, Electronic Colloquium on Computational Complexity (ECCC) (047): (2005). Also available in *Cryptology ePrint Archive: Report 2005/111*, 2005.

[BCM05] Endre Bangerter, Jan Camenisch, Ueli M. Maurer: Efficient Proofs of Knowledge of Discrete Logarithms and Representations in Groups with Hidden Order. Public Key Cryptography 2005: 154-171

[BBR97] 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.

[BH01] J. Buchmann, S. Hamdy A Survey on IQ Cryptography. In *Public-Key Cryptography and Computational Number Theory*, K. Alster, J. Urbanowicz, and H.C. Williams (Eds.), 2001, pp. 1-15

[BH03] Mark L. Bauer and Safuat Hamdy. On class group computations using the number field sieve, In Chi Sung Laih, editor, Advance in Cryptology – ASIACRYPT 2003, solume 2894 of LNCS, Springer-Verlag, 2003, 311-325

[BW88] Buchmann, J., and Williams, H. C. A key-exchange system based on imaginary quadratic _elds. Journal of Cryptology 1, 3 (1988), 107{118.

[C95] Cohen, H. A Course in Computational Algebraic Number Theory, vol.138 of GTM. Springer-Verlag, 1995.

[CL84] Cohen, H., and Lenstra, Jr., H. W. Heuristics on class groups. In Number Theory, New York 1982, D. V. Chudnovski, G. V. Chudnovski, H. Cohn, and M. B. Nathanson, Eds., vol. 1052 of LNM. Springer-Verlag, 1984, 26-36.

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

[E85] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Trans. Inf. Theory, IT-31*, 1985, pages 469-472.

[G95] Oded Goldreich, Foundations of Cryptography Fragments of a Book, 1995. publicized at http://www.eccc.uni-trier.de/eccc-local/ECCC-Books/eccc-books.html (Electronic Colloquium on Computational Complexity)

[H05] S. Hamdy, P. Dickinson, IQ-Cryptography Primitives and Schemes.

[HM00] S. Hamdy, B. Möller, Security of Cryptosystems Based on Class Groups of Imaginary Quadratic Orders. In *Advances in Cryptology -- ASIACRYPT 2000*, T. Okamoto (Ed.), vol. 1976 in *Lecture Notes of Computer Science*, Springer-Verlag, 2000, pp. 234-247.

[JSW01] Jacobson, Jr., M. J., Scheidler, R., and Williams, H. C. The efficiency and security of a real quadratic field based key exchange protocol. In Proceedings of Public Key Cryptography and Computational Number Theory, 2000 (2001), K. Alster, J. Urbanowicz, and H. C. Williams, Eds., deGruyter, 89-112.

[KMOV91] Kenji Koyama, Ueli M. Maurer, Tatsuaki Okamoto, Scott A. Vanstone: New Public-Key Schemes Based on Elliptic Curves over the Ring Z_n. CRYPTO 1991: 252-266

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

[M94] Ueli M. Maurer: Towards the Equivalence of Breaking the Diffie-Hellman Protocol and Computing Discrete Algorithms CRYPTO 1994: 271-281

[MOV93] Alfred Menezes, Tatsuaki Okamoto, Scott A. Vanstone: Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Transactions on Information Theory 39(5): 1639-1646 (1993)

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

[MW99] Ueli M. Maurer, Stefan Wolf: The Relationship Between Breaking the Diffie-Hellman Protocol and Computing Discrete Logarithms. SIAM J. Comput. 28(5): 1689-1721 (1999)

[R94] Riesel, H. "Carmichael's Function." *Prime Numbers and Computer Methods for Factorization, 2nd ed.* Boston, MA: Birkhäuser, pp. 273-275, 1994.

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

[RSA78] R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, *Communications of the ACM*, 21 (2), 1978, pages 120-126.

[SBW94] R. Scheidler, J. A. Buchmann and H.C. Williams, Implementation of a key exchange protocol using real quadratic fields. *Journal of Cryptology* **7**, 171-199 (1994).

[Sh85] Z. Shmuely: Composite Diffie-Hellman public-key generating systems are hard to break, Technical Report No. 356, Computer Science Department, Technion, Israel , 1985.

[U70] K. Uchida, unramified Galois of quadratic number fields, II, Tohoku Math. J. 22 (1970), 220-224.

[Y70] Y. Yamamoto: On unramified Galois extensions of quadratic number fields, Osaka J. Math., 7 (1970), 57–76.

[Y86] K. Yamamura: On unramified Galois extensions of real quadratic number fields, Osaka J. Math., 23 (1986), 471-478.

Appendix A

In this part we show that the theorem proved by the author, Mohajeri and Salmasizadeh about hardness of the composite Diffie-Hellman can be driven from our main theorem.

Theorem (AMS05) *If there exists a probabilistic polynomial-time oracle machine which* ε *-solves the DH-Problem module* N *for even-order bases and there exist a prime* $p < \log(N)$*, such that* $p \,||\, \lambda(N)$ *then there exist a poly-time algorithm which* ε *-factors the module* N *.*

As discussed in AMS05, such p can be detected effectively, so we suppose that we know a prime p such that $p \,||\, \lambda(N)$. We can do the following for factoring the module N :

1. Sample δ uniformly at random in Z_N^*
2. Compute $g = \delta^{p^2}$, and $\sigma = \delta^p$. Note that $p \,||\, \lambda(N)$*, so* $\gcd(p, ord(\sigma)) = 1$.
3. Invoke A to solve $DH_{N,g}$
4. Extract $w = R_{Z_N^*,p}(\sigma)$. According to the main theorem, since $\gcd(p, ord(\sigma)) = 1$ and $g = \sigma^p$, we can compute $R_{Z_N^*,p}(\sigma)$ by invoking A.
5. Compute $\gcd(w - \delta, N)$, according to [AM95] it yields a nontrivial factor of N with probability more than $1 - (1/p)$.