On The Security of The ElGamal Encryption Scheme and Damgård's Variant

J. Wu and D.R. Stinson*

David R. Cheriton School of Computer Science
University of Waterloo Waterloo, ON, Canada
{j32wu,dstinson}@uwaterloo.ca

Abstract. In this paper, we give security proofs for ElGamal encryption scheme and its variant by Damgård (DEG). For the ElGamal encryption, we show that (1) under the delayed-target discrete log assumption and a variant of the generalized knowledge-of-exponent assumption, ElGamal encryption is one-way under non-adaptive chosen cipher attacks; (2) one-wayness of ElGamal encryption under non-adaptive chosen cipher attacks is equivalent to the hardness of the delayed-target computational Diffie-Hellman problem. For DEG, (1) we give a new proof that DEG is semantically secure against non-adaptive chosen ciphertext attacks under the delayed-target decisional Diffie-Hellman assumption (although the same result has been presented in the literature before, our proof seems simpler); (2) we show that the DHK1 assumption, which was first proposed for DEG security proof, is stronger than necessary. A decisional (thus weaker) version of DHK1 assumption is sufficient for DEG security proof.

Keywords: ElGamal encryption, Damgård's ElGamal, security proof.

1 Introduction

The ElGamal encryption scheme [9] is one of the classic public key encryption schemes. For public key encryption schemes, three attack models are often used to analyze their security: chosen-plaintext attacks (CPA), non-adaptive chosen-ciphertext attacks (CCA1), and adaptive chosen-ciphertext attacks (CCA2). CCA2 is stronger than CCA1, and CCA1 is stronger than CPA (see, e.g., [1]). ElGamal encryption is provably secure under CPA [19], and is insecure under CCA2. It is conjectured to be secure under CCA1, but there has been no formal proof.

In [6], Damgård proposed a variant of ElGamal encryption (DEG) and a new assumption known as Knowledge-of-Exponent Assumption (KEA). In [2], Bellare et al pointed out a flaw in the security argument in [6], proposed a KEA variant named DHK1,[1] and proved that DEG is CCA1 secure based on DHK1. In [12], Gjøsteen proposed a new assumption named *Gap Subgroup Membership Assumption*. Using this assumption and the hash proof system approach, Gjøsteen proved that DEG is IND-CCA1 secure. There have been several hybrid DEG type systems proposed (e.g. [13], [8], [7], the twin ElGamal encryption scheme in [4]) as well as other discrete logarithm based cryptosystems (e.g. [5]) which provide stronger security guarantee or require weaker assumptions than DEG. But DEG may still be the most efficient IND-CCA1 secure public key encryption scheme having a security proof without random oracles.

In this paper, first we investigate the connection between the security of ElGamal encryption and some cryptographic assumptions, including a variant of the generalized knowledge-of-exponent assumption (GKEA), delayed-target discrete log assumption (DTDLA), and delayed-target computational Diffie-Hellman assumption (DTCDHA). DTDLA and DTCDHA are discussed in [14].

* research supported by NSERC discovery grant 203114-06.

[1] The KEA assumption is named DHK0 in [2]. DHK stands for Diffie-Hellman Knowledge.

GKEA is defined in [11] in the name of knowledge-of-exponent assumption, but it is actually a generalized version of the KEA in [6].

We show that under DTDLA and a variant of GKEA denoted SGKEA, ElGamal encryption is one-way under CCA1 (OW-CCA1), and one-wayness of ElGamal encryption under CCA1 is equivalent to the hardness of DTCDH problem. Since SGKEA is a new assumption, we provide a proof that it holds in the generic group model [17]. This provides some evidence of the security of schemes built using SGKEA.

We also give a new proof that DEG is semantically secure against CCA1 (IND-CCA1) under the delayed-target decisional Diffie-Hellman assumption (DTDDHA). Although the same result has been presented in [12], our proof seems simpler in that it uses a straightforward reduction. We note that our security proof for DEG overlaps that of Lipmaa's work [15]. However, these works are independent.

We show that DHK1 is stronger than necessary in DEG security proof, for which DHK1 (KEA) was originally proposed. We show that a decisional (thus weaker) version of DHK1 (DDHK1) assumption is sufficient for the DEG security proof.

The remainder of the paper is organized as follows. In Section 2, we present our security proof for the ElGamal encryption scheme, and discuss the relations between DTCDHA, DTDLA, and SGKEA. In Section 3, we propose the DDHK1 assumption and give security proof for DEG based on the DDHK1 and DDH assumptions. Section 4 concludes the paper.

2 Security Of ElGamal Encryption

2.1 Scheme Description

First we recall the basic ElGamal encryption scheme. Let G be a multiplicative group of prime order q and g be a generator of G. $k \approx \log_2 q$ will be used as the security parameter in the security analysis. The scheme consists of three algorithms: key generation, encryption, and decryption. G, g, q are default system parameters for these algorithms. In the following description, we use $x \xleftarrow{R} X$ to indicate that x is chosen from set X uniformly at random.

The key generation algorithm computes a public key u and a private key a as follows:

$$a \xleftarrow{R} \mathbb{Z}_q, u \leftarrow g^a.$$

The message space of the scheme is G. To encrypt a message $m \in G$, the encryption algorithm computes a ciphertext $c = (x, y) \in G \times G$ as follows:

$$r \xleftarrow{R} \mathbb{Z}_q, x \leftarrow g^r, y \leftarrow m \cdot u^r.$$

To decrypt a ciphertext $c = (x, y) \in G \times G$, the decryption algorithm computes

$$m \leftarrow y/x^a.$$

2.2 Security Analysis

First we present the Strong GKEA (SGKEA) and DTDLA.

Assumption 1 *The* Strong Generalized Knowledge-of-Exponent Assumption (SGKEA) *is as follows: Let G be a group of prime order q, g be a generator of G, and $k \approx \log_2 q$ be the security parameter. Let A be a polynomial time (in k) algorithm. A is given $(x_0, {x_0}^a, \cdots, x_n, {x_n}^a)$ where $x_0, \cdots, x_n \in G$ and $x_1, \cdots, x_n$ are chosen by A adaptively, n is polynomial in k, $a \in_R \mathbb{Z}_q$ and a is unknown to A. There exists an efficient compiler E such that for any A that outputs a pair $(x, y) \in G \times G$, E can compiles A to A' that satisfies the following conditions: 1. $\hat{A'}$ is polynomial time; 2. A' has the same input, output, and random tape accesses as A, except that in addition to x and y, A' also outputs $(c_0, \cdots, c_n)$ such that*

$$\Pr\left[\prod_{i=0}^{n} {x_i}^{c_i} = x \mid y = x^a\right] > 1 - \epsilon_{sgkea}$$

where ϵ_{sgkea} is negligible.

SGKEA is a variant of GKEA. GKEA was first defined in [11]. GKEA is the same as SGKEA except that it does not specify if A chooses $x_1, \cdots, x_n$.

Assumption 2 *The* Delayed-Target Discrete Log Assumption (DTDLA) *is as follows. Let G be a finite cyclic group, g be a generator of G, and $k \approx \log_2 |G|$. Let A be a probabilistic polynomial (in k) time algorithm that takes input g and has access to two oracles. The first is a discrete log oracle $DL_g()$, which on input $x \in G$ returns r such that $x = g^r$. The second is a challenge oracle $C_g()$ that, when invoked, returns $x \in_R G$. A can access $DL_g()$ n times, where n is polynomial in k. The DTDLA assumption assumes that after receiving a challenge x from $C_g()$, without further accesses to the oracle $DL_g()$, the probability that A outputs r such that $g^r = x$ is negligible.*

DTDLA is defined and discussed in [14].

Next we review the security notation. We define the following interactive game, Game 1, between a probabilistic polynomial time (PPT) challenger C and a PPT adversary A. In the game, A can ask for n decryptions from C. Then A tries to decrypt a fresh challenge ciphertext.

C		A
1.	$a \in_R \mathbb{Z}_q, u \leftarrow g^a$	$\xrightarrow{g, u}$
	Repeat 2 and 3 n times:	
2.		$\xleftarrow{x_i, y_i}$
3.	$m_i \leftarrow y_i / {x_i}^a$	$\xrightarrow{m_i}$
4.	$m \in_R G, r \in_R \mathbb{Z}_q, x \leftarrow g^r, y \leftarrow m \cdot u^r$	$\xrightarrow{x, y}$
5.		$\xleftarrow{m'}$

Game 1: ElGamal OW-CCA1 Game.

We use $\Pr_i[e]$ to denote the probability that an event e happens in Game i. We say that ElGamal encryption is one-way under non-adaptive chosen ciphertext attack (i.e., OW-CCA1 secure) if $\Pr_1[m' = m]$ is negligible.

We show that ElGamal encryption is OW-CCA1 secure if SGKEA and DTDLA hold. The sketch of the proof is as follows: assuming that SGKEA holds, if an adversary can break the scheme, then

using the adversary as a subroutine, a PPT algorithm can break the DTDLA. We follow the proof style suggested in [18] to structure the proof as a sequence of games.

Theorem 3. *If SGKEA and DTDLA hold, then the ElGamal encryption scheme is OW-CCA1 secure.*

Proof. We transform Game 1 to Game 2 by removing the value m in the messages. It is clear that

$$\Pr_1[m' = m] = \Pr_2[z = x^a]. \tag{1}$$

C		A
1.	$a \in_R \mathbb{Z}_q, u \leftarrow g^a$	$\xrightarrow{g,u}$
	Repeat 2 and 3 n times:	
2.		$\xleftarrow{x_i}$
3.	$z_i \leftarrow {x_i}^a$	$\xrightarrow{z_i}$
4.	$x \in_R G$	$\xrightarrow{x}$
5.		$\xleftarrow{z}$

Game 2:

We transform Game 2 to Game 3 by a conceptual change: instead of receiving x from C, A reads x from its random tape. Besides, A outputs x along with z. It holds that

$$\Pr_3[z = x^a] = \Pr_2[z = x^a]. \tag{2}$$

C		A
1.	$a \in_R \mathbb{Z}_q, u \leftarrow g^a$	$\xrightarrow{g,u}$
	Repeat 2 and 3 n times:	
2.		$\xleftarrow{x_i}$
3.	$z_i \leftarrow {x_i}^a$	$\xrightarrow{z_i}$
4.		$x \in_R G$
5.		$\xleftarrow{x,z}$

Game 3:

In Game 3, when A outputs the pair (x, z), by SGKEA, it can be compiled into A' that has the same input, output, and random tape accesses as A, except that, in addition to (x, z), A' also outputs $r_0, \cdots, r_n$, such that

$$\Pr\left[x = \prod_{0 \le i \le n} {x_i}^{r_i} | z = x^a\right] > 1 - \epsilon_{sgkea}. \tag{3}$$

C			A'
1.	$a \in_R \mathbb{Z}_q, u \leftarrow g^a$	$\xrightarrow{g,u}$	
	Repeat 2 and 3 n times:		
2.		$\xleftarrow{x_i}$	
3.	$z_i \leftarrow {x_i}^a$	$\xrightarrow{z_i}$	
4.			$x \in_R G$
5.		$\xleftarrow{x, z, r_0, \cdots, r_n}$	

Game 4:

Next we transform Game 3 to a new Game 4 by replacing A with A'.

Next we transform Game 4 to a new Game 5. In Game 5, C can query $DL_g(x)$ to compute the logarithm of x, and A' queries $C_g()$ to generate a random x. The oracles $DL_g()$ and $C_g()$ are as defined in the DTDLA assumption.

C			A'
1.	$a \in_R \mathbb{Z}_q, u \leftarrow g^a$	$\xrightarrow{g,u}$	
	Repeat 2 - 4 n times:		
2.		$\xleftarrow{x_i}$	
3.	$e_i \leftarrow DL_g(x_i)$		
4.	$z_i \leftarrow {x_i}^a$	$\xrightarrow{z_i}$	
5.			$x \leftarrow C_g$
6.		$\xleftarrow{x, z, r_0, \cdots, r_n}$	
7.	$e = r_0 + e_1 r_1 + e_2 r_2 + \cdots + e_n r_n$		

Game 5:

It is clear that

$$\Pr_5 [g^e = x] = \Pr_5 \left[x = \prod_{0 \le i \le n} {x_i}^{r_i} \right] \tag{4}$$

$$= \Pr_3 \left[x = \prod_{0 \le i \le n} {x_i}^{r_i} \right]. \tag{5}$$

In Game 5, $DL_g()$ is accessed n times, then $C_g()$ outputs a random challenge x. e is computed as a "guess" of the logarithm of x. Therefore,

$$\Pr_5 [g^e = x] = Adv^C_{dtdl} \tag{6}$$

where Adv^C_{dtdl} is the probability that the polynomial time algorithm C can solve the delayed-target DL problem.

Combining (1)-(6), it holds that

$$\Pr_1[m' = m] < \frac{Adv^C_{dtdl}}{1 - \epsilon_{sgkea}}.$$

We conclude that if SGKEA and DTDLA hold, then ElGamal is OW-CCA1 secure. □

2.3 Relations Between The Assumptions

First, we consider the relation between OW-CCA1 security of ElGamal encryption and the following delayed-target computational Diffie-Hellman assumption (DTCDHA). DTCDHA is defined in [10] and is discussed in [14].

Assumption 4 *The* Delayed-Target Computational Diffie-Hellman Assumption (DTCDHA) *is as follows. Let G be a finite cyclic group of order q, g be a generator of G, and $k \approx \log_2 q$. Let A be a probabilistic polynomial (in k) time algorithm that takes input $g, g^a \in G$ where $a \in_R \mathbb{Z}_q$. A has access to two oracles. The first is a CDH oracle $CDH_{g,g^a}()$, which on input $x \in G$ returns x^a. The second is a challenge oracle $C_g()$ that, when invoked, returns $x \in_R G$. A can access $CDH_{g,g^a}()$ n times where n is polynomial in k. The DTCDHA assumes that after receiving a challenge x from $C_g()$, without further access to the oracle $CDH_{g,g^a}()$, the probability that A outputs z such that $z = x^a$ is negligible.*

We observe that Game 10 is in fact a delayed-target computational Diffie-Hellman game. Therefore we have the result:

Theorem 5. *OW-CCA1 security of ElGamal encryption is equivalent to DTCDHA.*

Since DTDLA and SGKEA imply that the ElGamal encryption is OW-CCA1 secure, it also holds that

Corollary 1. *DTDLA and SGKEA imply DTCDHA.*

This result may be of independent interest in studying the relation between the assumptions.

In [3], Brown and Gallant presented an algorithm that can be used to recover a in the DTCDH problem. If the adversary knows u where $u|(q-1)$ and $u \approx q^{1/3}$, then the adversary can query the CDH oracle $\Theta(q^{1/3})$ times and recover a in time $\Theta(q^{1/3})$. This algorithm is more efficient than Pallard's ρ algorithm [16, §3.6], which solves a in time $O(q^{1/2})$ without querying the oracle.

3 Damgård ElGamal Encryption

In this section, we use the delayed-target decisional Diffie-Hellman assumption (DTDDHA), which is the Gap Subgroup Membership Assumption in prime order groups, to prove that DEG is IND-CCA1. Our proof is simpler than the one in [12] in that it uses a straightforward reduction. Then, we propose a decisional version of the DHK1 (Diffie-Hellman Knowledge) assumption [2], namely the DDHK1 assumption, prove that DEG is IND-CCA1 under the DDHK1 and DDH assumptions, and prove that DHK1 implies DDHK1. In [2], DHK1 is used to prove the security of DEG. Our result shows that DHK1 is stronger than necessary in the security proof of DEG.

3.1 Scheme Description

Let G be a group of prime order q and let g be a generator of G. DEG consists of three algorithms: key generation, encryption, and decryption. G, g, q are default system parameters for these algorithms.

The key generation algorithm computes a public key $(u, v) \in G \times G$ and a private key $(a, b) \in \mathbb{Z}_q \times \mathbb{Z}_q$ as follows:

$$a \in_R \mathbb{Z}_q, b \in_R \mathbb{Z}_q, u \leftarrow g^a, v \leftarrow g^b.$$

The message space of the scheme is G. To encrypt a message $m \in G$, the encryption algorithm computes a ciphertext $c = (x, y, z) \in G^3$ as follows:

$$r \in_R \mathbb{Z}_q, x \leftarrow g^r, y \leftarrow u^r, z \leftarrow m \cdot v^r.$$

To decrypt a ciphertext c, the decryption algorithm computes m as follows: if $y = x^a$, then

$$m \leftarrow z/x^b.$$

Otherwise, the decryption algorithm returns $\perp$ to indicate an invalid ciphertext.

3.2 Security Analysis

First we define the DTDDHA:

Assumption 6 *The* Delayed-Target Decisional Diffie-Hellman Assumption (DTDDHA) *is as follows: Let G be a group of prime order q, g be a generator of G, and $k \approx \log_2 q$. Let D be a probabilistic polynomial (in k) time algorithm that takes input $g, g^a \in G$ where $a \in_R \mathbb{Z}_q$ and A has access to two oracles. The first is a DDH oracle $DDH_{g,g^a}()$, which on input $(x, y) \in G \times G$ returns 1 if $y = x^a$ and returns 0 otherwise. The second is a challenge oracle $C_{g,g^a}()$ that, when invoked, returns a challenge (x, x^a) or (x, y) with equal probability where $x \in_R G$ and $y \in_R G$. A can access $DDH_{g,g^a}()$ for n times where n is polynomial in k. The DTDDHA assumes that after receiving a challenge (x, y) from $C_{g,g^a}()$, without further accesses to the oracle $DDH_{g,g^a}()$, the advantage of D in this game, defined as*

$$Adv^D_{dtddh} = \left|\Pr\left[D(x, y) = 1 | y = x^a\right] - \Pr\left[D(x, y) = 1 | y \in_R G\right]\right|,$$

is negligible.

DTDDHA is an instantiation of the Gap Subgroup Membership Assumption in [12].

Next we describe an interactive game, Game 6, between a PPT challenger C and a PPT adversary A to define the semantic security of DEG under CCA1.

The adversary's advantage in Game 6 is

$$Adv^A_{game6} = \left|\Pr_6\left[d' = d\right] - 1/2\right|.$$

We say that DEG is IND-CCA1 secure if Adv^A_{game6} is negligible.

Next we prove the result:

Theorem 7. *DEG is IND-CCA1 secure if DTDDHA holds.*

C		A
1. $a \in_R \mathbb{Z}_q, b \in_R \mathbb{Z}_q, u \leftarrow g^a, v \leftarrow g^b$	$\xrightarrow{g,u,v}$	
Repeat 2 - 5 n times:		
2.	$\xleftarrow{x_i,y_i,z_i}$	
3. if $y_i = {x_i}^a$ then $m_i \leftarrow z_i/{x_i}^b$		
4. else $m_i = \perp$		
5.	$\xrightarrow{m_i}$	
6.	$\xleftarrow{m'_0, m'_1}$	
7. $d \in_R \{0,1\}, r \in_R \mathbb{Z}_q, x \leftarrow g^r$ $y \leftarrow u^r, z' \leftarrow v^r, z \leftarrow m'_d z'$	$\xrightarrow{x,y,z}$	
8.	$\xleftarrow{d'}$	

Game 6: DEG CCA1 Game.

C		A
1. $a \in_R \mathbb{Z}_q, b \in_R \mathbb{Z}_q, u \leftarrow g^a, v \leftarrow g^b$	$\xrightarrow{g,u,v}$	
Repeat 2 - 5 n times:		
2.	$\xleftarrow{x_i,y_i,z_i}$	
3. if $y_i = {x_i}^a$ then $m_i \leftarrow z_i/{x_i}^b$		
4. else $m_i = \perp$		
5.	$\xrightarrow{m_i}$	
6.	$\xleftarrow{m'_0, m'_1}$	
7. $d \in_R \{0,1\}, r \in_R \mathbb{Z}_q, x \leftarrow g^r$ $y \in_R G, z' \leftarrow v^r, z \leftarrow m'_d z'$	$\xrightarrow{x,y,z}$	
8.	$\xleftarrow{d'}$	

Game 7: y is replaced with a random value.

Proof. We transform Game 6 to a new Game 7 by replacing y with a random element.

Then we construct an algorithm D_1 as shown in Algorithm 1 to solve the delayed-target DDH problem. Note D_1 uses A as a subroutine.

In algorithm D_1, if y is generated by C_{g,g^a} to be $y \leftarrow x^a$, then the computation of A proceeds as in Game 6, therefore

$$\Pr\left[D_1 = 1 | (y \leftarrow x^a)\right] = \Pr_6\left[d' = d\right].$$

If y is generated by C_{g,g^a} to be $y \in_R G$, then the computation of A proceeds as in Game 7, therefore

$$\Pr\left[D_1 = 1 | (y \in_R G)\right] = \Pr_7\left[d = d'\right].$$

It follows that

$$\begin{aligned}\left|\Pr_6\left[d = d'\right] - \Pr_7\left[d = d'\right]\right| &= \left|\Pr\left[D = 1 | (y \leftarrow x^a)\right] - \Pr\left[D = 1 | (y \in_R G)\right]\right| \\ &= Adv^{D_1}_{dtddh}.\end{aligned} \tag{7}$$

$D_1^{DDH_{g,g^a},C_{g,g^a}}(g,g^a)$		A
1. $b \in_R \mathbb{Z}_q, u \leftarrow g^a, v \leftarrow g^b$	$\xrightarrow{g,u,v}$	
Repeat 2 - 5 n times:		
2.	$\xleftarrow{x_i,y_i,z_i}$	
3. if $DDH_{g,g^a}(x_i,y_i)=1$ then $m_i \leftarrow z_i/{x_i}^b$		
4. else $m_i = \perp$		
5.	$\xrightarrow{m_i}$	
6.	$\xleftarrow{m'_0,m'_1}$	
7. $d \in_R \{0,1\}, (x,y) \leftarrow C_{g,g^a}(), z' \leftarrow x^b, z \leftarrow {m'}_d z'$		
8.	$\xrightarrow{x,y,z}$	
9.	$\xleftarrow{d'}$	
10. if $d'=d$ then return 1		
11. else return 0		

Algorithm 1: D_1

C		A
1. $a \in_R \mathbb{Z}_q, b \in_R \mathbb{Z}_q, u \leftarrow g^a, v \leftarrow g^b$	$\xrightarrow{g,u,v}$	
Repeat 2 - 5 n times:		
2.	$\xleftarrow{x_i,y_i,z_i}$	
3. if $y_i = {x_i}^a$ then $m_i \leftarrow z_i/{x_i}^b$		
4. else $m_i = \perp$		
5.	$\xrightarrow{m_i}$	
6.	$\xleftarrow{m'_0,m'_1}$	
7. $d \in_R \{0,1\}, r \in_R \mathbb{Z}_q, x \leftarrow g^r$ $y \in_R G, z' \in_R G, z \leftarrow m'_d z'$	$\xrightarrow{x,y,z}$	
8.	$\xleftarrow{d'}$	

Game 8: z' is replaced with a random value.

Next we transform Game 7 to Game 8 by replacing z' with a random element.

Then we construct an algorithm D_2 as shown in Algorithm 2 to solve the delayed-target DDH problem.

Let $b = ac$. Then in D_2, we have $v = u^c = g^{ac} = g^b$, and $z' = x^a \Leftrightarrow z'^c = x^{ac} = x^b$. Therefore, if in the challenge pair (x, z'), z' is generated by $z' \leftarrow x^a$, then the computation of A proceeds as in Game 7, and it holds that

$$\Pr\left[D_2 = 1 | (z' \leftarrow x^a)\right] = \Pr_7\left[d = d'\right].$$

If in the challenge pair (x, z'), z' is generated by $z' \in_R G$, then the computation of A proceeds as in Game 8, therefore

$$\Pr\left[D_2 = 1 | (z' \in_R G)\right] = \Pr_8\left[d = d'\right].$$

$D_2^{DDH_{g,g^a},C_{g,g^a}}(g,g^a)$		A
1. $c \in_R \mathbb{Z}_q, u \leftarrow g^a, v \leftarrow u^c$	$\xrightarrow{g,u,v}$	
Repeat 2 - 5 n times:		
2.	$\xleftarrow{x_i,y_i,z_i}$	
3. if $DDH_{g,g^a}(x_i,y_i)=1$ then $m_i \leftarrow z_i/{y_i}^c$		
4. else $m_i = \perp$		
5.	$\xrightarrow{m_i}$	
6.	$\xleftarrow{m'_0,m'_1}$	
7. $d \in_R \{0,1\}, (x,z') \leftarrow C_{g,g^a}(), y \in_R G, z \leftarrow m'_d {z'}^c$		
8.	$\xrightarrow{x,y,z}$	
9.	$\xleftarrow{d'}$	
10. if $d'=d$ then return 1		
11. else return 0		

Algorithm 2: D_2

It follows that

$$\left|\Pr_7\left[d=d'\right]-\Pr_8\left[d=d'\right]\right| = \left|\Pr\left[D_2=1|(z'\leftarrow x^a)\right]-\Pr\left[D_2=1|(z'\in_R G)\right]\right| \tag{8}$$
$$= Adv^{D_2}_{dtddh}.$$

We also have $\Pr_8\left[d=d'\right]=1/2$ since z is independent of m'_b in Game 8. Therefore

$$\left|\Pr_6\left[d'=d\right]-1/2\right| \leq Adv^{D_1}_{dtddh}+Adv^{D_2}_{dtddh}. \tag{9}$$

We conclude that, if DTDDH assumption holds, then DEG is IND-CCA1 secure. □

3.3 Decisional DHK1 Assumption

First we review the DHK1 assumption.

Assumption 8 *The* DHK1 *assumption is as follows: Let G be a group of prime order q, let g be a generator of G, and let $k \approx \log_2 q$. Let $a \in_R \mathbb{Z}_q$. Let O be an oracle that satisfies the following property: when O is queried with a pair $(x_i,y_i) \in G \times G$, O returns r_i such that $x_i = g^{r_i}$ if $y_i = {x_i}^a$. Given (g,g^a), for any polynomial (in k) time algorithm A that has access to O, if A outputs a pair $(x,y) \in G \times G$, then there exists a compiler E such that $A' = E(A)$, and A' satisfies the following conditions: (1) A' is polynomial time; (2) A' has the same input, output, oracle access, and random tape access behaviour as A, except that in addition to x and y, A' also outputs r such that*

$$\Pr\left[x=g^r|y=x^a\right] > 1-\epsilon_{dhk1},$$

or equivalently

$$\Pr\left[x\neq g^r, y=x^a\right] < \epsilon_{dhk1},$$

where ϵ_{dhk1} is negligible.

DHK1 is a generalization of KEA. KEA is the same as DHK1 except that A does not have access to the oracle O. KEA was originally proposed to prove the security of DEG in [6]. Bellare *et al.* pointed out a flaw in the security argument in [6], and proposed DHK1 to prove the security of DEG [2]. The above definition of DHK1 is different from that in [2] in expression, but their ideas are the same.

We observe that using the DDH assumption and the following decisional DHK1 (DDHK1), we can prove that DEG is IND-CCA1 secure.

Assumption 9 *The* Decisional DHK1 (DDHK1) assumption *is as follows: Let G be a group of prime order q, let g be a generator of G, and let $k \approx \log_2 q$. Let $a \in_R \mathbb{Z}_q$. Let O be an oracle. When O is queried with a pair $(x_i, y_i) \in G \times G$, O returns 1 if $y_i = {x_i}^a$ and returns 0 if $y_i \neq {x_i}^a$. Given (g, g^a), for any polynomial (in k) time algorithm A that has access to O, if A outputs a pair $(x, y) \in G \times G$, then there exists a compiler E such that $A' = E(A)$, and A' satisfies the following conditions: (1) A' is polynomial time; (2) A' has the same input, output, oracle access and random tape access behaviour as A, except that in addition to x and y, A' also outputs a bit b such that*

$$\Pr[b = 1, y = x^a] + \Pr[b = 0, y \neq x^a] > 1 - \epsilon$$

where ϵ is negligible.

First, we observe that DHK1 is stronger than DDHK1.

Lemma 1. *DHK1 implies DDHK1.*

Proof. We consider an assumption DHK1′. DHK1′ is the same as DHK1 except that the oracle O returns 1 if $y_i = {x_i}^a$ and returns 0 if $y_i \neq {x_i}^a$. We define the event that A wins DHK1 to be the event $g^r \neq x$ and $y = x^a$ in the DHK1 setting, the event that A wins DHK1′ to be the event $g^r \neq x$ and $y = x^a$ in the DHK1′ setting, and the event that A wins DDHK1 to be the event $b = 0$ and $y = x^a$ in the DDHK1 setting.

First we show that DHK1 implies DHK1′. In DHK1′, A can tell if $y_i = {x_i}^a$ by querying O. In DHK1, A can not only tell if $y_i = {x_i}^a$, but also get r_i such that $g^{r_i} = x_i$ when $y_i = {x_i}^{r_i}$. It is more likely that A in DHK1 can compute $(x, y = x^a)$ without choosing r where $g^r = x$ than A in DHK1′. We use $\Pr_{DHK1'}[e]$ and $\Pr_{DDHK1}[e]$ to denote the probability that an event e happens in DHK1′ setting and DDHK1 setting respectively. If A can compute $(x, y = x^a)$ with out knowing $r = \log x$, then A' would not be able to extract r from A. It holds that

$$\Pr_{DHK1}[A \text{ wins}] \geq \Pr_{DHK1'}[A \text{ wins}]$$
$$\Pr_{DHK1}[g^r \neq x, y = x^a] \geq \Pr_{DHK1'}[g^r \neq x, y = x^a]$$

Therefore, if DHK1 holds, then DHK1′ holds.

Next we show that DHK1′ implies DDHK1. Suppose that DHK1′ holds. We construct the algorithm A' in DDHK1 (denoted as A'_{DDHK1}) based on the algorithm A' in DHK1′ (denoted as $A'_{DHK1'}$). Let (r, x, y) be the output of the $A'_{DHK1'}$ and let (e, x, y) be the output of A'_{DDHK}. We define that A'_{DDHK} outputs $(1, x, y)$ if $x = g^r$ and $y = (g^a)^r$, otherwise A'_{DDHK} outputs $(0, x, y)$. It holds that

$$\Pr[e = 0 | y \neq x^a] = 1$$

and

$$\begin{aligned}\Pr[e=1|y=x^a] &\geq \Pr[e=1, x=g^r|y=x^a] \\ &= \Pr[e=1|x=g^r, y=x^a]\Pr[x=g^r|y=x^a] \\ &> 1-\epsilon_{dhk1}.\end{aligned}$$

It holds that

$$\begin{aligned}&\Pr[e=1, y=x^a]+\Pr[e=0, y\neq x^a] \\ &= \Pr[e=1|y=x^a]\Pr[y=x^a]+\Pr[e=0|y\neq x^a]\Pr[y\neq x^a] \\ &> (1-\epsilon_{dhk1})\Pr[y=x^a]+\Pr[y\neq x^a] \\ &= 1-\epsilon_{dhk1}\Pr[y=x^a].\end{aligned}$$

Therefore, if DHK1′ holds, then DDHK1 holds.

We conclude that DHK1 implies DDHK1. □

Next, we prove that the DDH and DDHK1 assumptions imply the DTDDH assumption.

Theorem 10. *DDH and DDHK1 assumptions imply DTDDH assumption.*

Proof. we define a DTDDH game as shown in Game 9. Let Adv^A_{DTDDH} be the probability that A

C		A
1. $a \in_R \mathbb{Z}_q, u = g^a$	$\xrightarrow{g,u}$	
Repeat 2 - 3 n times:		
2.	$\xleftarrow{x_i, y_i}$	
3. If $y_i = {x_i}^a$ then $e'_i \leftarrow 1$, otherwise, $e'_i \leftarrow 0$	$\xrightarrow{e'_i}$	
4.	$\xrightarrow{x,y}$	
5.	$\xleftarrow{e}$	
6. return e		

Game 9: DTDDH game

answers e correctly in a game.

We transform Game 9 to Game 10 by replacing A with $A' = E(A)$ where E and A' are as defined in the DDHK1 assumption.

Let $Adv^{A'}_{game_{10}}$ be the probability that A' answers e correctly in a game. It holds that

$$Adv^A_{dtddh} = Adv^{A'}_{game_{10}}.$$

Next we transform Game 10 to 11 in which C set $e'_i \leftarrow e_i$.

If the DDHK1 assumption holds, then in Step 3, e'_i is a correct answer with probability $(1-\epsilon)$ where ϵ is negligible. If in all n rounds, all the e'_i values are correct, then the computation of A' proceeds the same way as in Game 10. Therefore, it holds that

$$Adv^{A'}_{game_{11}} \geq Adv^{A'}_{game_{10}}(1-\epsilon)^n$$

C		A'
1. $a \in_R \mathbb{Z}_q, u = g^a$	$\xrightarrow{g,u}$	
Repeat 2 - 3 n times:		
2.	$\xleftarrow{e_i, x_i, y_i}$	
3. If $y_i = {x_i}^a$ then $e'_i \leftarrow 1$, otherwise, $e'_i \leftarrow 0$	$\xrightarrow{e'_i}$	
4.	$\xrightarrow{x,y}$	
5.	$\xleftarrow{e}$	
6. return e		

Game 10:

C		A'
1. $a \in_R \mathbb{Z}_q, u = g^a$	$\xrightarrow{g,u}$	
Repeat 2 - 3 n times:		
2.	$\xleftarrow{e_i, x_i, y_i}$	
3. $e'_i \leftarrow e_i$	$\xrightarrow{e'_i}$	
4.	$\xrightarrow{x,y}$	
5.	$\xleftarrow{e}$	
6. return e		

Game 11:

Note that in Game 11, C does not use a to compute e'_i. We can transform Game 11 to Game 12 where C takes a triple $(g^a, x, y) \in G^3$ as input and solves the DDH problem.

Let Adv^C_{DDH} be the probability that C correctly answers if $y = x^a$. It holds that

$$Adv^C_{DDH} = Adv^{A'}_{game_{11}}.$$

It follows that

$$Adv^C_{ddh} \geq Adv^A_{dtddh}(1-\epsilon)^n.$$

Note that n is polynomial in k and ϵ is negligible in k if the DDHK1 assumption holds. We conclude that if the DDDHK1 assumption holds, then the DDH assumption implies the DTDDH assumption; i.e., the DDH assumption and the DDHK1 assumption imply the DTDDH assumption. □

The above results prove that DHK1 is stronger than necessary in the security proof for DEG.

4 Conclusion

In this paper, we showed that the ElGamal encryption is OW-CCA1 under the strong generalized knowledge-of-exponent assumption (SGKEA) and the delayed-target discrete log assumption (DTDLA), and its security is equivalent to the hardness of the delayed-target computational Diffie-Hellman (DTCDH) problem. For DEG, we gave a simple proof that DEG is IND-CCA1 secure

$C(g^a, x, y)$		A'
1. $u = g^a$	$\xrightarrow{g, u}$	
Repeat 2 - 3 n times:		
2.	$\xleftarrow{e_i, x_i, y_i}$	
3. $e'_i = e_i$	$\xrightarrow{e'_i}$	
4.	$\xrightarrow{x, y}$	
5.	$\xleftarrow{e}$	
6. return e		

Game 12:

under the delayed-target decisional Diffie-Hellman assumption. We proposed a decisional DHK1 assumption (DDHK1), prove that DHK1 implies DDHK1, and DEG is IND-CCA1 secure under the DDHK1 and DDH assumptions.

References

1. M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations among notions of security for public-key encryption schemes. In *CRYPTO '98: Proceedings of the 18th Annual International Cryptology Conference on Advances in Cryptology*, pages 26–45, London, UK, 1998. Springer-Verlag.
2. M. Bellare and A. Palacio. Towards plaintext-aware public-key encryption without random oracles. In P.J. Lee, editor, *ASIACRYPT*, volume 3329 of *Lecture Notes in Computer Science*, pages 48–62. Springer, 2004.
3. Daniel R. L. Brown and Robert P. Gallant. The static diffie-hellman problem. Cryptology ePrint Archive, Report 2004/306, 2004. http://eprint.iacr.org/.
4. D. Cash, E. Kiltz, and V. Shoup. The twin Diffie-Hellman problem and applications. In Nigel P. Smart, editor, *EUROCRYPT*, volume 4965 of *Lecture Notes in Computer Science*, pages 127–145. Springer, 2008.
5. R. Cramer and V. Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. *SIAM J. Comput.*, 33(1):167–226, 2004.
6. I. Damgård. Towards practical public key systems secure against chosen ciphertext attacks. In *CRYPTO '91: Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology*, pages 445–456, London, UK, 1992. Springer-Verlag.
7. Y. Desmedt, H. Lipmaa, and D.H. Phan. Hybrid Damgård is CCA1-secure under the DDH assumption. In Matthew K. Franklin, Lucas Chi Kwong Hui, and Duncan S. Wong, editors, *Proceeding of The 7th International Conference on Cryptology And Network Security (CANS 2008)*, volume 5339 of *Lecture Notes in Computer Science*, pages 18–30. Springer-Verlag, 2008.
8. Y. Desmedt and D.H. Phan. A CCA secure hybrid damgård's ElGamal encryption. In Joonsang Baek, Feng Bao, Kefei Chen, and Xuejia Lai, editors, *ProvSec*, volume 5324 of *Lecture Notes in Computer Science*, pages 68–82. Springer, 2008.
9. T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Proceedings of CRYPTO 84 on Advances in Cryptology*, pages 10–18, New York, NY, USA, 1985. Springer-Verlag New York, Inc.
10. D. Freeman. Pairing-based identification schemes. Cryptology ePrint Archive, Report 2005/336, 2005. http://eprint.iacr.org/.
11. K. Gjøsteen. *Subgroup membership problems and public key cryptosystems.* PhD thesis, Norwegian University of Science and Technology, 2004.
12. K. Gjøsteen. A new security proof for Damgård's ElGamal. In D. Pointcheval, editor, *CT-RSA*, volume 3860 of *Lecture Notes in Computer Science*, pages 150–158. Springer, 2006.
13. E. Kiltz, K. Pietrzak, M. Stam, and M. Yung. A new randomness extraction paradigm for hybrid encryption. Cryptology ePrint Archive, Report 2008/304, 2008. http://eprint.iacr.org/.
14. N. Koblitz and A. Menezes. Another look at non-standard discrete log and Diffie-Hellman problems. *Journal of Mathematical Cryptology.*, 2(4):1862–2984, 2008.

15. H. Lipmaa. On CCA1-security of Elgamal And Damgård cryptosystems. Cryptology ePrint Archive, Report 2008/234, 2008. http://eprint.iacr.org/.
16. A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, 1996.
17. V. Shoup. Lower bounds for discrete logarithms and related problems. In *EUROCRYPT*, pages 256–266, 1997.
18. V. Shoup. Sequences of games: a tool for taming complexity in security proofs. Cryptology ePrint Archive, Report 2004/332, 2004. http://eprint.iacr.org/.
19. Y. Tsiounis and M. Yung. On the security of ElGamal based encryption. In H. Imai and Y. Zheng, editors, *Public Key Cryptography*, volume 1431 of *Lecture Notes in Computer Science*, pages 117–134. Springer, 1998.