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 discuss the security of the ElGamal encryption scheme and its variant by Damgård. For the ElGamal encryption, we show that (1) under the generalized knowledge-of-exponent assumption and the one-more discrete log 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 one-more computational Diffie-Hellman problem. For a variant of ElGamal encryption proposed by Damgård (DEG), we give a new proof that DEG is semantically secure against non-adaptive chosen ciphertext attacks under the one-more decisional Diffie-Hellman assumption (although the same result for DEG security has been presented in the literature before, our proof is simpler). We also give a new security proof for DEG based on the decisional Diffie-Hellman assumption (DDHA) and a weaker version of the knowledge-of-exponent assumption (KEA), and note that KEA is stronger than necessary in the security proof of DEG, for which KEA was originally proposed.

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

1 Introduction

The ElGamal encryption scheme [6] 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 [10], and is insecure under CCA2. It is conjectured to be secure under CCA1, but there has been no formal proof.

In [4], Damgård proposed a variant of ElGamal encryption (DEG) and a new assumption known as Knowledge-of-Exponent Assumption (KEA). Under an extension of of KEA named DHK1, DEG is semantically secure under CCA1 (IND-CCA1) [3]. In [7], 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. DEG is the most efficient IND-CCA1 secure public key encryption scheme having a security proof without random oracles [3].

In this paper, first we investigate the connection between the security of ElGamal encryption and some known cryptographic assumptions, including the generalized knowledge-of-exponent assumption (GKEA), one-more discrete log assumption (OMDLA), and one-more computational Diffie-Hellman assumption (OMCDHA). The OMDLA that we use is a variant of the OMDLA proposed in [2]. The relation between these two versions of OMDLA is discussed in [8]. OMCDHA

* research supported by an NSERC post-graduate scholarship.
** research supported by NSERC discovery grant 203114-06.

was first proposed in [5]. Its relation with other one-more variant of DH problems is also discussed in [8]. GKEA is first proposed in [11] to validate the use of KEA in some protocols in the literature.

We show that under GKEA and OMDLA, ElGamal encryption is one-way under CCA1 (OW-CCA1), and one-wayness of ElGamal encryption under CCA1 is equivalent to the hardness of OMCDH problem.

We also give a new proof that DEG is semantically secure against CCA1 (IND-CCA1) under the one-more decisional Diffie-Hellman assumption (OMDDHA). Although the same result has been presented in [7], our proof is simpler in that it uses a straightforward reduction without resorting to the hash proof system as in [7].

Our proof for DEG security based on OMDDHA can be transformed to a proof based on DDHA and a weaker version of KEA. This implies that KEA is stronger than necessary in the security proof of DEG, for which KEA was originally proposed for.

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 OMCDHA, OMDLA, and GKEA. In Section 3, we give our new proofs for DEG and discuss KEA. Section 4 concludes the paper.

2 Security Of ElGamal Encryption

2.1 Scheme Description

First we recall the 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 review GKEA and OMDLA.

Assumption 1 *The* Generalized Knowledge-of-Exponent Assumption (GKEA) *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 $x_1, \cdots, x_n \in G$, n is polynomial in k, and $a \xleftarrow{R} \mathbb{Z}_q$. If A outputs a pair $(x, y) \in G^2$, 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, and random tape accesses as A, except that in addition to x and y, A' also outputs $(c_0, \cdots, c_n)$ such that

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

where ϵ_{gkea} is negligible[1].

GKEA was first proposed in [11] to validate the use of KEA in some protocols in the literature.

Assumption 2 *The* One-More Discrete Log Assumption (OMDLA) *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 $x \xleftarrow{R} G$. A can access $DL_g()$ n times, where n is polynomial in k. The OMDLA 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.*

Next we review the security notation. We define the following interactive game, Game 0, 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.

Game 0		
C	Messages	A
1. $a \xleftarrow{R} \mathbb{Z}_q, u \leftarrow g^a$	$\xrightarrow{g, u}$	
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. $m \xleftarrow{R} G, r \xleftarrow{R} \mathbb{Z}_q, x \leftarrow g^r, y \leftarrow m \cdot u^r$	$\xrightarrow{x, y}$	
5.	$\xleftarrow{m'}$	

Let S_0 be the event that $m' = m$ in Game 0. We say that ElGamal encryption is one-way under non-adaptive chosen ciphertext attack (OW-CCA1 secure) if $\Pr[S_0]$ is negligible.

We show that ElGamal encryption is OW-CCA1 secure if GKEA and OMDLA hold. The sketch of the proof is as follows: assuming that GKEA holds, if an adversary can break the scheme, then using the adversary as a subroutine, a PPT algorithm can break the OMDLA. We follow the proof style suggested in [9] to structure the proof as a sequence of games.

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

Proof. We transform Game 0 to Game 1 by removing the values m in the messages.

[1] We say $\epsilon(k)$, a function of the security parameter k, is negligible if for any polynomial Q, for k large enough, it holds that $\epsilon(k) < 1/Q(k)$. For simplicity, we only write ϵ and make k implicit.

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

We define S_1 to be the event that $z = x^a$ in Game 1. It is clear that

$$\Pr[S_0] = \Pr[S_1]. \tag{1}$$

We transform Game 1 to Game 2 by a conceptual change: instead of receiving x from C, A generates a random x. Besides, A outputs x along with z.

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

We define S_2 to be the event that $z = x^a$ in Game 2. It is clear that

$$\Pr[S_2] = \Pr[S_1]. \tag{2}$$

In Game 2, A receives pairs $(x_0 = g, z_0 = g^a), (x_1, z_1 = {x_1}^a), \cdots, (x_n, z_n = {x_n}^a)$. When A outputs a pair (x, z), by GKEA, there is an extractor E such that $A' = E(A)$ and A' 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

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

We replace A with A' in Game 2 to generate Game 3. Note that A' generates random x the same way as A does.

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

Let S_3 be the event that $z = x^a$ in Game 3. It is clear that

$$\Pr[S_3] = \Pr[S_2]. \tag{3}$$

Let S_3' be the event that $x = \prod_{0 \le i \le n} {x_i}^{r_i}$. By GKEA we have

$$\Pr\left[S_3'\right] > \Pr[S_3](1 - \epsilon_{gkea}). \tag{4}$$

Next we transform Game 3 into Game 4. In Game 4, C can query $DL_g(x)$ to compute the logarithm of x, and A' queries $C_g()$ to receive a random x. The oracles $DL_g()$ and $C_g()$ are as defined in the OMDLA assumption.

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

Let S_4 be the event that $g^e = x$. It is clear that

$$\Pr[S_4] = \Pr\left[S_3'\right]. \tag{5}$$

In Game 4, $DL_g()$ is accessed n times, then $C_g()$ outputs a random challenge x. e is computed as a "guess" of the logarithm of x. Therefore,

$$\Pr[S_4] = Adv_{omdl}^C \tag{6}$$

where Adv_{omdl}^C is the probability that the polynomial time algorithm C can solve the one-more DL problem, which is negligible by OMDLA.

Combining (1) - (6), we conclude that $\Pr[S_0]$ is negligible and hence ElGamal encryption 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 one-more computational Diffie-Hellman assumption (OMCDHA).

Assumption 4 *The* One-More Computational Diffie-Hellman Assumption (OMCDHA) *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 $a \stackrel{R}{\leftarrow} \mathbb{Z}_q$. 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 $x \stackrel{R}{\leftarrow} G$. A can access $CDH_{g,g^a}()$ for n times where n is polynomial in k. The OMCDHA 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 1 is in fact a one-more computational Diffie-Hellman game. Therefore we have the result:

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

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

Corollary 1. *OMDLA and GKEA imply OMCDHA.*

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

3 Damgård ElGamal Encryption

In this section, we use the one-more decisional Diffie-Hellman assumption (OMDDHA), 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 [7] in that it uses a straightforward reduction without resorting to hash proof systems. Then, we transform this proof into a proof based on DDHA and a weaker version of KEA, which leads to an observation on KEA.

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:

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

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:

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

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 OMDDHA:

Assumption 6 *The* One-More Decisional Diffie-Hellman Assumption (OMDDHA) *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 $a \xleftarrow{R} \mathbb{Z}_q$ and A has access to two oracles. The first is a DDH oracle $DDH_{g,g^a}()$, which on input $(x, y) \in G^2$ 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 $x \xleftarrow{R} G$ and $y \xleftarrow{R} G$. A can access $DDH_{g,g^a}()$ for n times where n is polynomial in k. The OMDDHA 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*

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

is negligible.

Next we describe an interactive game, Game 0, between a PPT challenger C and a PPT adversary A to define the semantic security of DEG under CCA1.

Game 0		
C	Messages	A
1. $a \xleftarrow{R} \mathbb{Z}_q, b \xleftarrow{R} \mathbb{Z}_q, u \leftarrow g^a, v \leftarrow g^b$	$\xrightarrow{g, u, v}$	
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. $d \xleftarrow{R} \{0, 1\}, r \xleftarrow{R} \mathbb{Z}_q, x \leftarrow g^r$ $y \leftarrow u^r, z' \leftarrow v^r, z \leftarrow m'_d z'$	$\xrightarrow{x, y, z}$	
8.	$\xleftarrow{d'}$	

We define S_0 be the event that $d' = d$ in Game 0. The adversary's advantage in this game is

$$Adv^A_{game0} = \left| \Pr\left[S_0\right] - 1/2 \right|.$$

We say that DEG is IND-CCA1 secure if Adv^A_{game0} is negligible.

Next we prove the result:

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

Proof. We transform Game 0 to Game 1 by replacing y with a random element:

Game 1		
C	Messages	A
1. $a \xleftarrow{R} \mathbb{Z}_q, b \xleftarrow{R} \mathbb{Z}_q, u \leftarrow g^a, v \leftarrow g^b$	$\xrightarrow{g,u,v}$	
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. $d \xleftarrow{R} \{0,1\}, r \xleftarrow{R} \mathbb{Z}_q, x \leftarrow g^r$ $y \xleftarrow{R} G, z' \leftarrow v^r, z \leftarrow m'_d z'$	$\xrightarrow{x,y,z}$	
8.	$\xleftarrow{d'}$	

Let S_1 be the event that $d' = d$ in Game 1.

We construct the following algorithm D_1 to solve the one-more DDH problem.

$D_1^{DDH_{g,g^a},C_{g,g^a}}(g, g^a)$	Messages	A
1. $b \xleftarrow{R} \mathbb{Z}_q, u \leftarrow g^a, v \leftarrow g^b$	$\xrightarrow{g,u,v}$	
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. $d \xleftarrow{R} \{0,1\}, (x, y) \leftarrow C_{g,g^a}(), z' \leftarrow x^b, z \leftarrow {m'}_d z'$		
8.	$\xrightarrow{x,y,z}$	
9.	$\xleftarrow{d'}$	
10. if $d' = d$ then return 1		
11. else return 0		

If in the challenge pair (x, y), y is generated by $y \leftarrow x^a$, then the computation of A proceeds as in Game 0, therefore

$$\Pr[D_1 = 1 | (y \leftarrow x^a)] = \Pr[S_0].$$

If in the challenge pair (x, y), y is generated by $y \xleftarrow{R} G$, then the computation of A proceeds as in Game 1, therefore

$$\Pr\left[D_1 = 1 | (y \xleftarrow{R} G)\right] = \Pr[S_1].$$

It follows that

$$\begin{aligned} |\Pr[S_0] - \Pr[S_1]| &= \left|\Pr[D = 1|(y \leftarrow x^a)] - \Pr\left[D = 1|(y \xleftarrow{R} G)\right]\right| \\ &= Adv^{D_1}_{omddh}. \end{aligned} \tag{7}$$

Next we transform Game 1 to Game 2 by replacing z' with a random element:

Game 2		
C	Messages	A
1. $a \xleftarrow{R} \mathbb{Z}_q, b \xleftarrow{R} \mathbb{Z}_q, u \leftarrow g^a, v \leftarrow g^b$	$\xrightarrow{g,u,v}$	
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. $d \xleftarrow{R} \{0,1\}, r \xleftarrow{R} \mathbb{Z}_q, x \leftarrow g^r$ $y \xleftarrow{R} G, z' \xleftarrow{R} G, z \leftarrow m'_d z'$	$\xrightarrow{x,y,z}$	
8.	$\xleftarrow{d'}$	

Let S_2 be the event that $d' = d$ in Game 2. We construct the following algorithm D_2 to solve the one-more DDH problem.

$D_2^{DDH_{g,g^a},C_{g,g^a}}(g, g^a)$	Messages	A
1. $c \xleftarrow{R} \mathbb{Z}_q, u \leftarrow g^a, v \leftarrow u^c$	$\xrightarrow{g,u,v}$	
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. $d \xleftarrow{R} \{0,1\}, (x, z') \leftarrow C_{g,g^a}(), y \xleftarrow{R} G, z \leftarrow m'_d {z'}^c$		
8.	$\xrightarrow{x,y,z}$	
9.	$\xleftarrow{d'}$	
10. if $d' = d$ then return 1		
11. else return 0		

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 1, and it holds that

$$\Pr\left[D_2 = 1 | (z' \leftarrow x^a)\right] = \Pr\left[S_1\right].$$

If in the challenge pair (x, z'), z' is generated by $z' \xleftarrow{R} G$, then the computation of A proceeds as in Game 2, therefore

$$\Pr\left[D_2 = 1 | (z' \xleftarrow{R} G)\right] = \Pr\left[S_2\right].$$

It follows that

$$|\Pr[S_1] - \Pr[S_2]| = \left|\Pr\left[D_2 = 1|(z' \leftarrow x^a)\right] - \Pr\left[D_2 = 1|(z' \xleftarrow{R} G)\right]\right| \quad (8)$$
$$= Adv^{D_2}_{omddh}.$$

We also have $\Pr[S_2] = 1/2$ since z is independent of m'_b in Game 2. Therefore

$$|\Pr[S_0] - 1/2| \leq Adv^{D_1}_{omddh} + Adv^{D_2}_{omddh}. \quad (9)$$

We conclude that DEG is IND-CCA1 secure. □

3.3 An Observation On KEA

First we review the KEA assumption.

Assumption 8 *The* Knowledge-of-Exponent Assumption (KEA) *is as follows: Let G be a group of prime order q, g be a generator of G, and $k \approx \log_2 q$. Given g, g^a where $a \xleftarrow{R} \mathbb{Z}_q$, for any polynomial (in k) time algorithm A, if A outputs a pair $(x, y) \in G^2$, 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 and random tape access behaviour as A, except that in addition to x and y, A' also outputs r such that*

$$\Pr[x = g^r | y = x^a] > 1 - \epsilon_{kea}$$

where ϵ_{kea} is negligible.

KEA was originally proposed to prove the security of DEG. We observe that using the DDHA and the following weaker version of KEA, we can prove that DEG is IND-CCA1 secure.

Assumption 9 *The* Weak Knowledge-of-Exponent Assumption (WKEA) *is as follows: Let G be a group of prime order q, g be a generator of G, and $k \approx \log_2 q$. Given g, g^a where $a \xleftarrow{R} \mathbb{Z}_q$, for any polynomial (in k) time algorithm A, if A outputs a pair $(x, y) \in G^2$, 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 and random tape access behaviour as A, except that in addition to x and y, A' also outputs a bit e such that*

$$\Pr[e = 1 | y = x^a] - \Pr[e = 1 | y \neq x^a] > 1 - \epsilon_{wkea}$$

where ϵ_{wkea} is negligible.

First, we observe that KEA is stronger than WKEA.

Lemma 1. *KEA implies WKEA.*

Proof. Suppose that KEA holds. We construct the algorithm A' in WKEA (denoted as A'_{wkea}) based on the A' in KEA (denoted as A'_{kea}). Let (r, x, y) be the output of the A'_{kea} and let (e, x, y) be the output of A'_{wkea}. We define that A'_{wkea} outputs $(1, x, y)$ if $x = g^r$ and $y = (g^a)^r$, otherwise A'_{wkea} outputs $(0, x, y)$. It holds that

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

and

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

Therefore

$$\Pr[e=1|y=x^a] - \Pr[e=1|y\neq x^a] > 1-\epsilon_{kea}.$$

□

Informally speaking, WKEA says that A' can tell if $y=x^a$. On the other hand, KEA says that A' can tell if $y=x^a$, and if $y=x^a$, then A' can also find r such that $x=g^r$.

Next, we prove that DEG is IND-CCA1 secure if DDHA and WKEA hold.

Theorem 10. *DEG is IND-CCA1 secure if DDHA and WKEA hold.*

Proof. The proof is the same as that for Theorem 7 except that a different approach is used to prove that $|\Pr[S_0]-\Pr[S_1]|$ and $|\Pr[S_1]-\Pr[S_2]|$ are negligible.

To show that $|\Pr[S_0]-\Pr[S_1]|$ is negligible, we construct the following D_1 to solve the DDH problem. D_1 receives a triple $(g^a,x,y)\in G^3$, then outputs 1 to indicate that $y=x^a$ or outputs 0 to indicate that $y\neq x^a$. Note that D_1 interacts with $A'=E(A)$ where A' and E are as defined in WKEA.

$D_1(g^a,x,y)$	Messages	A'
1. $b \xleftarrow{R} \mathbb{Z}_q, u\leftarrow g^a, v\leftarrow g^b$	$\xrightarrow{g,u,v}$	
Repeat 2 - 5 n times:		
2.	$\xleftarrow{e_i,x_i,y_i,z_i}$	
3. if $e_i=1$ 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. $d \xleftarrow{R} \{0,1\}, z'\leftarrow x^b, z\leftarrow {m'}_d z'$		
8.	$\xrightarrow{x,y,z}$	
9.	$\xleftarrow{d'}$	
10. if $d'=d$ then return 1		
11. else return 0		

D_1 checks if $y_i={x_i}^a$ by checking if $e_i=1$. By WKEA, in each round, D_1 makes the correct decision with probability greater than $1-\epsilon_{wkea}$. If D_1 makes the correct decision in all n rounds, then the computation of A' proceeds the same way as A in Game 0 when $y=x^a$, and it proceeds the same way as A in Game 1 when $y\xleftarrow{R} G$ (here we overlook the difference between $y\neq x^a$ and $y\xleftarrow{R} G$ for simplicity). Therefore,

$$|\Pr[D_1=1|(y\leftarrow x^a)] - \Pr[S_0]| \leq 1-(1-\epsilon_{wkea})^n$$

and

$$\left|\Pr\left[D_1 = 1|(y \xleftarrow{R} G)\right] - \Pr\left[S_1\right]\right| \leq 1 - (1 - \epsilon_{wkea})^n.$$

It follows that

$$\begin{aligned}|\Pr[S_0] - \Pr[S_1]| &\leq 2\left(1 - (1 - \epsilon_{wkea})^n\right) + \left|\Pr[D_1 = 1|(y \leftarrow x^a)] - \Pr\left[D_1 = 1|(y \xleftarrow{R} G)\right]\right| \\ &= 2\left(1 - (1 - \epsilon_{wkea})^n\right) + Adv_{ddh}^{D_1}.\end{aligned}$$

Note n is polynomial in k. If WKEA holds, then ϵ_{wkea} is negligible in k and $\lim_{k\to\infty} n\epsilon_{wkea} = 0$. We have that

$$\begin{aligned}\lim_{k\to\infty} 2(1 - (1 - \epsilon_{wkea})^n) &= \lim_{k\to\infty} 2\left(1 - \left(1 - \frac{1}{\frac{1}{\epsilon_{wkea}}}\right)^{\frac{1}{\epsilon_{wkea}} n\epsilon_{wkea}}\right) \\ &= \lim_{k\to\infty} 2\left(1 - \left(\frac{1}{e}\right)^{n\epsilon_{wkea}}\right) \\ &= 0.\end{aligned}$$

Therefore, $|\Pr[S_0] - \Pr[S_1]|$ is negligible if WKEA and DDH hold.

To show that $|\Pr[S_1] - \Pr[S_2]|$ is negligible, we construct the following algorithm D_2 to solve the DDH problem. D_2 is given a triple $(g^a, x, z') \in G^3$, and outputs 1 to indicate that $z' = x^a$ or outputs 0 to indicate that $z' \neq x^a$.

$D_2(g^a, x, z')$	Messages	A'
1. $c \xleftarrow{R} \mathbb{Z}_q, u \leftarrow g^a, v \leftarrow u^c$	$\xrightarrow{g, u, v}$	
Repeat 2 - 5 n times:		
2.	$\xleftarrow{e_i, x_i, y_i, z_i}$	
3. if $e_i = 1$ 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. $d \xleftarrow{R} \{0,1\}, y \xleftarrow{R} G, z \leftarrow m'_d {z'}^c$		
8.	$\xrightarrow{x, y, z}$	
9.	$\xleftarrow{d'}$	
10. if $d' = d$ then return 1		
11. else return 0		

Using the same approach as in the case of D_1, we can show that

$$|\Pr[S_1] - \Pr[S_2]| \leq 2\left(1 - (1 - \epsilon_{wkea})^n\right) + Adv_{ddh}^{D_2}$$

which is negligible if WKEA and DDH holds. □

The above results suggest that KEA is stronger than necessary in the security proof of DEG, for which KEA was originally proposed for.

4 Conclusion

In this paper, we showed that the ElGamal encryption is OW-CCA1 under the generalized knowledge-of-exponent assumption (GKEA) and the one-more discrete log assumption (OMDLA), and its security is equivalent to the hardness of the one-more computational Diffie-Hellman (OMCDH) problem. For DEG, we gave a simple proof that DEG is IND-CCA1 secure under the one-more decisional Diffie-Hellman assumption. We also gave a proof that DEG is IND-CCA1 secure under the DDH assumption and a weaker version of the knowledge-of-exponent assumption (WKEA), which suggests that KEA is stronger than necessary for the security proof of DEG, for which KEA was originally proposed.

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. GQ and Schnorr identification schemes: proofs of security against impersonation under active and concurrent attacks. In *CRYPTO 2002 Proceedings*, volume 2442 of *Lecture Notes in Computer Science*. Springer, 2002.
3. 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.
4. 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.
5. D. Freeman. Pairing-based identification schemes. Cryptology ePrint Archive, Report 2005/336, 2005. http://eprint.iacr.org/.
6. T. El Gamal. 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.
7. 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.
8. N. Koblitz and A. Menezes. Another look at non-standard discrete log and Diffie-Hellman problems. Cryptology ePrint Archive, Report 2007/442, 2007. http://eprint.iacr.org/.
9. V. Shoup. Sequences of games: a tool for taming complexity in security proofs. Cryptology ePrint Archive, Report 2004/332, 2004. http://eprint.iacr.org/.
10. 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.
11. J. Wu and D.R. Stinson. Efficient identification protocols and the knowledge-of-exponent assumption. Cryptology ePrint Archive, Report 2007/479, 2007. http://eprint.iacr.org/.