mathematics

MDPI

Article

A Security-Mediated Encryption Scheme Based on ElGamal Variant

Boon Chian Tea [1,†], Muhammad Rezal Kamel Ariffin [1,*,†], Amir Hamzah Abd. Ghafar [1,2,†] and Muhammad Asyraf Asbullah [1,3,†]

[1] Institute for Mathematical Research (INSPEM), Universiti Putra Malaysia, Serdang 43400 UPM, Malaysia; gs48109@student.upm.edu.my (B.C.T.); amir_hamzah@upm.edu.my (A.H.A.G.); ma_asyraf@upm.edu.my (M.A.A.)
[2] Department of Mathematics and Statistics, Faculty of Science, Universiti Putra Malaysia, Serdang 43400 UPM, Malaysia
[3] Centre of Foundation Studies for Agricultural Science, Universiti Putra Malaysia, Serdang 43400 UPM, Malaysia
* Correspondence: rezal@upm.edu.my; Tel.: +603-9769-6838
† These authors contributed equally to this work.

Abstract: Boneh et al. introduced mediated RSA (mRSA) in 2001 in an attempt to achieve faster key revocation for medium-sized organizations via the involvement of a security mediator (SEM) as a semi-trusted third party to provide partial ciphertext decryption for the receiver. In this paper, a pairing-free security mediated encryption scheme based on an ElGamal variant is proposed. The scheme features a similar setting as in the mediated RSA but with a different underlying primitive. We show that the proposed security mediated encryption scheme is secure indistinguishably against chosen-ciphertext attack (IND-CCA) in the random oracle via the hardness assumption of the computational Diffie-Hellman (CDH) problem.

Keywords: computational diffie-hellman problem; EIGamal variant; encryption; fast revocation; pairing-free security mediated encryption scheme; security mediator

Citation: Tea, B.C.; Kamel Ariffin, M.R.; Abd. Ghafar, A.H.; Asbullah, M.A. A Security-Mediated Encryption Scheme Based on ElGamal Variant. *Mathematics* **2021**, *9*, 2642. https://doi.org/10.3390/math9212642

Academic Editors: Luis Hernández Encinas and Víctor Gayoso Martínez

Received: 25 August 2021
Accepted: 29 September 2021
Published: 20 October 2021

1. Introduction

In 2001, Boneh et al. proposed a fast key revocation scheme—the mediated RSA (mRSA). This scheme features a new semi-trusted role, the security mediator (SEM), which takes part in the decryption process. The idea behind this mediated scheme is that the user's secret key is effectively split into two parts, with one kept by SEM and the remaining one by the user. Whenever the user receives a ciphertext, he must relay it to SEM for partial decryption (token issuance) prior to recovering the full plaintext [1]. This property provides an advantage of instant revocation upon the certificate authority (CA) instructions. The SEM will stop assisting in the user's partial ciphertext decryption, not only to decrypt ciphertext received in the future, but also to re-decrypt the ciphertext that has been received and decrypted previously.

The introduction of mRSA has initiated various security mediated schemes following this path such as the IB-mRSA/OAEP, a type of identity-based encryption (IBE) scheme proposed by Ding and Tsudik in 2003 based on mRSA [2]. The designed IB-mRSA/OAEP is proven to be secure indistinguishably against adaptive chosen-ciphertext attack (IND-CCA) in the random oracle model. To this end, the authors stated that the security proof in the standard model remains an open problem.

Chow et al. then introduced the notion of security mediated certificateless (SMC) cryptography in 2006 that provides the solution to the key escrow problem described in other security mediated schemes [3]. Besides generalizing the framework of SMC, they also provided a lightweight version of SMC cryptography that is fully adaptive chosen-ciphertext attack secure in the random oracle model via the intractability assumption

of bilinear Diffie-Hellman (BDH) problem. In addition, Chow et al. claimed that their proposal is more efficient than Baek and Zheng's ID-based mediated encryption scheme [4].

Following the trend of SMC cryptography by Chow et al., Yap et al. subsequently explored the notion of SMC signature. They proposed the very first concrete provable secure SMC signature scheme that is bilinear pairing-free. Based on the intractability assumption of the discrete logarithm problem (DLP), their scheme is proven to be existentially unforgeable under chosen message attack (EUF-CMA) in the random oracle mode [5]. In the same year, Yang et al. [6] and Lo et al. [7] came out with efficient certificateless pairing-free encryption schemes and mediated revocation-free encryption schemes respectively. Unfortunately, both the proposed schemes suffered from partial decryption attacks as demonstrated in [8]. Wan et al. also proposed a similar efficient pairing-free SMC signature scheme, but with proof of security in the random oracle model based on the hardness assumption of factoring [9].

While the majority of follow-ups focus on mediated IBE and signature schemes, Chin et al. in 2013 devised the first efficient security mediated identity-based identification (SM-IBI) scheme. Via the computational Diffie-Hellman (CDH) assumption, they provided the security proof against impersonation under passive, active and concurrent attacks in the random oracle model [10]. In the following year, Chin et al. further improved the efficiency of the SM-IBI scheme by proposing two pairing-free versions via the intractability of RSA and discrete logarithm assumptions, with security proofs against impersonation under passive, active and concurrent attacks both in the random oracle models [11].

In this paper, we propose a new security mediated encryption scheme based on an IND-CCA secure ElGamal variant. The motivation of our work is based on current existing non-certificateless mediated schemes by Boneh et al. [1]. We consider the IND-CCA-secure ElGamal encryption scheme designed by [12] and prove that our scheme is secure indistinguishably against chosen-ciphertext attack (IND-CCA) in the random oracle model via the hardness assumption of the computational Diffie-Hellman (CDH) problem.

The rest of the paper is organized as follows. Section 2 outlines necessary preliminaries, followed by a formal security model and definition of security mediated encryption scheme. In Section 3, the construction of a new security mediated encryption scheme based on an ElGamal variant is presented. Next, we provide the security proof of our designed scheme in Section 4. The analysis about the efficiency and performance proceedes in Section 5. Finally, we conclude our work in Section 6.

2. Preliminaries

We provide some mathematical and cryptographic backgrounds related to our work in this section, including mathematical hard problems, security mediated encryption scheme model, and corresponding security model. We note that the primary reference of our definitions in this section are due to [13], but similar definitions can be found in [14].

2.1. Computational Diffie-Hellman (CDH) Problem

Definition 1 (Computational Diffie-Hellman Problem [13])**.** *Let g be a generator for $\mathbb{G}_p$ and let h_1, h_2 be non-zero elements of $\mathbb{G}_p$. Define $DH_g(h_1, h_2) = g^{\log_g h_1 \cdot \log_g h_2}$. That is, if $h_1 = g^{x_1}$ and $h_2 = g^{x_2}$, then*

$$DH_g(h_1, h_2) = g^{x_1 \cdot x_2} = h_1^{x_2} = h_2^{x_1}. \quad (1)$$

The CDH problem is to compute $DH_g(h_1, h_2)$ for uniform h_1 and h_2.

2.2. Security Mediated Encryption Scheme

A generic security mediated encryption scheme consists of three probabilistic polynomial-time algorithms:

1. **KeyGen.** On input of security parameter 1^n, generates system parameters (Params), user's public key (pk), and user–SEM secret keys $(K_{\mathsf{user}}, K_{\mathsf{sem}})$.

2. **ENCRYPT.** Sender takes in Params, pk and message m, encrypts message into ciphertext $c = \text{ENC}(\text{Params}, \text{pk}, m)$.
3. **DECRYPT.** Receiver firstly relay ciphertext c to SEM for partial decryption $m_1 = \text{DEC}(c, K_{\text{sem}})$ meanwhile computing his own part $m_2 = \text{DEC}(c, K_{\text{user}})$. Finally, receiver performs full decryption to recover message $m = m_1 * m_2$, where $*$ represents necessary operation according to different scheme's setting.

2.3. Security Model of Security Mediated Encryption Scheme

The following defines the IND-CCA security game corresponds to the security mediated encryption scheme above.

1. **Setup.** On input of security parameter 1^n, challenger $\mathcal{B}$ adapts and runs **KEYGEN** of the encryption scheme to generate $\{\text{Params}, \text{pk}, K_{\text{user}}, K_{\text{sem}}\}$. $\mathcal{B}$ provides adversary $\mathcal{A}$ with $\{\text{Params}, \text{pk}\}$ and retains the $\{K_{\text{user}}, K_{\text{sem}}\}$.
2. **Phase 1 (Decryption query).** The following queries may be asked adaptively.
   (a) SEM-Decryption: $\mathcal{A}$ queries SEM-decryption for the ciphertext C of his choice. $\mathcal{B}$ responds with the corresponding SEM's partial decryption to $\mathcal{A}$.
   (b) Full Decryption: $\mathcal{A}$ queries full decryption for the ciphertext C of his choice. $\mathcal{B}$ responds with decrypted plaintext m to $\mathcal{A}$.
3. **Challenge.** $\mathcal{A}$ produces two messages $\{m_0, m_1\}$ of equal length to be challenged. $\mathcal{B}$ randomly picks $b \in \{0, 1\}$ and outputs challenge ciphertext $C^* = \text{ENC}(\text{Params}, \text{pk}, m_b)$ to $\mathcal{A}$.
4. **Phase 2.** $\mathcal{A}$ may perform decryption queries for the ciphertext C of his choice as in **Phase 1**, except the challenge ciphertext C^*.
5. **Guess.** $\mathcal{A}$ output a guess of b', ending the simulation. $\mathcal{A}$ wins if $b' = b$.

Definition 2 (Indistinguishability against Chosen-Ciphertext Attack (IND-CCA) [13])**.** *A public-key encryption scheme* (PKE) *is said to be IND-CCA secure if the guessing advantage of a probabilistic polynomial-time (PPT)* $\mathcal{A}$*,* $\text{Adv}[\mathcal{A}]$ *is negligible. That is,*

$$\text{Adv}[\mathcal{A}] = \left| \Pr\left[\text{PKE}_{\mathcal{A}}^{ind\text{-}cca}(n) = 1\right] - \frac{1}{2} \right| \leq \varepsilon. \tag{2}$$

3. The Proposed Security Mediated ElGamal Encryption Scheme

We now describe the design of our security mediated encryption scheme based on the IND-CCA-secure ElGamal variant proposed by [12]. Our design involves some structural modifications in order to fit the concept of the security mediated cryptography. Hereafter, we use mediated ElGamal scheme (or abbreviated as mEG) to denote the proposed security mediated encryption scheme. We point out some highlights of our proposed mediated ElGamal scheme below.

1. The user's public key (abbreviated as mpk) X in the **KEYGEN** Algorithm 1 is generated by CA using the user's random master secret key (abbreviated as msk) x which is unknown to anyone except CA itself.
2. Next, the secret key x is split into two parts and sent securely to the user and SEM respectively as their decryption key.
3. Any party who wishes to initiate communication shall obtain the user's public key X from a public directory as part of the encryption procedure.

We now present the full mediated ElGamal scheme as follows. The Algorithm 1 of Key Generation describes the initial setting of system parameters including the public-private key pair, Algorithm 2 outlines the encryption procedures between sender and receiver, and Algorithm 3 shows the decryption of both SEM and receiver upon receiving the ciphertext.

Algorithm 1 Key Generation (**KeyGen**) of mEG

Require: Security parameter 1^n.

Ensure: System parameters $\{p, q, g, \hat{e}, \mathbb{G}_1, \mathbb{G}_2, H_1, H_2, H_3, H_4\}$, user's public key X, user's secret key x, user's decryption key x_{user}, and SEM's decryption key x_{sem}.

1: On input of security parameter 1^n, generates two large primes p, q with $|p| = |q| = n$, a generator g such that $\langle g \rangle = \mathbb{Z}_p^*$, and two groups $\mathbb{G}_1, \mathbb{G}_2$ of order q.

2: Generates the following pairing function $\hat{e}$ and hash functions H such that:

(a) $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$,
(b) $H_1 : \{0,1\}^n \times \mathbb{Z}_p^* \to \mathbb{Z}_p^*$,
(c) $H_2 : \mathbb{Z}_p^* \to \{0,1\}^n$,
(d) $H_3 : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$,
(e) $H_4 : \mathbb{Z}_p^* \times \{0,1\}^n \times \mathbb{Z}_p^* \to \mathbb{Z}_p^*$.

3: For each user i, computes $X_i \equiv g^{x_i} \pmod{p}$ for a random integer $x_i \in \mathbb{Z}_p^*$.

4: Randomly selects $x_{\mathsf{user}_i} \in \mathbb{Z}_p^*$ and computes $x_{\mathsf{sem}} \equiv x_i - x_{\mathsf{user}_i} \pmod{p-1}$.

5: Publish system parameters $\{p, q, g, \hat{e}, \mathbb{G}_1, \mathbb{G}_2, H_1, H_2, H_3, H_4\}$ and user i's mpk X_i, sends user i's decryption key x_{user_i} to user i and SEM's decryption key x_{sem} to SEM.

6: The integer x_i which is user i's secret key, is kept secret.

Algorithm 2 Encryption (**Encrypt**) of mEG

Require: System parameters $\{p, q, g, \hat{e}, \mathbb{G}_1, \mathbb{G}_2, H_1, H_2, H_3, H_4\}$, user's public key X, user's decryption key x_{user} and message m.

Ensure: Ciphertext $\{c_1, c_2, h_2, h_3, Y_i\}$.

1: User i who wishes to communicate will compute and publish his public key $Y_i \equiv g^{x_{\mathsf{user}_i}} \pmod{p}$ using his decryption key x_{user_i}.

2: Sender who wishes to send message m to user i obtains X_i and perform following computations:

(a) Selects a random string $\sigma \in \{0,1\}^n$ and computes $r = H_1(\sigma \parallel Y_i)$,
(b) Computes $c_1 \equiv g^r \pmod{p}$ and next $h_1 = H_2\left(X_i^r\right)$,
(c) Set $M = \sigma \parallel m$, and compute $h_2 = H_3(M)$,
(d) Computes $c_2 = M \oplus h_1$.
(e) Computes $h_3 = H_4(c_1, c_2, Y_i)^r$.

3: Sends ciphertext $C = \{c_1, c_2, h_2, h_3, Y_i\}$ to user i.

Algorithm 3 Decryption (**Decrypt**) of mEG

Require: System parameters $\{p, q, g, \hat{e}, \mathbb{G}_1, \mathbb{G}_2, H_1, H_2, H_3, H_4\}$, user's public key X, user's public key Y, user's decryption key x_{user}, SEM's decryption key x_{sem} and ciphertext $C = \{c_1, c_2, h_2, h_3, Y_i\}$.

Ensure: Message m.

SEM-Decryption:

1: User i upon receiving ciphertext $C = \{c_1, c_2, h_2, h_3, Y_i\}$, relays it to SEM.

2: SEM checks whether $\hat{e}(g, h_3) = \hat{e}(c_1, H_4(c_1, c_2, Y_i))$. If it does, computes partial decryption $c_1^{x_{\mathsf{sem}}}$ and replies it to user i. Otherwise, it rejects ciphertext C.

User-Decryption:

1: User i receives partial decryption from SEM, and next compute the following series of computations to recover message m:

(a) Checks whether $\hat{e}(g, h_3) = \hat{e}(c_1, H_4(c_1, c_2, Y_i))$. If it does, then continue the decryption procedures. Otherwise, it rejects ciphertext C,
(b) Computes $c_1^{x_{\mathsf{sem}}} \cdot c_1^{x_{\mathsf{user}_i}}$, and next $h_1' = H_2\left(c_1^{x_{\mathsf{sem}}} \cdot c_1^{x_{\mathsf{user}_i}}\right)$,
(c) Computes $M' = c_2 \oplus h_1'$, and checks whether $h_2 = H_3(M')$. If it does, then parse message m from $\sigma \parallel m$. Otherwise, it rejects ciphertext C.

2: Lastly, computes $r' = H_1(\sigma \parallel Y_i)$, and verifies whether $c_1 = g^{r'} \pmod{p}$.

Proof of correctness. The correctness of the proposed mediated ElGamal scheme begins with the ciphertext validation by SEM, that is

$$\begin{aligned}\hat{e}(g, h_3) &= \hat{e}\left(g, H_4(c_1, c_2, Y_i)^r\right) \\ &= \hat{e}(g^r, H_4(c_1, c_2, Y_i)) \\ &= \hat{e}(c_1, H_4(c_1, c_2, Y_i)).\end{aligned}$$

Next, one can easily verify the correctness of the combination of both the partial decryptions from SEM and user i respectively such that

$$\begin{aligned}c_1^{x_{\mathsf{sem}}} \cdot c_1^{x_{\mathsf{user}_i}} &= c_1^{x_{\mathsf{sem}} + x_{\mathsf{user}_i}} \\ &= c_1^{x_i} \\ &= g^{r x_i} \\ &= X_i^r\end{aligned}$$

so that $h_1 = H_2\left(X_i^r\right)$. Then, one can proceed with the decryption of $M = c_2 \oplus h_1$, followed by the verification of $h_2 = H_3(M)$. This next enables the extraction of σ and message m from the string of $\sigma \parallel m$ and finally checks whether $c_1 = g^{H_1(\sigma \| Y_i)}$. □

Remark 1. *As $\sigma \parallel m$ is the concatenation of σ and message m, while σ is of n-bit, it is possible for a user to extract σ and m efficiently from it for the next ciphertext c_1 integrity check.*

4. Security Proof of the Proposed Mediated ElGamal Scheme

We put forward in this section the indistinguishability against chosen-ciphertext attack (IND-CCA) security proof of our proposed mediated ElGamal scheme. Our proof is constructed based on the hardness assumption of solving the CDH problem.

Theorem 1. *Let mEG be the proposed mediated ElGamal scheme as described in Section 3, and $\mathcal{A}$ be a probabilistic polynomial-time (PPT) adversary that has access to mEG. Then the proposed mediated ElGamal scheme is secure indistinguishably against chosen-ciphertext attack (IND-CCA) in the random oracle model via assumption that solving the computational Diffie-Hellman (CDH) problem is hard. That is,*

$$\Pr\left[mEG_{\mathcal{A}}^{\mathsf{ind\text{-}cca}}(n) = 1\right] \leq \frac{1}{2} + \frac{\varepsilon}{q_{H_2}} + \frac{q_{H_1}}{p} + \frac{q_{H_3}}{2^{n-1}},$$

where ε denotes the negligible function, and q_{H_1}, q_{H_2} and q_{H_3} represent the number of H_1, H_2 and H_3 queries, respectively.

Proof. Suppose there exists an adversary $\mathcal{A}$ who can break the mediated ElGamal scheme, then we can construct a challenger $\mathcal{B}$ to solve the CDH problem. $\mathcal{B}$ is given the CDH instances of $\left(g, g^a, g^b\right)$ of cyclic group $\left\{\mathbb{Z}_p^*, p, g\right\}$, and modeled all H_1, H_2, H_3, H_4 as random oracles. We now describe the interaction between the challenger $\mathcal{B}$ and adversary $\mathcal{A}$ in the following game.

1. **Setup:** Challenger $\mathcal{B}$ initially takes on security parameter 1^n as input and runs **KeyGen** to output system parameters $\{p, q, g, \hat{e}, \mathbb{G}_1, \mathbb{G}_2, H_1, H_2, H_3, H_4\}$ and sets public key as $X = g^a$ where $a = x$. These system parameters and public key are sent to $\mathcal{A}$. Note that $\mathcal{B}$ does not know the secret integer x.
2. H**-query:** $\mathcal{B}$ prepares four different hash lists to record and store all the hash queries and responses. The lists are initially empty.
   (a) H_1-query: For any w_i query made, $\mathcal{B}$ checks if such query exist. If it does, it responds with the corresponding W_i. Otherwise, it randomly samples $W_i \leftarrow \mathbb{Z}_p^*$ and returns $H_1(w_i) = W_i$. Lastly, it adds (w_i, W_i) to the H_1-list.

(b) H_2-query: For any u_i query made, $\mathcal{B}$ checks if such query exist. If it does, it responds with the corresponding U_i. Otherwise, it randomly chooses $U_i \leftarrow \{0,1\}^n$ and returns $H_2(u_i) = U_i$. Lastly, it updates (u_i, U_i) to the H_2-list.

(c) H_3-query: For any v_i query made, $\mathcal{B}$ checks if such query exist. If it does, it responds with the corresponding V_i. Otherwise, it randomly chooses $V_i \leftarrow \{0,1\}^n$ and returns $H_3(v_i) = V_i$. Lastly, it adds (v_i, V_i) to the H_3-list.

(d) H_4-query: For any z_i query made, $\mathcal{B}$ checks if such query exist. If it does, it responds with the corresponding Z_i. Otherwise, it randomly samples $Z_i \leftarrow \mathbb{Z}_p^*$ and returns $H_4(z_i) = Z_i$. Lastly, it updates (z_i, Z_i) to the H_4-list.

3. **Phase 1 (Decryption query):**

(a) **SEM-Decryption query:** $\mathcal{A}$ queries the SEM-decryption of the ciphertext $C = \{c_1, c_2, h_2, h_3, Y_i\}$ of his choice. $\mathcal{B}$ firstly search through the H_1 and H_4-lists whether there exists the pairs of (w_i, W_i) and (z_i, Z_i) such that $c_1 = g^W$ and $\hat{e}(g, h_3) = \hat{e}(c_1, Z)$ are valid. If it does, it computes $\left(\frac{X}{Y_i}\right)^W$ as SEM's partial decryption and returns the SEM-Decryption result to $\mathcal{A}$. Otherwise, it returns $\perp$. Observe that

$$\begin{aligned} X &= g^x \\ &= g^{x_{\mathsf{sem}} + x_{\mathsf{user}_i}} \\ &= g^{x_{\mathsf{sem}}} \cdot g^{x_{\mathsf{user}_i}} \\ &= g^{x_{\mathsf{sem}}} \cdot Y_i. \end{aligned}$$

Then, $g^{x_{\mathsf{sem}}} = \frac{X}{Y_i}$ and

$$\left(\frac{X}{Y_i}\right)^W = (g^{x_{\mathsf{sem}}})^W = \left(g^W\right)^{x_{\mathsf{sem}}} = c_1^{x_{\mathsf{sem}}}$$

is a valid SEM's partial decryption in the simulation.

(b) **Full-Decryption query:** $\mathcal{A}$ queries the full decryption of the ciphertext $C = \{c_1, c_2, h_2, h_3, Y_i\}$ of his choice. $\mathcal{B}$ firstly search through all the H-lists whether there exists the pairs of $(w_i, W_i), (u_i, U_i), (v_i, V_i), (z_i, Z_i)$ such that

$$\begin{aligned} w &= \sigma \parallel Y_i \\ u &= X^W \\ v &= \sigma \parallel m \\ c_1 &= g^W \\ c_2 &= v \oplus U \\ \hat{e}(g, h_3) &= \hat{e}(c_1, Z). \end{aligned}$$

We consider the following possible scenarios:

i. **Case 1:** If all the above queries exists, it outputs and returns the corresponding m as decryption result.

ii. **Case 2:** Only (w_i, W_i), (v_i, V_i) and (z_i, Z_i) exist. Then $c_1 = g^W$ and $\hat{e}(g, h_3) = \hat{e}(c_1, Z)$ are valid. Also, by the knowledge of Y_i from C, $\mathcal{B}$ can extract σ from w and next to extract m from v. It can then compute $u = X^W$ and adds the new (u, U) query to the H_2-list. Note that it is easy to verify the validity of such additional query since by (v, V), $\mathcal{B}$ can invert $U = c_2 \oplus v$ to obtain U. If every query is valid, it returns m as decryption result, otherwise it returns $\perp$.

iii. **Case 3:** Only (w_i, W_i) and (z_i, Z_i) exist. Then $c_1 = g^W$ and $\hat{e}(g, h_3) = \hat{e}(c_1, Z)$ are valid. Also, by the knowledge of Y_i from C, $\mathcal{B}$ can extract

σ from w. It can next compute $u = X^W$ and samples a random U to updates both the new (u, U) and (v, V) queries to the H-lists. Note that it is easy to verify the validity of all such additional queries since by (u, U), $\mathcal{B}$ can invert $v = c_2 \oplus U$ to obtain v and sample a random V. In addition, the inverted v enables the extraction of m. If every query is valid, it returns m as decryption result, otherwise it returns $\perp$.

iv. **Case 4:** Only (w_i, W_i) exists. Then $c_1 = g^W$ is valid. Also, by the knowledge of Y_i from C, $\mathcal{B}$ can extract σ from w. It can next compute $u = X^W$ and samples a random U to updates all the new (u, U) and (v, V) and (z, Z) queries to the H-lists. Again, it is easy to decide the validity of all such additional queries since by (u, U), $\mathcal{B}$ can invert $v = c_2 \oplus U$ to obtain v and sample a random V. In addition, the inverted v enables the extraction of m. As for the query of (z, Z), $\mathcal{B}$ reverts $Z = h_3^{-W}$ and then samples z randomly, this is indistinguishable from the $\mathcal{A}$'s point of view. If every query is valid, it returns m as decryption result, otherwise it returns $\perp$.

v. **Case 5:** If none of the queries satisfy the ciphertext structures, it returns $\perp$.

4. **Challenge:** When $\mathcal{A}$ is ready to perform the attack, he sends two distinct messages of equal length $m_0, m_1 \in \{0,1\}^n$. $\mathcal{B}$ randomly selects bit $l \in \{0,1\}$, $\sigma^*, R_1, R_2 \in \{0,1\}^n$ and $Y^* \in \mathbb{Z}_p^*$. Next, it outputs challenge ciphertext C^* as

$$C^* = \left(g^b, R_1, h_2^*, R_2, Y^*\right), \tag{3}$$

where g^b is taken from the CDH instance. Observe that the challenge ciphertext could be treated as the encryption of message $m_l \in \{m_0, m_1\}$ using the random chosen string $\sigma^* \in \{0,1\}^n$ such that

(a) $b = H_1(\sigma^* \parallel Y^*)$,

(b) $R_1 = M \oplus H_2\left(X^b\right)$,

(c) $h_2^* = H_3(\sigma^* \parallel m_l)$,

(d) $R_2 = H_4\left(g^b, R_1, Y^*\right)^b$.

Hence, the challenge ciphertext C^* is a correct and valid ciphertext in the $\mathcal{A}$'s point of view if it does not query the following to random oracle:

$$\begin{aligned} u &= X^b \\ w &= \sigma^* \parallel Y^* \\ v &= \sigma^* \parallel m_l \\ z &= \left(g^b, R_1, Y^*\right). \end{aligned}$$

5. **Phase 2:** $\mathcal{A}$ is allowed to continue querying decryption of the ciphertext C of his choice, except the challenge ciphertext C^*.

6. **Guess:** $\mathcal{A}$ finally output his guess of l', ending the IND-CCA game. $\mathcal{A}$ wins the game if $l' = l$. Note that the challenge hash query is the Diffie-Hellman shared value $X^b = g^{ab}$ which is a query to the random oracle H_2. $\mathcal{B}$ randomly selects one of the queries $\left((u_1, U_1), ..., \left(u_{q_{H_2}}, U_{q_{H_2}}\right)\right)$ in H_2-list as the challenge hash query, and output the solution to the CDH problem.

It remains now to evaluate the advantage of the simulated game described above. We discuss the following two possible cases that could happen:

1. **Scenario 1.** If $\mathcal{A}$ does not query the challenge hash query $X^b = g^{ab}$, then the only alternative way that it could break the challenge ciphertext is to search for the existence of the following queries:

$$H_3(\sigma^* \parallel m_0) = h_2 \tag{4}$$

or

$$H_3(\sigma^* \parallel m_1) = h_2 \tag{5}$$

from the H_3-list; or

$$b \quad = \quad H_1(\sigma^* \parallel Y^*) \tag{6}$$

from H_1-list, which has the total negligible probability of $\left(\frac{q_{H_1}}{p} + \frac{2q_{H_3}}{2^n}\right)$, where q_{H_1}, q_{H_3} represents the total number of H_1 and H_3 queries, respectively.

2. **Scenario 2.** If $\mathcal{A}$ does query the challenge hash query $X^b = g^{ab}$, then it can gain advantage in guessing the encrypted message m_l correctly. Otherwise, it can only guess it with negligible advantage. As $\mathcal{A}$ has the advantage of ε in outputting the correct bit $l \in \{0, 1\}$ following the hardness assumption of breaking the CDH problem, such event could only occur if and only if the challenge hash query $X^b = g^{ab}$ exists in the H_2 list. Let q_{H_2} be the total number of H_2 queries in the simulated game, following the IND-CCA model, we have:

$$\mathrm{Adv}[\mathcal{A}] = \left|\Pr\left[\mathsf{mEG}_{\mathcal{A}}^{\mathsf{ind\text{-}cca}}(n) = 1\right] - \frac{1}{2}\right| \leq \frac{\varepsilon}{q_{H_2}}.$$

Putting both the above cases together, hence

$$\Pr\left[\mathsf{mEG}_{\mathcal{A}}^{\mathsf{ind\text{-}cca}}(n) = 1\right] \leq \frac{1}{2} + \frac{\varepsilon}{q_{H_2}} + \frac{q_{H_1}}{p} + \frac{q_{H_3}}{2^{n-1}}.$$

This completes the proof of security of the proposed mediated ElGamal scheme. □

5. Efficiency and Performance Analysis

We discuss the efficiency and performance about the proposed mediated ElGamal encryption scheme in Section 3. We emphasize a few important points based on our proposal as follows:

1. **Key escrow.** Our proposed mediated ElGamal scheme currently does not consider the issue of key escrow. In other words, our scheme suffered from key escrow problem, in which the CA has absolute control of the user's secret key. Therefore, we assume that CA is not compromise-able and is wholly trusted. We will address this issue in the subsequent work.
2. **Non-certificateless.** Our proposed mediated ElGamal scheme is not certificateless as in the SMC by [3]. In other words, users' public keys will need to be submitted to CA for authentication.
3. **Integrity.** As we apply the Fujisaki-Okamoto transformation in our design, the proposed mediated ElGamal scheme does provide ciphertext integrity checks either on the SEM side, or on the receiver side on top of ensuring confidentiality of the encrypted message.
4. **Pairing-free.** Unlike some other mediated encryption schemes, our mediated ElGamal scheme is pairing-free in the sense that we do not involve pairing computations in the encryption and decryption. One can observe easily that the pairing function in our scheme only serves to provide ciphertext validity check by SEM and the receiver. Hence, our scheme does not suffer from major efficiency and cost-computation drawbacks.

5. **Novelty.** Current security mediated cryptography focuses on ID-based, signature schemes, or is mostly designed based on pairing functions. Our proposed mediated ElGamal scheme on the other hand, utilized the ElGamal variant as our primitive and is also pairing-free in the encryption and decryption.

The overall computational efficiency of our proposed mediated ElGamal scheme is presented in Table 1 below.

Table 1. Computational Efficiency of The Proposed Mediated ElGamal Encryption Scheme.

Operation	X-OR	Subtraction/ Multiplication	Exponentiation	Hashing	Pairing
Key Generation	0	1	1	0	0
Encryption	1	0	4	4	0
SEM-Decryption	0	0	1	1	2
User-Decryption	1	1	2	4	2

Next, we summarize the performances of the current existing mediated encryption schemes, including both the traditional and IBE types in the following Table 2. We excluded the ciphertext validity check upon receiving the ciphertext tuple by either SEM or user in this summary, as some mediated schemes (i.e., in [6,7]) do not provide such computations in their original proposal.

In this Table 2, 'Exp' denotes exponentiation, 'Mul' indicates multiplication, '$\oplus$' represents exclusive-OR, 'H' denotes hash, and 'P' means pairing.

Table 2. Computation Performance of Security Mediated Encryption Schemes.

Scheme	Type	ENCRYPT	SEM-DECRYPT	User-DECRYPT	Pairing-Free	Certificate-Less	Escrow Freeness
mRSA [1]	Enc	1 Exp	1 Exp	1 Exp, 1 Mul	Yes	No	No
Our Scheme	Enc	4 Exp, 1 $\oplus$, 4 H	1 Exp	2 Exp, 1 Mul, 1 $\oplus$, 3 H	Yes	No	No
SMC [3]	IBE	3 Exp, 1 P, 1 H	3 P, 1 H	2 Mul, 1 $\oplus$, 2 H	No	Yes	Yes
MCL-PKE [6]	IBE	3 Exp, 1 Mul, 3 $\oplus$, 4 H	1 Exp, 1 H	2 Exp, 3 $\oplus$, 3 H	Yes	Yes	Yes
mRFPKE [7]	IBE	1 Exp, 1 Mul, 2 $\oplus$, 4 H, 2 P	1 P	2 Mul, 2 $\oplus$, 3 H, 1 P	No	Yes	Yes

Algebraically, our proposed mediated ElGamal scheme utilizes different primitive and at a glance, the performance is somewhat undesirable compared to mRSA [1]. Such occurrence is due to the Fujisaki-Okamoto transformation in the IND-CCA ElGamal variant, which is not required in mRSA.

Observe that the SEM that operates on the central server has the most extensive operational overhead upon deployment. This is because it caters to all the communication interactions. On the other hand, encryption and user-decryption occur at individual sites and occurs once in a while. One can assume long intervals of inactivity when compared to the server site.

In the context of cryptographic deployment, the current recommended key length required by RSA to achieve 128-bit security is 2048 bits and 1024 bits for discrete logarithm based cryptographic schemes. Hence, our scheme is notably better suited for high volume

communication than the pairing-free scheme mRSA.The high volume of operations at the server site is much more efficient via our scheme than mRSA.

For the security mediated IBE schemes, although MCL-PKE [6] gives better efficiency as it is pairing-free, only SMC [3] withstands various cryptanalysis and remain secure among the three. Both MCL-PKE [6] and mRFPKE [7] were broken under a partial decryption attack. Nonetheless, all these three mediated IBE schemes achieved certificateless property and are key-escrow free. On a non-apple-to-apple comparison between our pairing-free with pairing-based schemes, it is evident that our scheme performs better than the discrete logarithm scheme MCL-PKE. Our design has significantly fewer operations in each process. Moreover, further research on our scheme would strive towards certificateless and escrow freeness properties as in MCL-PKE [6].

6. Conclusions

In this paper, a new mediated encryption scheme based on the ElGamal variant is proposed and proved to be IND-CCA secure via the hardness assumption of the computational Diffie-Hellman problem. As this is our first attempt to utilize another well-known primitive in proposing a mediated encryption scheme, it exhibits the key-escrow problem and lack of certificateless property. Our next objective is to provide an overall mediated encryption scheme, resolving all the weaknesses addressed above. Our scheme can easily be transformed into an elliptic curve and pairing-based settings via the hardness assumption of the elliptic curve Diffie-Hellman (ECDH) and bilinear Diffie-Hellman (BDH) problems, respectively. Finally, we expect various schemes to be designed in the future based on the ElGamal variant, such as mediated IBE, signature, IBI, and certificateless-type schemes like those in the existing literature.

Author Contributions: Conceptualization, B.C.T. and M.R.K.A.; methodology, B.C.T. and M.R.K.A.; validation, M.R.K.A.; formal analysis, B.C.T.; investigation, B.C.T., M.R.K.A., A.H.A.G. and M.A.A.; resources, M.R.K.A.; writing—original draft preparation, B.C.T.; writing—review and editing, B.C.T., M.R.K.A., A.H.A.G. and M.A.A.; visualization, B.C.T., M.R.K.A., A.H.A.G. and M.A.A.; supervision, M.R.K.A.; project administration, M.R.K.A.; funding acquisition, M.R.K.A. All authors have read and agreed to the published version of the manuscript.

Funding: The present research was partially supported by the Universiti Putra Malaysia Grant with Project Number GP-IPS/2018/9657300.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The first author would like to further express appreciation to the Institute for Mathematical Research (INSPEM), Universiti Putra Malaysia (UPM) and Ministry of Higher Education (MOHE) for giving the opportunity to conduct this research.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

BDH	Bilinear Diffie-Hellman
CA	Certificate Authority
CDH	Computational Diffie-Hellman
DLP	Discrete Logarithm Problem
ECDH	Elliptic Curve Diffie-Hellman
EUF-CMA	Existential Unforgeable under Chosen-Message Attack

IBE	Identity-Based Encryption
IB-mRSA/OAEP	Identity-Based Mediated Rivest-Shamir-Adleman/ Optimal Asymmetric Encryption Padding
IND-CCA	Indistinguishable against Chosen-Ciphertext Attack
mEG	Mediated ElGamal
mpk	User's Public Key
mRSA	Mediated Rivest-Shamir-Adleman
msk	Master Secret Key
PKE	Public-Key Encryption
PPT	Probabilistic Polynomial Time
RSA	Rivest-Shamir-Adleman
SEM	Security Mediator
SMC	Security Mediated Certificateless
SM-IBI	Security Mediated Identity-Based Identification
X-OR	Exclusive-OR

References

1. Boneh, D.; Ding, X.; Tsudik, G.; Wong, C.M. A Method for Fast Revocation of Public Key Certificates and Security Capabilities. In Proceedings of the 10th Conference on USENIX Security Symposium, Washington, DC, USA, 13–17 August 2001.
2. Ding, X.; Tsudik, G. Simple Identity-Based Cryptography with Mediated RSA. In *Topics in Cryptology-CT-RSA 2003*; Lecture Notes in Computer Science; Joye, M., Ed.; Springer: Berlin/Heidelberg, Germany, 2003; Volume 2612, pp. 193–210.
3. Chow, S.S.M.; Boyd, C.; Nieto, J.M.G. Security-Mediated Certificateless Cryptography. In *Public Key Cryptography, PKC 2006*; Lecture Notes in Computer Science; Yung, M., Dodis, Y., Kiayias, A., Malkin, T., Eds.; Springer: Berlin/Heidelberg, Germany, 2006; Volume 3958, pp. 508–524.
4. Baek, J.; Zheng, Y. Identity-based Threshold Decryption. In *PKC 2004*; Lecture Notes in Computer Science; Bao, F., Deng, R., Zhou, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; Volume 2947, pp. 262–276.
5. Yap, W.S.; Chow, S.S.M.; Heng, S.H.; Goi, B.M. Security Mediated Certificateless Signatures. In *Applied Cryptography and Network Security*; Katz, J., Yung, M., Eds.; ACNS 2007; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2007; Volume 4521, pp. 459–477.
6. Yang, C.; Wang, F.; Wang, X. Efficient Mediated Certificateless Public-Key Encryption Scheme without Pairings. In Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), Niagara Falls, ON, Canada, 21–23 May 2007; pp. 109–112.
7. Lo, C.M.; Hwang, T.; Li, C.M. Revocation-Free Public-Key Encryption Based on Security-Mediated Public-Key Infrastructure. *Iet Inf. Secur.* **2007**, *1*, 134–141. [CrossRef]
8. Chow, S.S.M.; Yap, W.-S. Partial Decryption Attacks in Security-Mediated Certificateless Encryption. *IET Inf. Secur.* **2009**, *3*, 148–151. [CrossRef]
9. Wan, Z.; Weng, J.; Li, J. Security Mediated Certificateless Signatures without Pairing. *J. Comput.* **2010**, *5*, 1862–1869. [CrossRef]
10. Chin, J.J.; Behnia, R.; Heng, S.H.; Phan, R.C.W. An Efficient and Provable Secure Security-Mediated Identity-Based Identification Scheme. In Proceedings of the 2013 Eighth Asia Joint Conference on Information Security, Seoul, Korea, 25–26 July 2013; pp. 27–32.
11. Chin, J.J.; Tan, S.Y.; Heng, S.H.; Phan, R.C. Efficient and provable secure pairing-free security-mediated identity-based identification schemes. *Sci. World J.* **2014**, *2014*, 170906.
12. Asbullah, M.A.; Ariffin, M.R.K. A proposed CCA-secure encryption on an ElGamal variant. In Proceedings of the 2012 7th International Conference on Computing and Convergence Technology (ICCCT), Seoul, Korea, 3–5 December 2012; pp. 499–503.
13. Katz, L.; Lindell, Y. *Introduction to Modern Cryptography*; CRC Press: Boca Raton, FL, USA, 2015.
14. Lecture Notes: Introduction to Modern Cryptography. Available online: https://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf (accessed on 14 September 2021).