

Commutative-like Encryption: A New Characterization of ElGamal

DAI Wei *

Abstract

Commutative encryption is a useful but rather strict notion in cryptography. In this paper, we define a loose variation of commutative encryption-commutative-like encryption and give an example: the generalization of ElGamal scheme. The application of the new variation is also discussed.

Key words. ElGamal, commutative-like encryption, re-encryption.

1. Introduction

Informally, a commutative encryption is a pair of encryption functions f and g such that $f(g(v)) = g(f(v))$. Commutative encryption is extremely useful in modern cryptography since many protocols rely on the existence of commutative encryption[1, 2, 3, 4]. However, few encryption schemes are known to be commutative. In this paper, we introduce a loose notion of “commutative-like encryption” and propose a primitive: the generalization of ElGamal. First introduced by ElGamal[5], the ElGamal encryption is one of the most famous public key encryption schemes and has various applications[6, 7, 8]. Based on ElGamal encryption, this new characterization shares most advantages of commutative encryption and ElGamal while the definition itself is not as strict as commutative encryption.

2. Preliminaries

We first describe some relevant definitions that would be used in the paper.

2.1. Commutative encryption

Our definition of commutative encryption below is similar to the constructions used in [9, 10] and others. As showed above, a commutative encryption is a pair of encryption functions f and g such that $f(g(v)) = g(f(v))$. Thus by using the combination $f(g(v))$ to encrypt v , we can ensure that \mathcal{R} cannot compute the encryption of a value without the help of \mathcal{S} . In addition, even though the encryption is a combination of two functions, each party can apply their function first and still get the same result.

DEFINITION 1 (Indistinguishability). *Let $\Omega_k \subseteq \{0, 1\}^k$ be a finite domain of k -bit numbers. Let $\mathcal{D}_1 = \mathcal{D}_1(\Omega_k)$ and $\mathcal{D}_2 = \mathcal{D}_2(\Omega_k)$ be distributions over Ω_k . Let $A_k(x)$ be an algorithm that, given $x \in \Omega_k$, returns either true or false. We define distribution \mathcal{D}_1 of random variable $x \in \Omega_k$ to be computationally indistinguishable from distribution \mathcal{D}_2 if for any family of polynomial-step (w.r.t. k) algorithms $A_k(x)$, any positive polynomial $p(\cdot)$, and all sufficiently large k ,*

$$|\Pr[A_k(x)|x \sim \mathcal{D}_1] - \Pr[A_k(x)|x \sim \mathcal{D}_2]| < \frac{1}{p(k)}$$

*DAI Wei is at department of computer science and technology, Tsinghua University.

where $x \sim D$ denotes that x is distributed according to D , and $\Pr[A_k(x)]$ is the probability that $A_k(x)$ returns true.

Throughout this paper, we will use “indistinguishable” as shorthand for “computationally indistinguishable”.

DEFINITION 2 (Commutative Encryption). *A commutative encryption \mathcal{F} is a computable (in polynomial time) function $f : \text{Key } \mathcal{F} \times \text{Dom } \mathcal{F} \rightarrow \text{Dom } \mathcal{F}$, defined on finite computable domains, that satisfies all properties listed below. We denote $f_e(x) = f(e, x)$, and use “ \in_r ” to mean “is chosen uniformly at random from”.*

1. *Commutative. For all $e, e' \in \text{Key } \mathcal{F}$ we have*

$$f_e \circ f_{e'} = f_{e'} \circ f_e$$

2. *Each $f_e : \text{Dom } \mathcal{F} \rightarrow \text{Dom } \mathcal{F}$ is a bijection.*
3. *The inverse f_e^{-1} is also computable in polynomial-time given e .*
4. *The distribution of $\langle x, f_e(x), y, f_e(y) \rangle$ is indistinguishable from the distribution of $\langle x, f_e(x), y, z \rangle$, where $x, y, z \in_r \text{Dom } \mathcal{F}$ and $e \in_r \text{Key } \mathcal{F}$.*

2.2. ElGamal encryption

We define the ElGamal public-key encryption scheme. The ElGamal encryption scheme is based on the Diffie-Hellman assumption and it is a probabilistic encryption scheme, i.e., a specific message has many-exponential in the security parameter-possible encryptions. Formally,

DEFINITION 3 (ElGamal Public-Key Encryption Scheme[5, 11]) *The ElGamal public key encryption scheme is defined by a triplet (G, E, D) of probabilistic polynomial time algorithms, with the following properties:*

- *The system setup algorithm, \mathcal{S} , on input 1^n , where n is the security parameter, outputs the system parameters (P, Q, g) , where (P, Q, g) is an instance of the DLP collection, i.e., P is a uniformly chosen prime of length $P = n + \delta$ for a specified constant δ , and g is a uniformly chosen generator of the subgroup G_Q of prime order Q of Z_P^* , where $Q = (P - 1)/\gamma$ is prime and γ is a specified small integer.*
- *The key generating algorithm, G , on input (P, Q, g) , outputs a public key, $e = (P, Q, g, y)$, and a private key, $d = (P, Q, g, x)$, where $x \in_r Z_Q$, and $y \equiv g^x \pmod{P}$.*
- *The encryption algorithm, E , on input (P, Q, g, y) and a message $m \in G_Q$, uniformly selects an element $k \in_r Z_Q$ and outputs*

$$E((P, Q, g, y), m) = (g^k \pmod{P}, my^k \pmod{P})$$

- *The decryption algorithm, D , on input (P, Q, g, x) and a ciphertext (y_1, y_2) , outputs*

$$D((P, g, x), (y_1, y_2)) = y_2(y_1^x)^{-1} \pmod{P}$$

3. Re-encryption

In this section, we present a re-encryption algorithm of ElGamal. Unlike most other schemes, using ElGamal encryption we obtain ciphertext (y_1, y_2) , in this re-encryption algorithm, we need not to encrypt y_1 and y_2 respectively, details follow (to simplify the description, we still use the terms defined in the previous section):

- *To encrypt the plaintext m (i.e., the “first” encryption step), we use the ElGamal scheme:*
 - *Key generation: Let x_A be the element uniformly chosen from Z_Q , and $y_A \equiv g^{x_A} \pmod{P}$.*

- *Encryption:* On input (P, Q, g, y_A) and a message (plaintext) $m \in G_Q$, uniformly selects an element $k_A \in_r Z_Q$ and outputs

$$E((P, Q, g, y_A), m) = (g^{k_A} \pmod{P}, my_A^{k_A} \pmod{P})$$

- *To re-encrypt the plaintext $(y_1, y_2) = (g^{k_A} \pmod{P}, my_A^{k_A} \pmod{P})$ (i.e., the re-encryption step), we use an algorithm similar to the ElGamal scheme:*

- *Key generation:* Let x_B be the element uniformly chosen from Z_Q , and $y_B \equiv g^{x_B} \pmod{P}$.

- *Re-encryption:* The re-encryption algorithm E_R , On input (P, Q, g, y_B) and a ciphertext $(y_1, y_2) = (g^{k_A} \pmod{P}, my_A^{k_A} \pmod{P})$, uniformly selects an element $k_B \in_r Z_Q$ and outputs

$$E_R((P, Q, g, y_B), y_1, y_2) = (y_1, g^{k_B} \pmod{P}, y_2 y_B^{k_B} \pmod{P})$$

Note that since $(y_1, y_2) = (g^{k_A} \pmod{P}, my_A^{k_A} \pmod{P})$, the ciphertext (after re-encryption) is

$$E_R((P, Q, g, y_B), y_1, y_2) = (g^{k_A} \pmod{P}, g^{k_B} \pmod{P}, my_A^{k_A} y_B^{k_B} \pmod{P})$$

To simplify, let $(c_1, c_2, c_3) = (g^{k_A} \pmod{P}, g^{k_B} \pmod{P}, my_A^{k_A} y_B^{k_B} \pmod{P})$ and so $E_R((P, Q, g, y_B), (y_1, y_2)) = (c_1, c_2, c_3)$. Also, we use E_A and $E_B(E_A)$ to represent the encryption and re-encryption processes respectively (with key x_A and x_B).

The decryption is also similar to the ElGama scheme, but need to decrypt twice, details follow:

- *First round:* The decryption algorithm, D_B , on input (P, Q, g, x_B) and a ciphertext (c_1, c_2, c_3) , outputs

$$D_B((P, g, x_B), (c_1, c_2, c_3)) = (c_1, c_3(c_2^{x_B})^{-1} \pmod{P})$$

Now let us see what we obtain after this round: from $(c_1, c_2, c_3) = (g^{k_A} \pmod{P}, g^{k_B} \pmod{P}, my_A^{k_A} y_B^{k_B} \pmod{P})$ we come up with $c_1 = g^{k_A} \pmod{P}$ and

$$c_3(c_2^{x_B})^{-1} \pmod{P} = my_A^{k_A} \pmod{P}$$

Thus we end up with $D_B((P, g, x_B), (c_1, c_2, c_3)) = (y_1, y_2)$, using ElGamal scheme we could decrypt the ciphertext (y_1, y_2) :

- *The decryption algorithm, D_A , on input (P, Q, g, x_A) and a ciphertext (y_1, y_2) , outputs*

$$D_A((P, g, x_A), (y_1, y_2)) = y_2(y_1^{x_A})^{-1} \pmod{P} (= m)$$

In this paper, we directly present a theorem concerning the security of the re-encryption scheme without proving it. For the proof, we recommend readers to Ref.[11]

Theorem 1 *If the re-encryption scheme is not secure in the sense of indistinguishability, then there exists a probabilistic polynomial-time Turing Machine (p.p.t. TM) that solves the decision Diffie-Hellman problem with overwhelming probability.*

Furthermore, it is proved that breaking decision D-H problem is almost as hard as computing discrete logarithms[12], while computing discrete logarithms is as hard as languages in NPC unless the polynomial hierarchy (PH) collapses to the second level[13].

4. Commutative-like encryption

Commutative-like encryption is a new notion presented in this paper, before giving the definition of commutative-like encryption, let us first check one property of the above re-encryption scheme.

In the decryption scheme, we decrypt the re-encrypted ciphertext in a way corresponding to the order of encryption, however, we may apply a different order, details follow:

- *First round: The decryption algorithm, D_A , on input (P, Q, g, x_A) and a ciphertext (c_1, c_2, c_3) , outputs*

$$D_A((P, g, x_A), (c_1, c_2, c_3)) = (c_2, c_3(c_1^{x_A})^{-1} \pmod{P})$$

Now let us see what we obtain after this round: from $(c_1, c_2, c_3) = (g^{k_A} \pmod{P}, g^{k_B} \pmod{P}, my_A^{k_A} y_B^{k_B} \pmod{P})$ we come up with $c_2 = g^{k_B} \pmod{P}$ and

$$c_3(c_1^{x_A})^{-1} \pmod{P} = my_B^{k_B} \pmod{P}$$

Thus we end up with $D_A((P, g, x_A), (c_1, c_2, c_3)) = (y'_1, y'_2)$, where $y'_1 = g^{k_B} \pmod{P}$ and $y'_2 = my_B^{k_B} \pmod{P}$ using ElGamal scheme we could decrypt the ciphertext (y'_1, y'_2) :

- *The decryption algorithm, D_B , on input (P, Q, g, x_B) and a ciphertext (y'_1, y'_2) , outputs*

$$D_B((P, g, x_B), (y'_1, y'_2)) = y_2(y'_1^{x_B})^{-1} \pmod{P}$$

Clearly, in both decryption schemes, we have the plaintext at the last step. This suggests a “commutative-like” characterization: the result of decryption does not relies on the order of decryptions, more specifically, in the scheme, let m be the plaintext and (c_1, c_2, c_3) be the ciphertext, we have

$$D_A(D_B(c_1, c_2, c_3)) = D_B(D_A(c_1, c_2, c_3)) = m$$

or equivalently, we have

$$D_B(D_A(E_B(E_A(m)))) = m$$

Largely due to the probabilistic nature, this encryption cannot be termed as commutative encryption, since the each ciphertext of the same plaintext would be different in different time with overwhelming probability, or say, $(c_1, c_2, c_3) = E_B(E_A(m))$ is not fixed(in fact, the ciphertext is same unless the randomly chosen variables k_1, k_2 are fixed).

DEFINITION 4 (Commutative-like Encryption). *A commutative-like encryption \mathcal{F} is a computable (in polynomial time) function $f : \text{Key } \mathcal{F} \times \text{Dom } \mathcal{F} \rightarrow \text{Ran } \mathcal{F}$, defined on finite computable domains, that satisfies all properties listed below.*

1. *Commutative-like. For all $e, e' \in \text{Key } \mathcal{F}$ we have*

$$f_{e'}^{-1} \circ f_e^{-1} \circ f_{e'} \circ f_e = I$$

2. *The inverse f_e^{-1} is a deterministic process (i.e., every ciphertext maps only one plaintext, while a plaintext might map many ciphertext) and is also computable in polynomial-time given e .*

3. *The distribution of $\langle x, f_e(x), y, f_e(y) \rangle$ is indistinguishable from the distribution of $\langle x, f_e(x), y, z \rangle$, where $x, y \in_r \text{Dom } \mathcal{F}$, $z \in_r \text{Ran } \mathcal{F}$ and $e \in_r \text{Key } \mathcal{F}$.*

Informally, Property 1 says that when we compositely encrypt with two different keys, the result is the same irrespective of the order of decryption. Property 2 says that given an encrypted value $f_e(x)$ and the encryption key e , we can find x in polynomial time, and there is only one such x . Property 3 says that given a value x and its encryption $f_e(x)$ (but not the key e), for a new value y , we cannot distinguish between $f_e(y)$ and a random value z in polynomial time. Thus we can neither encrypt y nor decrypt $f_e(y)$ in polynomial time. Note that this property holds only if x is a random value from $\text{Dom } \mathcal{F}$, i.e., the adversary does not control the choice of x .

Now let us see how the encryption scheme fits the required properties. Obviously, the first and second properties comes directly from the algorithms, now we check the third property. Note that

if $\langle x, f_e(x), y, f_e(y) \rangle = \langle m_1, g^{k_A}, m_1 g^{k_A x}, m_2, g^{k_B}, m_2 g^{k_B x} \rangle$ (where $(\text{mod } P)$ is neglected) is distinguishable from $\langle m_1, g^{k_A}, m_1 g^{k_A x}, m_2, z_1, z_2 \rangle$ ($z_1, z_2 \in \text{Ran}\mathcal{F}$), then $\langle g^{k_A}, g^{k_A x}, g^{k_B}, g^{k_B x} \rangle$ is distinguishable from the distribution of $\langle g^{k_A}, g^{k_A x}, g^{k_B}, z \rangle$ where $z \in_r Z_Q$. the Decisional Diffie-Hellman hypothesis (DDH) claims that for any generating ($\neq 1$) element g , the distribution of $\langle g^a, g^b, g^{ab} \rangle$ is indistinguishable from the distribution of $\langle g^a, g^b, g^c \rangle$. A 3-tuple $\langle g^a, g^b, z \rangle$ from the DDH can be reduced to our 4-tuple $\langle g^{k_A}, g^{k_A x}, g^{k_B}, z \rangle$ by taking $d \in \text{Key}\mathcal{F}$ and making tuple $\langle g^d, (g^a)^d, g^b, z \rangle$. Now a plays the role of x , g^d of g^{k_A} , and g^b of g^{k_B} ; we test whether g^{ab} or is random. Thus, given DDH, $\langle g^{k_A}, g^{k_A x}, g^{k_B}, g^{k_B x} \rangle$ and $\langle g^{k_A}, g^{k_A x}, g^{k_B}, z \rangle$ are also indistinguishable, which contradicts our assumption.

5. Application Instance

Readers might wonder the real application of commutative-like encryption, and here we propose one possible application in oblivious transfer. Oblivious Transfer refers to a kind of two-party protocols where at the beginning of the protocol one party, the sender, has an input, and at the end of the protocol the other party, the receiver, learns some information about this input in a way that does not allow the sender to figure out what it has learned. Oblivious transfer is a fundamental primitive in the design and analysis of cryptographic protocols[14, 15]. Our scheme is a 1-out-of- n oblivious transfer: the sender has n secrets m_1, m_2, \dots, m_n and is willing to disclose exactly one of them to the receiver at its choice.

Now let us see how our protocol proceeds:

- The sender encrypts every item using its key x_A and gets $E_{x_A}(m_1), E_{x_A}(m_2), \dots, E_{x_A}(m_n)$. Then it reveals them to the receiver.
- On receiving the ciphertexts, the receiver chooses exactly one of them, say, $E_{x_A}(m_i)$ ($1 \leq i \leq n$), and encrypts it to obtain $E_{x_B}(E_{x_A}(m_i))$ and tells it to the sender.
- The sender decrypts it, gets $D_{x_A}(E_{x_B}(E_{x_A}(m_i)))$ and sends it to the receiver.
- The receiver obtains m_i by calculating $D_{x_B}(D_{x_A}(E_{x_B}(E_{x_A}(m_i))))$.

Instead of a formal proof, we explain how the protocol achieves its goal: according to the performance of commutative-like encryption, the receiver can get its desired message after interaction with the sender, i.e., $D_{x_B}(D_{x_A}(E_{x_B}(E_{x_A}(m_i)))) = D_{x_A}(D_{x_B}(E_{x_B}(E_{x_A}(m_i)))) = m_i$, thus the protocol is correct. Furthermore, the receiver receives nothing other than m_i : it can hardly deduce anything from the ciphertexts $E_{x_A}(m_i)$ ($1 \leq i \leq n$). As for the privacy of the receiver, the sender does not know the receiver's choice i : it does not suggest m_i from $E_{x_B}(E_{x_A}(m_i))$.

It should be noted that by trivially performing the protocol m times, we would obtain an m -out-of- n oblivious transfer protocol.

6. Conclusion

In this paper, we define the notion of commutative-like encryption, which is a useful variation of commutative encryption. As an example, it is showed that the ElGamal scheme could be such a commutative-like scheme. Also, we discussed one possible application of commutative-like encryption.

References

- [1] S. Lian, Z. Liu, R. Zhen *et al.* Commutative watermarking and encryption for media data. Opt. Eng., 45(8), 080510, 2006.

- [2] P. Lafourcade. Intruder Deduction for the Equational Theory of Exclusive-or with Commutative and Distributive Encryption. *Electronic Notes in Theoretical Computer Science*, 171(4): 37-57, 2007.
- [3] Veronique Cortier, Stephanie Delaune and Pascal Lafourcade. A survey of algebraic properties used in cryptographic protocols. *Journal of Computer Security*, 14(1): 1-43, 2006.
- [4] S. A. Weis. New foundations for efficient authentication, commutative cryptography, and private disjointness testing. Massachusetts Institute of Technology, Cambridge, MA, 2006.
- [5] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inform. Theory*. 31(4): 469-472, 1985.
- [6] W. B. Lee, C. Wua and W. J. Tsaur. A novel deniable authentication protocol using generalized ElGamal signature scheme. *Inform. Sci.*, 177(6): 1376-1381, 2006.
- [7] E. J. Yoon, E. K. Ryu and K. Y. Yoo. Efficient remote user authentication scheme based on generalized ElGamal signature scheme. *IEEE Trans. Consum. Electr.*, 50(2): 568-570, 2004.
- [8] S. J. Hwang and Y. H. Lee. Repairing ElGamal-like multi-signature schemes using self-certified public keys. *Appl. Math. Comput.*, 156(1): 73-83, 2004.
- [9] R. Agrawal, A. Evfimievski and R. Srikant. Information Sharing Across Private Databases. *Proceedings of the 2003 ACM SIGMOD international conference on Management of data*, 86-97, 2003.
- [10] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory*, 22(6): 644-654, 1976.
- [11] Y. Tsiounis and M. Yung. On the Security of ElGamal Based Encryption. In H. Imai and Y. Zheng (Eds.): *Public Key Cryptography, PKC'98*, LNCS 1431, 117-134, 1998.
- [12] U. M. Maurer. Towards the Equivalence of Breaking the Diffie-Hellman Protocol and Computing Discrete Logarithms. *Advances in Cryptology-CRYPTO'94* (LNCS 839), 271-281, 1994.
- [13] T. Okamoto, K. Sakurai and H. Shizuya. How intractable is the discrete logarithm for a general finite group. LNCS 658, 402-468, 1993.
- [14] Y. Z. Ding, D. Harnik, A. Rosen *et al.* Constant-Round Oblivious Transfer in the Bounded Storage Model. *J. Cryptol.*, 20(2): 165-202, 2007.
- [15] M. Naor and B. Pinkas. Computationally Secure Oblivious Transfer. *J. Cryptol.*, 18(1): 1-35, 2005.