A Note On Boneh-Gentry-Waters Broadcast Encryption Scheme and Its Like

Zhengjun Cao\textsuperscript{1}, Lihua Liu\textsuperscript{2,*}

Abstract. Key establishment is any process whereby a shared secret key becomes available to two or more parties, for subsequent cryptographic use such as symmetric-key encryption. Though it is widely known that the primitive of encryption is different from key establishment, we find some researchers have confused the two primitives. In this note, we shall clarify the fundamental difference between the two primitives, and point out that the Boneh-Gentry-Waters broadcast encryption scheme and its like are key establishment schemes, not encryption schemes.

Keywords. key establishment; encryption; broadcast encryption

1 Introduction

Keeping information secret from all but those who are authorized to see it, is a main objective of cryptography. The primitive of encryption can provide the functionality. Over the centuries, a lot of mechanisms have been created to deal with the information security issue.

In 1976, Diffie and Hellman introduced the concept of public-key cryptography and also provided a new method for key establishment. But they had not put forth any public-key encryption scheme at the time. In 1978, Rivest, Shamir, and Adleman discovered the first practical public-key encryption and signature scheme which is based on the hard mathematical problem of factorization. To date, the computational performance of public-key encryption is inferior to that of symmetric-key encryption because of much larger working parameters needed. So, public-key encryption schemes are generally used to establish a key for a symmetric-key system being used by communicating entities. That is to say, key establishment is really intertwined with encryption. Then, what is the fundamental difference between key establishment and encryption?

We find all literatures have not specified the difference. We also find some researchers have confused key establishment and encryption. In this note, we shall clarify the difference between the two primitives, and point out that the Boneh-Gentry-Waters broadcast encryption scheme and its like are key establishment schemes, not encryption schemes.

\textsuperscript{1}Department of Mathematics, Shanghai University, Shanghai, China. \textsuperscript{2}Department of Mathematics, Shanghai Maritime University, Shanghai, China. * liuh@shmtu.edu.cn
2 Key establishment

Definition 1 \[14\] Key establishment is any process whereby a shared secret key becomes available to two or more parties, for subsequent cryptographic use.

Key establishment can be broadly subdivided into key agreement and key transport. A key transport protocol is a key establishment technique where one party creates or otherwise obtains a secret value, and securely transfers it to the other(s). A key agreement protocol is a key establishment technique in which a shared secret is derived by two (or more) parties as a function of information contributed by, or associated with, each of these, such that no party can predetermine the resulting value. Key establishment protocols result in shared secrets which are typically used to derive, session keys. For example, the Diffie-Hellman key agreement scheme is such a protocol.

| Table 1: Diffie-Hellman key agreement (basic version) |
|-----------------|-------------------------------------------------|
| Setup           | A prime \( p \) and generator \( g \) of \( \mathbb{Z}_p^* \) are selected and published. |
| Protocol actions| (a) A picks a random \( x, 1 \leq x \leq p - 2 \), and sends \( g^x \mod p \) to B. |
|                 | (b) B picks a random \( y, 1 \leq x \leq p - 2 \), and sends \( g^y \mod p \) to A. |
|                 | (c) B computes the shared key as \( K = (g^x)^y \mod p \). |
|                 | (d) A computes the shared key as \( K = (g^y)^x \mod p \). |
| Result          | The shared secret \( K \) is known to both parties A and B. |

3 Encryption

Definition 2 \[14\] Let \( A \) be a finite set called the alphabet of definition, \( \mathcal{M} \) be a set called the message space, \( \mathcal{C} \) be a set called the ciphertext space, \( \mathcal{K} \) be a set called the key space. Each element \( e \in \mathcal{K} \) uniquely determines a bijection from \( \mathcal{M} \) to \( \mathcal{C} \), denoted by \( E_e \). \( E_e \) is called an encryption function or an encryption transformation. For each \( d \in \mathcal{K} \), \( D_d \) denotes a bijection from \( \mathcal{C} \) to \( \mathcal{M} \). \( D_d \) is called a decryption function or decryption transformation. An encryption scheme consists of a set \( \{E_e : e \in \mathcal{K}\} \) of encryption transformations and a corresponding set \( \{D_d : d \in \mathcal{K}\} \) of decryption transformations with the property that for each \( e \in \mathcal{K} \) there is a unique key \( d \in \mathcal{K} \) such that \( D_d(E_e(m)) = m \) for all \( m \in \mathcal{M} \).

The above definition is somewhat tedious. We refer to RSA system for a concrete example of encryption scheme, which is a well-known public-key encryption and signature scheme. Note that at the end of the scheme, both the sender and the intended receiver know the message.
### Table 2: RSA encryption

| Setup | Pick two distinct odd primes \( p \) and \( q \), compute \( n = pq \), \( \phi(n) = (p - 1)(q - 1) \). Pick \( e \in \mathbb{Z}_n^* \), compute \( d = e^{-1} \mod \phi(n) \). Publish \( n, e \) and keep \( d, p, q \) in secret. |
|--------|--------------------------------------------------|
| Encrypting | For a message \( m \in \mathbb{Z}_n \), compute \( c = m^e \mod n \). |
| Decrypting | Use the secret key \( d \) to recover \( m = c^d \mod n \). |

### 4 A difference between key establishment and encryption

As we see, both Diffie-Hellman key agreement and RSA encryption can ensure the two participators to know a same thing, whether we call it a shared key or a message. Then, what are the differences between key establishment and encryption? It is a pity that we find all literatures have not specified the differences. We think the fundamental difference between two primitives is that

|          |          |
|----------|----------|
| Computation |          |
| RSA encryption | \( c = m^e \mod n, m = c^d \mod n. \) |
| Diffie-Hellman key agreement | \( g^x \mod p, g^y \mod p, K = (g^y)^x \mod p = (g^x)^y \mod p. \) |

| Result |          |
|--------|----------|
| RSA encryption | Both the two parties know \( m \). |
| Diffie-Hellman key agreement | Both the two parties know \( K \). |

| Characteristic |          |
|----------------|----------|
| RSA encryption | \( m \) is pre-existing. |
| Diffie-Hellman key agreement | \( K \) is not pre-existing. |

### 5 The Boneh-Gentry-Waters “broadcast encryption” scheme and its like are not true encryption schemes

#### 5.1 The Boneh-Gentry-Waters “broadcast encryption” scheme

The primitive of broadcast encryption was formalized by Fiat and Naor \[5\], which requires that the broadcaster encrypts a message such that a particular set of users can decrypt the message sent over a broadcast channel. The Fiat-Naor broadcast encryption and the following works \[6, 7, 10, 17, 18\] use a combinatorial approach. This approach has to right the balance between the efficiency and the number of colluders that the system is resistant to. Recently, Boneh et al \[2\] have constructed some “broadcast encrypt” systems. In these systems, the public parameters must be updated to
allow more users. But we find the Boneh-Gentry-Waters “broadcast encryption” scheme and its like [1, 4, 8, 9, 11–13] are not true encryption schemes. They are key establishment schemes. For convenience, we now relate the Boneh-Gentry-Waters scheme as follows.

**Setup** \((n)\): Suppose there are \(n\) users in the system. Let \(G\) be a bilinear group of prime order \(p\). Pick a random generator \(g \in G\) and random numbers \(\alpha, \gamma \in \mathbb{Z}_p\). Compute \(v = g^\gamma\) and \(g_i = g^{(\alpha^i)}\) for \(i = 1, 2, \cdots, n, n + 2, \cdots, 2n\). The public key is set as:

\[
PK = (g, g_1, \cdots, g_n, g_{n+2}, \cdots, g_{2n}, v).
\]

The private key for user \(i \in \{1, \cdots, n\}\) is set as: \(d_i = g_i^\gamma\).

**Encrypt** \((S, PK)\): Let \(S\) be the set of the intending receivers. Pick a random \(t \in \mathbb{Z}_p\) and set \(K = e(g_{n+1}, g)^t\). The value \(e(g_{n+1}, g)\) can be computed as \(e(g_n, g_1)\). Next, set

\[
Hdr = \left( g^t, (v \cdot \prod_{j \in S} g_{n+1-j})^t \right)
\]

and output the pair \((Hdr, K)\).

**Decrypt** \((S, i, d_i, Hdr, PK)\): Parse \(Hdr\) as \((C_0, C_1)\) and compute

\[
K = e(g_i, C_1)/e(d_i \cdot \prod_{j \in S, j \neq i} g_{n+1-j+i}, C_0).
\]

### 5.2 Analysis

It is easy to see that in the Boneh-Gentry-Waters scheme the shared thing \(K\) is not pre-existing. It depends on the choice of the encrypter. Moreover, the encrypter has to use its secret component \(t\) for other computations. Of course, the scheme can be transformed into a regular encryption scheme. It only needs to set \(c = M \cdot e(g_{n+1}, g)^t\) for a given message \(M \in G\) in the Encryption phase. To recover \(M\), the user with \(d_i\) can compute

\[
M = c \cdot e(d_i \cdot \prod_{j \in S, j \neq i} g_{n+1-j+i}, C_0)/e(g_i, C_1).
\]

But we should remark that pairings including Weil pairing and Tate pairing are derived from elliptic curves [16]. Both \(K, M\) are in the extension field \(\mathbb{F}_{q^k}\) where \(\mathbb{F}_q\) is the base field of the elliptic curve defined over. \(k\) is called the embedding degree which is the smallest positive integer such that \(p\) divides \((q^k - 1)\). That means the scheme has to work in some extension of the base field, even though the inputting parameters are defined over the base field. That is to say, the scheme has to work in a running environment with parameters of 1024 bits, not 160 bits as supposed (someone has confused the inputting-parameter’s size with the working-parameter’s size), so as to offer 80 bits security level. The shortcoming makes the scheme lose its competitive advantages significantly.
6 Conclusion

We clarify the fundamental difference between encryption and key establishment. To the best of our knowledge, it is the first time to put forth such an explicit principle to discriminate the two primitives. We also remark some schemes are not true encryption schemes, instead key establishment schemes.

References

[1] N. Attrapadung, J. Furukawa, and H. Imai. Forward-secure and searchable broadcast encryption with short ciphertexts and private keys. In the proceeding of Asiacrypt 2006, LNCS, Vol. 4284, pages 161-177. Springer-Verlag (2006)

[2] D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In the proceeding of Crypto 2005, LNCS, vol. 3494, pages 258-275. Springer-Verlag (2005)

[3] W. Diffie and M. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, 22: 644-654, 1976.

[4] C. Delerablée, P. Paillier, and D. Pointcheval. Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys. In the proceeding of Pairing 2007, LNCS, vol. 4575, pages 39-59. Springer-Verlag (2007)

[5] A. Fiat and M. Naor. Broadcast encryption. In the proceeding of Crypto 1993, LNCS, vol. 773, pages 480-491. Springer-Verlag (1993)

[6] E. Gafni, J. Staddon, and Y.L. Yin. Efficient methods for integrating traceability and broadcast encryption. In the proceeding of Crypto 1999, LNCS, vol. 1666, pages 372-387. Springer-Verlag (1999)

[7] J. Garay, J. Staddon, and A. Wool. Long-lived broadcast encryption. In the proceeding of Crypto 2000, LNCS, vol. 1880, pages 333-352. Springer-Verlag (2000)

[8] C. Gentry and B. Waters. Adaptive security in broadcast encryption systems. In the proceeding of Eurocrypt 2009, LNCS, vol. 5479, pages 171-188. Springer-Verlag (2009)

[9] P. Junod and A. Karlov. An efficient public-key attribute-based broadcast encryption scheme allowing arbitrary access policies. In the proceeding of DRM 2010, ACM Press (2010)

[10] R. Kumar, S. Rajagopalan, and A. Sahai. Coding constructions for blacklisting problems without computational assumptions. In the proceeding of Crypto 1999, LNCS, vol. 1666, pages 609-623, Springer-Verlag (1999)

[11] K. Lee, et al. Self-updatable encryption: time constrained access control with hidden attributes and better efficiency. In the proceeding of Asiacrypt 2013, LNCS, vol. 8269, page 235-254, Springer-Verlag (2013)

[12] K. Lee. Self-updatable encryption with short public parameters and its extensions. Cryptology ePrint Archive: Report 2014/231

[13] B. Malek and A. Miri. Adaptively secure broadcast encryption with short ciphertexts. International Journal of Network Security, Vol.14, No.2, pages 71-79, 2012.
[14] A. Menezes, P. Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[15] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21: 120C126, 1978.

[16] J. Silverman. *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.

[17] D. Stinson. On some methods for unconditionally secure key distribution and broadcast encryption. *Des. Codes Cryptography*, 12(3), 215-243, 1997.

[18] D. Stinson and T. Trung. Some new results on key distribution patterns and broadcast encryption. *Des. Codes Cryptography*, 14(3), 261-279, 1998.