行政院國家科學委員會補助專題研究計畫 □ 成 果 報 告 ☑期中進度報告

具密文與金鑰效率之公開式廣播加密系統之研究

Public-Key Broadcast Encryption with Efficient Ciphertext and Private Keys

計畫類別：☑ 個別型計畫　□整合型計畫
計畫編號：NSC 96-2628-E-009-011-MY3
執行期間： 96 年 8 月 1 日至 99 年 7 月 31 日

計畫主持人：曾文貴 教授
計畫參與人員：林煥宗、陳宏達、簡韶瑩、劉思維、陳毅睿、陳證傑

成果報告類型(依經費核定清單規定繳交)：☑精簡報告　□完整報告

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
V 出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、列管計畫及下列情形者外，得立即公開查詢
□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位：國立交通大學 資訊科學系

中 華 民 國 97 年 6 月 30 日

中文摘要

本研究計畫將研究公開式廣播加密系統，現今最好的公開式廣播加密系統的私密金鑰大小、公開金鑰和傳輸量能無法和私密式的廣播系統相比，我們覺得可以使之達到更佳的效率：分別為 O(r), O(log n) 和 O(1)，同時計算量也可控制在合理的範圍之內，不像 BGW 的方法需要 O(n)。

今年度我們發展出兩個公開廣播加密協定，第一個協定可以達到 O(r)密文長度，O(log n)私密金鑰及 O(1)公開金鑰，計算量需要 O(r)。第二個協定可以達到 O(r)密文長度，$O(\log^2 n)$私密金鑰及 O(1)公開金鑰，計算量只需要 O(1)。論文已在今年的 PKC 會議上發表。

關鍵詞：廣播加密、公開金鑰。

英文摘要

In this project we study the public-key broadcast encryption system, in which one can broadcast to a set of authorized users. To our best knowledge, the best public-key broadcast encryption system is not very efficient in the size of the header, public key and private key of users, compared to the secret-key broadcast encryption system. One of the goals of this research is to design and analyze efficient public-key broadcast encryption schemes.

In this year, we have designed two efficient public-key broadcast encryption schemes. The first scheme achieves O(1) public-key size, O(r) header size and O(log n) private keys per user. The decryption time is reasonably O(r). Our second scheme achieves O(1) public-key size, O(r) header size and $O(\log^2 n)$ private keys per user. Although the private key size is less efficient than the first one, its decryption time is remarkably O(1). The paper of these results has been published in prestigious PKC conference.

Keywords: Broadcast encryption, public key system.

一、計畫緣起及目的

廣播加密是一種有效率的金鑰管理及訊息傳播機制。對於大量的使用者，管理中心可以傳播訊息給任意指定(未被註銷)的使用者，指定的使用者收到訊息後，可依表頭的內容解開資訊；而被註銷的使用者，即使共謀也無法從中得到資訊。廣播加密在生活上有很多應用，如付費電視、線上影片等。廣播加密的正式討論最早是在 1993 年由 Fiat 和 Naor 所提出，在廣播加密的機制中，一開始管理中心會分配每位使用者 u 一些金鑰 k。廣播時，中心首先會使用一把金鑰 SK 對欲傳送的訊息 M 做加密，接著依照接收使用者的集合，使用某些 k 對金鑰 SK 做加密，此為表頭，連結欲傳送之加密訊息，形成下列的廣播格式：

$$< E_{k_1}(SK), E_{k_2}(SK), \ldots E_{SK}(M) >$$

使用者接收到訊息後，首先利用表頭和所擁有的金鑰來解出 SK，接著用 SK 即可還原訊息 M。

根據使用者一開始所分配的金鑰改變與否，廣播加密可分為有狀態加密機制(stateful)和無狀態加密機制 (stateless)，在無狀態加密機制中，使用者的金鑰分配完成後即不再更改，此法符合許多裝置的限制，大幅的提升了廣播加密的應用性，如使用在 DVD 和 VCD 分區上。無狀態加密機制方法中，又可再區分為私密式廣播加密 及公開式廣播加密系統，其中差別在於私密式廣播加密系統，只有知道所有使用者秘鑰 (如設置中心)才可廣播，而公開式廣播加密則是每人皆可廣播，並只有擁有相對秘鑰者才可解開訊息。

Naor 和 Naor 等人於 2001 年所提出一個可行性高的無狀態私密金鑰廣播加密機制演算法，他們把廣播加密轉換成為 Subset Cover 問題的想法，同時在擬亂數產生器是安全的假設下，利用擬亂數產生器來衍生金鑰，大幅減少使用者金鑰儲存的數量，並突破了原本 Luby 所計算出在完全（unconditionally）安全性上傳輸量和計算量關係的下限。後來許多學者提出了各種架構來改進廣播加密的方法。

公開金鑰廣播加密系統的成果比較少，最早的論文為 Boneth and Franklin 提出，之後 Tzeng and Tzeng 提出用多項式插值的技術來達到剔除使用者與追蹤背叛者 (traitor)的功能，後來 Kurosawa and Yoshida 將其推廣到使用任何 linear error correcting code 皆可。最近 Boneth, Gentry and Waters 提出廣播量和儲存金鑰量都很少的公開金鑰廣播加密的方法，缺點是公開金鑰的量非常大。2003 年，Dodis and Fazio 提出了利用 IBE (identity-based encryption)系統把私密式廣播加密系統轉化成公開式廣播加密的系統的方法，轉換出來的系統的各項參數和原來的私密金鑰系統的皆相同。

在廣播加密之中，重要的參數有下列幾個，第一個是表頭大小 t (Header size)也就是傳輸量，第二則是金鑰的儲存量，第三則是每個使用者所需的計算量。在一些研究中，某些方法會限制註銷使用者共謀的個數，然而在此篇文章中，我們著重在探討無限制註銷者共謀(collusion resistant)的方法。關於金鑰分配和傳輸量之間的關係，直覺的想法，假設現在有 n 位使用者，每位使用者擁有一把自己專屬的金鑰，則當我們註銷掉任意 r 位使用者時，我們需要對其餘 n-r 位使用者一一加密，因此，此方法所需的傳輸量為 n-r，每位使用者金鑰的儲存量則為 1，計算量方面，由於使用者收到後可直接使用金鑰解開表頭，因此計算量也為 1 (以上這種方法我們取名為(a)列於下表之中)。相反的，若我們分給每位使用者 2n-1 把金鑰，每把金鑰分別代表自己之外其餘 n-1 個使用者註銷的情形，則當我們註銷 r 個使用者時，我們所需的傳輸量為 1，每位使用者金鑰儲存量即為 2n-1 (以上這種方法我們取名為(b)列於下表之中)，且我們需要 O(n)的金鑰查詢時間。

由上述兩種方法我們觀察可得知，當每個使用者金鑰儲存量少的時候，傳輸量多；當儲存量少之時，所需傳輸量就大，而如何能有個好方法能在這兩者間取得平衡？亦或是使這兩者參數皆小，並在計算量上所需最小，便是我們研究的主要課題。

二、研究成果

本年度(第一年度)的研究成果為提出兩個有效率公開金鑰廣播加密系統，第一個協定可以達到 O(r)密文長度，O(log n)私密金鑰及 O(1)公開金鑰，計算量需要 O(r)。第二個協定可以達到 O(r)密文長度，$O(\log^2 n)$私密金鑰及 O(1)公開金鑰，計算量更只需要 O(1)，非常不可思議。這兩個系統的效率超越先前的公開金鑰廣播加密系統。

詳細的方法請見附件的論文，在此我們簡述這兩個協定。在原理上，這兩個協定都是使用多項式插值法（polynomial interpolation）來達到目的，但是直接的應用導致使用過多的參數，公開金鑰數目過多，且解密時間無法達到 O(1)。因以，對於多項式的係數，我們不使用如先前的隨意取，而是使用雜湊函數來計算，這樣可以將公開參數的數目快速的降為 O(1)；然而這樣做雖然可以降低公開金鑰的數目，但確導致無法給定使用者私密金鑰，因此我門們引入了雙線性的 pairing 函數，把使用者的私密金鑰放入該函數中，使得系統可以設定使用者的私密金鑰。如此，我們的到了第一個協定。

第一個協定的主要問題是解密時間需要 O(r)，第二個協定非常有技巧的把多項式插值法引入 SD 私密金鑰廣播系統中，我們使用

degree-1 的多項式，因此作插值時只需常數的時間，達到解密時間為 O(1)。

三、計畫成果自評

我們的研究結果發表了一篇會議論文 "Public key broadcast encryption with low number of keys and constant decryption time" 在 PKC08 國際會議上，PKC 國際公開金鑰密碼系統會議是密碼領域的一線國際會議，論文接受率低於 20%，許多會議論文的發表者和與會者是密碼領域裡的傑出學者，可見其重要性。以成果來看，我們達成了本計畫第一年度的目的。

參考文獻

1. N. Attrapadung, H. Imai. Graph-decomposition-based frameworks for subset-cover broadcast encryption and efficient instantiations. In *Proceedings of Advances in Cryptology - Asiacrypt 05*, Lecture Notes in Computer Science 3788, pp.100-120, Springer, 2005.
2. D. Boneh, X. Boyen, E.-J. Goh. Hierarchical identity based encryption with constant size ciphertext. In *Proceedings of Advances in Cryptology - Eruocrypt 05*, Lecture Notes in Computer Science 3494, pp.440-456, Springer, 2005.
3. D. Boneh, M. Franklin. An efficient public key traitor tracing scheme. In *Proceedings of Advances in Cryptology - Crypto 99*, Lecture Notes in Computer Science 1666, pp.338-353, Springer, 1999.
4. D. Boneh, C. Gentry, B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In *Proceedings of Advances in Cryptology -Crypto 05*, Lecture Notes in Computer Science 3621, pp.258-275, Springer, 2005.
5. D. Boneh, B. Waters. A fully collusion resistant broadcast trace, and revoke system. In *Proceedings of the ACM Conference on Computer and Communications Security - CCS 06*, pp.211-220, ACM Press, 2006.
6. Y. Dodis, N. Fazio. Public key broadcast encryption for stateless receivers. In *Proceedings of Digital Right Management 02 - DRM 02*, Lecture Notes in Computer Science 2696, pp.61-80, Springer, 2002.
7. Y. Dodis, N. Fazio. Public key broadcast encryption secure against adaptive chosen ciphertext attack. In *Proceedings of Public Key Cryptography - PKC 03*, Lecture Notes in Computer Science 2567, pp.100-115, Springer, 2003.
8. A. Fiat, M. Naor. Broadcast encryption. In *Proceedings of Advances in Cryptology - Crypto 93*, Lecture Notes in Computer Science 773, pp.480-491, Springer, 1993.
9. E. Fujisaki, T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In *Proceedings of Advances in Cryptology - Crypto 99*, Lecture Notes in Computer Science 1666, pp.537-554, Springer, 1999.
10. D. Galindo. Boneh-Franklin identity based encryption revisited. In Proceedings of ICALP 05, Lecture Notes in Computer Science 3580, pp.791-802, Springer, 2005.
11. M.T. Goodrich, J.Z. Sun, R. Tamassia. Efficient Tree-Based Revocation in Groups of Low-State Devices. In Proceedings of Advances in Cryptology - Crypto 04, Lecture Notes in Computer Science 3152, pp.511-527, Springer, 2004.
12. D. Halevy, A. Shamir. The LSD broadcast encryption scheme. In *Proceedings of Advances in Cryptology - Crypto 02*, Lecture Notes in Computer Science 2442, pp.47-60, Springer, 2002.
13. K. Kurosawa, Y. Desmedt. Optimum traitor tracing and symmetric schemes. In *Proceedings of Advances in Cryptology - Eurocrypt 98*, Lecture Notes in Computer Science 1403, pp.145-157, Springer, 1998.
14. K. Kurosawa, T. Yoshida. Linear code implies public-key traitor tracing. In *Proceedings of Public Key Cryptography*, Lecture Notes in Computer Science 2274, pp.172-187, Springer, 2002.
15. J.W. Lee, Y.H. Hwang, P.J. Lee. Efficient public key broadcast encryption using identifier of receivers. In *Proceedings of International Conference on Information Security Practice and Experience - ISPEC 06*, Lecture Notes in Computer Science 3903, pp.153-164, Springer, 2006.

16. D. Naor, M. Naor, J. Lotspiech. Revocation and tracing schemes for stateless receivers. In *Proceedings of Advances in Cryptology - Crypto 01*, Lecture Notes in Computer Science 2139, pp.41-62, Springer, 2001.

17. M. Naor, B. Pinkas. Efficient trace and revoke schemes. In *Proceedings of Financial Cryptography 00*, Lecture Notes in Computer Science 1962, pp.1-20, Springer, 2000.

18. A. Shamir. How to share a secret. *Communications of the ACM*, 22(11), pp.612-613, 1979.

19. W.-G. Tzeng, Z.-J. Tzeng. A public-key traitor tracing scheme with revocation using dynamic shares. In *Proceedings of Public Key Cryptography - PKC 01*, Lecture Notes in Computer Science 1992, pp.207-224, Springer, 2001.

20. P. Wang, P. Ning, D.S. Reeves. Storage-efficient stateless group key revocation. In *Proceedings of the 7th Information Security Conference - ISC 04*, Lecture Notes in Computer Science 3225, pp.25-38, Springer, 2005.

21. E.S. Yoo, N.-S. Jho, J.J. Cheon, M.-H. Kim. Efficient broadcast encryption using multiple interpolation methods. In *Proceedings of ICISC 04*, Lecture Notes in Computer Science 3506, pp.87-103, Springer, 2005.

22. M. Yoshida, T. Fujiwara. An efficient traitor tracing scheme for broadcast encryption. In *Proceedings of 2000 IEEE International Symposium on Information Theory*, pp.463, IEEE Press, 2000.

Public Key Broadcast Encryption with Low Number of Keys and Constant Decryption Time*

Yi-Ru Liu and Wen-Guey Tzeng

Department of Computer Science
National Chiao Tung University
Hsinchu, Taiwan 30050
wgtzeng@cs.nctu.edu.tw

Abstract. In this paper we propose three public key BE schemes that have efficient complexity measures. The first scheme, called the BE-PI scheme, has $O(r)$ header size, $O(1)$ public keys and $O(\log N)$ private keys per user, where r is the number of revoked users. This is the first public key BE scheme that has both public and private keys under $O(\log N)$ while the header size is $O(r)$. These complexity measures match those of efficient secret key BE schemes.
Our second scheme, called the PK-SD-PI scheme, has $O(r)$ header size, $O(1)$ public key and $O(\log^2 N)$ private keys per user. They are the same as those of the SD scheme. Nevertheless, the decryption time is remarkably $O(1)$. This is the first public key BE scheme that has $O(1)$ decryption time while other complexity measures are kept low. The third scheme, called, the PK-LSD-PI scheme, is constructed in the same way, but based on the LSD method. It has $O(r/\epsilon)$ ciphertext size and $O(\log^{1+\epsilon} N)$ private keys per user, where $0 < \epsilon < 1$. The decryption time is also $O(1)$.
Our basic schemes are one-way secure against *full collusion of revoked users* in the random oracle model under the BDH assumption. We can modify our schemes to have indistinguishably security against adaptive chosen ciphertext attacks.

Keywords: Broadcast encryption, polynomial interpolation, collusion.

1 Introduction

Assume that there is a set $\mathcal{U}$ of N users. We would like to broadcast a message to a subset S of them such that only the (authorized) users in S can obtain the message, while the (revoked) users not in S cannot get information about the message. Broadcast encryption is a bandwidth-saving method to achieve this goal via cryptographic key-controlled access. In broadcast encryption, a dealer sets up the system and assigns each user a set of private keys such that the

* Research supported in part by NSC projects 96-2628-E-009-011-MY3, 96-3114-P-001-002-Y (iCAST), and 96-2219-E-009-013 (TWISC).

broadcasted messages can be decrypted by authorized users only. Broadcast encryption has many applications, such as pay-TV systems, encrypted file sharing systems, digital right management, content protection of recordable data, etc.

A broadcasted message M is sent in the form $\langle Hdr(S,m),\ E_m(M)\rangle$, where m is a session key for encrypting M via a symmetric encryption method E. An authorized user in S can use his private keys to decrypt the session key m from $Hdr(S,m)$. Since the size of $E_m(M)$ is pretty much the same for all broadcast encryption schemes, we are concerned about the header size. The performance measures of a broadcast encryption scheme are the header size, the number of private keys held by each user, the size of public parameters of the system (public keys), the time for encrypting a message, and the time for decrypting the header by an authorized user. A broadcast encryption scheme should be able to resist the collusion attack from revoked users. A scheme is *fully collusion-resistant* if even all revoked users collude, they get no information about the broadcasted message.

Broadcast encryption schemes can be stateless or stateful. For a stateful broadcast encryption scheme, the private keys of a user can be updated from time to time, while the private keys of a user in a stateless broadcast encryption scheme remain the same through the lifetime of the system. Broadcast encryption schemes can also be public key or secret key. For a public key BE scheme, any one (broadcaster) can broadcast a message to an arbitrary group of authorized users by using the public parameters of the system, while for a secret key broadcast encryption scheme, only the special dealer, who knows the system secrets, can broadcast a message.

In this paper we refer "stateless public key broadcast encryption" as "public key BE".

1.1 Our Contribution

We propose three public key BE schemes that have efficient complexity measures. The first scheme, called the BE-PI scheme (broadcast encryption with polynomial interpolation), has $O(r)$ header size, $O(1)$ public keys, and $O(\log N)$ private keys per user[1], where r is the number of revoked users. This is the first public key BE scheme that has both public and private keys under $O(\log N)$ while the header size is $O(r)$. These complexity measures match those of efficient secret key BE schemes [11, 20, 21]. The idea is to run $\log N$ copies of the basic scheme in [17, 19, 22] in parallel for lifting the restriction on a priori fixed number of revoked users. Nevertheless, if we implement the $\log N$ copies straightforwardly, we would get a scheme of $O(N)$ public keys. We are able to use the properties of bilinear maps as well as special private key assignment to eliminate the need of $O(N)$ public keys and make it a constant number.

Our second scheme, called the PK-SD-PI scheme (public key SD broadcast encryption with polynomial interpolation), is constructed by combining the polynomial interpolation technique and the subset cover method in the SD

[1] log is based on 2 if the base is not specified.

Table 1. Comparison of some fully collusion-resistant public key BE schemes.

	header size	public-key size	private-key size	decryption cost[♮]
PK-SD-HIBE[†]	$O(r)$	$O(1)$	$O(\log^2 N)$	$O(\log N)$
BGW-I [4]	$O(1)$	$O(N)^{\flat}$	$O(1)$	$O(N-r)$
BGW-II [4]	$O(\sqrt{N})$	$O(\sqrt{N})^{\flat}$	$O(1)$	$O(\sqrt{N})$
BW[5]	$O(\sqrt{N})$	$O(\sqrt{N})^{\flat}$	$O(\sqrt{N})$	$O(\sqrt{N})$
LHL[§] [15]	$O(rD)$	$O(2C)^{\flat}$	$O(D)$	$O(C)$
P-NP, P-TT, P-YF[‡]	$O(r)$	$O(N)$	$O(\log N)$	$O(r)$
Our work: BE-PI	$O(r)$	$O(1)$	$O(\log N)$	$O(r)$
Our work: PK-SD-PI	$O(r)$	$O(1)$	$O(\log^2 N)$	$O(1)$
Our work: PK-LSD-PI	$O(r/\epsilon)$	$O(1)$	$O(\log^{1+\epsilon} N)$	$O(1)$

N - the number of users.
r - the number of revoked users.
[†] - the transformed SD scheme [6] instantiated with constant-size HIBE [2].
[‡] - the parallel extension of [17, 19, 22].
[♭] - the public keys are needed for decrypting the header by a user.
[§] - $N = C^D$.
[♮] - group operation/modular exponentiation and excluding the time for scanning the header.

scheme [16]. The PK-SD-PI scheme has $O(r)$ header size, $O(1)$ public key and $O(\log^2 N)$ private keys per user. They are the same as those of the SD scheme. Nevertheless, the decryption time is remarkably $O(1)$. This is the first public key broadcast encryption scheme that has $O(1)$ decryption time while other complexity measures are kept low. The third scheme, called the PK-LSD-PI scheme, is constructed in the same way, but based on the LSD method. It has $O(r/\epsilon)$ ciphertext size and $O(\log^{1+\epsilon} N)$ private keys per user, where $0 < \epsilon < 1$. The decryption time is also $O(1)$.

Our basic schemes are one-way secure against *full collusion of revoked users* in the random oracle model under the BDH assumption. We modify our schemes to have indistinguishably security against adaptive chosen ciphertext attacks. The comparison with some other public key BE schemes with full collusion resistance is shown in Table 1.

1.2 Related Work

Fiat and Naor [8] formally proposed the concept of static secret key broadcast encryption. Many researchers followed to propose various broadcast encryption schemes, e.g., see [11, 12, 16, 17, 20].

Kurosawa and Desmedt [13] proposed a pubic-key BE scheme that is based on polynomial interpolation and traces at most k traitors. The similar schemes of Noar and Pinkas [17], Tzeng and Tzeng [19], and Yoshida and Fujiwara [22] allow revocation of up to k users. Kurosawa and Yoshida [14] generalized the polynomial interpolation (in fact, the Reed-Solomon code) to any linear code for constructing public key BE schemes. The schemes in [7, 13, 14, 17, 19, 22] all

have $O(k)$ public keys, $O(1)$ private keys, and $O(r)$ header size, $r \leq k$. However, k is a-priori fixed during the system setting and the public key size depends on it. These schemes can withstand the collusion attack of up to k revoked users only. They are not fully collusion-resistant.

Yoo, et al. [21] observed that the restriction of a pre-fixed k can be lifted by running $\log N$ copies of the basic scheme with different degrees (from 2^0 to N) of polynomials. They proposed a scheme of $O(\log N)$ private keys and $O(r)$ header size such that r is not restricted. However, their scheme is secret key and the system has $O(N)$ secret values. In the public key setting, the public key size is $O(N)$.

Recently Boneh, et al. [4] proposed a public key BE scheme that has $O(1)$ header size, $O(1)$ private keys, and $O(N)$ public keys. By trading off the header size and public keys, they gave another scheme with $O(\sqrt{N})$ header size, $O(1)$ private keys and $O(\sqrt{N})$ public keys. Lee, et al. [15] proposed a better trade-off by using receiver identifiers in the scheme. It achieves $O(1)$ public key, $O(\log N)$ private keys, but, $O(r \log N)$ header size. Boneh and Waters [5] proposed a scheme that has the traitor tracing capability. This type of schemes [4, 5, 15] has the disadvantage that the public keys are needed by a user in decrypting the header. Thus, the de-facto private key of a user is the combination of the public key and his private key.

It is possible to transform a secret key BE scheme into a public key one. For example, Dodis and Fazio [6] transformed the SD and LSD schemes [12, 16] into public key SD and LSD schemes, shorted as PK-SD and PK-LSD. The transformation employs the technique of hierarchical identity-based encryption to substitute for the hash function. Instantiated with the newest constant-size hierarchical identity-based encryption [2], the PK-SD scheme has $O(r)$ header size, $O(1)$ public keys and $O(\log^2 N)$ private keys. The PK-LSD scheme has $O(r/\epsilon)$ header size, $O(1)$ public keys and $O(\log^{1+\epsilon} N)$ private keys, where $0 < \epsilon < 1$ is a constant. The decryption costs of the PK-SD and PK-LSD schemes are both $O(\log N)$, which is the time for key derivation incurred by the original relation of private keys. If we apply the HIBE technique to the secret key BE schemes of $O(\log N)$ or $O(1)$ private keys [1, 11, 20], we would get their public key versions with $O(N)$ private keys and $O(N)$ decryption time.

2 Preliminaries

Bilinear map. We use the properties of bilinear maps. Let G and G_1 be two (multiplicative) cyclic groups of prime order q and $\hat{e}$ be a bilinear map from $G \times G$ to G_1. Then, $\hat{e}$ has the following properties.

1. For all $u, v \in G$ and $x, y \in Z_q$, $\hat{e}(u^x, v^y) = \hat{e}(u, v)^{xy}$.
2. Let g be a generator of G, $\hat{e}(g, g) = g_1 \neq 1$ is a generator of G_1.

BDH hardness assumption. The BDH problem is to compute $\hat{e}(g, g)^{abc}$ from given (g, g^a, g^b, g^c). We say that BDH is (t, ϵ)-hard if for any probabilistic algorithm A with time bound t, there is some k_0 such that for any $k \geq k_0$,

$$\Pr[A(g, g^a, g^b, g^c) = \hat{e}(g, g)^{abc} : g \stackrel{u}{\leftarrow} G; a, b, c \stackrel{u}{\leftarrow} Z_q] \leq \epsilon.$$

Broadcast encryption. A public key BE scheme Π consists of three probabilistic polynomial-time algorithms:

- Setup(1^z, ID, $\mathcal{U}$). Wlog, let $\mathcal{U} = \{U_1, U_2, \ldots, U_N\}$. It takes as input the security parameter z, a system identity ID and a set $\mathcal{U}$ of users and outputs a public key PK and N private key sets $SK_1, SK_2, \ldots, SK_N$, one for each user in $\mathcal{U}$.
- $Enc(PK, S, M)$. It takes as input the public key PK, a set $S \subseteq \mathcal{U}$ of authorized users and a message M and outputs a pair $\langle Hdr(S, m), C\rangle$ of the ciphertext header and body, where m is a randomly generated session key and C is the ciphertext of M encrypted by m via some standard symmetric encryption scheme, e.g., AES.
- $Dec(SK_k, Hdr(S, m), C)$. It takes as input the private key SK_k of user U_k, the header $Hdr(S, m)$ and the body C. If $U_k \in S$, it computes the session key m and then uses m to decrypt C for the message M. If $U_k \notin S$, it cannot decrypt the ciphertext.

The system is correct if all users in S can get the broadcasted message M.

Security. We describe the indistinguishability security against adaptive chosen ciphertext attacks (IND-CCA security) for broadcast encryption as follows [4]. Here, we focus on the security of the session key, which in turn guarantees the security of the ciphertext body C. Let Enc^* and Dec^* be like Enc and Dec except that the message M and the ciphertext body C are omitted. The security is defined by an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$ via the following game.

Init. The adversary $\mathcal{A}$ chooses a system identity ID and a target set $S^* \subseteq \mathcal{U}$ of users to attack.

Setup. The challenger $\mathcal{C}$ runs Setup(1^z, ID, $\mathcal{U}$) to generate a public key PK and private key sets $SK_1, SK_2, \ldots, SK_N$. The challenger $\mathcal{C}$ gives SK_i to $\mathcal{A}$, where $U_i \notin S^*$.

Query phase 1. The adversary $\mathcal{A}$ issues decryption queries Q_i, $1 \le i \le n$, of form $(U_k, S, Hdr(S, m))$, $S \subseteq S^*, U_k \in S$, and the challenger $\mathcal{C}$ responds with $Dec^*(SK_k, Hdr(S, m))$, which is the session key encrypted in $Hdr(S, m)$.

Challenge. The challenger $\mathcal{C}$ runs $Enc^*(PK, S^*)$ and outputs $y = Hdr(S^*, m)$, where m is randomly chosen. Then, $\mathcal{C}$ chooses a random bit b and a random session key m^* and sets $m_b = m$ and $m_{1-b} = m^*$. $\mathcal{C}$ gives $(m_0, m_1, Hdr(S^*, m))$ to $\mathcal{A}$.

Query phase 2. The adversary $\mathcal{A}$ issues more decryption queries Q_i, $n{+}1 \le i \le q_D$, of form (U_k, S, y'), $S \subseteq S^*, U_k \in S, y' \neq y$, and the challenger $\mathcal{C}$ responds with $Dec^*(SK_k, y')$.

Guess. $\mathcal{A}$ outputs a guess b' for b.

In the above the adversary A is static since it chooses the target set S^* of users before the system setup. Let $\mathrm{Adv}^{ind\text{-}cca}_{\mathcal{A},\Pi}(z)$ be the advantage that $\mathcal{A}$ wins

the above game, that is,

$$\begin{aligned}\mathrm{Adv}^{ind\text{-}cca}_{\mathcal{A},\Pi}(z) = 2 \cdot \Pr[\mathcal{A}^{\mathcal{O}}(PK, SK_{\mathcal{U}\setminus S^*}, m_0, m_1, Hdr(S^*, m)) = b : \\ S^* \subseteq \mathcal{U}, (PK, SK_{\mathcal{U}}) \leftarrow Setup(1^z, \mathrm{ID}, \mathcal{U}), \\ Hdr(S^*, m) \leftarrow Enc^*(PK, S^*), b \stackrel{u}{\leftarrow} \{0,1\}] - 1,\end{aligned}$$

where $SK_{\mathcal{U}} = \{SK_i : 1 \leq i \leq N\}$ and $SK_{\mathcal{U}\setminus S^*} = \{SK_i : U_i \notin S^*\}$.

Definition 1. *A public key BE scheme Π=(Setup, Enc, Dec) is (t, ϵ, q_D)-IND-CCA secure if for all t-time bounded adversary $\mathcal{A}$ that makes at most q_D decryption queries, we have $Adv^{ind\text{-}cca}_{\mathcal{A},\Pi}(z) < \epsilon$.*

In this paper we first give schemes with one-way security against chosen plaintext attacks (OW-CPA security) and then transform them to have IND-CCA security via the Fujisaki-Okamoto transformation [9]. The OW-CPA security is defined as follows.

Init. The adversary $\mathcal{A}$ chooses a system identity ID and a target set $S^* \subseteq \mathcal{U}$ of users to attack.
Setup. The challenger $\mathcal{C}$ runs Setup(1^z, ID, $\mathcal{U}$) to generate a public key PK and private key sets $SK_1, SK_2, \ldots, SK_N$. The challenger $\mathcal{C}$ gives SK_i to $\mathcal{A}$, where $U_i \notin S^*$.
Challenge. The challenger $\mathcal{C}$ runs $Enc^*(PK, S^*)$ and outputs $Hdr(S^*, m)$, where m is randomly chosen.
Guess. $\mathcal{A}$ outputs a guess m' for m.

Since $\mathcal{A}$ can always encrypt a chosen plaintext by himself, the oracle of encrypting a chosen plaintext does not matter in the definition. Let $\mathrm{Adv}^{ow\text{-}cpa}_{\mathcal{A},\Pi}(z)$ be the advantage that $\mathcal{A}$ wins the above game, that is,

$$\begin{aligned}\mathrm{Adv}^{ow\text{-}cpa}_{\mathcal{A},\Pi}(z) = \Pr[\mathcal{A}(PK, SK_{\mathcal{U}\setminus S^*}, Hdr(S^*, m)) = m : S^* \subseteq \mathcal{U}, \\ (PK, SK_{\mathcal{U}}) \leftarrow Setup(1^z, \mathrm{ID}, \mathcal{U}), Hdr(S^*, m) \leftarrow Enc^*(PK, S^*)].\end{aligned}$$

Definition 2. *A public key BE scheme Π=(Setup, Enc, Dec) is (t, ϵ)-OW-CPA secure if for all t-time bounded adversary $\mathcal{A}$, we have $Adv^{ow\text{-}cpa}_{\mathcal{A},\Pi}(z) < \epsilon$.*

3 The BE-PI Scheme

Let G and G_1 be the bilinear groups with the pairing function $\hat{e}$, where q is a large prime. Let $H_1, H_2 : \{0,1\}^* \rightarrow G_1$ be two hash functions and E be a symmetric encryption with key space G_1.

The idea of our construction is as follows. For a polynomial $f(x)$ of degree t, we assign each user U_i a share $f(i)$. The secret is $f(0)$. We can compute the secret $f(0)$ from any $t+1$ shares. If we want to revoke t users, we broadcast their shares. Any non-revoked user can compute the secret $f(0)$ from his own share and the broadcasted ones, totally $t+1$ shares. On the other hand, any collusion

of revoked users cannot compute the secret $f(0)$ since they have t shares only, including the broadcasted ones. If less than t users are revoked, we broadcast the shares of some dummy users such that t shares are broadcasted totally. In order to achieve $O(r)$ ciphertexts, we use $\log N$ polynomials, each for a range of the number of revoked users.

1. **Setup**(1^z, ID, $\mathcal{U}$): z is the security parameter, ID is the identity name of the system, and $\mathcal{U} = \{U_1, U_2, \ldots, U_N\}$ is the set of users in the system. Wlog, let N be a power of 2. Then, the system dealer does the following:
   - Choose a generator g of group G, and let $\lg = \log_g$ and $g_1 = \hat{e}(g, g)$.
   - Compute $h_i = H_1(\text{ID}\|i)$ for $1 \leq i \leq \log N$.
   - Compute $g^{a_j^{(i)}} = H_2(\text{ID}\|i\|j)$ for $0 \leq i \leq \log N$ and $0 \leq j \leq 2^i$.
     Remark. The underlying polynomials are, $0 \leq i \leq \log N$,

$$f_i(x) = \sum_{j=0}^{2^i} a_j^{(i)} x^j \pmod{q}.$$

     The system dealer does not know the coefficients $a_j^{(i)} = \lg H_2(\text{ID}\|i\|j)$. But, this does not matter.
   - Randomly choose a secret $\rho \in Z_q$ and compute g^ρ.
   - Publish the public key $PK = (\text{ID}, H_1, H_2, E, G, G_1, \hat{e}, g, g^\rho)$.
   - Assign a set $SK_k = \{s_{k,0}, s_{k,1}, \ldots, s_{k,\log N}\}$ of private keys to user U_k, $1 \leq k \leq N$, where

$$s_{k,i} = (g^{r_{k,i}}, g^{r_{k,i} f_i(k)}, g^{r_{k,i} f_i(0)} h_i^\rho)$$

     and $r_{k,i}$ is randomly chosen from Z_q, $1 \leq i \leq \log N$.
2. **Enc**(PK, S, M): $S \subseteq \mathcal{U}$, $R = \mathcal{U} \backslash S = \{U_{i_1}, U_{i_2}, \ldots, U_{i_l}\}$ is the set of revoked users, where $l \geq 1$. M is the sent message. The broadcaster does the following:
   - Let $\alpha = \lceil \log l \rceil$ and $L = 2^\alpha$.
   - Compute $h_\alpha = H_1(\text{ID}\|\alpha)$.
   - Randomly select distinct $i_{l+1}, i_{l+2}, \ldots, i_L > N$. These $U_{i_t}, l+1 \leq t \leq L$, are dummy users.
   - Randomly select a session key $m \in G_1$.
   - Randomly select $r \in Z_q$ and compute, $1 \leq t \leq L$,

$$g^{r f_\alpha(i_t)} = (\prod_{j=0}^{L} H_2(\text{ID}\|\alpha\|j)^{i_t^j})^r.$$

   - The ciphertext header $Hdr(S, m)$ is

$$(\alpha, m\hat{e}(g^\rho, h_\alpha)^r, g^r, (i_1, g^{r f_\alpha(i_1)}), (i_2, g^{r f_\alpha(i_2)}), \ldots, (i_L, g^{r f_\alpha(i_L)})).$$

   - The ciphertext body is $C = E_m(M)$.
3. **Dec**($SK_k, Hdr(S, m), C$): $U_k \in S$. The user U_k does the following.

– Compute $b_0 = \hat{e}(g^r, g^{r_{k,\alpha} f_\alpha(k)}) = g_1^{r r_{k,\alpha} f_\alpha(k)}$.
– Compute $b_j = \hat{e}(g^{r_{k,\alpha}}, g^{r f_\alpha(i_j)}) = g_1^{r r_{k,\alpha} f_\alpha(i_j)}$, $1 \le j \le L$.
– Use the Lagrange interpolation method to compute

$$g_1^{r r_{k,\alpha} f_\alpha(0)} = \prod_{j=0}^{L} b_j^{\lambda_j}, \tag{1}$$

where $\lambda_j = \frac{(-i_0)(-i_1)\cdots(-i_{j-1})(-i_{j+1})\cdots(-i_L)}{(i_j-i_0)(i_j-i_1)\cdots(i_j-i_{j-1})(i_j-i_{j+1})\cdots(i_j-i_L)} \pmod q$, $i_0 = k$.
– Compute the session key

$$\frac{m\hat{e}(g^\rho, h_\alpha)^r \cdot g_1^{r r_{k,\alpha} f_\alpha(0)}}{\hat{e}(g^r, g^{r_{k,\alpha} f_\alpha(0)} h_\alpha^\rho)} = \frac{m\hat{e}(g^\rho, h_\alpha)^r \cdot g_1^{r r_{k,\alpha} f_\alpha(0)}}{\hat{e}(g^r, h_\alpha^\rho) \cdot g_1^{r r_{k,\alpha} f_\alpha(0)}} = m. \tag{2}$$

– Use m to decrypt the ciphertext body C to obtain the message M.

Correctness. We can easily see that the scheme is correct by Equation (2).

3.1 Performance Analysis

For each system, the public key is $(\text{ID}, H_1, H_2, E, G, G_1, \hat{e}, g, g^\rho)$, which is of size $O(1)$. Since all systems can use the same $(H, E, G, G_1, \hat{e}, g)$, the public key specific to a system is simply (ID, g^ρ). Each system dealer has a secret ρ for assigning private keys to its users. Each user U_k holds private keys $SK_k = \{s_{k,0}, s_{k,1}, \ldots, s_{k,\log N}\}$, each corresponding to a share of polynomial f_i in the masked form, $0 \le i \le \log N$. The number of private keys is $O(\log N)$. When r users are revoked, we choose the polynomial f_α of degree 2^α for encrypting the session key, where $2^{\alpha-1} < r \le 2^\alpha$. Thus, the header size is $O(2^\alpha) = O(r)$. It is actually no more than $2r$.

To prepare a header, the broadcaster needs to compute one pairing function, $2^\alpha+2$ hash functions, and $2^\alpha+2$ modular exponentiations, which is $O(r)$ modular exponentiations.

For a user in S to decrypt a header, with a little re-arrangement of Equation (1) as

$$\prod_{j=0}^{L} b_j^{\lambda_j} = b_0^{\lambda_0} \cdot \hat{e}(g^{r_{k,\alpha}}, \prod_{j=1}^{L} (g^{r f_\alpha(i_j)})^{\lambda_j}),$$

the user needs to perform 3 pairing functions and 2^α modular exponentiations, which is $O(r)$ modular exponentiations. The evaluation of λ_j's can be done in $O(L) = O(2r)$ if the header consists of

$$\tilde{\lambda}_j = \frac{(-i_1)\cdots(-i_{j-1})(-i_{j+1})\cdots(-i_L)}{(i_j-i_1)\cdots(i_j-i_{j-1})(i_j-i_{j+1})\cdots(i_j-i_L)} \bmod q, 1 \le j \le L.$$

The user can easily compute λ_j's from $\tilde{\lambda}_j$'s. Inclusion of $\tilde{\lambda}_j$'s in the header does not affect the order of the header size.

3.2 Security Analysis

We show that it has OW-CPA security in the random oracle model under the BDH assumption.

Theorem 1. *Assume that the BDH problem is (t_1, ϵ_1)-hard. Our BE-PI scheme is $(t_1 - t', \epsilon_1)$-OW-CPA secure in the random oracle model, where t' is some polynomially bounded time.*

Proof. We reduce the BDH problem to the problem of computing the session key from the header by the revoked users. Since the polynomials $f_i(x) = \sum_{j=0}^{L} a_j^{(i)} x^j$ and secret shares of users for the polynomials are independent for different i's, we simply discuss security for a particular α. Wlog, let $R = \{U_1, U_2, \ldots, U_L\}$ be the set of revoked users and the target set of attack be $S^* = \mathcal{U} \backslash R$. Note that S^* was chosen by the adversary in the **Init** stage. Let the input of the BDH problem be (g, g^a, g^b, g^c), where the pairing function is implicitly known. We set the system parameters as follows:

1. Randomly select $\tau, \kappa, \mu_1, \mu_2, \ldots, \mu_L, w_1, w_2, \ldots, w_L \in Z_q$.
2. Set the public key of the system:
   (a) Let the input g be the generator g in the system.
   (b) Set $g^\rho = g^a$.
   (c) The public key is $(\text{ID}, H_1, H_2, E, G, G_1, \hat{e}, g, g^a)$.
   (d) The following is implicitly computed.
      – Set $f_\alpha(i) = w_i, 1 \le i \le L$.
      – Let $g^{a_0^{(\alpha)}} = g^{f_\alpha(0)} = g^a \cdot g^\tau = g^{a+\tau}$.
      – Compute $g^{a_i^{(\alpha)}}$, $1 \le i \le L$, from $g^{a_0^{(\alpha)}}$ and $g^{f_\alpha(j)} = g^{w_j}, 1 \le j \le L$, by the Lagrange interpolation method over exponents.
      – Set $h_\alpha = g^b \cdot g^\kappa = g^{b+\kappa}$.
      – For $j \ne \alpha$, choose a random polynomial $f_j(x)$ and set $h_j = g^{z_j}$, where z_j is randomly chosen from Z_q.
3. Set the secret keys $(g^{r_{i,j}}, g^{r_{i,j} f_j(i)}, g^{r_{i,j} f_j(0)} h_j^\rho)$, $0 \le j \le \log N$, of the revoked user $U_i, 1 \le i \le L$, as follows:
   (a) For $j = \alpha$, let $g^{r_{i,\alpha}} = g^{-b+\mu_i}$, $g^{r_{i,\alpha} f_\alpha(i)} = (g^{r_{i,\alpha}})^{w_i}$, and $g^{r_{i,\alpha} f_\alpha(0)} h_\alpha^\rho = g^{(-b+\mu_i)(a+\tau)} (g^{b+\kappa})^a = g^{a(\mu_i+\kappa) - b\tau + \mu_i \tau}$.
   (b) For $j \ne \alpha$, randomly choose $r_{i,j} \in Z_q$ and compute $g^{r_{i,j}}$, $g^{r_{i,j} f_j(i)}$ and $g^{r_{i,j} f_j(0)} h_j^\rho = g^{r_{i,j} f_j(0)} (g^a)^{z_j}$.
4. Set the header $(\alpha, m\hat{e}(g^\rho, h_\alpha)^r, g^r, (1, g^{r f_\alpha(1)}), (2, g^{r f_\alpha(2)}), \ldots, (L, g^{r f_\alpha(L)}))$ as follows:
   (a) Let $g^r = g^c$.
   (b) Compute $g^{r f_\alpha(i)} = (g^c)^{w_i}, 1 \le i \le L$.
   (c) Randomly select $y \in G_1$ and set $m\hat{e}(g^\rho, h_\alpha)^r = y$. We do not know what m is. But, this does not matter.

Assume that the revoked users together can compute the session key m. During computation, the users can query H_1 and H_2 hash oracles. If the query is of the form $H_2(\text{ID} \| i \| j)$ or $H_1(\text{ID} \| i)$, we set them to be $g^{a_j^{(i)}}$ and h_i, respectively.

If the query has ever been asked, we return the stored hash value for the query. For other non-queried inputs, we return random values in G.

We should check whether the distributions of the parameters in our reduction and those in the system are equal. We only check those related to α since the others are correctly distributed. Since $\tau, w_1, w_2, \ldots, w_L$ are randomly chosen, $g^{a_i^{(\alpha)}}, 0 \leq i \leq L$ are uniformly distributed over G^{L+1}. Due to the random oracle model, their corresponding system parameters are also uniformly distributed over G^{L+1}. Since $\kappa, \mu_1, \mu_2, \ldots, \mu_L$ are randomly chosen, the distribution of h_α and $g^{r_{i,\alpha}}, 1 \leq i \leq L$, are uniform over G^{L+1}, which is again the same as that of the corresponding system parameters. The distributions of g^r in the header and g^ρ in the public key are both uniform over G since they are set from the given input g^c and g^a, respectively. Since the session key m is chosen randomly from G_1, $m\hat{e}(g^\rho, h_\alpha)^r$ is distributed uniformly over G_1. We set it to a random value $y \in G_1$. Even though we don't know about m, it does not affect the reduction. Other parameters are dependent on what have been discussed. We can check that they are all computed correctly. So, the reduction preserves the right distribution.

If the revoked users compute m from the header with probability ϵ, we can solve the BDH problem with the same probability $\epsilon_1 = \epsilon$ by computing the following:

$$\begin{aligned} y \cdot m^{-1} \cdot \hat{e}(g^a, g^c)^{-\kappa} &= \hat{e}(g^\rho, h_\alpha)^r \cdot \hat{e}(g, g)^{-ac\kappa} \\ &= \hat{e}(g^a, g^{b+\kappa})^c \cdot \hat{e}(g, g)^{-ac\kappa} \\ &= \hat{e}(g, g)^{abc}. \end{aligned} \tag{3}$$

Let t' be the time for this reduction and the solution computation in Equation (3). We can see that t' is polynomially bounded. Thus, if the collusion attack of the revoked users takes $t_1 - t'$ time, we can solve the BDH problem within time t_1.

4 The BE-PI Scheme with IND-CCA Security

In Theorem 1, we show that the session key in the header is one-way secure against any collusion of revoked users. There are some standard techniques of transforming OW-CPA security to IND-CCA security. Here we present such a scheme Π' based on the technique in [9].

The IND-CCA security of the Fujisaki-Okamoto transformation depends only on the OW-CPA security of the public key encryption scheme, the FG security of a symmetric encryption scheme $\mathcal{E}$, and the γ-uniformity of the public key encryption scheme. The FG-security is the counterpart of the IND-security for symmetric encryption. A public key encryption scheme is γ-uniform if for every key pair (pk, sk), every message x, and $y \in \{0,1\}^*$, $\Pr[E_{pk}(x) = y] \leq \gamma$. Before applying the transformation, we check the following things:

1. The transformation applies to public key encryption, while ours is public key broadcast encryption. Nevertheless, if the authorized set S is fixed, our public

key broadcast encryption scheme is a public key encryption scheme with public key $pk = (PK, S)$. In the definition of IND-CCA security (Definition 1), the adversary $\mathcal{A}$ selects a target set S^* of users to attack in the **Init** stage and S^* is fixed through the rest of the attack. Thus, we can discuss the attack of $\mathcal{A}$ with a fixed target set S^*. Note that $\mathcal{A}$ is a static adversary.

2. Let S be a fixed authorized set of users. For every m and every $y \in \{0,1\}^*$, $\Pr[Hdr(S,m) = y]$ is either 0 or $1/q \simeq 1/2^z$, where z is the security parameter (the public key size). Thus, our broadcast encryption scheme is 2^{-z}-uniform if the authorized set is fixed.

Let $\mathcal{E} : K \times G_1 \to G_1$ be a symmetric encryption scheme with FG-security, where K is the key space of $\mathcal{E}$. Let $H_3 : G_1 \times G_1 \to Z_q$ and $H_4 : G_1 \to K$ be two hash functions. The modification of Π for Π' is as follows.

- In the **Setup** algorithm, add $\mathcal{E}, H_3, H_4$ to PK.
- In the **Enc** algorithm,

$$Hdr(S,m) = (g^r, \sigma\hat{e}(g^\rho, h_\alpha)^r, \mathcal{E}_{H_4(\sigma)}(m), \\ (i_1, g^{rf_\alpha(i_1)}), (i_2, g^{rf_\alpha(i_2)}), \ldots, (i_L, g^{rf_\alpha(i_L)})),$$

  where σ is randomly chosen from G_1 and $r = H_3(\sigma, m)$.
- In the **Dec** algorithm, we first compute $\bar{\sigma}$ as described in the BE-PI scheme. Then, we compute the session key $\bar{m}$ from $\mathcal{E}_{H_4(\sigma)}(m)$ by using $\bar{\sigma}$. We check whether $\sigma\hat{e}(g^\rho, h_\alpha)^r = \bar{\sigma}\hat{e}(g^\rho, h_\alpha)^{H_3(\bar{\sigma},\bar{m})}$ and $g^{rf_\alpha(i_j)} = g^{f_\alpha(i_j)H_3(\bar{\sigma},\bar{m})}$, $1 \le j \le L$. If they are all equal, $\bar{m}$ is outputted. Otherwise, $\perp$ is outputted.

Let q_{H_3}, q_{H_4} and q_D be the numbers of queries to H_3, H_4 and the decryption oracles, respectively. Our scheme Π' is IND-CCA-secure.

Theorem 2. *Assume that the BDH problem is (t_1, ϵ_1)-hard and the symmetric encryption $\mathcal{E}$ is (t_2, ϵ_2) FG-secure. The scheme Π' is $(t, \epsilon, q_{H_3}, q_{H_4}, q_D)$-IND-CCA secure in the random oracle model, where t' is some polynomially bounded time,*

$$t = \min\{t_1 - t', t_2\} - O(2z(q_{H_3} + q_{H_4})) \ \textit{and}$$
$$\epsilon = (1 + 2(q_{H_3} + q_{H_4})\epsilon_1 + \epsilon_2)(1 - 2\epsilon_1 - 2\epsilon_2 - 2^{-z+1})^{-q_D} - 1.$$

This theorem is proved by showing that if Π' is not IND-CCA-secure, then either Π is not OW-CPA-secure or $\mathcal{E}$ is not FG-secure directly. The OW-CPA security of Π is based on the BDH assumption. We note that the application of the transformation to other types of schemes could be delicate. Galindo [10] pointed out such a case. Nevertheless, the problem occurs in the proof and is fixable without changing the transformation or the assumption. The detailed proof will be given in the full version of the paper.

5 A Public Key SD Scheme

In the paradigm of subset cover for broadcast encryption [16], the system chooses a collection $\mathcal{C}$ of subsets of users such that each set S of users can be covered by the subsets in $\mathcal{C}$, that is, $S = \cup_{i=1}^{w} S_w$, where $S_i \in \mathcal{C}$ are disjoint, $1 \leq i \leq w$. Each subset S_i in $\mathcal{C}$ is associated with a private key k_i. A user is assigned a set of keys such that he can derive the private keys of the subsets to which he belongs. The subset keys k_i cannot be independent. Otherwise, each user may hold too many keys. It is preferable that the subset keys have some relations, for example, one can be derived from another. Thus, each user U_k is given a set SK_k of keys so that he can derive the private key of a subset to which he belongs. A subset-cover based broadcast encryption scheme plays the art of choosing a collection $\mathcal{C}$ of subsets, assigning subset and user keys, and finding subset covers.

5.1 The PK-SD-PI Scheme

We now present our PK-SD-PI scheme, which is constructed by using the polynomial interpolation technique on the collection of subsets in [16]. The system setup is similar to that of the BE-PI scheme. Consider a complete binary tree T of $\log N + 1$ levels. The nodes in T are numbered differently. Each user in $\mathcal{U}$ is associated with a different leaf node in T. We refer to a complete subtree rooted at node i as "subtree T_i". For each subtree T_i of η levels (level 1 to level η from top to bottom), we define the degree-1 polynomials

$$f_j^{(i)}(x) = a_{j,1}^{(i)} x + a_{j,0}^{(i)} \pmod{q},$$

where $a_{j,0}^{(i)} = \lg H_2(\text{ID} \| i \| j \| 0)$ and $a_{j,1}^{(i)} = \lg H_2(\text{ID} \| i \| j \| 1)$, $2 \leq j \leq \eta$. For a user U_k in the subtree T_i of η levels, he is given the private keys

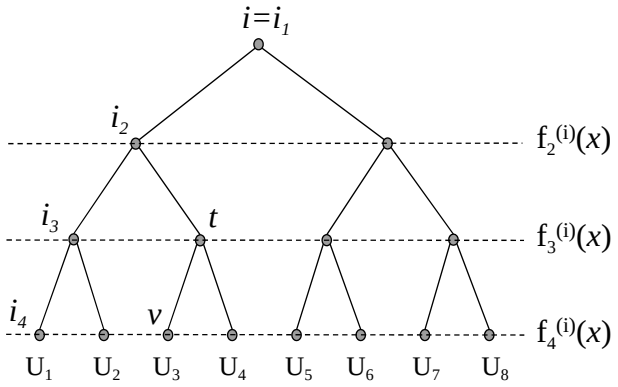
$$s_{k,i,j} = (g^{r_{k,i,j}}, g^{r_{k,i,j} f_j^{(i)}(i_j)}, g^{r_{k,i,j} f_j^{(i)}(0)} h^{\rho})$$

for $2 \leq j \leq \eta$, where nodes $i_1, i_2, \ldots, i_\eta$ are the nodes in the path from node i to the leaf node for U_k (including both ends). We can read $s_{k,i,j}$ as the private key of U_k for the jth level of subtree T_i. In Figure 1, the private keys (in the unmasked form) of U_1 and U_3 for subtree T_i with $\eta = 4$ are given. Here, we use h^{ρ} in all private keys in order to save space in the header.

Recall that in the SD scheme, the collection $\mathcal{C}$ of subsets is

$$\{S_{i,t} : \text{ node } i \text{ is a parent of node } t, i \neq t\},$$

where $S_{i,t}$ denotes the set of users in subtree T_i, but not in subtree T_t. By our design, if the header contains a masked share for $f_j^{(i)}(t)$, where node t is in the j-th level of subtree T_i, only user U_k in $S_{i,t}$ can decrypt the header by using his private key $s_{k,i,j}$, that is, the masked form of $f_j^{(i)}(s)$, for some $s \neq t$. In Figure 1, the share $f_3^{(i)}(t)$ is broadcasted so that only the users in $S_{i,t}$ can decrypt the header.



– U_1 holds masked shares of $f_2^{(i)}(i_2)$, $f_3^{(i)}(i_3)$, $f_4^{(i)}(i_4)$
– U_3 holds masked shares of $f_2^{(i)}(i_2)$, $f_3^{(i)}(t)$, $f_4^{(i)}(v)$
– For subset $S_{i,t}$, a masked share of $f_3^{(i)}(t)$ is broadcasted so that U_3 and U_4 cannot decrypt, but others can.

Fig. 1. Level polynomials, private keys and broadcasted shares for subtree T_i.

For a set R of revoked users, let S_{i_1,t_1}, $S_{i_2,t_2}, \ldots$, S_{i_z,t_z} be a subset cover for $\mathcal{U}\backslash R$, the header is

$$(m\hat{e}(g^{\rho},h)^{r}, g^{r}, (i_1,t_1,g^{rf_{j_1}^{(i_1)}(t_1)}), \ldots, (i_z,t_z,g^{rf_{j_z}^{(i_z)}(t_z)})),$$

where node t_k is in the j_k-th level of subtree T_{i_k}, $1 \leq k \leq z$.

For decryption, a non-revoked user finds $i_k, t_k, g^{rf_{j_k}^{(i_k)}(t_k)}$ (corresponding to S_{i_k,t_k} where he is in) from the header and applies the Lagrange interpolation to compute the session key m.

Performance. The public key is $O(1)$, which is the same as that of the BE-PI scheme. Each user belongs to at most $\log N + 1$ subtrees and each subtree has at most $\log N + 1$ levels. For the subtree of η levels, the user in the subtree holds $\eta - 1$ private keys. Thus, the total number of shares (private keys) held by each user is $\sum_{i=1}^{\log N} i = O(\log^2 N)$. According to [16], the number z of subsets in a subset cover is at most $2|R| - 1$, which is $O(r)$

When the header streams in, a non-revoked user U_k looks for his containing subset S_{i_j,t_j} to which he belongs. With a proper numbering of the nodes in T, this can be done very fast, for example, in $O(\log \log N)$ time. Without considering the time of scanning the header to find out his containing subset, each user needs to perform 2 modular exponentiations and 3 pairing functions. Thus, the decryption cost is $O(1)$.

Security. We first show that the scheme is one-way secure.

Theorem 3. *Assume that the BDH problem is $(t_1,\ \epsilon_1)$-hard. Our PK-SD-PI scheme is $(t_1 - t', \epsilon_1)$-OW-CPA secure in the random oracle model, where t' is some polynomially bounded time.*

Proof. The one-way security proof for the PK-SD-PI scheme is similar to that for the BE-PI scheme. In the PK-SD-PI scheme, all polynomials $f_j^{(i)}(x)$ are of degree one. Let (g, g^a, g^b, g^c) be the input to the BDH problem. Let $S_{i_1,t_1}, S_{i_2,t_2}, \ldots, S_{i_z,t_z}$ be a subset cover for $S^* = \mathcal{U}\backslash R$. Due to the random oracle assumption for H_1 and H_2, all polynomials are independent. Thus, we can simply consider a particular $S_{\alpha,t}$ in the subset cover for $S^* = \mathcal{U}\backslash R$, where t is at level β of subtree T_α. The corresponding polynomial is $f(x) = f_\beta^{(\alpha)}(x) = a_1 x + a_0 \pmod q$. Wlog, let $\{U_1, U_2, \ldots, U_l\}$ be the set of revoked users that have the secret share about $f(t)$. The reduction to the BDH problem is as follows. Recall that the public key of the PK-SD-PI method is $(\text{ID}, H_1, H_2, E, G, G_1, \hat{e}, g, g^\rho)$.

1. Let g be the generator in the system and $g^\rho = g^a$.
2. Set $f(t) = w$ and compute $g^{f(t)} = g^w$, where w is randomly chosen from Z_q.
3. Let $g^{a_0} = g^{f(0)} = g^a \cdot g^\tau$, where τ is randomly chosen from Z_q.
4. Compute g^{a_1} from $g^{f(t)}$ and g^{a_0} via the Lagrange interpolation.
5. The (random) hash values $H_2(\text{ID}\|\alpha\|\beta\|0)$ and $H_2(\text{ID}\|\alpha\|\beta\|1)$ are set as g^{a_0} and g^{a_1} respectively.
6. Set $h = g^b \cdot g^\kappa$, where κ is randomly chosen from Z_q.
7. The $f(x)$-related secret share of $U_i, 1 \le i \le l$, is computed as $(g^{r_i},\ g^{r_i f(t)},\ g^{r_i f(0)} h^\rho)$, where $g^{r_i} = g^{-b} \cdot g^{\mu_i}$ and μ_i is randomly chosen from Z_q. Note that $g^{r_i f(0)} h^\rho = g^{a(\mu_i+\kappa)-b\tau+\mu_i\tau}$ can be computed from the setting in the previous steps.
8. The non-$f(x)$-related secret shares of $U_i, 1 \le i \le l$, can be set as follows. Let f' be a polynomial related to subtree α' and level β', where t' is in the β'-th level and $U_i \in S_{\alpha',t'}$. The secret share $(g^{r_i'}, g^{r_i' f'(t')}, g^{r_i' f'(0)} h^\rho)$ of U_i is computed from $(g^{r_i}, g^{r_i f(t)}, g^{r_i f(0)} h^\rho)$. Let $f'(t') = w'$, $f'(0) = f(0) + a'$ and $r_i' = r_i + r'$, where w', a', and r' are randomly chosen from Z_q. Thus, $g^{r_i'} = g^{r_i} \cdot g^{r'}$, $g^{r_i' f'(t')} = (g^{r_i'})^{w'}$ and $g^{r_i' f'(0)} h^\rho = (g^{r_i f(0)} h^\rho) \cdot g^{r' f(0)} \cdot g^{r_i a'} \cdot g^{r' a'}$. Note that the hash values $H_2(\text{ID}\|\alpha'\|\beta'\|0)$ and $H_2(\text{ID}\|\alpha'\|\beta'\|1)$ can be answered accordingly.
9. Set the challenge as

$$(y, g^c, (i_1, t_1, g^{c f_{j_1}^{(i_1)}(t_1)}), (i_2, t_2, g^{c f_{j_2}^{(i_2)}(t_2)}), \ldots, (i_z, t_z, g^{c f_{j_z}^{(i_z)}(t_z)})),$$

   where y is randomly chosen from G and thought as $m\hat{e}(g^\rho, h)^c$. Note that $g^{c f_{j_k}^{(i_k)}(t_k)}, 1 \le k \le z$, can be computed since $f_{j_k}^{(i_k)}(t_k)$ is a number randomly chosen from Z_q, as described in Step 2.

If the revoked users $U_1, U_2, \ldots, U_l$ can together compute the session key m from the challenge with probability ϵ_1, we can compute

$$\begin{aligned} y \cdot m^{-1} \cdot \hat{e}(g^a, g^c)^{-\kappa} &= \hat{e}(g^\rho, h)^c \cdot \hat{e}(g, g)^{-ac\kappa} \\ &= \hat{e}(g^a, g^{b+\kappa})^c \cdot \hat{e}(g, g)^{-ac\kappa} = \hat{e}(g, g)^{abc} \end{aligned} \tag{4}$$

with the same probability ϵ_1. This contradicts the BDH assumption.

Let t' be the time for the reduction and solution computation in Equation (4), where t' is polynomially bounded. Thus, if the collusion attack takes $t_1 - t'$, we can solve the BDH problem in time t_1.

Similarly, we can modify our PK-SD-PI scheme to have IND-CCA security like Section 4

5.2 The PK-LSD-PI Scheme

The LSD method is an improvement of the SD method by using a sub-collection $\mathcal{C}'$ of $\mathcal{C}$ in the SD method. The basic observation is that $S_{i,t}$ can be decomposed to $S_{i,k} \cup S_{k,t}$. The LSD method delicately selects C' such that each $S_{i,t} \in \mathcal{C}$ is either in $\mathcal{C}'$ or equal to $S_{i,k} \cup S_{k,t}$, where $S_{i,k}$ and $S_{k,t}$ are in $\mathcal{C}'$. The subset cover found for $\mathcal{U} \backslash R$ in the SD method is used except that each $S_{i,t}$ in the cover, but not in C', is replaced by two subsets $S_{i,k}$ and $S_{k,t}$ in C'. Thus, each user belongs to a less number of $S_{i,t}$'s in C' such that it holds a less number of private keys.

We consider the basic case of the LSD method, in which each user holds $(\log n)^{3/2}$ private keys. There are $\sqrt{\log n}$ "special" levels in T. The root is at a special level and every level of depth $k \cdot \sqrt{\log n}$, $1 \leq k \leq \sqrt{\log n}$, is special. A layer is the set of the levels between two adjacent special levels. Each layer has $\sqrt{\log n}$ levels. The collection $\mathcal{C}'$ of the LSD method is

$$\{S_{i,t} : \text{ nodes } i \text{ and } t \text{ are in the same layer, or node } i \text{ is at a special level}\}.$$

There are two types of $S_{i,t}$'s in $\mathcal{C}'$. The first type is that node i is in a special level and the second type is that nodes i and t are in the same layer. Every non-revoked set $\mathcal{U} \backslash R$ can be covered by at most $4|R| - 2$ disjoint subsets in $\mathcal{C}'$.

Our PK-LSD-PI scheme is as follows. Since $\mathcal{C}'$ is just a sub-collection of $\mathcal{C}$ in the SD method, our PK-LSD-PI scheme is almost the same as the PK-SD-PI scheme except that some polynomials for type-2 $S_{i,t} \in \mathcal{C}'$ are unnecessary. Consider a user U_k (or its corresponding leaf node). For his ancestor node i at a special layer (type-1 $S_{i,t}$'s), U_k is given the private keys (corresponding to subtree T_i) by the same way as the PK-SD-PI method. There are $\sqrt{\log n}$ such i's and each T_i has at most $\log n$ levels. In this case, U_k holds $(\log n)^{3/2}$ private keys. For his ancestor node i and nodes t in the same layer (type-2 $S_{i,t}$'s), choose degree-1 polynomials for the levels between i and its (underneath) adjacent special level only. There are at most $\sqrt{\log n}$ such polynomials and U_k is assigned corresponding $\sqrt{\log n}$ private keys as the PK-SD-PI scheme does. In this case, U_k holds at most $\log n \cdot \sqrt{\log n}$ private keys since U_k has $\log n$ ancestors. Overall, each user U_k holds at most $2(\log n)^{3/2}$ private keys.

Security. We show that the scheme described in this subsection is one-way secure.

Theorem 4. *Assume that the BDH problem is (t_1, ϵ_1)-hard. Our PK-LSD-PI scheme is $(t_1 - t', \epsilon_1)$-OW-CPA secure in the random oracle model, where t' is some polynomially bounded time.*

Proof. The collection of $S_{i,t}$'s for covering $\mathcal{U}\backslash R$ in the LSD method is a sub-collection of that in the SD method. The way of assigning private keys to users is the same as that of the PK-SD-PI scheme except that we omit the polynomials that are never used due to the way of choosing a subset cover in the LSD method. In the random oracle model, we can simply consider a particular $S_{\alpha,t}$ in the subset cover for $\mathcal{U}\backslash R$. Since all conditions are the same, the rest of proof is the same as that in Theorem 3.

With the same extension in [12], we can have a PK-LSD-PI scheme that has $O(1)$ public keys and $O(\log^{1+\epsilon})$ private keys, for any constant $0 < \epsilon < 1$. The header size is $O(r/\epsilon)$, which is $O(r)$ for a constant ϵ. The decryption cost excluding the time of scanning the header is again $O(1)$.

6 Conclusion

We have presented very efficient public key BE schemes. They have low public and private keys. Two of them even have a constant decryption time. Our results show that the efficiency of public key BE schemes is comparable to that of private-key BE schemes.

We are interested in reducing the ciphertext size while keeping other complexities low in the future.

Acknowledgement

We thank Eike Kiltz and Michel Abdalla for valuable comments on the manuscript.

References

1. N. Attrapadung, H. Imai. Graph-decomposition-based frameworks for subset-cover broadcast encryption and efficient instantiations. In *Proceedings of Advances in Cryptology - Asiacrypt 05*, Lecture Notes in Computer Science 3788, pp.100-120, Springer, 2005.
2. D. Boneh, X. Boyen, E.-J. Goh. Hierarchical identity based encryption with constant size ciphertext. In *Proceedings of Advances in Cryptology - Eruocrypt 05*, Lecture Notes in Computer Science 3494, pp.440-456, Springer, 2005.
3. D. Boneh, M. Franklin. An efficient public key traitor tracing scheme. In *Proceedings of Advances in Cryptology - Crypto 99*, Lecture Notes in Computer Science 1666, pp.338-353, Springer, 1999.
4. D. Boneh, C. Gentry, B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In *Proceedings of Advances in Cryptology - Crypto 05*, Lecture Notes in Computer Science 3621, pp.258-275, Springer, 2005.
5. D. Boneh, B. Waters. A fully collusion resistant broadcast, trace, and revoke system. In *Proceedings of the ACM Conference on Computer and Communications Security - CCS 06*, pp.211-220, ACM Press, 2006.
6. Y. Dodis, N. Fazio. Public key broadcast encryption for stateless receivers. In *Proceedings of Digital Right Management 02 - DRM 02*, Lecture Notes in Computer Science 2696, pp.61-80, Springer, 2002.

7. Y. Dodis, N. Fazio. Public key broadcast encryption secure against adaptive chosen ciphertext attack. In *Proceedings of Public Key Cryptography - PKC 03*, Lecture Notes in Computer Science 2567, pp.100-115, Springer, 2003.
8. A. Fiat, M. Naor. Broadcast encryption. In *Proceedings of Advances in Cryptology - Crypto 93*, Lecture Notes in Computer Science 773, pp.480-491, Springer, 1993.
9. E. Fujisaki, T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In *Proceedings of Advances in Cryptology - Crypto 99*, Lecture Notes in Computer Science 1666, pp.537-554, Springer, 1999.
10. D. Galindo. Boneh-Franklin identity based encryption revisited. In Proceedings of ICALP 05, Lecture Notes in Computer Science 3580, pp.791-802, Springer, 2005.
11. M.T. Goodrich, J.Z. Sun, R. Tamassia. Efficient Tree-Based Revocation in Groups of Low-State Devices. In *Proceedings of Advances in Cryptology - Crypto 04*, Lecture Notes in Computer Science 3152, pp.511-527, Springer, 2004.
12. D. Halevy, A. Shamir. The LSD broadcast encryption scheme. In *Proceedings of Advances in Cryptology - Crypto 02*, Lecture Notes in Computer Science 2442, pp.47-60, Springer, 2002.
13. K. Kurosawa, Y. Desmedt. Optimum traitor tracing and asymmetric schemes. In *Proceedings of Advances in Cryptology - Eurocrypt 98*, Lecture Notes in Computer Science 1403, pp.145-157, Springer, 1998.
14. K. Kurosawa, T. Yoshida. Linear code implies public-key traitor tracing. In *Proceedings of Public Key Cryptography*, Lecture Notes in Computer Science 2274, pp.172-187, Springer, 2002.
15. J.W. Lee, Y.H. Hwang, P.J. Lee. Efficient public key broadcast encryption using identifier of receivers. In *Proceedings of International Conference on Information Security Practice and Experience - ISPEC 06*, Lecture Notes in Computer Science 3903, pp.153-164, Springer, 2006.
16. D. Naor, M. Naor, J. Lotspiech. Revocation and tracing schemes for stateless receivers. In *Proceedings of Advances in Cryptology - Crypto 01*, Lecture Notes in Computer Science 2139, pp.41-62, Springer, 2001.
17. M. Naor, B. Pinkas. Efficient trace and revoke schemes. In *Proceedings of Financial Cryptography 00*, Lecture Notes in Computer Science 1962, pp.1-20, Springer, 2000.
18. A. Shamir. How to share a secret. *Communications of the ACM*, 22(11), pp.612-613, 1979.
19. W.-G. Tzeng, Z.-J. Tzeng. A public-key traitor tracing scheme with revocation using dynamic shares. In *Proceedings of Public Key Cryptography - PKC 01*, Lecture Notes in Computer Science 1992, pp.207-224, Springer, 2001.
20. P. Wang, P. Ning, D.S. Reeves. Storage-efficient stateless group key revocation. In *Proceedings of the 7th Information Security Conference - ISC 04*, Lecture Notes in Computer Science 3225, pp.25-38, Springer, 2005.
21. E.S. Yoo, N.-S. Jho, J.J. Cheon, M.-H. Kim. Efficient broadcast encryption using multiple interpolation methods. In *Proceedings of ICISC 04*, Lecture Notes in Computer Science 3506, pp.87-103, Springer, 2005.
22. M. Yoshida, T. Fujiwara. An efficient traitor tracing scheme for broadcast encryption. In *Proceedings of 2000 IEEE International Symposium on Information Theory*, pp.463, IEEE Press, 2000.

出席 2008 公開金鑰密碼會議 (PKC 2008) 報告

一、 時間與地點：3/9 - 3/12, 2008，巴塞隆納 西班牙。

二、 參加會議經過

第十一屆公開金鑰密碼會議（11th International Workshop on Practice and Theory in Public Key Cryptography，簡稱為 PKC 2008）為國際密碼研究學會（International Association for Cryptologic Research，簡稱為 IACR)主辦，今年的承辦單位為西班牙巴塞隆納市的 Universitat Politenica de Catalunya (UPC)。會議在 UPC 的北校園舉行，與會人數約 100 人，其中來自台灣的與會者只有筆者一人。會議為期四天（3/9~3/12），會議中安排了三場邀請演講，每天一場，相當精采，其餘皆是論文發表，3/10 下午有一參觀古修道院的活動。整體來說，這次的會議因為在學校內舉辦，較為簡單，但會場內討論的氣氛卻很熱烈，大家的發問都很踴躍，休息時間也可看到許多相互交流與討論。

三、 發表論文介紹

我們這次所發表的論文為 ”Public Key Encryption Schemes with Low Number of Keys and Constant Decryption Time”，主要是公開金鑰廣播加密的問題，廣播加密分為私密金鑰式的和公開金鑰式的，差別在於第三者是否可以廣播訊息給使用者。已往對於私密金鑰式廣播加密系統的問題已提出最佳解，因此研究轉到公開金鑰式的系統，先前的研究對於一些效率參數還無法達到很好，本篇論文提出第一個公開金鑰式廣播加密系統，具有 O (1)公開金鑰、每位使用者 O(log N) 私密金鑰及 O (r) 密文大小。其中還有一個系統的解密時間是 O(1)。這些系統是目前最好的公開金鑰式廣播加密協定。在我報告完後，與會的學者表達了高度的興趣，認為使用多項式在這樣的系統上，用得很巧妙，再加上雙線性函數與雜湊函數的使用，實在是一個很不錯的創新。

詳細的內容請見論文。

四、 與會心得

本次會議共有 71 篇論文送審，最後有 21 篇論文發表，每篇發表的時間為 30 分鐘，分為 8 個不同的主題：

1. Algebraic and Number Theoretical Cryptanalysis (I)
2. Theory of Public Key Encryption
3. Digital Signatures (I)
4. Identification, Broadcast and Key Agreement
5. Implementation of Fast Arithmetic

6. Digital Signatures (II)
7. Algebraic and Number Theoretical Cryptanalysis (II)
8. Public Key Encryption

由於會議主旨是討論公開金鑰密碼系統，因此大部分的論文都與公開金鑰系統相關。來自台灣的只有筆者的論文。大部分的論文都在一些目前比較熱門的題目上面做變化，增強安全性或效率，或是修改使其能擴充應用範圍，真正提出新概念的論文較少。今年的最佳論文是由 Vadim Lyubashevsky 所發表的「Lattice-Based Identification Schemes Secure Under Active Attacks」。以下我們就針對幾篇還不錯的論文，做一些簡單的介紹：

1. Vadim Lyubashevsky, "Lattice-Based Identification Schemes Secure Under Active Attacks"

   本篇論文是今年度的 PKC 最佳論文，以往有關 3 步驟 (3-move) 的 identification 都是基於一些困難的數論問題，較少基於其他類型的困難問題，本篇論文提出基於 lattice 困難問題的 identification scheme，只有三步驟。論文中有用了有名的 leftover hash lemma，筆者也曾在一篇論文中使用這個定理，可以這個定理的用途很廣。

2. Pierre-Alain Fouque, Gilles Macario-Rat, Ludovic Perret, Jacques Stern, "Total Break of the l-IC Signature Scheme"

   破解密碼協定是密碼研究重要的一環，本篇論文破解一篇在 PKC 2007 上發表的論文（Ding, Wolf, Yang, "l-Invertible Cycles for Multivariate Quadratic Pulic Key Cryptography"），該論文是屬於 multivariate cryptography，使用多變數多方程式來是設計密碼系統，目前這類的密碼協定都宣稱其計算速度較快，較有效率，因為不需做指數運算。但是近來發展的一些攻擊技術使得這類的密碼協定常遭受攻擊。本論文使用 Dubois 等人發展來攻擊 SFLASH 簽章的技術，破解了 l-IC 簽章，是完全破解，可以得到一把等價的簽名金鑰。

3. Miaoqing Huang, Kris Gaj, Soonhak Kwon, Tarek El-Ghazawi, "An Optimized Hardware Architecture for the Montgomery Multiplication Algorithm".

   本論文是針對有名的 Montgomery 乘法演算法設計新的硬體架構，主要是利用部分計算的觀念，先預測最高位元的值。本論文使用新設計的 radix-2 架構，而且已經利用 FPGA 實做出來驗證過。

五、 建議

和以往的重要的密碼會議一樣，這次會議看到許多很優秀的論文發表，發表論文的學者在論文的撰寫上面都很有經驗，各種安全性的定義及證明都寫得非常正式與嚴謹，這是我國密碼學者應該仿效與學習的目標，以現在的環境來說，一定要能夠寫出像他們一樣嚴謹的定義與證明才有可能在好的國際會議發表，否則就算構想再好，沒有這些基礎的功力，還是沒辦法受到青睞。由於在密碼學的領

域當中，好的國際會議往往是各國學者注目的焦點，發表在這些會議上，才容易會受到大家的重視與肯定。另外，各國學者在會議期間積極的討論與交流的態度，也是我們該學習的項目，希望我國學者能多與國外學者交流與的討論，如此才能提升研究的水準，與世界的密碼研究接軌。

六、 攜回資料名稱與內容

1. PKC 2008 論文集一本。
2. 參加人員名單與聯繫資料一份。
3. 相關會議的 CFP。