J Ambient Intell Human Comput (2015) 6:121–129
DOI 10.1007/s12652-014-0253-8

ORIGINAL RESEARCH

Improved broadcast encryption schemes with enhanced security

Lishan Ke · Zongxiang Yi · Yan Ren

Received: 14 August 2014 / Accepted: 28 October 2014 / Published online: 23 December 2014

Abstract A broadcast encryption scheme is one of important primitives to achieve message confidentiality in distributed network, which supports one-to-many encryption under insecure channels. In this paper, we show that any balanced incomplete block design constructed by perpendicular array can be used to realize secure BE schemes. Its broadcast rate, broadcast information rate and the upper bound of the number of collusion resistant are also obtained. According to the characteristics of the block, a more efficient broadcast encryption, using the strong part balanced incomplete block design constructed by rational normal curve is presented. This scheme is secure under an enhanced security model compared with the first construction. Particularly, even any two users are absent in the block, it can achieve fully collusion resistant. Moreover, an improved scheme is given based on the efficiency comparison of these two schemes, in which the broadcast rate is invariant while its broadcast information rate is significantly higher than that of the first construction. Finally, we propose a block reservation scheme, which provides the function of appending users dynamically.

L. Ke (✉) · Z. Yi
College of Mathematics and Information Science, Key Laboratory of Mathematics and Interdisciplinary Sciences of Guangdong Higher Education Institutes, Guangzhou University, Guangzhou, Guangdong 510006, People's Republic of China
e-mail: keyao1986@163.com

Z. Yi
Guangdong University of Science and Technology, Guangzhou, DongGuan 523000, People's Republic of China
e-mail: tpu01yzx@gmail.com

Y. Ren
Department of Applied Mathematics, Yuncheng University, Yuncheng, Shanxi 044000, People's Republic of China

Keywords Broadcast encryption · Block designs · Dual designs · Forward secrecy

1 Introduction

Broadcast encryption (BE) is an important primitive for broadcasting messages to a group of users with only one-time encryption. It can dynamically select user groups in order to send messages. In this way, only the privileged users are able to obtain their information while the unauthorized users cannot decrypt and extract the message even they collude. The concept of BE was firstly introduced by Fiat and Naor (1994). After that, many BE schemes and some related properties (Boneh and Franklin 1999; Dodis and Fazio 2002; Boneh et al. 2005; Naor et al. 2001; Halevy and Shamir 2002; Stinson and Van Trung 1998; Shamir 1979; Libert et al. 2012; Li et al. 2010, 2013; Zhao and Zhang 2011; Fazio and Perera 2012) were proposed to achieve different functions such as the better efficiency or enhanced security et al. These works are divided into two categories, that is, the symmetric BE and asymmetric BE.

In asymmetric BE, each user is issued a public and private key pair. There is no broadcast center and any user is able to encrypt a message to a set of users. However, in symmetric BE, each user only has private keys, which is issued from a central authority. The symmetric broadcast encryption always achieves better efficiency compared with the asymmetric BE (Boneh and Franklin 1999; Dodis and Fazio 2002; Boneh et al. 2005). Thus, most applications utilize the symmetric BE to save the computational cost.

In a symmetric BE, there are three phases including set-up phase, transmission phase, decryption phase. It allows users to pre-distribute secret information (Stinson 1997;

Quinn 1994) by the center during the set-up phase of this system. After each user in the group gets a private key, they can communicate with each through efficient BE. In the transmission phase, to encrypt a message, a session key is generated and the message is encrypted using the session key. After that, the user also encrypts the session key with public parameters and public keys of the set of privileged users. In the decryption phase, a privileged user uses his/her secret information to obtain one of the keys with which the session key has been encrypted. There are two important parameters of a BE scheme from the perspective of efficiency. They are broadcast rate and broadcast information rate. Moreover, the tolerance of maximum number of colluding users is also an important security parameter of a BE scheme. Thus, how to construct a efficient BE scheme with better broadcast rate and broadcast information rate is a challenge.

1.1 Related work

As mentioned before, broadcast encryption allows a sender to select an arbitrary set of receivers S, in the encryption algorithm (Fiat and Naor 1994). Naor et al. (2001) proposed the first fully collusion-resistant BE scheme called NNL-BE, which uses a tree structure. The NNL-BE scheme (Naor et al. 2001) is defined for n users where n is a power of two, i.e, $n = 2^{l_0}$ for some $l_0 > 0$. During the construction of the tree, each user is considered to be a leaf of a full binary tree with l_0 levels. A subsequent work by Halevy and Shamir (2002) introduced a variant of the SD method, which is called the layered subset difference (LSD) scheme. However, this work is also defined for n users where $n = 2^{l_0}$. Different from the above one, the basic idea is to partition the tree into several layers.

Another important tool for the construction of BE was introduced by Stinson and Van Trung (1998), which is called balanced incomplete block design (BIBD) method. Unlike the previous works, this scheme allows arbitrary number of users, without the restriction of the number of users. In BIBD, any subset of users is considered to be the blocks while users are considered to be the points of the block. Two important parameters, namely broadcast rate and broadcast information rate in BE scheme, are defined (Stinson and Van Trung 1998).

There are two kinds of security definitions for BE, that is, the BE with adaptive security and static security. Most of the previous can only achieve static security (Yao et al. 2008). To dynamically allow users to join or leave the system, it additionally has to rely some trusted authority in these works. In more details, the adaptive security allows the adversary to see some corrupted users' private keys and public keys adaptively. For static security, the adversary can only determine the set of the corrupted users before the setup of the system. Thus, for practical applications, it prefers the adaptive security. There are also some results on how to transform a BE with static security to adaptive security. Therefore, it is only necessary to construct a static BE in theory as it can be transformed into adaptive secure BE. However, such direct transformation has some restriction as the huge computational overhead.

1.2 Our contributions

In this paper, according to the BIBD technique introduced in Stinson and Van Trung (1998), we prove that the BE scheme can be constructed from any BIBD. Then we prove that perpendicular array can construct BIBD where broadcast rate and broadcast information rate are $t\left(n\lambda_t\binom{s-\tau}{t-\tau}\right)^{-1}$ and $\left(\lambda_t\binom{s}{t}\right)^{-1}$, respectively. Furthermore, the tolerance of the maximum number of colluding users is $\lfloor\frac{1}{2}+\frac{1}{2}\sqrt{1+8\frac{s-1}{n(n-1)}}\rfloor$.

Considering the demand for reducing the number of blocks, we point out that scheme based on strong partly balanced incomplete block design (SPBIBD) achieves better performance. Particularly, when colluding users do not belong to the same group, they can not learn any secret information. Increasing broadcast information rate is another contribution of our work. The construction using block design has a low rate of broadcast information because of its huge number of blocks. Thus in this paper, we use dual design to improve the basic construction and optimize broadcast information rate.

Ensuring the forward secrecy is another contribution in this paper. We point out that a method of "reserve block" ensures that the keys of members remain the same. However, the public key for blocks can be automatically updated when a new member joins.

2 Preliminaries

In this section, we briefly introduce some definitions of blocks design technique.

2.1 Broadcast structure

In this section, we briefly introduce some definitions for broadcast encryption.

Definition 2.1 Let $\mathcal{V}$ and $\mathcal{B}$ be two disjoint sets, and $\mathcal{I}$be a binary relation between $\mathcal{V}$ and $\mathcal{B}$, namely $\mathcal{I} \subseteq \mathcal{V} \times \mathcal{B}$. Then we say that $\mathcal{D} = (\mathcal{V}, \mathcal{B}, \mathcal{I})$ is an incidence structure.

The elements of $\mathcal{V}$ and $\mathcal{B}$ are defined for point and block, and $\mathcal{I}$ is called incidence relation.

Let $p \in \mathcal{V}, B \in \mathcal{B}$, if $(p, B) \in \mathcal{I}$, namely p and B are of incidence relation. It is described as $p\mathcal{I}B$.

Let $\mathcal{D} = (\mathcal{V}, \mathcal{B}, \mathcal{I})$ be a limited incidence structure, in which $\mathcal{V}$ and $\mathcal{B}$ are limited sets. If $p \in \mathcal{V}, B \in \mathcal{B}$, let r_p be the multiplicity of p while k_B be the capacity of B. If S be any t-subset of $\mathcal{V}$, then λ_s is the number of blocks which is of incidence relation with every point of S.

We also give the following definitions used in this construction.

1. Regularity: There are constants r such that for all $p \in \mathcal{V}$, we have $r_p = r$;
2. Uniformity There are constants k such that for all $B \in \mathcal{B}, k_B = k$;
3. t-equilibration: For a given positive integer t, there are a constant λ such that for any t-subset $S, \lambda_s = \lambda$.

Particularly, 1-equilibration is regularity, while 2-equilibration is equilibration. The limited incidence structure which satisfies the conditions of regularity, uniformity and equilibration is called balanced incomplete block design.

2.2 Balanced incomplete block design

In this section, we show some notions and definitions of balanced incomplete block design.

Definition 2.2 (Colbourn and Charles 1996) A balanced incomplete block design (BIBD) is a pair $(\mathcal{V}, \mathcal{B})$ where $\mathcal{V}$ is a $v-$set and $\mathcal{B}$ is a collection of b $k-$set of $\mathcal{V}$ (blocks) such that each element of $\mathcal{V}$ is contained in exactly r block and any 2-subset of $\mathcal{V}$ is contained in exactly λ blocks. The number v, b, r, k, λ are parameters of the BIBD.

Lemma 2.3 (Colbourn and Charles 1996) *Trivial condition for the existence of a BIBD* (v, b, r, k, λ) *are* (1) $vr = bk$, *and* (2) $r(k-1) = \lambda(v-1)$. *Parameter sets that satisfy* (1) *and* (2) *are admissible*.

Defination 2.4 (Colbourn and Charles 1996) Let $\mathcal{V}$ be a $v-$ set, $\mathcal{B} = \{B_1, \ldots, B_b\}$ in which $B_j \subseteq \mathcal{B}(j = 1, 2 \ldots, b)$ is a k-subset, then B_j is called a block. $(\mathcal{V}, \mathcal{B})$ is called a t-partly balanced design, namely $t-(v, k, \lambda, 0)-$ design. For any $t-$ subset of $\mathcal{V}$, it is either absent in any blocks of B or it is contained in exactly λ blocks of B (where v, k, t, λ are integers).

Definition 2.5 (Colbourn and Charles 1996) The design of $(\mathcal{V}, \mathcal{B})$ mentioned above is a strong partially balanced incomplete block design (SPBIBD) for a given positive integer r, where $r \leq t$. $(\mathcal{V}, \mathcal{B})$ is a r-partly balanced incomplete block design.

In this paper, the broadcast encryption scheme is constructed by 2-strong partly balanced incomplete block design.

2.3 Perpendicular array

Definition 2.6 (Colbourn and Charles 1996) A perpendicular array $PA_\lambda(s, n, v)$ is a $\lambda\binom{v}{s} \times n$, $A = (a_{j,i})$, with entries from a $v-$set, say Y, such that the following properties are satisfied:

- each row of A contains n different elements of Y.
- for any $s-$set of Y, and for any s columns of A, there are exactly λ rows of A in which the s given elements occur in the s given columns (in predefined order).

2.4 Rational normal curve

Definition 2.7 [Pei (2006)] We define a curve $\mathcal{C}$ in $PG(n, \mathcal{F}_q)$ to be the image of the map

$$PG(1, \mathcal{F}_q) \to PG(n, \mathcal{F}_q),$$
$$(x_0, x_1) \mapsto (x_0^n, x_0^{n-1}x_1, \ldots, x_1^n).$$

The projective line $PG(1, \mathcal{F}_q)$ consists of the following $q+1$ points:

$$\{(1, a) : a \in \mathcal{F}_q\} \bigcup \{(0, 1)\}.$$

Therefore, the curve $\mathcal{C}$ consists of the following $q+1$ points:

$$\{(1, a, a^2, \ldots, a^n) : a \in \mathcal{F}_q\} \bigcup \{(0, 0, \ldots, 0, 1)\} \quad (2)$$

It is easy to see that the $q+1$ points in (2) are all the solutions of the following system of homogeneous equations:

$$\begin{cases} X_i^2 - X_{i-1}X_{i+1} = 0, 1 \leq i \leq n-1 \\ X_1X_{n-1} - X_0X_n = 0. \end{cases}$$

We call the image of the curve $\mathcal{C}$ under any projective transformation a rational normal curve.

3 A BE scheme based on BIBD

In this section, we first show how to design an efficient BE scheme based on BIBD. Then, we show its performance with respect to the broadcast rate and broadcast information rate etc.

3.1 The construction

According to Stinson's scheme (Stinson and Van Trung 1998), let N be a set of all users. Then, $\mathcal{B} = \{B_1, B_2, B_b\}$ is the set of users. Let P be a set of privileged users in broadcast and the number of users is $|N| = \eta$. Generally, a

typical symmetric broadcast encryption system includes the following three phases, that is, Setup, Broadcast and Decrypt.

1. Setup: Input a safety parameter l, a set of all users $N = \{u_1, u_2, \ldots, u_\eta\}$, and all user subsets $B_1, B_2, \ldots, B_m$. Then a BIBD is selected for users subsets. For $1 \le i \le m$, CA outputs sub-key $\{s_{B_i}, s_{B_i}, u_i^1, \ldots, s_{B_i}, u_i^{k-1}, s_{B_i}, u_i^{k+1}, \ldots, s_{B_i}, u_i^\tau\}$ for every user u_i^k of B_i.
2. Broadcast: Let $q \ge r+1$ be a prime power and CA randomly selects r nonzero numbers $a_i \in \mathcal{GF}_q (0 \le i \le r-1)$ which are non-identical to each other. Then a $r-1$ order polynomial is constructed: $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{r-1} x^{r-1} \cdots\cdots (1)$, where a_0 is a secret information in broadcast. CA input the set of privileged users P, then these users are existed in some B_i. They compute blocks shared as follow:
   - For any $B_i (1 \le i \le m)$, randomly select $x_{B_i} \in \mathcal{GF}_q$, calculate $f(x_{B_i})$. Let $y_{B_i} = (x_{B_i}, f(x_{B_i})) \cdots\cdots (2)$ as a share of block B_i;
   - Let the subsets of privileged users are $P_i = B_i \bigcap P$, then the public key of privileged users in P_i is $K_{B_i \bigcap P} = s_{B_i} + \sum_{\{u \in B_i, u \notin B_i \bigcap P\}} s_{B_i,u} \cdots\cdots (3)$;
   - Calculate the share of each block $b_{B_i} = y_{B_i} + K_{B_i \bigcap P}$;
   - Output cipher in broadcast $b_p = (b_{B_i}) \cdots\cdots (5) (1 \le i \le m)$.
3. Decrypt: When privileged users receive the cipher, they firstly judge which subset they are included in. If $u \in P$, let $A_u = B, u \in B$, then u use his sub-key to dispose as follow: For each $B \in A_u$, he calculates $K_{B_i \bigcap P} = s_{B_i} + \sum_{\{u \in B_i, u \notin B_i \bigcap P\}} s_{B_i,u}$, Then for B's corresponding share $y_B = b_B - K_{B_i \bigcap P}$.

Because $|A_u| = r$, the user can obtain r block shares and recover r order polynomial. Consequently, he could get the secret information a_0.

3.2 Broadcast and broadcast information rate

Let the set of key be $\mathcal{K} \subset GF(q)$ and q be a prime power. Generally, each key $\kappa (\kappa \subset \mathcal{K})$ is equal to any element in $GF(q)$. According to information theory, the information rate of key is $H(K_P) = \log q$. Then we define the broadcast rate and broadcast information rate as follow:

- The broadcast rate: $\rho = min\{\frac{H(K_p)}{H(U_j)} | 1 \le j \le n, p \in P\}$;
- The broadcast information rate: $\rho_B = min\{\frac{H(K_p)}{H(B_p)} | p \in P\}$;

We also have the following notions. Specifically, $H(U_j)$ means the information rate of user j and $H(B_p)$ means the information rate of user group.

4 BE Scheme Based on Perpendicular Array

In this section, we prove perpendicular array (PA) is able to construct BIBD and show how to implement the BE scheme.

4.1 BIBD based on Perpendicular Array

Lemma 4.1 *Suppose that* $t \le \frac{1}{2}(n+1)$ *is a positive integer and* $1 \le \tau \le t-1$. *Then, for any* $PA_{\lambda_t (t,n,s)}$, *there exists a* $PA_{\lambda_t (\tau,n,s)}$, *where* $\lambda_\tau = \dfrac{\lambda_t \binom{s-\tau}{t-\tau}}{\binom{t}{\tau}}$.

Theorem 1 *Let A be a perpendicular array* $PA_{\lambda_t (t,n,s)}$. *There exists a* $(v, \beta, r, \lambda) - BIBD$ *with the following properties:*

1. The number of point set is $|\mathcal{V}| = v = s$;
2. The number of block is $|\mathcal{B}| = \beta = \lambda_t \binom{s}{t}$;
3. For any $p \in \mathcal{V}$, $r_p = r = \lambda_1 = \dfrac{\lambda_t \binom{s-1}{t-1}}{t}$;
4. For any $p, q \in \mathcal{V}$, $p \ne q$, $\lambda_{\{p,q\}} = \lambda = \lambda_2 \binom{n}{2} = \dfrac{\lambda_t \binom{s-2}{t-2} \binom{n}{2}}{\binom{t}{2}}$, where v, β, r, λ are given positive integers.

Proof Suppose A be a perpendicular array $PA_{\lambda_t (t,n,s)}$. Let point set $\mathcal{V}$ be S and the number of $\mathcal{V}$ be $|\mathcal{V}| = s$. Let $A = (A_1, A_2, \ldots, A_N)$, where A_i is row i of the matrix $(1 \le i \le N)$. Let $B_i = A_i$, we construct a set of block $\mathcal{B} = \{B_1, B_2, \ldots, B_N\}$, then $|\mathcal{B}| = \beta = N = \lambda_t \binom{s}{t}$.

To get the conclusions of (3) and (4), we only need to prove the following two facts:

(1) For any point p belongs to $\mathcal{V}$, p is contained in exactly r-blocks, where $r = \dfrac{\lambda_t \binom{s-1}{t-1}}{t}$.

(2) For any 2-subset of $\mathcal{V}$, when they are not equal to each other, they are contained in exactly λ-blocks,

Table 1 The Number of Shared Block

	The number of blocks (one belonged to)	The number of block keys	The number of block shared
$x \in P$			
1	49	49	49
5	49	49	49
8	49	49	49
$x \in F$			
3, 6	42	42	42

$$\text{where } \lambda = \frac{{}^{\lambda_t}\binom{s-2}{t-2}\binom{n}{2}}{\binom{t}{2}}.$$

By the lemma above and the properties of PA, every element of S occurs in any row in A at most once and appears exactly λ_1 times in each column in S, where $\lambda_1 = \frac{{}^{\lambda_t}\binom{s-1}{t-1}}{t}$. According to the construction of blocks and the point set $\mathcal{V}$ mentioned above, any point $p \in \mathcal{V}$ exactly belongs to r_p blocks, where $r_p = r = \lambda_1 n = \frac{{}^{n\lambda_t}\binom{s-1}{t-1}}{t}$.

On the other hand, we can get any 2-subset of S appear exactly λ_2 times in matrix A, where $\lambda_2 = \frac{{}^{\lambda_t}\binom{s-2}{t-2}}{\binom{t}{2}}$. In the matrix A, to gain two different columns has $\binom{n}{2}$ methods and any 2-subset appears λ_2 times in each of them. (Because any two elements are not repeated in the same line). Thus, any 2-subset of S appear exactly in $\lambda_2\binom{n}{2}$ rows. Thus, the conclusion is established. □

4.2 Example

According to the structure of the theorem 1, we can direct implementation BE. Using BIBD structured by PA to realize BE, we can select proper PA to divide registered users in setup phase. In the structure of $PA_{\lambda_1(3,7,8)}$, CA selects eight keys to every block containing 7 users. Because each registered user appears in 49 blocks, each of them will get 49×8 keys in key pre-distribution phase. In the broadcast phase, CA achieve message encryption and give broadcasting according to the Sect. 3. Given the PA, CA distributes keys to the users and constructs a 48-polynomial. Suppose the set of privileged users is $P = \{1, 5, 8\}$, and the set of collusion attack users is $F = \{3, 6\}$, then the following Table 1 shows the number of blocks that they belong to, the number of block keys that they can calculate, and the number of blocks that they share.

The table shows that privileged users are able to reconstruct the 48-polynomial, which can obtain the broadcasting information plaintext $M = a_0$. But if $\omega(\omega = 2)$ illegal users in collusion, they cannot reconstruct the original polynomial, thus fail to obtain the secret information.

Theorem 2 *Suppose there is a* $(v, \beta, r, \lambda) - BIBD$, *then there exists a BE scheme based on it, having broadcast rate* $\rho = t(n\lambda_t\binom{s-\tau}{t-\tau})^{-1}$ *and broadcast information rate* $\rho_B = (\lambda_t\binom{s}{t})^{-1}$. *The upper bound of the number of users in collusion is* $\lfloor \frac{1}{2} + \frac{1}{2}\sqrt{1 + 8\frac{s-1}{n(n-1)}} \rfloor$.

In a BE scheme, the number of secrets to be stored by a user is $r \times n$, where $r = \frac{{}^{\lambda_t}\binom{s-\tau}{t-\tau}}{t}$. The number of block is β, where $\beta = \lambda_t\binom{s}{t}$. As defines in 3.2, $H(U_j) = rn \log q$ and $H(B_p) = \beta$. The broadcast rat and broadcast information rate can be gained. On the other hand, suppose $\omega = |F|$, where F is the set of unauthorized users. If the number of secrets they have is less than the order of polynomial, then they can not attack the security of the scheme.

5 A BE scheme based on rational normal curve

In this section, we use SPBIBD, which is weaker than BIBD, to effectively improve the security of BE scheme. We prove that rational normal curve (RNC) can be constructed as SPBIBD. We also present its security and efficiency.

5.1 Property of rational normal curve and structure of SPBIBD

Lemma 5.1 (Pei et al. 2010) *There are* $q + 1$ *points on each RNC in* $PG(N, F_q)$. *For* $n \leq q$, *any* $n + 1$ *points on a RNC are linearly independent.*

Lemma 5.2 (Pei et al. 2010) *Suppose that* $q \geq n + 2$. *For any* $n + 3$ *points in* $PG(N, F_q)$, *among which any* $n + 1$ *points are linearly independent, there exists a unique RNC passing through these* $n + 3$ *points.*

Lemma 5.3 (Pei et al. 2010) *Let* $n \geq 2$ *be an integer and* $q \geq n+2$ *be a prime power. Then the total number of RNCs in* $PG(N, F_q)$ *is* $\frac{1}{2}qn(n+1) - \prod(q^i - 1)$.

Lemma 5.4 Let $t \geq 5$ *be a positive integer, and* $q \geq t-1$ *be a prime power. There exists a* $t-(v, \kappa, 1, 0)$ *design, where* $v = (q^{t-2}-1)(q-1)^{-1}$ *and* $k = q+1$.

It is also a $r-(v, \kappa, \lambda_r, 0)$-design $(3 \leq r \leq t-1)$ and a $r-(v, \kappa, \lambda_r)$ design $(1 \leq r \leq 2)$, where $\lambda_1 = q^{\frac{1}{2}(t-2)(t-3)-1} \prod_{i=2}^{t-3}(q^i-1)$, $\lambda_r = q^{\frac{1}{2}(t-2-r)(r+t-3)-1} \prod_{i=1}^{t-3-r}(q^i-1) \prod_{i=1}^{r-2}(q-i)$, $(2 \leq r \leq t-3)$, $\lambda_{t-2} = (q=1)^{t-4} \prod_{i=1}^{t-4}(q^i-1)$, $\lambda_{t-1} = \prod_{i=2}^{t-3}(q-1)$. Especially, when $r=2$, $\prod_{i=1}^{r-2}(q-i) = 1$.

Let $t \geq 5$ be a positive integer, and let $n = t-3$, $M = PG(N, F_q)$. Then the blocks of $\mathcal{B}$ are equal to the number of RNCs in M. According to lemma5.4, $(M, \mathcal{B})$ is a t-SPBIBD. We let $r = \lambda_1$ and $\lambda = \lambda_2$, having this correspondence, we can construct SPBIBD as follow:

Theorem 3 *Let* $t \geq 5$ *be a positive integer,* $q \geq t-1$ *be a prime power, there exists a* $(v, b, \kappa, \gamma, \lambda) - SPBIBD$, *where* $v, b, \kappa, \gamma, \lambda$ *are all positive integers and* $|M| = v$, $|\mathcal{B}| = b$, $k = q+1$.

Theorem 4 *Suppose that there is a secure SPBIBD. Then there exists a BE scheme based on it, with rate* $\rho = (q+1)^{-1} q^{1-\frac{1}{2}(t-2)(t-3)} \prod_{i=2}^{t-3}(q^i-1)^{-1}$ *and broadcast information rate* $\rho_B = q^{1-\frac{1}{2}(t-2)(t-3)} \prod_{i=2}^{t-3}(q^i-1)^{-1}$. *When any two users collude in the block, it could achieve fully collusion resistant. Otherwise, the upper bound is* $\lfloor \frac{1}{2} + \frac{1}{2}\sqrt{1 + 8vq(q^{t-3}-1)\sum q^i} \rfloor$.

Proof In this application, SPBIBD is different from BIBD from the perspective of presence of the two points. Similar to theorem 2, the broadcast rate and broadcast information rate respectively depend on the number of secret information that the user stored and the number of block. In lemma 5.4, $n \times r = (q+1) q^{\frac{1}{2}(t-2)(t-3)-1} \prod_{i=2}^{t-3}(q^i-1)$ and $\beta = q^{\frac{1}{2}(t-2)(t-3)-1} \prod_{i=2}^{t-3}(q^i-1)$, thus ρ and ρ_B can be calculated easily.

To illustrate the advantage of SPBIBD in resisting collusion attack, we make the following analysis. Suppose that there are a number of unauthorized users conspire to obtaining secret information a_0 in broadcast. Let the set of unauthorized users be F, and $|F| \leq \omega$, obviously $F \bigcap P = \emptyset$. Obviously, any unauthorized users $x \notin P$ are unable to obtain secret information a_0 in broadcasting. Assumes that F and B $(B \bigcap P \neq \emptyset)$ have two or more common users, then the public key $k_{B \bigcap P}$ of block B can be calculated by the defected users of B. Denote the set of these blocks by $A_F = \{B \subset \mathcal{B} || B \bigcap F| \geq 2 \text{ and } F \bigcap P = \emptyset\}$, then $A_F \leq \lambda \binom{\omega}{2}$, because $|F| \leq \omega$ (in this scenario, r and λ are constants. With this conclusion, we can get the upper bound of the number of resist conspiracy attacks in above scheme:

- Case 1: when $\lambda = 0$, any unauthorized users collusion can not get any information.(There exists no example in BIBD)
- Case 2: when $\lambda \neq 0$, if $\lambda_2 \binom{\omega}{2} < \lambda_1$, similar to case 1, illegal users can not recover $r-1$ order polynomial $f(x)$ and fail to obtain the plaintext a_0. The users of the set F conspired can only calculate $\lambda_1 - 1$ public keys at most. They can gain $r-1$ shares corresponding to public key and can not recover $r-1$ order polynomial $f(x)$. Thus, the plaintext is kept secure.

If the probability of above two cases is relatively low, we use probability to measure the success rate of collusion attack. Let ϑ be the probability of any two users of F occurred in any block, where $0 \leq \vartheta \leq 1$. The number of keys that the collusion attackers can gain is $\lambda_1(1-\vartheta)\binom{\omega}{2} + \lambda_2 \vartheta \binom{\omega}{2}$, where $\lambda_1 = 0$. Thus, this scheme can prevent ω unauthorized users' collusion attack, where $\lambda_1(1-\vartheta)\binom{\omega}{2} + \lambda_2\vartheta\binom{\omega}{2} < r$. □

Table 2 Comparison of schemes' security

	The number of $K_{B \bigcap P}$	The range of the number of collusion resistant
Stinson scheme	$\lambda \binom{\omega}{2}$	$\omega \leq \lfloor \frac{1}{2} + \frac{1}{2}\sqrt{1+8q} \rfloor$
Scheme of Sect. 4	$\lambda_2 \binom{\omega}{2}$	$\omega \leq \lfloor \frac{1}{2} + \frac{1}{2}\sqrt{1 + 8\frac{q-1}{n(n-1)}} \rfloor$ if $v \neq 0, \omega \leq \lfloor \frac{1}{2} + \frac{1}{2}$
Scheme of Sect. 5	$\lambda_2 \binom{\omega}{2}$	if $v = 0, \omega \to \infty$ $\sqrt{1 + 8vq(q^{t-2}-1)\sum_{i=0}^{t-5} q^i} \rfloor$

Considering the parameters into number field, the security of schemes is shown as follow (Table 2):

6 An improved construction

In this section, we use dual design to improvement program, and compare the performance differences between schemes.

Table 3 Comparison of efficiency

	PA	RNC
ρ_B (original scheme)	$\frac{1}{\lambda_t\binom{s}{t}}$	$q^{-\frac{1}{2}(t-2)(t-3)+1}\prod_{i=2}^{t-3}(q^i-1)^{-1}$
ρ_B (improvement scheme)	$\frac{1}{s}$	$\frac{q-1}{q^{t-2}-1}$

Definition 6.1 (Colbourn and Charles 1996) Let $\mathcal{D} = (\mathcal{V}, \mathcal{B}, I)$ be a limited correlation structure. Let $\mathcal{D}^* = (\mathcal{V}^*, \mathcal{B}^*, I^*)$, where $\mathcal{V}^* = \mathcal{B}$, $\mathcal{B}^* = \mathcal{V}$. we say that $\mathcal{D}^*$ is the dual design of D if and only if $\mathcal{B}^* I P^*$ having $P^* I^* \mathcal{B}^*$ for any $P^* \in \mathcal{V}^*$,$\mathcal{B}^* \in \mathcal{B}^*$.

Obviously, this kind of special designs exists dual designs when $\lambda_t = 1$. So we have proposition as follow:

Theorem 5 *For a* $PA(t, s)$, *there exists a* $\left(s, \binom{s}{t}, t^{-1}\binom{s-1}{t-1}, \binom{s-2}{t-2}\binom{n}{2}\binom{t}{2}^{-1}\right)$ *-design, and its dual scheme is* $(\binom{s}{t}), s, n, t-1)-$ *design.*

Theorem 6 *Let* $t \geq 5$ *be a positive integer, for any prime power* $q \geq t-1$. *There exists a* $((q-1)^{-1}(q^{t-2}-1), \beta, q+1, \beta, 1:0)-$ *design, and its dual scheme is* $(\beta, (q-1)^{-1}(q^{t-2}-1), q+1, t-1)-$ *design, where* $\beta = q^{\frac{(t-2)(t-3)}{2}-1}\prod_{i=2}^{t-3}(q^i-1)$.

The key distinction between design and its dual design to construct a BE scheme is that in the original construction, the users corresponding to points of blocks, user groups corresponding to the blocks. While using the dual design scheme, the user groups corresponding to points of blocks, users corresponding to the blocks. Thus, the improvement program can improve the broadcast information rate more obvious (Table 3).

By using the list above, the broadcast information rate of improvement scheme is improved significantly. For example, in Sect. 5, let $q = 5, n = 2$, then we can construct a $(31, 3000, 600, 5)-$design. That is, this construction only accommodates 32 users with 3000-user group having $\rho_B = \frac{1}{3000}$. It is not optimal obviously. While using its dual design, namely exchange points and blocks, then we get a $(3000, 31, 6, 4)-$design. Its broadcast information rate becomes $\frac{1}{31}$. In practice, the broadcast encryption involves large numbers of user. When the number of users is determined, we can realize BE scheme by selecting the appropriate q. So, dual design not only conforms to the actual demand but also improve the efficiency of it.

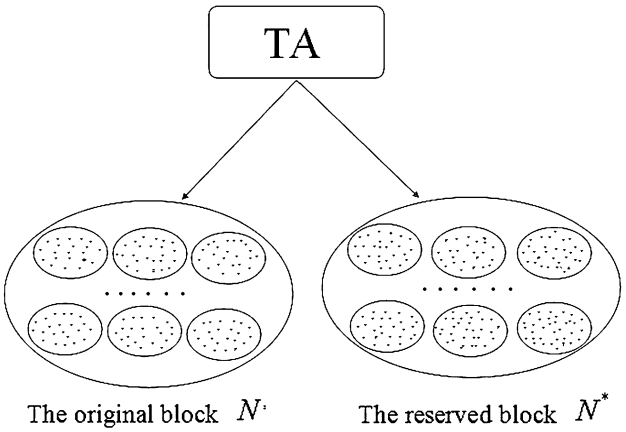

Fig. 1 The structure chart of differentiated users with blocks reservation

7 Block reservation

In the BE schemes based on BIBD, when adding new users, it has to update all the keys held by authorized users. The scheme even has to be updated in the whole system. In this section, we introduce a new solution where the authorized users are treated as points in reserved blocks (see Fig. 1). Thus, the number of new users and authorized users is related with the searching block design. Then, the work including key pre-distribution as well as initialization can be performed easily. For example, in the block reserved PA scheme, broadcasting center (BC) selects an appropriate PA according to the number mentioned above. Then, the user allocation and key pre-distribution can be done by the blocks of this PA, while the keys corresponding to the reserved blocks are stored by BC for the registration of new users.

7.1 Block reservation scheme

A typical block reservation BE system based on BIBD includes five phases, that is, system initialization, key pre-distribution, registration of new users, sending broadcast message, receiving broadcast message. Without loss generality, we assume that the number of new users and old users are equal to each other.

1. System Initialization. The trusted authority (TA) selects a BD instance satisfying the numbers of old users and new users, such that each old user can be mapped into a different point in this BD instance.
2. Key Pre-distribution. After generating all the keys required by the system, almost one half of keys are transmitted to old users by Stinson Scheme (Stinson and Van Trung 1998) and the other half which are

intended to be transmitted to new users are stored by TA. Now one set of keys, one point of BD instance and one user are linked together.

3. Registration of New Users. Once new users are requiring for joining this network, the TA is to transmit the prior stored keys to them respectively by mapping them to points.
4. Sending Broadcast Message. When a set of legal users is chosen, BC encrypts and broadcasts a message by the method introduced in Sect. 3.
5. Receiving Broadcast Message. Any legal user in this set can decrypt the message through the keys he owns, while the illegal users can not.

7.2 Comparison of block reservation schemes

We compare the proposed constructions in this paper in terms of the storage and length of messages.

- Storage: The storage of user keys is determined by the repetitions of this user (a point) r and the size of user group (a block) k. Since the reserved blocks are concatenated by some blocks, both r and k are constant. Therefore, the storage of block reservation schemes is the same as that of the original one (Table 4).
- Length of Message: Let $N^{'}$ be the number of old users and N^{*} be the number of new users. The total number of users is $N = N^{'} + N^{*}$. Let $S^{'}$ be the number of blocks and S^{*} be the number of reserved blocks. According to the definition of broadcast information rate, the length of broadcast message is the number of blocks that have legal users. In the worse case that all blocks have legal users, the length of broadcast message in block reservation scheme is $S = S^{'} + S^{*}$ for new users are in reserved blocks. Specially in the case $N^{'} = N^{*}$, the performance comparison of schemes is shown in Table 5.

For the block reservation scheme, the storage overhead is the same as that of the original constructions while the length of message increases with the number of blocks. Thus, the information rate keeps the same, and the broadcast information rate increases with the number of blocks decrease.

7.3 Security analysis

Block reservation scheme is an extension of the original scheme. It guarantees that it is as secure as the original one. It is necessary to look into the forward security that new registered users are not able to decrypt the broadcast message sent before registration. In block reservation scheme, the keys associated with block and reserved block are independent and old message is encrypted under those keys, so that the new joined users will not be issued with those keys and are not able to get any information of the message before their registrations. Consequently, the forward security is achieved.

Table 4 The storage of scheme with blocks reservation

Scheme	Storage
Block reservation scheme of PA	$\frac{n}{t}\binom{q-1}{t-1}$
Block reservation scheme of RNC	$(q+1)\, q^{\frac{1}{2}(t-2)(t-3)-1} \prod_{i=2}^{t-3}(q^i-1)$

Table 5 Comparision of scheme performances with blocks reservation

Scheme	Storage	
Block reservation scheme of PA	$\frac{n}{t}\binom{q-1}{t-1}$	$2q$
Block reservation scheme of RNC	$(q+1)\, q^{\frac{1}{2}(t-2)(t-3)-1} \prod_{i=2}^{t-3}(q^i-1)$	$\frac{2(q^{t-2}-1)}{q-1}$

8 Conclusion

In this paper, we showed that any BIBD can be used to realize secure BE schemes. According to the characteristics of the block, a more efficient broadcast encryption, using the SPBIBD constructed by rational normal curve was also presented. This scheme is secure under an enhanced security model compared with the first construction. Moreover, an improved scheme was given based on the efficiency comparison of these two schemes, in which the broadcast rate is invariant while its broadcast information rate is significantly higher than that of the first construction. We also calculated the broadcast rate, the broadcast information rate and the maximum number of collusion resistant. Finally, we proved that higher broadcast information rate can be achieved in these constructions.

References

Boneh D, Franklin M (1999) An efficient public key traitor tracing scheme. Advances in Cryptology-CRYPTO99. Springer, Berlin Heidelberg, pp 338–353

Boneh D, Gentry C, Waters B (2005) Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Advances in CryptologyCCRYPTO 2005. Springer, Berlin Heidelberg, pp 258–275

Colbourn, Charles J (ed) (1996) Handbook of combinatorial designs. CRC Press

Dodis Y, Fazio N (2002) Public key trace and revoke scheme secure against adaptive chosen ciphertext attack. In: Public Key Cryptography-PKC 2003. Springer, Berlin Heidelberg, pp 100–115

Fiat A, Naor M (1994) Broadcast encryption. Advances in Cryptology-CRYPTO93. Springer, Berlin Heidelberg, pp 480–491

Fazio N, Perera I M (2012) Outsider-anonymous broadcast encryption with sublinear ciphertexts. In: Public Key CryptographyCPKC 2012. Springer, Berlin Heidelberg, pp 225–242

Halevy D, Shamir A (2002) The LSD broadcast encryption scheme. In: Advances in Cryptology-CRYPTO 2002. Springer, Berlin Heidelberg, pp 47–60

Li J, Wang Q, Wang C, et al (2010) Fuzzy keyword search over encrypted data in cloud computing. In: INFOCOM, 2010 Proceedings IEEE, pp 1–5

Li J, Chen X, Li M, et al (2013) Secure deduplication with efficient and reliable convergent key management

Libert B, Paterson K G, Quaglia E A (2012) Anonymous broadcast encryption: Adaptive security and efficient constructions in the standard model. In: Public Key Cryptography-CPKC 2012 Springer, Berlin Heidelberg, pp 206–224

Naor D, Naor M, Lotspiech J (2001) Revocation and tracing schemes for stateless receivers. In: Advances in Cryptology-CRYPTO 2001. Springer, Berlin Heidelberg, pp 41–62

Pei D (2006) Authentication codes and combinatorial designs. CRC Press

Pei DY, Dong JW, Rong CM (2010) A novel key pre-distribution scheme for wireless distributed sensor networks. Sci China Inf Sci 53(2):288–298

Quinn KAS (1994) Some constructions for key distribution patterns. Des Codes Cryptogr 4(2):177–191

Shamir A (1979) How to share a secret. Commun ACM 22(11): 612–613

Stinson D R (1997) On some methods for unconditionally secure key distribution and broadcast encryption. In: Selected Areas in Cryptography. Springer, US, pp 3–31

Stinson DR, Van Trung T (1998) Some new results on key distribution patterns and broadcast encryption. Des Codes Cryptogr 14(3):261–279

Yao D, Fazio N, Dodis Y, Lysyanskaya A (2008) Forward-secure hierarchical IBE with applications to broadcast encryption schemes. In: IOS.Press Cryptology and Information Security Series on Identity-Based Cryptography, vol 7. pp 101–119

Zhao X, Zhang F (2011) Traitor tracing against public collaboration. In: Information Security Practice and Experience. Springer, Berlin Heidelberg, pp 302–316