Combinatorial Constructions of 3- and 4-Secure Codes

Yejing Wang[1], Jennifer Seberry[1], Beata J. Wysocki[2], Tadeusz A. Wysocki[2],
Willy Susilo[1], Tianbing Xia[1], Ying Zhao[1] and Le Chung Tran[2]

[1]Centre for Computer Security Research
School of Information Technology and Computer Science
University of Wollongong
Wollongong 2522, Australia
Email: [yejing,jennie,wsusilo,txia,yz03]@uow.edu.au

[2]School of Electrical, Computer and Telecommunications Engineering
University of Wollongong
Wollongong 2522, Australia
Email: beata@elec.uow.edu.au, [wysocki,lct71]@uow.edu.au

Abstract

In this paper, 3- and 4-secure codes are constructed from combinatorial designs. Both constant weight and non-constant weight codes are shown.

1. Introduction

Collusion secure fingerprinting codes are introduced by Boneh and Shaw [1]. A fingerprint is a string over an alphabet. A fingerprinting code is a collection of fingerprints and is used to protect the ownership of digital objects. A fingerprint is embedded into a copy of the digital object, when the copy is sold, in such a way that each fingerprint is unique to a copy so that the distributor of the object is able to identify illegal redistribution by extracting the fingerprint. The fingerprint is not known to the buyer so that it is not easy to tamper with.

However, if one has multiple copies of the same object with different fingerprints, he may compare the copies and detect where the marks are different and he might be able to change the mark on the detected positions. Collusion secure codes are considered as a fingerprinting code with the following property. Suppose a pirate copy is found with a fingerprint not identical to any fingerprint from the fingerprinting code, at least one of the fingerprints can be traced with a high probability when the pirate copy was produced by a certain number of copies. Boneh etc firstly constructed [1,2] binary c-secure codes with a tracing error ε.

In this paper we construct c-secure codes from combinatorial designs for c=3 and c=4.

2. Preliminaries

Let $\Gamma \subseteq \{0,1\}^v$ be a binary code and $C \subseteq \Gamma$ be a collusion of size c>1. Suppose

$$C=\{u_1, u_2, \ldots, u_c\}, \quad u_i=(a_{i,1}, a_{i,2}, \ldots, a_{i,v}).$$

Boneh etc [1,2] used a so-called Marking Assumption. It is assumed that the fingerprints can be only modified at the detective positions by a collusion. A detective position for C is a position j, $1 \le j \le v$, where

$$|\{a_{1,j}, a_{2,j}, \ldots, a_{c,j}\}|>1.$$

Denote by

$$D(C)=\{j: |\{a_{1,j}, a_{2,j}, \ldots, a_{c,j}\}|>1\} \subseteq \{1, 2, \ldots, v\}$$

$$F(C)=\{(x_1,x_2, \ldots, x_v): x_j=a_{1,j}\ \forall j \notin D(C)\} \subseteq \{0,1,?\}^v$$

the symbol '?' indicates a mark on the corresponding position is erased. The set F(C) consists of all strings produced by C subject to the Marking Assumption. A tracing algorithm A outputs a subset of Γ on any input $x \in \{0,1,?\}^*$. It is expected that the chance of $A(x) \subseteq C$, for all $x \in F(C)$, is as high as possible. c-Secure codes are defined as follows.

Definition 1 ([1,2])
Let ε > 0. A code $\Gamma \subseteq \{0,1\}^v$ is called c-secure with tracing error ε if there exists a tracing algorithm A satisfying condition: if $C \subseteq \Gamma$, $|C| \le c$, produces an $x \in \{0,1,?\}^v$, then $\Pr[A(x) \subseteq C]>1- \varepsilon$.

For binary strings

$$x=(x_1,x_2, \ldots, x_v), \ \ y=(y_1,y_2, \ldots, y_v),$$

denote

$$w(x)=x_1+x_2+ \ldots +x_v$$
$$\mu(x, y)=x_1y_1+x_2y_2+ \ldots +x_vy_v.$$

If $x=(x_1,x_2, \ldots, x_v)$, $y=(y_1,y_2, \ldots, y_v) \in \{0,1,?\}^v$, we define w(x) and μ(x, y) as above by treating symbol '?' as 0. Let Γ be a binary code, denote

$$\mu = \max_{u,v \in \Gamma} \mu(u, v).$$

Define a function $T: \{0,1,?\}^v \rightarrow 2^\Gamma$ as

$$T(x)=\{u_i \in \Gamma: \mu(u_i, x)=\max_{u \in \Gamma} \mu(u, x)\}$$

Let $C=\{u_1, \ldots, u_c\} \subseteq \Gamma$ and $x \in F(C)$. Suppose

$$\mu(x, u_1) \ge \ldots \ge \mu(x, u_c).$$

Then $\mu(x,u_1) \ge w(x)/c$. For any $u \in \Gamma \backslash C$, we have

$$\mu(x, u) \le \mu(u_1,u)+ \ldots + \mu(u_c, u) \le c\mu.$$

It is obtained that $T(x) \subseteq C$ provided that

$$w(x)>c^2\mu \qquad (1)$$

and $x \in F(C)$.

3. 3-Secure Codes

Consider a block design (X, **B**) where |X|=v. For B_i, $B_j \in \mathbf{B}$, we define

$\mu(B_i, B_j)=|B_i \cap B_j|$
$\delta(B_i, B_j)=|B_i \setminus B_j|+|B_j \setminus B_i|$
$\mu=\max_{B_i,B_j\in \mathbf{B}, i\neq j} \mu(B_i, B_j)$
$\delta=\min_{B_i, B_j\in \mathbf{B}, i\neq j} \delta(B_i, B_j)$

There is a one-to-one correspondence between a subset of X and a binary string of length v. We shall use the same notation for a block and the corresponding binary string.

Let $C=\{B_1, B_2, B_3\} \subseteq \mathbf{B}$. Then F(C) is written as follows.

$F(C)=\{P\subseteq X: B_1 \cap B_2 \cap B_3 \subseteq P \subseteq B_1 \cup B_2 \cup B_3\}$.

D(C) is partitioned into the following six subsets

$B_1\cap B_2\setminus B_3$, $B_1 \setminus (B_2\cup B_3)$,
$B_1\cap B_3\setminus B_2$, $B_2\setminus (B_1 \cup B_3)$,
$B_2\cap B_3\setminus B_1$, $B_3 \setminus (B_1\cup B_2)$.

So we have

$3|D(C)|=|D(C)|+\delta(B_1,B_2)+\delta(B_1,B_3)+\delta(B_2,B_3)$.

That is

$$|D(C)| \geq 3\delta/2. \qquad (2)$$

Theorem 1

Let ε>0 be given. If there is a block design (X, **B**) such that

$$\mu < \frac{3\varepsilon}{3\varepsilon+18} v \qquad (3)$$

then there is a 3-secure code with tracing error ε.

Proof Let $C=\{B_1, B_2, B_3\}$, $\mu'=|B_1\cap B_2 \cap B_3|$. Noted that $v=\mu+\delta$, inequality (3) provides

$$9\mu < \frac{3}{2}\delta\varepsilon$$

Further from (2) we have

$$9\mu - \mu' < \frac{3}{2}\delta\varepsilon \leq \varepsilon\, |D(C)|$$

Define a tracing algorithm A as

$$A(x)=\begin{cases} T(x), & w(x)>9\mu \\ \Phi, & otherwise \end{cases}$$

For $x\in F(C)$, we have $w(x)\geq\mu'$. Considering (1) we obtain that

$$\Pr[A(x)=\Phi]=\frac{\sum_{w=\mu'}^{9\mu}\binom{|D(C)|}{w}}{2^{|D(C)|}}<\varepsilon$$

The theorem is proved. □

4. 4-Secure Codes

Let (X,**B**) be a block design and $C=\{B_1, B_2, B_3, B_4\} \subseteq \mathbf{B}$. Then

$F(C)=\{P\subseteq X: B_1\cap B_2\cap B_3\cap B_4\subseteq P\subseteq B_1\cup B_2\cup B_3\cup B_4\}$

and D(C) is partitioned into the following 14 subsets.

$B_1\cap B_2 \cap B_3 \setminus B_4$, $B_1\cap B_2\cap B_4 \setminus B_3$,
$B_1\cap B_3 \cap B_4 \setminus B_2$, $B_2\cap B_3\cap B_4 \setminus B_1$,
$B_1\cap B_2 \setminus (B_3\cup B_4)$, $B_1\cap B_3 \setminus (B_2\cup B_4)$,
$B_1\cap B_4 \setminus (B_2\cup B_3)$, $B_2\cap B_3 \setminus (B_1\cup B_4)$,
$B_2\cap B_4 \setminus (B_1\cup B_3)$, $B_3\cap B_4 \setminus (B_1\cup B_2)$,
$B_1 \setminus (B_2\cup B_3\cup B_4)$, $B_2 \setminus (B_1\cup B_3\cup B_4)$,
$B_3 \setminus (B_1\cup B_2\cup B_4)$, $B_4 \setminus (B_1\cup B_2\cup B_3)$.

From this we have

$$\begin{aligned}
&6|D(C)| \\
&= 3|D(C)| - |B_1\cap B_2 \setminus (B_3\cup B_4)| - |B_1\cap B_3 \setminus (B_2\cup B_4)| \\
&\quad - |B_1\cap B_4 \setminus (B_2\cup B_3)| - |B_2\cap B_3 \setminus (B_1\cup B_4)| \\
&\quad - |B_2\cap B_4 \setminus (B_1\cup B_3)| - |B_3\cap B_4 \setminus (B_1\cup B_2)| \\
&\quad + \delta(B_1\cap B_2) + \delta(B_1\cap B_3) + \delta(B_1\cap B_4) \\
&\quad + \delta(B_2\cap B_3) + \delta(B_2\cap B_4) + \delta(B_3\cap B_4)
\end{aligned}$$

Note that for any sets R, S, T, the following holds

$|R \setminus (S\cup T)| = |R| - |R\cap S| - |R\cap T| + |R\cap S\cap T|$

Then we have

$$\begin{aligned}
&3|D(C)| \\
&=\delta(B_1\cap B_2) + \delta(B_1\cap B_3) + \delta(B_1\cap B_4) + \delta(B_2\cap B_3) \\
&\quad + \delta(B_2\cap B_4) + \delta(B_3\cap B_4) - \mu(B_1\cap B_2) - \mu(B_1\cap B_3) \\
&\quad - \mu(B_1\cap B_4) - \mu(B_2\cap B_3) - \mu(B_2\cap B_4) - \mu(B_3\cap B_4) \\
&\quad + 3\mu(B_1\cap B_2\cap B_3) + 3\mu(B_1\cap B_2\cap B_4) \\
&\quad +3\mu(B_1\cap B_3\cap B_4) + 3\mu(B_2\cap B_3\cap B_4) \\
&\quad - 6\mu(B_1\cap B_2\cap B_3\cap B_4) \\
&\geq 6\delta - 6\mu
\end{aligned}$$

So it is obtained that

$$|D(C)| \geq 2\delta-2\mu \qquad (4)$$

Theorem 2

Let ε>0 be given. If there is a block design (X, **B**) such that

$$\mu < \frac{\varepsilon}{2\varepsilon+8} v \qquad (5)$$

then there is a 4-secure code with tracing error ε.

Proof Let $C=\{B_1, B_2, B_3, B_4\}$, $\mu''=|B_1\cap B_2\cap B_3\cap B_4|$. Noted that $v=\mu+\delta$, inequality (5) provides

$$16\mu < \varepsilon(2\delta-2\mu)$$

Further from (4) we have

$$16\mu - \mu'' < \varepsilon(2\delta-2\mu) \leq \varepsilon\, |D(C)|$$

Define a tracing algorithm A as

$$A(x)=\begin{cases} T(x), & w(x)>16\mu \\ \Phi, & otherwise \end{cases}$$

For $x\in F(C)$, it must be $w(x) \geq\mu''$. Considering (1) we obtain that

$$\Pr[A(x)=\Phi]=\frac{\sum_{w=\mu''}^{16\mu}\binom{|D(C)|}{w}}{2^{|D(C)|}}<\varepsilon$$

The theorem is proved.

5. Existence

We shall show families of block designs with parameters satisfying (3) in section 5.1 and with parameters satisfying (5) in section 5.2.

5.1 Families of 3-secure codes

We firstly show the existing group divisible designs whose parameters satisfy (3) and hence that define 3-secure codes with constant weight. We secondly show the existing pairwise balanced designs whose parameters satisfy (3) and that define 3-secure codes with non-constant weight.

Definition 2([3])
Let K and G be sets of positive integers and let λ be a positive integer. A group divisible design of index λ and order v, denoted by (K,λ)-GDD, is a triple (X, **G**, **B**), where X is a finite set of cardinality v, **G** is a partition of X into parts (groups) whose sizes lie in G, and **B** is a family of subsets (blocks) of X which satisfy the properties:

1. If B∈**B**, then |B|∈K.
2. Every pair of distinct elements of X occurs in exactly λ blocks or one group, but not both.
3. |**G**|>1.

If $v=a_1g_1+a_2g_2+ \dots +a_sg_s$, and if there are a_i groups of size g_i, i=1,2, …, s, then the (K,λ)-GDD is of type

$$g_1^{a_1} g_2^{a_2} \cdots g_s^{a_s}$$

If K={k}, then the (K,λ)-GDD is a (k, λ)-GDD. If λ=1, then the (K,λ)-GDD is a K-GDD. Furthermore, a (k,1)-GDD is a k-GDD.

Corollary 1
Let ε>0. A K-GDD defines a 3-secure code with error ε provided that

$$v > \frac{3\varepsilon+18}{3\varepsilon}$$

Proof It is straightforward from theorem 1 by noting that μ=1 in a K-GDD. □

Theorem 3 ([3])
For any prime power q, there exists a (q+1)-GDD of type $(q^2-q)^{q+1}(q^2)^1$.

If (X, **B**) is a (q+1)-GDD of type $(q^2-q)^{q+1}(q^2)^1$, the cardinality of X is

$$v=(q+ 1)(q^2-q)+ q^2=q^3+q^2-q$$

For any given ε>0, a prime power q satisfying

$$q^3+q^2-q > \frac{3\varepsilon+18}{3\varepsilon}$$

exists and so does a 3-secure code with tracing error ε. The code has a constant weight q+1.

Theorem 4 ([3])
Suppose that there exists a resolvable BIBD(v,k,1), which contains u mutually disjoint parallel classes. Let n=v/k. Then there exists a (k+1)-GDD of type $k^n(u-1)^1$.

If (X, **B**) is a (k+1)-GDD of type $k^n(u-1)^1$, the cardinality of X is

$$nk+(u-1)=v+u-1$$

which can be chosen such that

$$v+u-1 > \frac{3\varepsilon+18}{3\varepsilon}$$

for a given ε>0. Hence a 3-secure code with a constant weight k+1 is obtained.

Definition 3 ([3])
A pairwise balanced design PBD(K,λ;v) is a pair (X, **B**) where X is a set of v points and **B** is a collection of subsets (blocks) of X which satisfies the following two properties:

1. If B ∈ **B**, then |B| ∈ K.
2. Every pair of distinct points of X occurs in exactly λ blocks of **B**.

When λ=1, the PBD(K,λ;v) is a PBD(v,K). Suppose k∈K. We say a PBD(v,K) has a mandatory block of size k if it contains a block of size k, and we denote this design by PBD(v,K∪{k*}).

Similar to corollary 1 the following corollary is straightforward.

Corollary 2
Let ε>0. A PBD(K,1;v) defines a 3-secure code with error ε provided that

$$v > \frac{3\varepsilon+18}{3\varepsilon}$$

Theorem 5 ([3])
Let $N_{\geq 3}$={n∈**Z**: n≥3}. Then a PBD(v,$N_{\geq 3}$∪{k*}) exists if and only if v≥2k+1 except when

1. v=2k+1 and k=0 (mod 2);
2. v=2k+2 and k≠4 (mod 6), k>1;
3. v=2k+3 and k=0 (mod 2), k>6;
4. (v,k)∈{(7,2), (8,2), (9,2),(10,2), (11,4), (12,2), (13,2), (17,6)}.

For any given ε>0, there is a v>(3ε+18)/3ε such that a PBD(v, $N_{\geq 3}$∪{k*}) exists. From this design, a 3-secure code is obtained. The code has variety weights, one of the weights is k≤(v-1)/2.

Theorem 6 ([3])
Let N_{odd} denote the set of all odd positive integers. Let v and k be odd positive integers that satisfy v≥2k+1. Then there exists a PBD(v, N_{odd} ∪{k*}).

Similarly, a 3-secure code with variety weights is obtained from PBD(v, N_{odd}∪{k*}).

5.2 Families of 4-secure codes

We show families of block designs whose parameters satisfy (5) in terms of group divisible designs and pairwise balanced designs. These designs give 4-secure codes with constant and non-constant weight, respectively.

Corollary 3
Let ε>0. A K-GDD defines a 4-secure code with tracing error ε provided that

$$v > \frac{2\varepsilon + 8}{\varepsilon}$$

Let ε>0 be given, q be a prime power satisfying

$$(q+1)(q^2-q)+q^2 > \frac{2\varepsilon + 8}{\varepsilon}$$

then the (q+1)-GDD of type $(q^2-q)^{q+1}(q^2)^1$ defines a 4-secure code with tracing error ε. The code has a constant weight q+1.

In the (k+1)-GDD of type $k^n(u-1)^1$, the cardinality of X is chosen such that

$$v+u-1 > \frac{2\varepsilon + 8}{\varepsilon}$$

for a given ε>0. Then a 4-secure code with a constant weight k+1 is obtained.

Corollary 4
Let ε>0. A PBD(K,1;v) defines a 4-secure code with tracing error ε provided that

$$v > \frac{2\varepsilon + 8}{\varepsilon}$$

For any given ε>0, there is a v>(2ε+8)/ε such that a PBD(v, $N_{\geq 3} \cup \{k^*\}$) exists. From this design, a 4-secure code is obtained. The code has variety weights, one of the weights is k≤(v-1)/2.

Similarly, a 4-secure code with variety weights is obtained from PBD(v, $N_{odd} \cup \{k^*\}$).

6. Conclusion

Since the first construction [1,2] of collusion secure codes given by Boneh etc., there have been a few constructions of 2-, 3-secure codes in [4,5,6]. We constructed families of 3- and 4-secure codes from combinatorial designs in this paper. The tracing algorithm is simple.

References

[1] D. Boneh and J.Shaw, *Collusion-secure fingerprinting for digital data*, Advances in Cryptology CRYPTO'95, LNCS Vol.963, pp.453-465, Springer-Verlag, 1995.

[2] D. Boneh and J. Shaw, *Collusion-secure fingerprinting for digital data*, IEEE Transactions on Information Theory, Vol. 44, No. 5:1897-1905, 1998.

[3] C. J. Colbourn and J. H. Dinitz Eds. CRC Handbook of Combinatorial Designs, CRC Press, 1996.

[4] J. Domingo-Ferrer and J. Herrera-Joancomarti, *Short collusion-secure fingerprints based on dual binary Hamming code*, Electronics Letters, Vol. 36, No. 20, pp. 1697-1699, 2000.

[5] D. To, R. Safavi-Naini and Y. Wang, *A 2-secure code with efficient tracing algorithm*, Progress in Cryptology - INDOCRYPT'02, LNCS Vol. 2551, Springer-Verlag, pp. 149-162, 2002.

[6] F. Sebe and J. Domingo-Ferrer, *Short 3-secure fingerprinting codes for copyright protection*, Proceedings of ACISP'02, LNCS Vol. 2384, Springer-Verlag, pp. 316-327, 2002.