# On Cover-Free Family

Hossein Hajiabolhassan

Joint work with Farokhlagha Moazami

Department of Mathematical Sciences
Shahid Beheshti University, G.C.
Tehran, Iran

IUT Combinatorics Day
Isfahan University of Technology
Isfahan, Iran

Wednesday, February 23, 2011

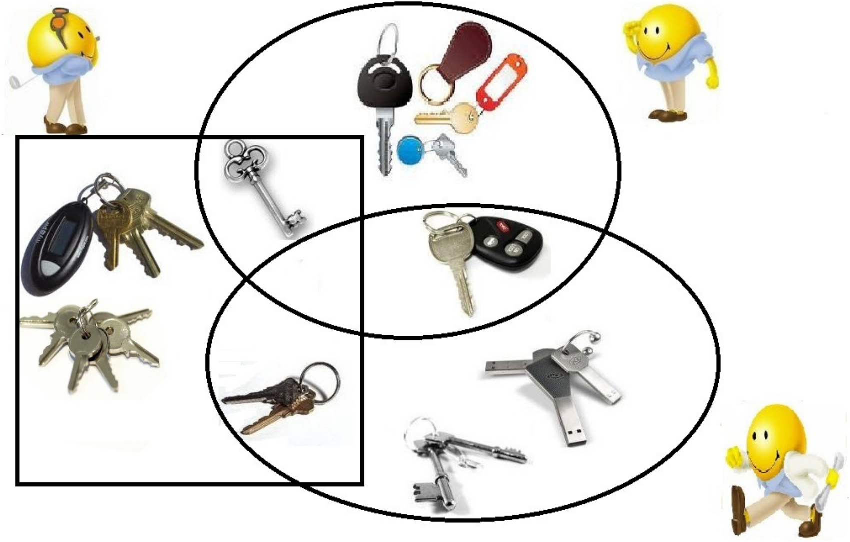
# Outline

1. Key Distribution Scheme
2. Key Predistribution Pattern
3. Cover-Free Family
4. Group Testing
5. Frameproof Code
6. Biclique Covering

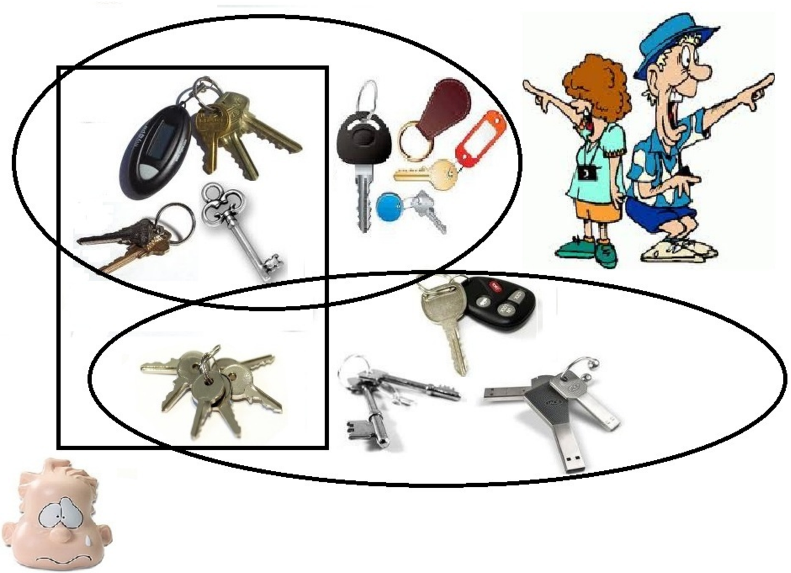
**Definition**

A Key Predistribution Scheme is a mechanism of distributing information among a set of users in such away that every user in a group in some specified family is able to compute individually a common key associated with that group.

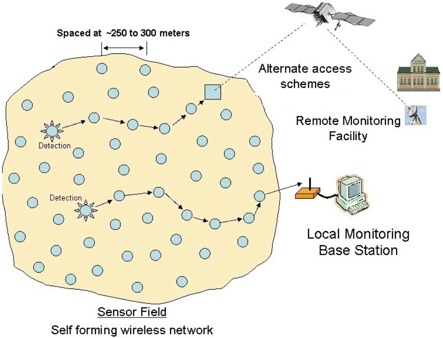
# Key Predistribution Scheme

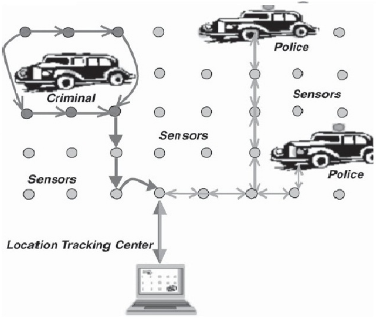


# Key Predistribution Scheme



# Wireless Sensor Network

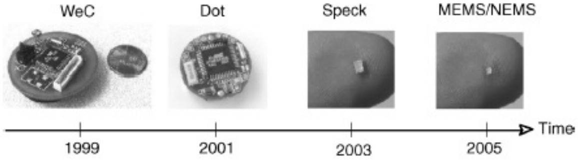



Law enforcement–national security applicatio

- Sensor network can measure various physical characteristic, such as sound, temperature, pressure, etc. They monitor and collect various information.
- The sensor nodes in DSNs should be able to communicate with each other in order to relay or accumulate secret information.

# Wireless Sensor Network

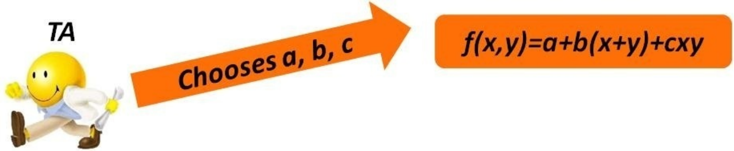



## Properties

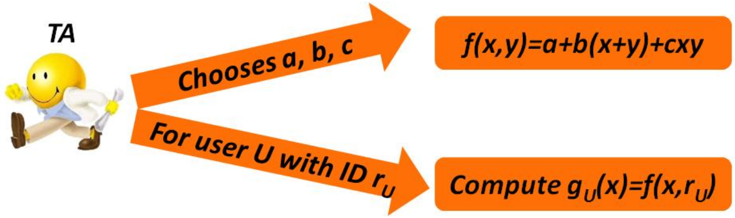
- Unpredictable topology.
- Limited battery power.
- Limited memory.
- Limited computational and communication capability.
- Large number of sensor.
- Wireless sensors are not tamper resistant.

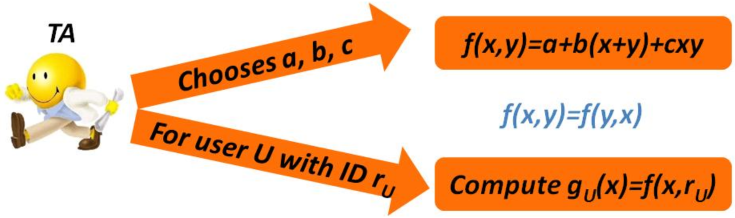
# Blom scheme

# Blom scheme

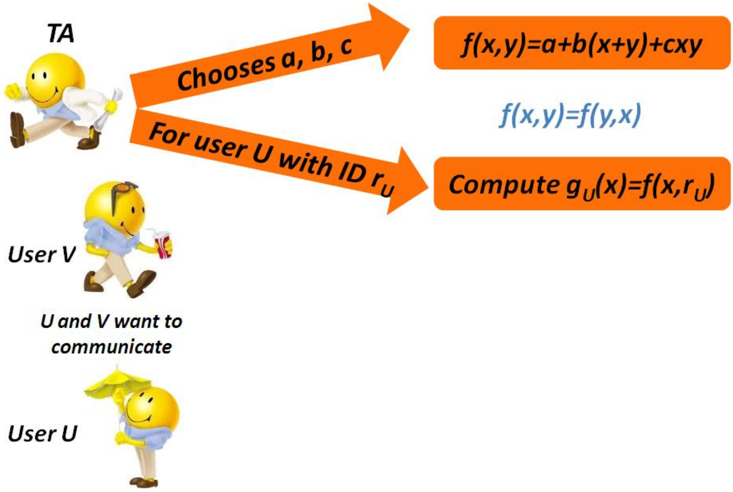


# Blom scheme

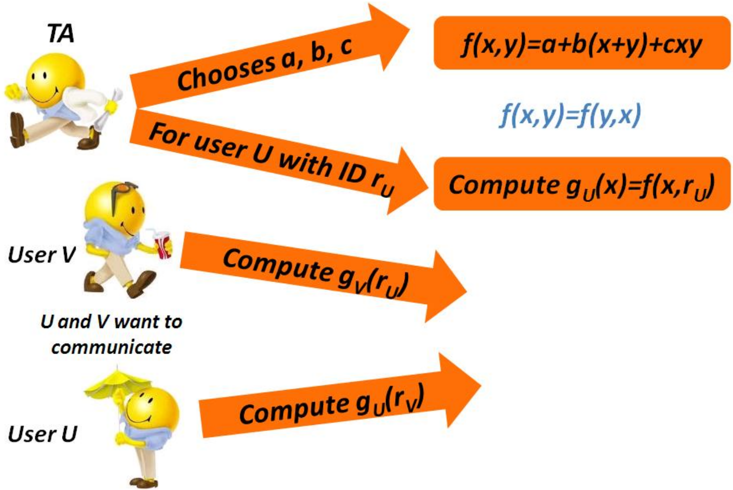

TA
Chooses a, b, c
f(x,y)=a+b(x+y)+cxy
For user U with ID $r_U$
Compute $g_U(x)=f(x,r_U)$


TA
Chooses a, b, c
For user U with ID $r_U$
$f(x,y)=a+b(x+y)+cxy$
$f(x,y)=f(y,x)$
Compute $g_U(x)=f(x,r_U)$

# Blom scheme

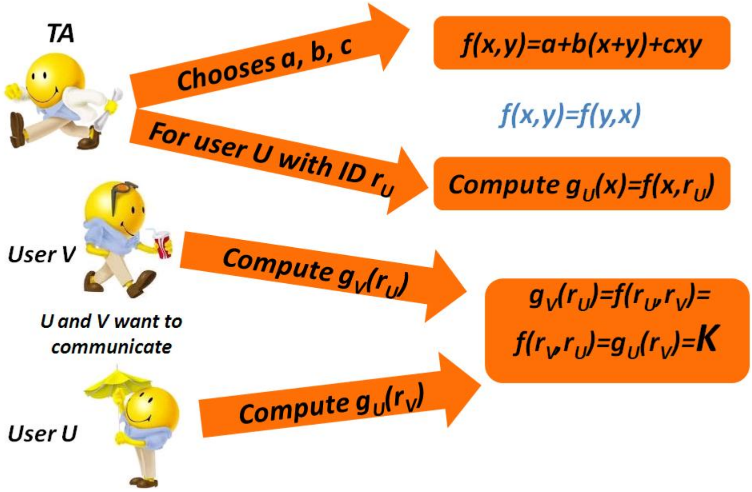

TA
Chooses a, b, c
f(x,y)=a+b(x+y)+cxy
f(x,y)=f(y,x)
For user U with ID $r_U$
Compute $g_U(x)=f(x,r_U)$
User V
U and V want to communicate
User U

# Blom scheme



TA
Chooses a, b, c
f(x,y)=a+b(x+y)+cxy
f(x,y)=f(y,x)
For user U with ID r_U
Compute g_U(x)=f(x,r_U)
User V
Compute g_V(r_U)
U and V want to communicate
User U
Compute g_U(r_V)

# Blom scheme



TA
Chooses a, b, c
f(x,y)=a+b(x+y)+cxy
f(x,y)=f(y,x)
For user U with ID $r_U$
Compute $g_U(x)=f(x,r_U)$
User V
Compute $g_V(r_U)$
U and V want to communicate
$g_V(r_U)=f(r_U,r_V)=$
$f(r_V,r_U)=g_U(r_V)=K$
User U
Compute $g_U(r_V)$

1. TA chooses a random and secret symmetric matrix $D_{w+1,w+1}$ over the finite field $GF(q)$.

# Blom scheme

1. TA chooses a random and secret symmetric matrix $D_{w+1,w+1}$ over the finite field $GF(q)$.
2. New users Alice and Bob want to join the key exchanging group. TA chooses public identifiers for each of them; i.e., $w+1$-element vectors: $ID_{\text{Alice}} = V$, $ID_{\text{Bob}} = U \in GF(q)^{w+1}$.

1. TA chooses a random and secret symmetric matrix $D_{w+1,w+1}$ over the finite field $GF(q)$.

2. New users Alice and Bob want to join the key exchanging group. TA chooses public identifiers for each of them; i.e., $w+1$-element vectors: $ID_{\mathrm{Alice}} = V$, $ID_{\mathrm{Bob}} = U \in GF(q)^{w+1}$.

3. TA gives to Alice and Bob their personal Keys, i.e., $DV$ and $DW$, respectively.

1. TA chooses a random and secret symmetric matrix $D_{w+1,w+1}$ over the finite field $GF(q)$.
2. New users Alice and Bob want to join the key exchanging group. TA chooses public identifiers for each of them; i.e., $w+1$-element vectors: $ID_{\text{Alice}} = V$, $ID_{\text{Bob}} = U \in GF(q)^{w+1}$.
3. TA gives to Alice and Bob their personal Keys, i.e., $DV$ and $DW$, respectively.
4. The common key of Alice and Bob is: $W^t DV = (V^t DW)^t = V^t DW$.

# Key Distribution Pattern

- Suppose we have a TA and a network of $v$ users, $U = \{u_1, \ldots, u_v\}$.

# Key Distribution Pattern

- Suppose we have a TA and a network of $v$ users, $U = \{u_1, \ldots, u_v\}$.
- A key distribution pattern is a public $n$ by $v$ incidence matrix, denoted by $M$, which has entries in $\{0, 1\}$.

# Key Distribution Pattern

- Suppose we have a TA and a network of $v$ users, $U = \{u_1, \ldots, u_v\}$.
- A key distribution pattern is a public $n$ by $v$ incidence matrix, denoted by $M$, which has entries in $\{0, 1\}$.
- The TA chooses $n$ random keys, say $k_1, \ldots, k_n \in \mathcal{K}$, where $(\mathcal{K}, +)$ is an additive abelian group, and gives a different subset of keys to each user.

# Key Distribution Pattern

- Suppose we have a TA and a network of $v$ users, $U = \{u_1, \ldots, u_v\}$.
- A key distribution pattern is a public $n$ by $v$ incidence matrix, denoted by $M$, which has entries in $\{0, 1\}$.
- The TA chooses $n$ random keys, say $k_1, \ldots, k_n \in \mathcal{K}$, where $(\mathcal{K}, +)$ is an additive abelian group, and gives a different subset of keys to each user.
- $M$ specifies which users are to receive which keys: user $u_j$ is given the key $k_i$ if and only if $M[i, j] = 1$.

# Key Distribution Pattern

- Suppose we have a TA and a network of $v$ users, $U = \{u_1, \ldots, u_v\}$.
- A key distribution pattern is a public $n$ by $v$ incidence matrix, denoted by $M$, which has entries in $\{0, 1\}$.
- The TA chooses $n$ random keys, say $k_1, \ldots, k_n \in \mathcal{K}$, where $(\mathcal{K}, +)$ is an additive abelian group, and gives a different subset of keys to each user.
- $M$ specifies which users are to receive which keys: user $u_j$ is given the key $k_i$ if and only if $M[i, j] = 1$.
- $$M = \begin{array}{c|cccc} & u_1 & u_2 & u_j & u_v \\ \hline k_1 & 0 & 1 & 1 & 0 \\ k_2 & 1 & 1 & 1 & 1 \\ & & & & \\ k_i & 1 & 0 & 0 & 1 \\ & & & & \\ k_n & 0 & 1 & 1 & 0 \end{array}$$

# Key Distribution Pattern

1. For a key distribution pattern $M$ and a subset of users $P \subseteq \mathcal{U}$ , define $keys(P) = \{k_i : M(i,j) = 1, \ \forall U_j \in P\}$, i.e., $keys(P) = \bigcap_{U_i \in P} keys(U_i)$.

# Key Distribution Pattern

1. For a key distribution pattern $M$ and a subset of users $P \subseteq \mathcal{U}$ , define

$$keys(P) = \{k_i : M(i,j) = 1,\ \forall U_j \in P\}, \text{ i.e., } keys(P) = \bigcap_{U_i \in P} keys(U_i).$$

2. If $keys(P) \neq \varnothing$, then the group key for $P$ is $k_P = \sum_{k_i \in Keys(P)} k_i$.

# Key Distribution Pattern

1. For a key distribution pattern $M$ and a subset of users $P \subseteq \mathcal{U}$ , define $keys(P) = \{k_i : M(i,j) = 1,\ \forall U_j \in P\}$, i.e., $keys(P) = \bigcap_{U_i \in P} keys(U_i)$.

2. If $keys(P) \neq \varnothing$, then the group key for $P$ is $k_P = \sum_{k_i \in Keys(P)} k_i$.

3. The coalition $F$ can compute $k_P$ if the following condition holds:

$$Keys(P) \subseteq \bigcup_{U_j \in F} Keys(U_j).$$

# Key Distribution Pattern

1. For a key distribution pattern $M$ and a subset of users $P \subseteq \mathcal{U}$ , define

$$keys(P) = \{k_i : M(i,j) = 1,\ \forall U_j \in P\}, \text{ i.e., } keys(P) = \bigcap_{U_i \in P} keys(U_i).$$

2. If $keys(P) \neq \varnothing$, then the group key for $P$ is $k_P = \sum_{k_i \in Keys(P)} k_i$.

3. The coalition $F$ can compute $k_P$ if the following condition holds:

$$Keys(P) \subseteq \bigcup_{U_j \in F} Keys(U_j).$$

4. Unconditional Security: There is an element $i$ where

$$k_i \in Keys(P) \setminus \bigcup_{U_j \in F} Keys(U_j).$$

# Mitchell-Piper Key Distribution Patterns

A Mitchell-Piper $(r, w)$-KDP (or more briefly, an $(r, w)$-KDP) is a KDP in which there is a key for every group of $r$ users, and each such key is secure against any disjoint coalition of at most $w$ users.

A Mitchell-Piper $(r, w)$-KDP (or more briefly, an $(r, w)$-KDP) is a KDP in which there is a key for every group of $r$ users, and each such key is secure against any disjoint coalition of at most $w$ users.

$u_1$ $u_{i_1}$ $u_{i_2}$ $u_{i_r}$ $u_t$

$k_1$

$k_n$

# Mitchell-Piper Key Distribution Patterns

A Mitchell-Piper $(r, w)$-KDP (or more briefly, an $(r, w)$-KDP) is a KDP in which there is a key for every group of $r$ users, and each such key is secure against any disjoint coalition of at most $w$ users.

$$
\begin{array}{c|cccccc}
 & u_1 & u_{i_1} & u_{i_2} & & u_{i_r} & u_t \\
\hline
k_1 & & & & & & \\
 & & & & & & \\
k_i & & 1 & 1 & & 1 & \\
 & & & & & & \\
k_n & & & & & &
\end{array}
$$

# Mitchell-Piper Key Distribution Patterns

A Mitchell-Piper $(r, w)$-KDP (or more briefly, an $(r, w)$-KDP) is a KDP in which there is a key for every group of $r$ users, and each such key is secure against any disjoint coalition of at most $w$ users.

$$
\begin{array}{c|cccccccc}
 & u_1 & u_{i_1} & u_{j_1} & u_{i_2} & u_{j_2} & u_{j_w} & u_{i_r} & u_t \\
k_1 & & & & & & & & \\
k_i & & 1 & 0 & 1 & 0 & 0 & 1 & \\
k_n & & & & & & & &
\end{array}
$$

## Definition

A set system is a pair $(X, \mathcal{B})$, where $X$ is a finite set of elements called points and $\mathcal{B}$ is a set of subsets of $X$ called blocks.

# Cover-Free Family

**Definition**

A set system is a pair $(X, \mathcal{B})$, where $X$ is a finite set of elements called points and $\mathcal{B}$ is a set of subsets of $X$ called blocks.

**Definition**

Let $w$ and $r$ be positive integers, a set system $(X, \mathcal{B})$ where $|X| = n$ and $\mathcal{B} = \{B_1, \ldots, B_t\}$ is called an $(r, w) - CFF(n, t)$ if for any two sets of indices $L, M \subseteq [t]$ such that $L \cap M = \varnothing$, $|L| = r$, and $|M| = w$, we have

$$\bigcap_{l \in L} B_l \nsubseteq \bigcup_{m \in M} B_m.$$

Incidence matrix of an $(r, w)$-cover free family

$$\begin{array}{cccccc} & x_1 & x_2 & & & x_n \\ B_1 & & & & & \\ \vdots & & & & & \\ B_t & & & & & \end{array}$$

Incidence matrix of an $(r, w)$-cover free family

$$\begin{array}{l|cccc} & x_1 & x_2 & \cdots & x_n \\ B_1 & & & & \\ B_{i_1} & & & & \\ B_{i_2} & & & & \\ B_{i_r} & & & & \\ B_t & & & & \end{array}$$

Incidence matrix of an $(r, w)$-cover free family

$$
\begin{array}{c|cccc}
 & x_1 & x_2 & & x_n \\
B_1 & & & & \\
B_{i_1} & & & & \\
B_{j_1} & & & & \\
B_{i_2} & & & & \\
 & & & & \\
B_{j_w} & & & & \\
 & & & & \\
B_{i_r} & & & & \\
B_t & & & &
\end{array}
$$

Incidence matrix of an $(r, w)$-cover free family

$$\begin{array}{c|cccc} & x_1 & x_2 & x_i & x_n \\ B_1 & & & & \\ B_{i_1} & & & & \\ B_{j_1} & & & & \\ B_{i_2} & & & & \\ B_{j_w} & & & & \\ B_{i_r} & & & & \\ B_t & & & & \end{array}$$

# Cover-Free Family

Incidence matrix of an $(r, w)$-cover free family

$$
\begin{array}{c|cccc}
 & x_1 & x_2 & x_i & x_n \\
B_1 & & & & \\
B_{i_1} & & & 1 & \\
B_{j_1} & & & & \\
B_{i_2} & & & 1 & \\
B_{j_w} & & & & \\
B_{i_r} & & & 1 & \\
B_t & & & &
\end{array}
$$

Incidence matrix of an $(r, w)$-cover free family

$$\begin{array}{c|cccc}
 & x_1 & x_2 & x_i & x_n \\
B_1 & & & & \\
B_{i_1} & & & 1 & \\
B_{j_1} & & & 0 & \\
B_{i_2} & & & 1 & \\
 & & & & \\
B_{j_w} & & & 0 & \\
 & & & & \\
B_{i_r} & & & 1 & \\
B_t & & & &
\end{array}$$

# Cover-Free Family

Incidence matrix of an $(r, w)$-cover free family

$$
\begin{array}{c|cccc}
 & k_1 & k_2 & k_i & k_n \\
 & x_1 & x_2 & x_i & x_n \\
\hline
B_1 & & & & \\
B_{i_1} & & & 1 & \\
B_{j_1} & & & 0 & \\
B_{i_2} & & & 1 & \\
 & & & & \\
B_{j_w} & & & 0 & \\
 & & & & \\
B_{i_r} & & & 1 & \\
B_t & & & &
\end{array}
$$

# Cover-Free Family

Incidence matrix of an $(r, w)$-cover free family

$$
\begin{array}{ccccccc}
 & & k_1 & k_2 & k_i & k_n \\
 & & x_1 & x_2 & x_i & x_n \\
u_1 & B_1 & & & & \\
u_{i_1} & B_{i_1} & & & 1 & \\
u_{j_1} & B_{j_1} & & & 0 & \\
u_{i_2} & B_{i_2} & & & 1 & \\
 & & & & & \\
u_{j_w} & B_{j_w} & & & 0 & \\
 & & & & & \\
u_{i_r} & B_{i_r} & & & 1 & \\
u_{i_t} & B_t & & & &
\end{array}
$$

# Generalized Cover-Free Family

## Definition

Let $w$ and $r$ be positive integers, a set system $(X, \mathcal{B})$ where $|X| = n$ and $\mathcal{B} = \{B_1, \ldots, B_t\}$ is called an $(r, w; d) - CFF(n, t)$ if for any two sets of indices $L, M \subseteq [t]$ such that $L \cap M = \varnothing$, $|L| = r$, and $|M| = w$, we have

$$| \bigcap_{l \in L} B_l \setminus \bigcup_{m \in M} B_m | \geq d.$$

# History

1964 Kautz and Singleton introduced the concept of CFF to investigate the properties of the non-random binary superimposed codes.

# History

1964 Kautz and Singleton introduced the concept of CFF to investigate the properties of the non-random binary superimposed codes.

1985 Erdös, Frankl and Füredi have studied this concept as a generalization of Sperner system.

# History

1964 Kautz and Singleton introduced the concept of CFF to investigate the properties of the non-random binary superimposed codes.

1985 Erdös, Frankl and Füredi have studied this concept as a generalization of Sperner system.

1988 Mitchell and Piper defined the concept of key distribution pattern which is in fact a generalized type of cover-free family.

# History

1964 Kautz and Singleton introduced the concept of CFF to investigate the properties of the non-random binary superimposed codes.

1985 Erdös, Frankl and Füredi have studied this concept as a generalization of Sperner system.

1988 Mitchell and Piper defined the concept of key distribution pattern which is in fact a generalized type of cover-free family.

2000 Stinson, Tran van Trung and Wei have studied the relationship between secure frame proof codes, group testing algorithms, cover free families and other combinatorial structures.

# History

1964 Kautz and Singleton introduced the concept of CFF to investigate the properties of the non-random binary superimposed codes.

1985 Erdös, Frankl and Füredi have studied this concept as a generalization of Sperner system.

1988 Mitchell and Piper defined the concept of key distribution pattern which is in fact a generalized type of cover-free family.

2000 Stinson, Tran van Trung and Wei have studied the relationship between secure frame proof codes, group testing algorithms, cover free families and other combinatorial structures.

2004 Stinson and Wei generalized the definition of cover-free family.

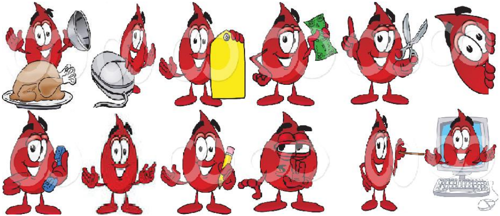
# Group Testing

In combinatorial mathematics, group testing is a set of problems with the objective of reducing the cost of identifying certain elements of a set. In fact, we like to find a small number of defective/interesting items from a large set.

# Group Testing

1. Given $v$ items with at most $d$ positive ones.

# Group Testing

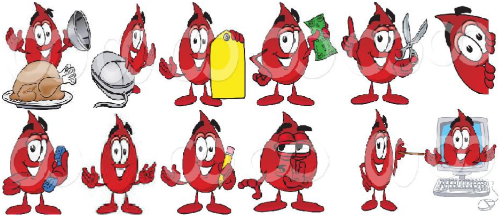


1. Given $v$ items with at most $d$ positive ones.
2. Identify all positive ones by the minimum number of tests.

# Group Testing

1. Given $v$ items with at most $d$ positive ones.
2. Identify all positive ones by the minimum number of tests.
3. Each test is on a subset of items.

# Group Testing



1. Given $v$ items with at most $d$ positive ones.
2. Identify all positive ones by the minimum number of tests.
3. Each test is on a subset of items.
4. Positive test outcome: there exists a positive item in the subset.

# Group Testing

1. Given $v$ items with at most $d$ positive ones.
2. Identify all positive ones by the minimum number of tests.
3. Each test is on a subset of items.
4. Positive test outcome: there exists a positive item in the subset.
5. Sequential group testing needs less number of tests, but longer time.

# Group Testing

1. Given $v$ items with at most $d$ positive ones.
2. Identify all positive ones by the minimum number of tests.
3. Each test is on a subset of items.
4. Positive test outcome: there exists a positive item in the subset.
5. Sequential group testing needs less number of tests, but longer time.
6. Non-adaptive group testing needs more tests, but shorter time.

# Group Testing

1. Given $v$ items with at most $d$ positive ones.
2. Identify all positive ones by the minimum number of tests.
3. Each test is on a subset of items.
4. Positive test outcome: there exists a positive item in the subset.
5. Sequential group testing needs less number of tests, but longer time.
6. Non-adaptive group testing needs more tests, but shorter time.
7. In molecular biology, non-adaptive group testing is usually taken.

# Group Testing

Let $X$ be a set of $v$ samples that are to be tested. Also, let each $B_i$ represents a subset of samples (called a group) that are to be combined and tested together.

# Group Testing

Let $X$ be a set of $v$ samples that are to be tested. Also, let each $B_i$ represents a subset of samples (called a group) that are to be combined and tested together.

$$x_1 \quad x_2 \quad x_3 \qquad \cdots \quad x_{v-1} \quad x_v$$

# Group Testing

Let $X$ be a set of $v$ samples that are to be tested. Also, let each $B_i$ represents a subset of samples (called a group) that are to be combined and tested together.

$$\begin{array}{ccccccc} & x_1 & x_2 & x_3 & \cdots & x_{v-1} & x_v \\ B_1 & 0 & - & + & \cdots & 0 & 0 \end{array}$$

# Group Testing

Let $X$ be a set of $v$ samples that are to be tested. Also, let each $B_i$ represents a subset of samples (called a group) that are to be combined and tested together.

$$
\begin{array}{ccccccccc}
 & x_1 & x_2 & x_3 & \cdots & x_{v-1} & x_v & & \\
B_1 & 0 & - & + & \cdots & 0 & 0 & & \\
 & & & & \vdots & & & & \\
B_i & - & 0 & + & \cdots & 0 & - & \longrightarrow & + \\
 & & & & \vdots & & & & \\
B_j & 0 & - & - & \cdots & 0 & - & \longrightarrow & -
\end{array}
$$

# Group Testing

Let $X$ be a set of $v$ samples that are to be tested. Also, let each $B_i$ represents a subset of samples (called a group) that are to be combined and tested together.

$$
\begin{array}{ccccccccc}
 & x_1 & x_2 & x_3 & \cdots & x_{v-1} & x_v & & \\
B_1 & 0 & - & + & \cdots & 0 & 0 & & \\
 & & & & \vdots & & & & \\
B_i & - & 0 & + & \cdots & 0 & - & \longrightarrow & + \\
 & & & & \vdots & & & & \\
B_j & 0 & - & - & \cdots & 0 & - & \longrightarrow & - \\
 & & & & \vdots & & & & \\
B_b & 0 & 0 & - & \cdots & - & - & \longrightarrow & -
\end{array}
$$

# Non-Adaptive Group Testing

Consider a set $N$ of $v$ items consisting of at most $d$ positive items.

# Non-Adaptive Group Testing

Consider a set $N$ of $v$ items consisting of at most $d$ positive items.

In Adaptive Group Testing, we specify tests one at a time, using the outcome of the previous tests, while in Non-Adaptive Group Testing, we must specify all the tests before seeing the outcomes of any of them.

# Non-Adaptive Group Testing

Consider a set $N$ of $v$ items consisting of at most $d$ positive items.

In Adaptive Group Testing, we specify tests one at a time, using the outcome of the previous tests, while in Non-Adaptive Group Testing, we must specify all the tests before seeing the outcomes of any of them.

Assume that $x_i$ is a negative sample and $x_{i_1}, \ldots, x_{i_d}$ are positive samples.

# Non-Adaptive Group Testing

Consider a set $N$ of $v$ items consisting of at most $d$ positive items.
In Adaptive Group Testing, we specify tests one at a time, using the outcome of the previous tests, while in Non-Adaptive Group Testing, we must specify all the tests before seeing the outcomes of any of them.
Assume that $x_i$ is a negative sample and $x_{i_1}, \ldots, x_{i_d}$ are positive samples.

$$
\begin{array}{c|cccc}
 & k_1 & k_2 & k_j & k_b \\
\hline
u_1 & & & & \\
u_{i_1} & & & 0 & \\
u_i & & & 1 & \\
u_{i_d} & & & 0 & \\
u_v & & & &
\end{array}
$$

The incidence matrix of a $(1, d) - CFF(b, v)$

$$
\begin{array}{cc|ccccc}
 & & x_1 & x_{i_1} & x_i & x_{i_d} & x_v \\
 & & u_1 & u_{i_1} & u_i & u_{i_d} & u_v \\
\hline
B_1 & k_1 & & & & & \\
B_2 & k_2 & & & & & \\
B_j & k_j & & 0 & 1 & 0 & \\
B_b & k_b & & & & &
\end{array}
\quad \rightarrow \quad -
$$

This is a $d$-NAGTA$(v; b)$

# Frameproof Codes

# Frameproof Codes


■ = "detectable positions"

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *pirate #1* | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |
| #2 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| #3 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |
| #4 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 |
| Attacked Content | 1 | 0/1 | 1 | 0 | 0/1 | 0 | 1 | 0/1 | 0/1 | 0 | 0/1 | 1 |

■ = "detectable positions"

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *pirate #1* | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |
| #2 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| #3 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |
| #4 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 |
| Attacked Content | 1 | 0/1 | 1 | 0 | 0/1 | 0 | 1 | 0/1 | 0/1 | 0 | 0/1 | 1 |

**Marking Assumption (D. Boneh and J. Shaw, 1998)**

Pirates detect fingerprint positions by finding differences in their copies. They make changes only in the detectable positions.

Suppose $C = \{w^{(u_1)}, w^{(u_2)}, \ldots, w^{(u_d)}\} \subseteq \Gamma$. Let $U(C)$ be the set of undetectable bit positions for $C$. Set

$$F(C) = \{x \in \{0,1\}^v : x|_{U(C)} = w^{(u_i)}|_{U(C)} \text{ for all } w^{(u_i)} \in C\}.$$

Suppose $C = \{w^{(u_1)}, w^{(u_2)}, \ldots, w^{(u_d)}\} \subseteq \Gamma$. Let $U(C)$ be the set of undetectable bit positions for $C$. Set

$$F(C) = \{x \in \{0,1\}^v : x|_{U(C)} = w^{(u_i)}|_{U(C)} \text{ for all } w^{(u_i)} \in C\}.$$

## Definition

Suppose that $\Gamma$ is a $(v, t)$-code. $\Gamma$ is said to be an *r-secure frameproof code* if for any $C_1, C_2 \subseteq \Gamma$ such that $|C_1| \leq r$, $|C_2| \leq r$ and $C_1 \cap C_2 = \varnothing$, we have that $F(C_1) \cap F(C_2) = \varnothing$. We will say that $\Gamma$ is an $r - SFPC(v, t)$ for short.

Suppose $C = \{w^{(u_1)}, w^{(u_2)}, \ldots, w^{(u_d)}\} \subseteq \Gamma$. Let $U(C)$ be the set of undetectable bit positions for $C$. Set

$$F(C) = \{x \in \{0,1\}^v : x|_{U(C)} = w^{(u_i)}|_{U(C)} \text{ for all } w^{(u_i)} \in C\}.$$

**Definition**

Suppose that $\Gamma$ is a $(v,t)$-code. $\Gamma$ is said to be an $r$-secure frameproof code if for any $C_1, C_2 \subseteq \Gamma$ such that $|C_1| \leq r$, $|C_2| \leq r$ and $C_1 \cap C_2 = \varnothing$, we have that $F(C_1) \cap F(C_2) = \varnothing$. We will say that $\Gamma$ is an $r - SFPC(v,t)$ for short.

**Theorem. (D.R. Stinson, Tran van Trung, R. Wei, 2000)**

If there exists an $r - SFPC(v,t)$, then there exists an $(r,r) - CFF(2v,t)$.

**Definition**

A $t-(v,k,\lambda)$ packing design is a set system $(X,\mathcal{B})$, where $|X|=v, |\mathcal{B}|=k$ for every $B\in\mathcal{B}$, and every $t$-subset of $X$ occurs in at most $\lambda$ blocks in $\mathcal{B}$.

**Definition**

A $t-(v,k,\lambda)$ packing design is a set system $(X,\mathcal{B})$, where $|X|=v, |\mathcal{B}|=k$ for every $B\in\mathcal{B}$, and every $t$-subset of $X$ occurs in at most $\lambda$ blocks in $\mathcal{B}$.

**Theorem. (Wei, 2006)**

If there exists a $t-(v,k,1)$ packing design having $b$ blocks, then there exists a $(r,1;d)-CFF(v,b)$, where $r=\lfloor (k-d-2)/(t-1)\rfloor$.

# Bounds

- $N((r, w; d), t)$ denote the minimum number of points in any $(r, w; d) - CFF$ having $t$ blocks.

# Bounds

- $N((r,w;d),t)$ denote the minimum number of points in any $(r,w;d)-CFF$ having $t$ blocks.

**Theorem. (D.R. Stinson and R. Wei, 2004)**

Let $r$, $w$, and $t$ be positive integers where $t \geq r+w$. Then

$$N((r,w;d),t) \geq 2c\frac{\binom{w+r}{w}}{\log(w+r)}\log t + \frac{1}{2}c\binom{w+r}{w}(d-1)$$

**Theorem. (D.R. Stinson and R. Wei, 2004)**

TheoremLet $r$, $w$, and $t$ be positive integers where $t \geq r+w$. Then

$$N((r,w;d),t) \geq 0.7c\frac{\binom{w+r}{w}(w+r)}{\log(w+r)}\log t + \frac{1}{2}c\binom{w+r}{w}(d-1)$$

**Definition**

A biclique cover of a graph $G$ is a collection of bicliques (complete bipartite graphs) of $G$ such that each edge of $G$ is in at least one of the bicliques. The number of bicliques in a minimum biclique covering of $G$ is called the biclique covering number of $G$ and denoted by $bc(G)$.

### Definition

A biclique cover of a graph $G$ is a collection of bicliques (complete bipartite graphs) of $G$ such that each edge of $G$ is in at least one of the bicliques. The number of bicliques in a minimum biclique covering of $G$ is called the biclique covering number of $G$ and denoted by $bc(G)$.

### Definition

A $d$- biclique cover of a graph $G$ is a collection of bicliques of $G$ such that each edge of $G$ is in at least $d$ of the bicliques. The number of bicliques in a minimum $d$-biclique covering of $G$ is called the $d$-biclique covering number of $G$ and denoted by $bc_d(G)$.

# Biclique covering

**Definition**

For $0 < w \leq r \leq t$, the bi-intersection graph $I_t(r,w)$ is a bipartite graph whose vertices are the $w$- and $r$-subsets of a $t$-element set where two vertices are adjacent if and only if their intersection is empty.

**Theorem. (H. H. and F. Moazami, 2010)**

For every positive integer $r$, $w$, $d$ and $t$, where $t \geq r + w$ we have

$$N((r,w;d),t) = bc_d(I_t(r,w)).$$

**Theorem. (H. H. and F. Moazami, 2010)**

For every positive integer $r$, $w$, $d$ and $t$, where $t \geq r + w$ we have

$$N((r,w),t) \geq \binom{r+w-2}{r-1} \mathcal{R}(t-r-w+2).$$

**Theorem. (H. H. and F. Moazami, 2010)**

For every integer $0 \leq s < w \leq r$ and $t \geq r + w$,

$$N((r,w;d),t) \geq \sum_{i=0}^{s} \binom{s}{i} N((r-i, w-s+i; d), t-s).$$

H.Hajiabolhassan and F. Moazami, Cover-Free Families Through Biclique Cover.
manuscript 2010, arXiv:1008.3691.

D. R. Stinson and R. Wei., Combinatorial properties and constructions of traceability schemes and frameproof codes.
*SIAM J. Discrete Math.*, 11 (1998), 41–53 .

D. R. Stinson, R. Wei, and L. Zhu, Some new bounds for cover-free families.
*J. Combin. Theory Ser. A*, 90 (2000), 224–234.

# Thank You!

I would like to acknowledge Ms. Farokhlagha Moazami for her useful comments.