Fingerprinting & Broadcast Encryption for Content Protection
Outline

- Introduction
- Fingerprinting & Traitor Tracing
- Broadcast Encryption
Introduction

- Fingerprinting
- Traitor tracing
- Broadcast encryption
Fingerprinting & Traitor Tracing

- Marking assumption
- Traceability scheme
- Frameproof code
- $c$-secure code
- $c$-TA code & $c$-IPP code
- Combinatorial properties
- Fingerprinting methods
- Tracing algorithm
<Definition> undetectable positions

Let \( \Gamma = \{w^{(1)}, \ldots, w^{(n)}\} \) be an \((l, n)\) - code and \( C \) be a coalition of users. For \( i \in \{1, \ldots, l\} \) we say that position \( i \) is undetectable for \( C \) if the words assigned to users in \( C \) match in their \( i \)th position. Formally, suppose \( C = \{u_1, \ldots, u_c\} \).

Then position \( i \) is undetectable if \( w_{i}^{(u_1)} = w_{i}^{(u_2)} = \ldots = w_{i}^{(u_c)} \).

<Definition> feasible set

Let \( \Gamma = \{w^{(1)}, \ldots, w^{(n)}\} \) be an \((l, n)\) - code and \( C \) be a coalition of users. Let \( R \) be the set of undetectable positions for \( C \). Define the feasible set of \( C \) as \( F(C; \Gamma) = \{w \in (\Sigma \cup \{\}\})' \ s.t. \ w R = w^{(u)} R \} \) for some user \( u \) in \( C \). Thus the feasible set contains all words which match the coalition's undetectable bits. Usually we omit the \( \Gamma \) and denote \( F(C; \Gamma) \) by \( F(C) \).
Fingerprinting & Traitor Tracing - Marking assumption

e.g. A: 3 2 3 1 2
    B: 1 2 2 1 2

\[ F(AB) = \Sigma' \cdot 2 \cdot \Sigma' \cdot 1 \cdot 2 \]

- Definition > Marking Assumption
  any coalition of \( \mathcal{C} \) users is only capable of creating an object whose fingerprint lies in the feasible set of the coalition
<Definition> Traitor tracing schemes
(B. Chor, A. Fiat, M. Naor, and B. Pinkas, 1994)

A traitor tracing scheme consists of three components:

1. A user initialization scheme, used by the data supplier to add new users. The data supplier has a meta-key $\alpha$ that defines a mapping $P_{\alpha}: U \mapsto \{0,1\}^s$ where $U$ is the set of possible users and $s$ is the number of bits in the personal key that each user gets.

2. An encryption scheme $E_{\alpha}: \{0,1\}^* \mapsto \{0,1\}^*$ used by the data supplier to encrypt messages and a decryption scheme $D_{\beta}: \{0,1\}^* \mapsto \{0,1\}$ used by every user to decrypt those messages.

3. A traitor tracing algorithm, used upon confiscation of a pirate decoder, to determine the identity of a traitor.
<Definition> \(c\)-Frameproof codes

(James Shaw, 1995 (1998))

A code \(\Gamma\) is \(c\)-frameproof if every set \(W \subset \Gamma\), of size at most \(c\), satisfies \(F(W) \cap \Gamma = W\)
<Definition> totally $c$-secure code

A code $\Gamma$ is totally $c$-secure if there exists a tracing algorithm $A$ satisfying the following condition: if a coalition $C$ of at most $c$ users generates a word $x$ then $A(x) \in C$.

<Lemma>

If $\Gamma$ is a totally $c$-secure code then

$$C_1 \cap \ldots \cap C_r = 0 \Rightarrow F(C_1) \cap \ldots \cap F(C_r) = 0$$

for all coalitions $C_1, \ldots, C_r$ of at most $c$ users each.
Fingerprinting & Traitor Tracing
- c-TA code & c-IPP code

- A. Silverberg, J. Staddon, 2001

- **<Definition>** c-TA (traceability)

  A code $C$ is a c-TA code if for all coalitions $C_i$ of size at most $c$, if $w \in \text{desc}(C_i)$ then there exists $x \in C_i$ such that $|I(x, w)| > |I(z, w)|$ for all $z \in C - C_i$.

- **<Definition >** c-IPP (identifiable parent property)

  A code $C$ is a c-IPP code if for all $w \in \text{desc}_c(C)$, the intersection of the coalitions $C_i$ of size at most $c$ such that $w \in \text{desc}(C_i)$ is nonempty.
<Lemma> Every $c$-TA code is a $c$-IPP code.

<proof>

Suppose $C$ is a $c$-TA code.
if $w \in \text{desc}_c(C)$, $\exists C_i \in C$ where $|C_i| = c$, s.t. $w \in \text{desc}(C_i)$.

Let $y \in C_i$ s.t. $|I(w,y)| \geq |I(w,x)|$ for all $x \in C_i$.

Thus $|I(w,y)| \geq |I(w,x)|$ for any $x \in C$ by the definition of a $c$-TA code.

We will show that, for any $C_j \subseteq C$ with $|C_j| \leq c$,

$w \in \text{desc}(C_j) \Rightarrow y \in C_j$.

In fact, if $y \not\in C_j$, then $\exists z \in C_j$ s.t. $|I(w,z)| \geq |I(w,y)|$ by the definition of a a $c$-TA code.

$\rightarrow\leftarrow$
Fingerprinting & Traitor Tracing
- Combinatorial properties

- “Combinatorial properties and constructions of traceability schemes and frameproof codes”, D. R. Stinson, R. Wei, 1997(2001)
- Investigate combinatorial properties and constructions of two recent topics of cryptographic interest:
  - frameproof codes
  - traceability scheme
Fingerprinting & Traitor Tracing
- Combinatorial properties

- **<Definition>** \( c\text{-FPC}(v,b) \)
  
  A \((v,b)\) - code \( \Gamma \) is called a \( c \) - frameproof code if, for every \( W \subseteq \Gamma \) such that \(|W| \leq c\), we have \( F(w) \cap \Gamma = W \).
  
  We say that \( \Gamma \) is a \( c\text{-FPC}(v,b) \).

- **<Definition>** \( c\text{-TS}(k,b,v) \)
  
  If \(|F \cap P(U)| \geq |F \cap P(V)|\) for all users \( V \neq U \), then \( U \) is defined to be an exposed user.
  
  Suppose any exposed user \( U \) is a member of the coalition \( C \) whenever a pirate decoder \( F \) is produced by \( C \) and \(|C| \leq c\). Then the scheme is called a \( c \) - traceability scheme and it is denoted by \( c\text{-TS}(k,b,v) \).
  
  Traitor detection would be done by computing \(|F \cap P(U)|\) for all users \( U \).
<Theorem>

\[ \exists a \text{-FPC}(v, b) \iff \exists \text{a set system } (\mathcal{X}, \mathcal{B}) \text{ such that } |\mathcal{X}| = v, \]
\[ |\mathcal{B}| = b \text{ and for any subset of } d \leq c \text{ blocks } B_1, B_2, ..., B_d \in \mathcal{B}, \]
there does not exist a block \( B \in \mathcal{B} \setminus \{B_1, B_2, ..., B_d\} \) such that
\[ \bigcap_{i=1}^{d} B_i \subseteq B \subseteq \bigcup_{i=1}^{d} B_i. \]
Fingerprinting & Traitor Tracing - Combinatorial properties

- <Theorem>

\[ \exists \text{ a } c-TS(k, b, v) \iff \exists \text{ a set system } (\mathcal{X}, \mathcal{B}) \text{ such that } |\mathcal{X}| = v, \]
\[ |\mathcal{B}| = b \text{ and } |\mathcal{B}| = k \text{ for every } B \in \mathcal{B}, \text{ with the property that } \]
\[ \text{for every choice of } d \leq c \text{ blocks } B_1, B_2, \ldots, B_d \in \mathcal{B} \text{ and for any } \]
\[ k\text{-subset } F \subseteq \bigcup_{j=1}^{d} B_j, \text{ there does not exist a block } \]
\[ B \in \mathcal{B}\setminus\{B_1, B_2, \ldots, B_d\} \text{ such that } |F \cap B_j| \leq |F \cap B| \text{ for } 1 \leq j \leq d \]
<Theorem> If there exists a $c$-TS$(k, b, \nu)$, then there exists a $c$-FPC$(\nu, b)$. 

<proof>

Let $(\mathcal{X}, \mathcal{B})$ be the set system corresponding to a $c$-TS$(k, b, \nu)$. We prove that $(\mathcal{X}, \mathcal{B})$ is a $c$-FPC$(\nu, b)$. 

Suppose no; then there exist $d \leq c$ blocks, $B_1, B_2, \ldots, B_d \in \mathcal{B}$, and a block $B \in \mathcal{B}\backslash\{B_1, B_2, \ldots, B_d\}$ such that $B \subseteq \bigcup_{i=1}^{d} B_i$. 

Then $|B \cap B_j| \leq |B \cap B|$ for $1 \leq j \leq d$. 

$\rightarrow \leftarrow$
Fingerprinting & Traitor Tracing
- Fingerprinting methods

- AND-resilient codes
  - Trivial AND-ACC
  - $\Gamma_0$
  - AND-ACC (Trape et al., 2003)
  - The fingerprinting scheme based on projective space (Dittmam, 2000)

- Selection-resilient codes
  - $\Gamma_0$ combined with $(L,N,D)_q$-ECC, $D > L(1-(1/c))$
  - $(L,N,D)_q$-ECC with $D >= L(1-1/c^2)$ (Staddon, 2001)
Fingerprinting & Traitor Tracing
- Tracing algorithms

- scenario
  - The center broadcasts the encrypted content to users
  - One encryption key and multiple distinct decryption keys
  - One cannot compute a new decryption key from a given set of keys
Fingerprinting & Traitor Tracing
- Tracing algorithms

- Static tracing
  - Used upon confiscation of a pirate decoder, to determine the identity of a traitor
  - Such scheme would be ineffective if the pirate were simply to rebroadcast the original content
  - Use watermarking methods to allow the broadcaster to generate different versions of the original content
  - Use the watermarks found in the pirate copy to trace its supporting traitors
  - Drawback: requires one copy of content for each user and so requires very high bandwidth
Fingerprinting & Traitor Tracing

- Tracing algorithms

- Dynamic tracing (Fiat & Tassa, 2001)
  - The content is divided into consecutive segments
  - Embed one of the q marks in each segment, hence creating q versions of the segment (watermarking method)
  - In each interval, the user group is divided into q subsets and each subset receives on version of the segment
  - The subsets are varied in each interval using the rebroadcasted content
  - Trace all colluders with lower bandwidth
  - Drawback:
    - Vulnerable to a delayed rebroadcast attack
    - High real-time computation for regrouping the users and allocating marks to subsets
Fingerprinting & Traitor Tracing
- Tracing algorithms

- Sequential tracing (Reihaneh, 2003)
  - The channel feedback is only used for tracing and not for allocation of marks to users
  - The mark allocation table is predefined and there is no need for real-time computation to determine the mark allocation of the next interval
    - The need for real-time computation will be minimized
    - Protects against the delayed reboradcast attack
  - The traitors are identified sequentially
Broadcast Encryption

- Key pre-distribution schemes
- Key management
Broadcast Encryption
- Key pre-distribution scheme

- In a key pre-distribution scheme, the trusted authority (TA) generates and distributes keys to each user.

- The goal is to allow TA to broadcast the secure message to a dynamically changing privileged subset of users in such a way that non-privileged users cannot learn the message while minimizing key management related-transmissions.
Broadcast Encryption
- Key pre-distribution scheme

- <Definition> $(\mathcal{P}, \mathcal{F})$-KPS
  $(\mathcal{P}, \mathcal{F})$-Key Predistribution Scheme
  The scheme is a $(\mathcal{P}, \mathcal{F})$-Key Predistribution Scheme if it satisfies:
  - Each user $i$ in any privileged set $P \in \mathcal{P}$ can compute $k_p$
  - No forbidden subset $F \in \mathcal{F}$ disjoint from any privileged subset $P$ has no information on $k_p$
Broadcast Encryption
- Key pre-distribution scheme

- **Trivial KPS**
- **Shamir threshold KPS (Shamir, 1979)**
- **Blom KPS (1984)**
- **Fiat-Naor KPS (1993)**
<Definition> \((\mathcal{P}, \mathcal{F})\)-One-Time Broadcast Encryption Scheme

We say that the scheme is a \((\mathcal{P}, \mathcal{F})\)-One-Time Broadcast Encryption Scheme \(((\mathcal{P}, \mathcal{F})\text{-OTBES})\) if it satisfies:

1. Without knowing the broadcast, no subset of users has any information about \(m_p\), even given all the secret information \(U_v\).
2. The message for a privileged user is uniquely determined by the single broadcast and the user's secret information.
3. After receiving the broadcast, no forbidden subset \(F\) disjoint from \(P\) has any information on \(m_p\).
Broadcast Encryption
- Key pre-distribution scheme

- Beimel-Chor OTBES (1993)
Broadcast Encryption
- Key pre-distribution scheme

- **<Definition>** $(\mathcal{P}, \mathcal{F})$-Key Distribution Pattern
  (Mitchell & Piper, 1988)

  $\mathcal{U}$: a set of users
  $\mathcal{B} = \{B_1, ..., B_\beta\}$: a set of subsets of $\mathcal{U}$ called blocks
  $(\mathcal{U}, \mathcal{B})$ is a $(\mathcal{P}, \mathcal{F})$ - Key Distribution Pattern
  ($(\mathcal{P}, \mathcal{F})$ - KDP)

  if $\{B_j : P \subseteq B_j$ and $F \cap B_j = \phi\} \neq \phi$

  $\forall P \in \mathcal{P}$ and $F \in \mathcal{F}$ s.t. $P \cap F = \phi$
Broadcast Encryption
- Key pre-distribution scheme

- A KDP can be represented by an \( n \times \beta \) incidence matrix \( A = (a_{ij}) \) which is defined as follows:

\[
a_{ij} = \begin{cases} 
1 & \text{if } i \in B_j \\
0 & \text{otherwise.}
\end{cases}
\]

- The KDP can be used to construct KPS.
Theorem> Suppose \((\mathcal{U}, \mathcal{B})\) is a \((\mathcal{P}, \mathcal{F})\)-KDP, then exists a \((\mathcal{P}, \mathcal{F})\)-KPS with information rate
\[\frac{1}{\max\{r_i: 1 \leq i \leq n\}} \quad r_i = |\{B_j : i \in B_j\}|\]
and total information rate
\[\frac{1}{\beta}\]

The trivial KPS and Fiat-Naor KPS are both in fact KDPs
- The trivial KPS is obtained by taking \(\mathcal{B}\) to be all \(t\)-subsets of \(\mathcal{U}\)
- The Fiat-Naor KPS is produced by taking \(\mathcal{B}\) to be all subsets of \(\mathcal{U}\) of cardinality at least \(n-w\)
Broadcast Encryption
- Key pre-distribution scheme

- **OA KDP (Stinson, 1997)**
- **PA KDP (Stinson, 1997)**
Broadcast Encryption
- Key management

- The purpose of key management is to provide secure procedures for handling cryptographic keying material to be used in symmetric or asymmetric cryptographic mechanisms.

- The Open Systems Interconnection (OSI) Security Architecture defines key management as “the generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy”.

Broadcast Encryption
- Key management

- Access control schemes
  - The bit-vector scheme
  - The block-by-block scheme
  - The extended-header scheme
  - The VSPACE scheme
  - The tree scheme
The state update problem

- Content is encrypted using a group key which is known to a group of users in many scenarios.
- When users leave or join the group, the group key must be changed.
  - Prevent leaving members from decrypting content in the future.
  - Prevent joining members from decrypting previous content (backward secrecy).
- \( O(n) \) messages.

How to reduce the overhead of the key update messages?
Broadcast Encryption - Key management

The LKH (Logical Key Hierarchy) Scheme
Introduction-Fingerprinting

- Fingerprinting is the process of assigning an unique key for each user
- The purpose is to identify the person who acquired a particular copy

Implementation
- Embed an unique key inside the content for each user
- Encrypt the content and each user has his own decryption key to recover the content
Introduction-Traitor Tracing

- Collusion attack
  - A group of malicious users (traitors) can collude by combining their keys to create a new pirate key (pirate decoder)
  - A traitor tracing algorithm is used to trace at least one of the colluders or the group containing the colluders
Introduction-Broadcast Encryption

- Broadcast encryption schemes enable a trusted authority to broadcast a message to the users in a network so that a certain specified subset of authorized users can decrypt it.

- It involves the problems of the key pre-assignment, key management and even the traceability schemes.
Fingerprinting & Traitor Tracing
- Fingerprinting methods

- Consist of all $n$-bit binary vectors that have only a single 0 bit

- e.g. $n=4$
  
  $C=\{1110,1101,1011,0111\}$
Fingerprinting & Traitor Tracing
- Fingerprinting methods

- **<Definition>** \( \Gamma_0 \)
  the \((n,n)\)-code containing all \(n\)-bit binary words with exactly one 1

  e.g. \( \Gamma_0 (3) = \{100, 010, 001\} \)
### Fingerprinting & Traitor Tracing

- **Fingerprinting methods**

  - **Use BIBD to construct an AND-ACC**
  
  - **<Theorem>** Let \((X,A)\) be a \((v,k,1)\)-BIBD and \(M\) the corresponding incidence matrix. If the codevectors are assigned as the bit complement of the columns of \(M\), then the resulting scheme is a \((k-1)\)-resilient AND-ACC.

  - **e.g. \((7,3,1)\)-BIBD**

<table>
<thead>
<tr>
<th>(C)</th>
</tr>
</thead>
</table>
| \[
\begin{bmatrix}
0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 \\
\end{bmatrix}
\] |
Fingerprinting & Traitor Tracing
- Fingerprinting methods

- Constructions using $t$-designs

- <Definition> $t$-$(v, k, \lambda )$ design

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

- BIBD’s are 2-$(v, k, \lambda )$ design

- e.g. 2-$(9, 3,1)$ design

  \{0,1,6\}, \{0,2,5\}, \{0,3,4\}, \{1,2,4\}, \{3,5,6\}, \{1,5,7\},
  \{5,4,8\}, \{4,6,7\}, \{6,2,8\}, \{2,3,7\}, \{3,1,8\}, \{0,7,8\}
Fingerprinting & Traitor Tracing
- Fingerprinting methods

- Use techniques from finite projective geometry to construct d-detecting fingerprinting scheme

- e.g. PG(2,2) 2-detecting
<Lemma>
Let $\Gamma$ be a $\epsilon$-frameproof $(L,\ell,p)$-code and $C$ be an $(L,N,D)_p$-ECC. Let $\Gamma'$ be the composition of $\Gamma$ and $C$. Then $\Gamma'$ is a $\epsilon$-frameproof code, provided $D > L(1 - (1/\epsilon))$. 

Fingerprinting & Traitor Tracing
- Fingerprinting methods
Suppose that $C$ is an $(L,N,D)_q$ - ECC having minimum Hamming distance $D > L(1-1/c^2)$. Then $C$ is $c$ - TA code.
Broadcast Encryption
- Key pre-distribution scheme

- Trivial KPS 1
  give every user $u_i \in U$ its own key and transmit an individually encrypted message $E_{u_i}(m)$ to every member $u_j \in P$
  $\rightarrow$ long transmission time

- Trivial KPS 2
  for every $t$-subset $P \subseteq U$, the TA gives $k_p$ to every member of $P$
  $\rightarrow$ every user stores a huge number of keys
**Broadcast Encryption**

- **Key pre-distribution scheme**

- **Blom KPS**

  \( t = 2 \)

1. The TA chooses \( n \) distinct random numbers \( s_i \in GF(q) \), and gives \( s_i \) to user \( i \) (\( 1 \leq i \leq n \)). These values do not need to be secret.

2. The TA constructs a random polynomial

   \[
   f(x, y) = \sum_{i=0}^{w} \sum_{j=0}^{w} a_{ij} x^i y^j
   \]

   having coefficients in \( GF(q) \), s.t \( a_{ij} = a_{ji} \) \( \forall \ i, j \)

3. The TA computes the polynomial

   \[
   g_i(x) = f(x, s_i) = \sum_{j=0}^{w} b_{ij} x^j
   \]

4. The TA gives the \( w + 1 \) values \( b_{ij} \) to user \( i \)

   \[
   k_r = g_i(s_j) = g_j(s_i)
   \]
Broadcast Encryption
- Key pre-distribution scheme

- Blom KPS
  e.g.

\[ t = 2 \]
\[ n = 3, q = 17, w = 1, s_1 = 12, s_2 = 7, s_3 = 1 \]
\[ f(x, y) = 8 + 7(x + y) + 2xy \]
\[ g_1(x) = 7 + 14x, g_2(x) = 6 + 4x, g_3(x) = 15 + 9x \]
\[ u_1(x) = (7, 14), u_2(x) = (6, 4), u_3(x) = (15, 9) \]
\[ k_{\{1,2\}} = 3, k_{\{1,3\}} = 4, k_{\{2,3\}} = 10 \]
Broadcast Encryption
- Key pre-distribution scheme

- Fiat-Naor KPS

For every subset $F \subseteq U$ with $|F| \leq w$,
the TA chooses a random value $s_F \in GF(q)$
and gives $s_F$ to every member of $U \setminus F$.
→ The key associated with a privileged set $P$ is defined to be

$$k_P = \sum_{\{F \in \mathcal{F} : F \cap P = \emptyset\}} s_F$$
Broadcast Encryption
- Key pre-distribution scheme

- Fiat-Naor KPS

e.g.

\[ n = 3, q = 17, w = 1 \]
\[ s_\phi = 11, s_{\{1\}} = 8, s_{\{2\}} = 3, s_{\{3\}} = 8 \]
\[ k_\phi = 13, \]
\[ k_{\{1\}} = 5, k_{\{2\}} = 10, k_{\{3\}} = 5, \]
\[ k_{\{1,2\}} = 2, k_{\{1,3\}} = 14, k_{\{2,3\}} = 2, \]
\[ k_{\{1,2,3\}} = 11 \]
Beimel-Chor OTBES

Suppose $t \equiv 0 \mod l$, let $l = 2$

1. A $(2, t + w - 2)$ Blom scheme in $GF(q)$ is set up.
2. Suppose that the privileged set $P = \{i_1, ..., i_t\}$.

The complete graph $K_t$ on vertex set $P$ and edge set $E$, can be partitioned into one-factor (perfect matchings).

$\forall e = \{i, j\} \in E \exists$ a unique one-factor containing it,

and a unique key $k_e$ determined by the Blom scheme

Suppose that the one-factors are named $F_1, ..., F_{t-1}$.

3. $b_p = (m_i + k_e : e \in F_i, 1 \leq i \leq t-1)$
Broadcast Encryption
- Key pre-distribution scheme

- Beimel-Chor OTBES

\( t = 4, P = \{i_1, ..., i_4\} \)
\( F_1 = \{\{i_1, i_2\}, \{i_3, i_4\}\} \)
\( F_2 = \{\{i_1, i_3\}, \{i_2, i_4\}\} \)
\( F_3 = \{\{i_1, i_4\}, \{i_2, i_3\}\} \)

\( m_p = (m_1, m_2, m_3) \)
\( b_p = (m_1 + k_{\{i_1, i_2\}}, m_1 + k_{\{i_3, i_4\}}, m_2 + k_{\{i_1, i_3\}}, m_2 + k_{\{i_2, i_4\}}, m_3 + k_{\{i_1, i_4\}}, m_3 + k_{\{i_2, i_3\}}) \)
Secret Sharing Schemes

Let $X$ be a set of $n$ users, $\Gamma \subseteq 2^X$ be a set of subsets called authorized subsets. In a secret sharing scheme, the TA has one secret value $k \in GF(q)$, called the key. The TA will distribute secret information to each user in $X$, in such a way that any authorized subset can compute $k$ from the shares they jointly hold, but no unauthorized subset has any information about $k$. The secret information given to user $i$ will be denoted $u_i$ and is called the share of user $i$. 
Broadcast Encryption
- Key pre-distribution scheme

■ Shamir threshold KPS

Let \( q \geq n + 1 \) be a prime power

1. The TA chooses \( n \) distinct non-zero random numbers \( x_i \in GF(q) \), and gives \( x_i \) to user \( i \) (\( 1 \leq i \leq n \)).
These values do not need to be secret.

2. The TA constructs a random polynomial of degree at most \( t-1 \)
\[
f(x) = \sum_{i=0}^{t-1} a_i x_i
\]
having coefficients in \( GF(q) \).
The key is the constant term \( a_0 \).

3. The TA computes the polynimail
\[
y_i = f(x_i)
\]
and gives \( y_i \) to user \( i \).
Shamir threshold KPS

e.g.

Suppose we construct a scheme in \( GF(17) \) and the public values are \( x_i = i, 1 \leq i \leq 5 \).

Suppose that the TA chooses the polynomial

\[ f(x) = 13 + 10x + 2x^2, \]

so the key is 13.

The shares that are distributed are

\[ y_1 = f(1) = 8, \quad y_2 = f(2) = 7, \quad y_3 = f(3) = 10, \]
\[ y_4 = f(4) = 0, \quad y_5 = f(5) = 11 \]

Any 3 of the ordered pairs (1,8), (2,7), (3,10), (4,0), (5,11) can be used to reconstruct the polynomial \( f \).
Broadcast Encryption
- Key pre-distribution scheme

- **<Definition> Orthogonal Array**

An orthogonal array \( OA_\lambda (s,n,v) \) is a \( \lambda v^s \times n \) array, \( A = (a_{j,i}) \), with entries from a \( v \)-set, say \( Y \), s.t., for any \( s \) columns of \( A \), say \( \gamma_1,...,\gamma_s \), there are exactly \( \lambda \) rows of \( A \) in which the entry \( u_i \) occurs in column \( \gamma_i \) for all \( i, 1 \leq i \leq s \).
<Theorem> OA KDP

Suppose there is an $OA_{\lambda}(s,n,v)$ with $s \geq 3$. Suppose that $1 \leq z \leq v-1$ and $2 \leq t \leq s-1$, and define $m = (v-z)^t \lambda v^w$. Suppose that $q$ is a prime power s.t. $q \geq (v-z)^t \lambda v^w - 1$. Then there exists a $(t,s-t)$ - KPS for a set of $n$ users, having key set $[GF(q)]^m$. 
<Definition> Perpendicular Arrays

A perpendicular array $PA_\lambda(s,n,v)$ is a $\lambda \binom{v}{s} \times n$ array, $A = (a_{j,i})$, with entries from a $v$-set, say $Y$, s.t. the following properties are satisfied:

1. each row of $A$ contains $n$ different elements of $Y$,
2. for any $s$-subset of $Y$, and for any $s$ columns of $A$, there are exactly $\lambda$ rows of $A$ in which the $s$ given elements occur in the $s$ given columns (in some order).
<Theorem> PA KDP

Suppose there is a $PA_{\lambda} (s,n,v)$ with $3 \leq s \leq (n+1)/2$.

Suppose that $1 \leq z \leq v-1$ and $2 \leq t \leq s-1$,

$$m = \sum_{i=0}^{s-t} (-1)^i \frac{\lambda_{v-t-i}^{s-t-i} \binom{s-t}{i} \binom{v-z}{t+i}}{\binom{s}{t+i}}, q \geq \frac{\lambda_{v-t}^{s-t} \binom{v-z}{t}}{\binom{s}{t}} - 1.$$  

Then there exists a $(t,s-t)$ - KDP for a set of $n$ users, having key set $[GF(q)]^m$.  


Broadcast Encryption
- Key pre-distribution scheme

- PA KPS

E.g.

We consider the $PA_4(3,7,8)$. A is a $56 \times 7$ array with symbols from the set $S = \{\infty, 0, 1, 2, 3, 4, 5, 6\}$. The array $A$ is obtained by developing the following rows modulo 7:

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>$\infty$</td>
</tr>
<tr>
<td>$\infty$</td>
<td>3</td>
<td>6</td>
<td>1</td>
<td>5</td>
<td>4</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>$\infty$</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>6</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>$\infty$</td>
<td>5</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>5</td>
<td>$\infty$</td>
<td>6</td>
<td>2</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>1</td>
<td>6</td>
<td>$\infty$</td>
<td>0</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>6</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>$\infty$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>0</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>$\infty$</td>
<td></td>
</tr>
</tbody>
</table>
Broadcast Encryption
- Key pre-distribution scheme

- PA KDP

E.g. Suppose $Z = \{0,1,2,3\}$. Then we can construct a (2,1) - KDP $(\mathcal{U}, \mathcal{B})$ from $A$, where $\mathcal{U} = \{1,2,3,4,5,6,7\}$ and the 56 blocks of $\mathcal{B}$ are given below.

\[
\begin{array}{cccccccc}
5 & 6 & 7 & 1 & 3 & 5 & 6 & 2 & 3 & 6 & 7 & 1 & 2 & 3 & 4 \\
4 & 5 & 6 & 1 & 2 & 5 & 6 & 1 & 2 & 3 & 7 & 2 & 3 & 4 & 6 \\
3 & 4 & 5 & 1 & 2 & 6 & 7 & 1 & 2 & 3 & 5 & 2 & 3 & 6 & \\
2 & 3 & 4 & 1 & 2 & 4 & 7 & 1 & 2 & 5 & 3 & 5 & 6 & \\
1 & 2 & 3 & 1 & 4 & 7 & 2 & 4 & 5 & 3 & 5 & 7 & & \\
1 & 2 & 7 & 1 & 3 & 4 & 2 & 4 & 6 & 1 & 3 & 5 & 7 & \\
1 & 6 & 7 & 1 & 3 & 5 & 2 & 4 & 6 & 7 & 1 & 3 & 4 & 7 & \\
3 & 4 & 5 & 7 & 1 & 4 & 5 & 1 & 2 & 6 & 2 & 4 & 7 & \\
3 & 4 & 7 & 1 & 5 & 7 & 1 & 3 & 6 & 2 & 4 & 5 & 7 & \\
4 & 6 & 7 & 2 & 5 & 7 & 1 & 3 & 4 & 6 & 1 & 4 & 5 & 7 & \\
1 & 4 & 6 & 2 & 3 & 5 & 7 & 3 & 4 & 6 & 7 & 1 & 5 & 6 & 7 & \\
1 & 2 & 4 & 6 & 2 & 3 & 5 & 6 & 4 & 5 & 6 & 7 & 1 & 3 & 6 & 7 & \\
1 & 2 & 4 & 5 & 3 & 4 & 5 & 6 & 2 & 5 & 6 & 7 & 3 & 6 & 7 & \\
2 & 3 & 4 & 5 & 1 & 4 & 5 & 6 & 2 & 5 & 6 & 7 & 2 & 3 & 7 & \\
\end{array}
\]
The bit-vector scheme

- Popular access control scheme
  (analog European satellite TV system,
  Sky VideoCrypt systems, ...)
- All the programs are encrypted with the same key, which is stored in every set-top terminal (STT)
- The STT decrypts a program $p$ only if the $p$-th bit of bit-vector $b[p] = 1$. 
Broadcast Encryption
- Key management

- The block-by-block scheme
  - The programs are split into $n$ disjoint blocks, and all the programs belonging to a block are encrypted using the same key
  - The STT stores the keys for each block that the user buys
Broadcast Encryption
- Key management

- The extended-header scheme
  - Attach cryptographic header information to each program
  - Arrange the programs into predefined packages, and each package has a key
  - Need large headers to each program in order to achieve flexibility in packaging the programs
Broadcast Encryption
- Key management

- The VSPACE scheme
  - Attach only the single n-bit cryptographic identifier (CID) to a program
  - The encryption key of a program is function of its CID $p$:
    $$\text{Key}(p) = Mp$$
    The columns of $M$ are master keys, which are linearly independent vectors.