Key Distribution Patterns

- suppose we have a TA and a network of n users, $\mathcal{U} = \{U_1, \ldots, U_n\}$
- the TA chooses v random keys, say $k_1, \ldots, k_v \in \mathcal{K}$, where $(\mathcal{K}, +)$ is an additive abelian group, and gives a (different) subset of keys to each user
- a *key distribution pattern* is a public v by n incidence matrix, denoted M, which has entries in $\{0, 1\}$
- M specifies which users are to receive which keys: user U_j is given the key k_i if and only if $M[i, j] = 1$
- for a subset $P \subseteq \mathcal{U}$, define

$$keys(P) = \{i : M[i, j] = 1 \text{ for all } U_j \in P\}$$

Key Distribution Patterns (cont.)

- observe that
$$keys(P) = \bigcap_{U_j \in P} keys(U_j)$$
- if $keys(P) \neq \emptyset$, then the *group key* k_P for the set P is defined to be
$$k_P = \sum_{i \in keys(P)} k_i$$
- each member of P can compute k_P (no interaction requred)
- suppose $F \cap P = \emptyset$
- the coalition F can compute k_P if and only if
$$keys(P) \subseteq \bigcup_{U_j \in F} keys(U_j)$$

A Trivial Example

Suppose $n = 4$, $v = 6$, and the matrix M is as follows:

$$M = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

$keys(U_1) = \{1, 2, 3\}$, $keys(U_2) = \{1, 4, 5\}$, and $keys(U_1, U_2) = \{1\}$, so $k_{\{U_1, U_2\}} = k_1$.

A Trivial Generalization

- it is always possible to construct a trivial $\binom{n}{2}$ by n KDP, in which any two users have exactly one common key, and each key is given to exactly two users
- in this KDP, each user must store $n-1$ keys
- the group key for any two users is the unique key that they both possess
- there are $\binom{n}{2}$ group keys
- each group key $k_{\{U_j, U_{j'}\}}$ is secure against the coalition $\mathcal{U} \backslash \{U_j, U_{j'}\}$ having size $n-2$

A More Interesting Example

Suppose $n = 7$, $v = 7$, and the matrix M is as follows:

$$M = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$keys(U_1) = \{1, 4, 6, 7\}$, $keys(U_2) = \{1, 2, 5, 7\}$, and $keys(U_1, U_2) = \{1, 7\}$, so $k_{\{U_1, U_2\}} = k_1 + k_7$.

Example (cont.)

- no other user has both k_1 and k_2, so $k_{\{U_1,U_2\}}$ is secure against any other individual user
- however, U_3 and U_4 (for example) together can compute $k_{\{U_1,U_2\}}$ by pooling their secret information
- in this example, every pair of users can compute a key that is secure against any other individual user
- this scheme enables the construction of $\binom{7}{2} = 21$ group keys for pairs of users

Fiat-Naor KDPs

- let $1 \leq w \leq n$ and define

$$v = \sum_{i=0}^{w} \binom{n}{i}$$

- the *Fiat-Naor w-KDP* is the v by n matrix whose rows are the incidence vectors of all subsets of $\mathcal{U}$ having cardinality at least $n - w$
- there is a group key for any subset $P \subseteq \mathcal{U}$, that is secure against any disjoint coalition F of size at most w
- Proof: $|F| \leq w$, so $|\mathcal{U} \backslash F| \geq n - w$. Hence, there exists a key k_i given to the users in $\mathcal{U} \backslash F$ and to no other user. $P \subseteq (\mathcal{U} \backslash F)$, so all users in P have k_i and no user in F has k_i.

An Example

Suppose $n = 6$ and $w = 1$. The Fiat-Naor 1-KDP has $v = 7$, and the matrix M is as follows:

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$keys(U_1) = \{1,2,3,4,5,6\}$, $keys(U_3) = \{1,2,3,4,6,7\}$, $keys(U_4) = \{1,2,3,5,6,7\}$, and $keys(U_1, U_3, U_4) = \{1,2,3,6\}$, so $k_{\{U_1,U_3,U_4\}} = k_1 + k_2 + k_3 + k_6$. No other single user can compute this key.

Cover-free Families

- a *set system* is a pair $(X, \mathcal{A})$, where X is a finite set of *points* and $\mathcal{A}$ is a set of subsets of X called *blocks*
- denote $X = \{x_1, \ldots, x_v\}$ and denote $\mathcal{A} = \{A_1, \ldots, A_n\}$
- $(X, \mathcal{A})$ is a (t, w)-*cover-free family* provided that, for any two disjoint subsets of blocks $P, F \subseteq \mathcal{A}$, where $|P| = t$ and $|F| = w$, it holds that
$$\bigcap_{A_i \in P} A_i \not\subseteq \bigcup_{A_j \in F} A_j$$
- a (t, w)-cover-free family will be denoted as a (t, w)-CFF(v, n) if $|X| = v$ and $|\mathcal{A}| = n$

Mitchell-Piper KDPs

- the *incidence matrix* of $(X, \mathcal{A})$ is the $v \times n$ matrix $M = (m_{i,j})$ in which
$$m_{i,j} = \begin{cases} 1 & \text{if } x_i \in A_j \\ 0 & \text{otherwise} \end{cases}$$
- a *Mitchell-Piper* (t, w)*-KDP* is a KDP in which there is a key for every group of t users, and each such key is secure against any disjoint coalition of at most w users
- the KDP given by a $v \times n$ matrix M yields a Mitchell-Piper (t, w)-KDP if and only if M is the incidence matrix of a (t, w)-CFF(v, n)
- the blocks of the CFF correspond to the columns of M (i.e., the blocks are $keys(U_1), \ldots, keys(U_n)$)

A $(2,1)$-CFF$(7,7)$

$$
\begin{aligned}
M &= \begin{pmatrix}
1 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 1
\end{pmatrix} \\
X &= \{1, \dots, 7\}, \quad \text{and} \\
\mathcal{A} &= \{\{1,4,6,7\}, \{1,2,5,7\}, \{1,2,3,6\}, \{2,3,4,7\}, \\
& \quad \{1,3,4,5\}, \{2,4,5,6\}, \{3,5,6,7\}\}
\end{aligned}
$$

Non-constructive Existence Results

- given t, w and n, we want to construct (t, w)-CFF(v, n) for v as small as possible
- let M be a v by n matrix, having entries from $\{0, 1\}$, whose columns are labelled $1, \ldots, n$
- let $0 < \rho < 1$, and suppose that every entry of M is (independently) defined to be a "1" with probability ρ
- the probability that the matrix M constructed in this fashion is a (t, w)-CFF(v, n) will be shown to be positive, provided that certain numerical conditions on the parameters are satisfied
- this will prove (non-constructively) that a (t, w)-CFF(v, n) exists for certain values of t, w, v and n

Non-constructive Existence Results (cont.)

- let the matrix M be given
- suppose that $P, F \subseteq \{1, \ldots, n\}$, $|P| = t$, $|F| = w$ and $P \cap F = \emptyset$
- then, a given row i of M satisfies the property (*) provided that the entries in the columns in P are all "1"s and the entries in the columns in F are all "0"s
- define a random variable

$$X(P,F) = \begin{cases} 0 & \text{if there exists a row } i \text{ such that (*) is satisfied} \\ 1 & \text{otherwise} \end{cases}$$

- **First Observation:** if $X(P,F) = 1$, then M is not the incidence matrix of a (t,w)-CFF(v,n)

Non-constructive Existence Results (cont.)

- the probability that (*) is satisfied with respect to a given row is $\rho^t(1-\rho)^w$
- the probability that (*) is not satisfied with respect to all v rows is $(1-\rho^t(1-\rho)^w)^v$
- the expected value of $X(P,F)$ is

$$\begin{aligned}\mathsf{Exp}[X(P,F)] &= \mathsf{Pr}[X(P,F)=0]\times 0+\mathsf{Pr}[X(P,F)=1]\times 1\\ &= \mathsf{Pr}[X(P,F)=1]\\ &= \left(1-\rho^t(1-\rho)^w\right)^v\end{aligned}$$

- in order to minimize $\mathsf{Exp}[X(P,F)]$, we should maximize $\rho^t(1-\rho)^w$
- elementary calculus shows that we should define $\rho = t/(t+w)$

Non-constructive Existence Results (cont.)

- define the random variable

$$X = \sum_{\{(P,F):|P|=t,|F|=w,P\cap F=\emptyset\}} X(P,F)$$

- **Second Observation:** $X = 0$ if and only if M is the incidence matrix of a (t,w)-CFF(v,n)

- it is easy to see that

$$\begin{aligned}
\mathsf{Exp}[X] &= \sum_{\{(P,F):|P|=t,|F|=w,P\cap F=\emptyset\}} \mathsf{Exp}[X(P,F)] \\
&= \binom{n}{t}\binom{n-t}{w}\left(1-\rho^t(1-\rho)^w\right)^v \\
&< n^{t+w}\left(1-\frac{t^t w^w}{(t+w)^{t+w}}\right)^v
\end{aligned}$$

Non-constructive Existence Results (cont.)

- if $\mathsf{Exp}[X] < 1$, then there is a (t,w)-CFF(v,n)
- define
$$p_{t,w} = 1 - \frac{t^t w^w}{(t+w)^{t+w}}$$
- $\mathsf{Exp}[X] < 1$ if
$$\begin{aligned} n^{t+w}(p_{t,w})^v &< 1 \quad \Leftrightarrow \\ (t+w)\log_2 n + v\log_2(p_{t,w}) &< 0 \quad \Leftrightarrow \\ v &> \frac{(t+w)\log_2 n}{-\log_2(p_{t,w})} \end{aligned}$$
- in other words, there exist (t,w)-CFF(v,n) in which v is $O(\log n)$ (for any fixed t and w)

Example

- suppose $t = 2$ and $w = 1$
- then

$$\begin{aligned} \rho &= 2/3 \\ p_{2,1} &= 1 - \frac{2^2 1^1}{3^3} = \frac{23}{27}, \quad \text{and} \\ \frac{2+1}{-\log_2 p_{2,1}} &\approx 12.97 \end{aligned}$$

- for all $n \geq 2$, there exists a $(1,2)$-CFF(v,n) in which $v \leq 13 \log_2 n$