Broadcast Encryption to Arbitrary Subsets of Users

- a TA wants to broadcast an encrypted message to an *arbitrary* subset P of the n users, that is secure against coalitions of size at most w
- we construct BES as follows:
  1. split the message K into shares $s_1, \ldots, s_v$ using an (r, v) threshold scheme (for some positive integer $r \leq v$)
  2. encrypt every share s_i with a key k_i, in such a way that
     (a) every user $U_j \in P$ can compute at least r of the keys $k_1, \ldots, k_v$
     (b) any coalition F, such that $F \cap P = \emptyset$ and $|F| \leq w$, can compute at most $r - 1$ of the keys
- the keys k_i are obtained from key predistribution scheme(s)

Efficient BES

- we construct a collection of v different Fiat-Naor 1-KDPs, each of which is constructed on a certain subset of participants
- a v by n incidence matrix, M, having entries from $\{0, 1\}$, is used to define which users are associated with which schemes
- the v schemes are denoted $\mathcal{F}_1, \ldots, \mathcal{F}_v$
- user U_j is given keys from the KDP $\mathcal{F}_i$ if and only if $M[i, j] = 1$
- for $1 \leq i \leq v$, let

  $$users(i) = \{U_j : M[i, j] = 1\}$$

  and for $1 \leq j \leq n$, let

  $$schemes(j) = \{i : M[i, j] = 1\}$$

- suppose that $|schemes(j)| = r$ for every j, $1 \leq j \leq n$

Encryption Steps

On input K, the TA performs the following operations:

1. the TA uses the share generation algorithm of an (r, v) threshold scheme to construct v shares, $s_1, \ldots, s_v$
2. for $1 \leq i \leq v$, the TA constructs the group key k_i to be the group key for $P \cap users(i)$ in the scheme $\mathcal{F}_i$
3. for $1 \leq i \leq v$, the TA computes $b_i = e_{k_i}(s_i)$
4. the TA broadcasts the vector $b_P = (b_1, \ldots, b_v)$

Step 2: Constructing the Group Keys

- for $1 \leq i \leq v$, the scheme $\mathcal{F}_i$ is a Fiat-Naor 1-KDP defined on the subset $users(i)$
- to set up $\mathcal{F}_i$, the TA distributes keys as follows:
  1. a key ℓ_i is given to every user in $users(i)$
  2. for every $U_j \in users(i)$, a key $\ell_{i,j}$ is given to every user in the set $users(i) \backslash \{U_j\}$
- the group key for the subset $users(i) \cap P$ is defined to be

$$k_i = \ell_i + \sum_{\{j : U_j \in users(i) \backslash P\}} \ell_{i,j}$$

- k_i can be computed (non-interactively) by all members of $users(i) \cap P$
- no individual user not in $users(i) \cap P$ can compute k_i, but a subset of (at least) two users in $users(i) \backslash P$ can compute k_i

Decryption Steps

On input $b_P = (b_1, \ldots, b_v)$, a user $U_j \in P$ performs the following operations:

1. for all $i \in \mathit{schemes}(j)$, U_j constructs the group key k_i for $P \cap \mathit{users}(i)$ in the scheme $\mathcal{F}_i$
2. for all $i \in \mathit{schemes}(j)$, U_j computes $s_i = d_{k_i}(b_i)$
3. U_j uses the share reconstruction algorithm of the (r, v) threshold scheme to compute K from the r shares in the set $\{s_i : i \in \mathit{schemes}(j)\}$

Example of a BES

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

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

$$\begin{aligned} users(1) &= \{U_1, U_2, U_4\} \\ users(2) &= \{U_2, U_3, U_5\} \\ users(3) &= \{U_3, U_4, U_6\} \\ users(4) &= \{U_4, U_5, U_7\} \\ users(5) &= \{U_1, U_5, U_6\} \\ users(6) &= \{U_2, U_6, U_7\} \\ users(7) &= \{U_1, U_3, U_7\} \end{aligned}$$

Note that every user is associated with $r = 3$ schemes.

Example (cont.)

In the set-up phase, a total of nine keys will be given to each user, as indicated below:

U_1	U_2	U_3	U_4	U_5	U_6	U_7
ℓ_1	ℓ_1	ℓ_2	ℓ_1	ℓ_2	ℓ_3	ℓ_4
$\ell_{1,2}$	$\ell_{1,1}$	$\ell_{2,2}$	$\ell_{1,1}$	$\ell_{2,2}$	$\ell_{3,3}$	$\ell_{4,4}$
$\ell_{1,4}$	$\ell_{1,4}$	$\ell_{2,5}$	$\ell_{1,2}$	$\ell_{2,3}$	$\ell_{3,4}$	$\ell_{4,5}$
ℓ_5	ℓ_2	ℓ_3	ℓ_3	ℓ_4	ℓ_5	ℓ_6
$\ell_{5,5}$	$\ell_{2,3}$	$\ell_{3,4}$	$\ell_{3,3}$	$\ell_{4,4}$	$\ell_{5,1}$	$\ell_{6,2}$
$\ell_{5,6}$	$\ell_{2,5}$	$\ell_{3,6}$	$\ell_{3,6}$	$\ell_{4,7}$	$\ell_{5,5}$	$\ell_{6,6}$
ℓ_7	ℓ_6	ℓ_7	ℓ_4	ℓ_5	ℓ_6	ℓ_7
$\ell_{7,3}$	$\ell_{6,6}$	$\ell_{7,1}$	$\ell_{4,5}$	$\ell_{5,1}$	$\ell_{6,2}$	$\ell_{7,1}$
$\ell_{7,7}$	$\ell_{6,7}$	$\ell_{7,7}$	$\ell_{4,7}$	$\ell_{5,6}$	$\ell_{6,7}$	$\ell_{7,3}$

Example (cont.)

- suppose that the TA wants to broadcast a message to the set $P = \{U_1, U_2, U_3\}$
- the following will be the keys used in the seven Fiat-Naor schemes:

i	$users(i) \cap P$	k_i
1	$\{U_1, U_2\}$	$\ell_1 + \ell_{1,4}$
2	$\{U_2, U_3\}$	$\ell_2 + \ell_{2,5}$
3	$\{U_3\}$	$\ell_3 + \ell_{3,4} + \ell_{3,6}$
4	$\emptyset$	$\ell_4 + \ell_{4,4} + \ell_{4,5} + \ell_{4,7}$
5	$\{U_1\}$	$\ell_5 + \ell_{5,5} + \ell_{5,6}$
6	$\{U_2\}$	$\ell_6 + \ell_{6,6} + \ell_{6,7}$
7	$\{U_1, U_3\}$	$\ell_7 + \ell_{7,7}$

Security (Example)

- we can prove that the example BES is secure against coalitions of size $w = 2$
- let $F = \{U_j, U_{j'}\}$ be an arbitrary coalition of size two
- the incidence matrix M has the property that there is only one set $users(i)$ such that $F \subseteq users(i)$
- F can compute only one of the seven group keys
- the threshold $r = 3$ and the coalition can decrypt only one share, so the scheme is secure

Security Properties of Incidence Matrices for BES

- in general, M is required to be a v by n incidence matrix in which there are exactly r “1”s in each column
- let $(\mathcal{U}, \mathcal{A})$ be the set system in which the blocks are formed by the *rows* of M (i.e., the subsets $users(i)$)
- note that we previously considered set systems (namely, cover-free families) associated with the *columns* of KDPs
- there are n points and v blocks in $(\mathcal{U}, \mathcal{A})$
- every point (user) is in exactly r blocks (schemes)
- suppose that every pair of points occur in at most λ blocks
- then a coalition of size w can compute *at most* $\lambda\binom{w}{2}$ group keys
- the BES is secure against coalitions of size w if $r > \lambda\binom{w}{2}$

Security Properties of Incidence Matrices (cont.)

- summarizing, we want to construct an incidence matrix such that the associated set system $(\mathcal{U}, \mathcal{A})$ satisfies the following properties:
  1. $|\mathcal{U}| = n$ (there are n points)
  2. $|\mathcal{A}| = v$ (there are v blocks)
  3. every point occurs in exactly r blocks
  4. every pair of points occurs in at most λ blocks
  5. $r > \lambda\binom{w}{2}$
- then M can be used to construct a BES secure against coalitions of size at most w
- clearly, we want v to be small (given n and w)

A Polynomial-based Construction

- let q be prime and let $d \leq q$
- $v = q^2$ and $n = q^d$
- the columns of M are labelled by d-tuples $(a_0, \ldots, a_{d-1}) \in (\mathbb{Z}_q)^d$ (a d-tuple corresponds to a polynomial in $\mathbb{Z}_q[x]$ having degree at most $d-1$)
- the rows of M are labelled by 2-tuples $(x, y) \in (\mathbb{Z}_q)^2$
- the entries of M are defined as follows:

$$M[(x,y),(a_0,\ldots,a_{d-1})] = 1 \Leftrightarrow \sum_{i=0}^{d-1} a_i x^i \equiv y \pmod{q}$$

- it is clear that $r = q$, because every polynomial takes on a unique y-value, given any x-value

Example

Suppose $q = 3$ and $d = 2$; then $n = v = 9$, and M is as follows:

(x,y)	0	1	2	x	$1+x$	$2+x$	$2x$	$1+2x$	$2+2x$
$(0,0)$	1	0	0	1	0	0	1	0	0
$(0,1)$	0	1	0	0	1	0	0	1	0
$(0,2)$	0	0	1	0	0	1	0	0	1
$(1,0)$	1	0	0	0	0	1	0	1	0
$(1,1)$	0	1	0	1	0	0	0	0	1
$(1,2)$	0	0	1	0	1	0	1	0	0
$(2,0)$	1	0	0	0	1	0	0	0	1
$(2,1)$	0	1	0	0	0	1	1	0	0
$(2,2)$	0	0	1	1	0	0	0	1	0

Computing λ

- suppose we have two columns, $(a_0, \ldots, a_{d-1})$ and $(a'_0, \ldots, a'_{d-1})$
- these define two polynomials, $a(x)$ and $a'(x)$, respectively
- we want to determine an upper bound on

$$|\{(x,y) : a(x) = a'(x) = y\}| = |\{x : a(x) = a'(x)\}|$$

- this quantity is at most $d-1$, because the values at d points determine a *unique* polynomial of degree at most $d-1$
- hence, $\lambda = d-1$
- therefore we have $v = q^2$, $n = q^d$, $r = q$ and $\lambda = d-1$
- the BES is secure against coalitions of size at most w provided that $q > (d-1)\binom{w}{2}$
- if $w = 2$ in the example, then $q = 3 > (d-1)\binom{w}{2} = 1$