Required Properties of Incidence Matrices

- suppose we have 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

Parameters of the Polynomial-based Construction

- let q be prime and let $d < q$
- there exists a matrix M with $v = q^2$, $n = q^d$, $r = q$, and $\lambda = d - 1$
- the resulting BES is secure against coalitions of size at most w provided that $q > (d-1)\binom{w}{2}$, i.e., if

$$d < 1 + \frac{q}{\binom{w}{2}}$$

- note that this condition implies the weaker condition $d < q$

Example

Suppose $q = 3$ and $d = 2$; then $n = v = 9$, $r = 3$ and $\lambda = 1$, 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

Choosing Parameters (Numerical Examples)

- suppose we want to have $w = 3$
- for any prime q, we can take $d < 1 + \frac{q}{3}$
- we get a w-secure BES for $n = q^d$ users, based on $v = q^2$ Fiat-Naor KDPs
- the size of the broadcast is v (elements of $\mathbb{Z}_p$)
- some sample parameters:

q	d	v	n
7	3	49	343
13	5	169	371,293
19	7	361	893,871,739

Choosing Parameters (An Asymptotic Analysis)

- suppose that values for the parameters n and w are given
- define $q \approx w^2 \log_2 n$ and $d \approx \log_2 n$
- $q^d > 2^{\log_2 n} = n$ and $d < q$, so the incidence matrix M exists
- $q = w^2 d > (d-1)\binom{w}{2}$, so the security condition holds
- we obtain a BES secure against coalitions of size w
- the size of the broadcast is $v = q^2 = w^4 (\log_2 n)^2$
- for fixed w, v is $O((\log n)^2)$

Storage Requirements

- consider the set system $(X, \mathcal{A})$ corresponding to an incidence matrix M (points correspond to users, and blocks correspond to Fiat-Naor KDPs)
- if $x \in A$, where $A \in \mathcal{A}$, then the corresponding user must store $|A|$ keys from the Fiat-Naor scheme associated with the block A
- in the polynomial scheme, every point is in $r = q$ blocks, and the blocks have size q^{d-1}
- therefore every user stores $q^d = n$ keys in total

An Efficiency Improvement

- in the BES, recall that each user in P can decrypt r shares, and the coalition F can (collectively) decrypt at most $\lambda\binom{w}{2}$ shares, where $\lambda\binom{w}{2} < r$
- the use of an (r, v) threshold scheme ensures that the secret K cannot be computed, given $r - 1$ shares
- if $\lambda\binom{w}{2} < r - 1$, then the security provided by the threshold scheme is stronger than required
- in this situation, it is possible to replace the threshold scheme by a *ramp scheme*
- we can maintain the same security of the BES, while allowing more information to be broadcast

Ramp Schemes

- let t_{low}, t_{high} and n be non-negative integers, $t_{low} < t_{high} \leq n$
- there is a trusted authority, denoted TA, and n users, denoted $U_1, \ldots, U_n$
- the TA has a secret value $K \in \mathcal{K}$
- the TA uses a *share generation algorithm* to split K into n *shares*, denoted $s_1, \ldots, s_n$
- each share $s_i \in \mathcal{S}$, where $\mathcal{S}$ is a specified finite set
- a (t_{low}, t_{high}, n) *ramp scheme* satisfies the following two properties:
  1. a *reconstruction algorithm* can be used to reconstruct the secret, given any t_{high} of the n shares,
  2. no set of at most t_{low} shares reveals any information as to the value of the secret

Generalized Shamir (Ramp) Scheme

- let $p \geq n+1$ be a prime
- define $t_0 = t_{high} - t_{low}$
- in a threshold scheme, $t_0 = 1$
- let $\mathcal{K} = (\mathbb{Z}_p)^{t_0}$ and let $\mathcal{S} = \mathbb{Z}_p$
- in an initialization phase, $x_1, x_2, \ldots, x_n$ are defined to be n distinct non-zero elements of $\mathbb{Z}_p$
- the TA gives x_i to U_i, for all i, $1 \leq i \leq n$
- the x_i's are public information

Share Generation for the Ramp Scheme

- given a secret $K = (a_0, \ldots, a_{t_0-1}) \in \mathbb{Z}_p$, the share generation algorithm is as follows:

  1. the TA chooses $a_{t_0}, \ldots, a_{t_{high}-1}$ independently and uniformly at random from $\mathbb{Z}_p$
  2. the TA defines

  $$a(x) = \sum_{j=0}^{t_{high}-1} a_j \, x^j$$

     (note that $a(x) \in \mathbb{Z}_p[x]$ is a random polynomial of degree at most $t_{high} - 1$, such that the first t_0 coefficients comprise the secret, K)
  3. for $1 \leq i \leq n$, the TA constructs the share $s_i = a(x_i)$

Reconstruction Algorithm for the Ramp Scheme

- suppose users $U_{i_1}, \ldots, U_{i_{t_{high}}}$ want to determine K
- they know that $s_{i_j} = a(x_{i_j})$, $1 \leq j \leq t_{high}$
- since $a(x)$ is a polynomial of degree at most $t_{high} - 1$, they can determine

$$a(x) = \sum_{j=0}^{t_{high}-1} a_j\, x^j$$

by Lagrange interpolation

- then $K = (a_0, \ldots, a_{t_0-1})$

Security of the Ramp Scheme

- suppose t_{low} users, say $U_{i_1}, \ldots, U_{i_{t_{low}}}$, pool their shares in an attempt to determine some information about K
- let $(a'_0, \ldots, a'_{t_0-1})$ be a guess for the secret
- then there exists a unique polynomial $a'(x)$ of degree at most $t_{high} - 1$ such that
  1. the first t_0 coefficients of $a'(x)$ are $a'_0, \ldots, a'_{t_0-1}$, and
  2. $s_{i_j} = a'(x_{i_j})$, $1 \leq j \leq t_{low}$
- this is because there are are t_{low} remaining coefficients of $a'(x)$, and the value of $a'(x)$ is known at t_{low} points
- therefore no information about K can be computed

Ramp Schemes and BES

- the BES remains secure if a $\left(\lambda\binom{w}{2}, r, v\right)$ ramp scheme is used to construct shares of the secret
- this allows the size of the secret to be increased: $K \in (\mathbb{Z}_p)^{t_0}$, where

$$t_0 = r - \lambda\binom{w}{2}$$

- shares are still elements of $\mathbb{Z}_p$, however
- therefore the *broadcast ratio* (the length of the broadcast divided by the length of the secret) has been decreased by a factor of t_0, from v to v/t_0

Choosing Parameters (An Asymptotic Analysis)

- as before, define $q \approx w^2 \log_2 n$ and $d \approx \log_2 n$ in the polynomial scheme
- we have

$$\begin{aligned} t_0 &= r - \lambda\binom{w}{2} \\ &= q - (d-1)\binom{w}{2} \\ &\approx w^2 \log_2 n - (\log_2 n)\binom{w}{2} \\ &\approx \frac{w^2 \log_2 n}{2} \end{aligned}$$

- the length of the broadcast is $v = q^2 = w^4 (\log_2 n)^2$
- the broadcast ratio is $O(w^2 \log_2 n)$, which is $O(\log n)$ for fixed w