Ideal Ramp Schemes and Related Combinatorial Objects

Douglas R. Stinson

David R. Cheriton School of Computer Science
University of Waterloo

CMS 2017 Winter Meeting
Waterloo, December 8–11, 2017

(t, n)-Threshold Schemes

- We informally define a (t, n)-**threshold scheme**
- Let t and n be positive integers, $t \leq n$.
- A secret value K is "split" into n **shares**, denoted $s_1, \ldots, s_n$.
- The following two properties should hold:
  1. The secret can be reconstructed, given **any t of the n shares**.
  2. **No $t - 1$ shares** reveal any information as to the value of the secret.
- Threshold schemes were invented independently by Blakley and Shamir in 1979.
- Shamir's threshold scheme is based on **polynomial interpolation** over $\mathbb{Z}_p$, where $p \geq n + 1$ is prime.

Shamir Threshold Scheme

- The set of possible secrets (and shares) is $\mathbb{Z}_p$.
- $x_1, x_2, \ldots, x_n$ are defined to be n **public, distinct, non-zero** elements of $\mathbb{Z}_p$.
- For a given secret $K \in \mathbb{Z}_p$, shares are created as follows:
    1. Let $a(x) \in \mathbb{Z}_p[x]$ be a **random polynomial of degree at most $t-1$**, such that the constant term is the secret, K.
    2. For $1 \leq i \leq n$, the share $\boldsymbol{s_i = a(x_i)}$ (so the shares are evaluations of the polynomial $a(x)$ at n non-zero points).
- Suppose we have t shares $s_{i_j} = a(x_{i_j})$, $1 \leq j \leq t$.
- Since $a(x)$ is a polynomial of degree at most $t-1$, we can determine $a(x)$ by **Lagrange interpolation**; then $\boldsymbol{K = a(0)}$.

Ideal Threshold Schemes

- Suppose $\mathcal{K}$ is the set of **possible secrets** and $\mathcal{X}$ is the set of **possible shares** for any (t, n) threshold scheme
- Then $|\mathcal{K}| \leq |\mathcal{X}|$.
- If equality holds, then the threshold scheme is **ideal**.
- Clearly the Shamir scheme is ideal.
- We observe that the Shamir scheme is basically a **Reed-Solomon code** in disguise.
- **Reed-Solomon codes** are examples of **maximum distance separable codes**, which are equivalent to **orthogonal arrays with index 1**.

Ideal Threshold Schemes and Orthogonal Arrays

An **orthogonal array with index 1**, denoted $\mathrm{OA}(t,k,v)$, is a v^t by k array A defined on an alphabet $\mathcal{X}$ of cardinality v, such that **any t of the k columns** of A contain all possible k-tuples from $\mathcal{X}^t$ exactly once.

Theorem 1 (Keith Martin, 1991)

There exists an ideal (t,k)-threshold scheme with v possible shares (and v possible secrets) **if and only if** *there exists an* $\mathrm{OA}(t,k+1,v)$.

Proof Ideas

- Suppose A is an $\mathrm{OA}(t, k+1, v)$.
- The **first k columns** are associated with the k **players** and the **last column** corresponds to the **secret** .
- Each row of A gives rise to a **distribution rule** which assigns shares corresponding to a particular value of the secret to the k players.
- The result is easily seen to be an ideal threshold scheme.

Proof Ideas

- Suppose A is an $\mathrm{OA}(t, k+1, v)$.
- The **first k columns** are associated with the k **players** and the **last column** corresponds to the **secret**.
- Each row of A gives rise to a **distribution rule** which assigns shares corresponding to a particular value of the secret to the k players.
- The result is easily seen to be an ideal threshold scheme.

- **Conversely**, suppose we start with a (t, k)-threshold scheme with shares from an alphabet of size v.
- WLOG, suppose $\mathcal{K} = \mathcal{X}$.
- Write out all the possible distribution rules (which can be regarded as $(k+1)$-tuples) as rows of an array.
- **With a bit of work,** the resulting array can be shown to be an $\mathrm{OA}(t, k+1, v)$.

Example

We present an $\mathrm{OA}(2, 4, 3)$, which gives rise to a $(2, 3)$-threshold scheme with shares and secrets in $\mathbb{Z}_3$. There are nine distribution rules, three for each possible value of the secret.

s_1	s_2	s_3	K
0	0	0	0
1	1	1	0
2	2	2	0
0	1	2	1
1	2	0	1
2	0	1	1
0	2	1	2
1	0	2	2
2	1	0	2

(Ideal) Ramp Schemes

- An (s, t, n)-**ramp scheme** is a generalization of a threshold scheme in which there are **two thresholds** s and t, where $s < t$.
    1. The secret can be reconstructed given **any t of the n shares**.
    2. **No s shares** reveal any information as to the value of the secret.
- If $\boldsymbol{s = t - 1}$, then we have a threshold scheme.
- Ramp schemes **weaken** the security requirement, but permit **larger secrets** to be shared for a given share size.
- If $\mathcal{K}$ is the set of possible secrets and $\mathcal{X}$ is the set of possible shares for any (s, t, n)-ramp scheme, then $|\boldsymbol{\mathcal{K}}| \leq |\boldsymbol{\mathcal{X}}|^{\boldsymbol{t-s}}$.
- If equality holds, then the ramp scheme is **ideal**.

Orthogonal Arrays and Ideal Ramp Schemes

- It is easy to construct an ideal ramp scheme from an orthogonal array.
- Suppose A is an $\mathrm{OA}(t, k+t-s, v)$.
- The **first k columns** are associated with the k **players** and the **last $t-s$ columns** correspond to the **secret**.
- **Main question:** Is the converse true?
- Jackson and Martin (1996) showed that a **strong** ideal ramp scheme implies the existence of an $\mathrm{OA}(t, k+t-s, v)$.
- However, the additional properties that define a strong ideal ramp scheme are rather technical, and not particularly natural.
- We give a new, "tight" characterization of "general" ideal ramp schemes, and we construct examples of **ideal ramp schemes that are not strong**, answering a question from Jackson and Martin (1996).

Augmented Orthogonal Arrays

Definition 2

An **augmented orthogonal array**, denoted $\mathrm{AOA}(s,t,k,v)$, is a v^t by $k+t-s$ array A that satisfies the following properties:

1. the **first k columns** of A form an orthogonal array $\mathrm{OA}(t,k,v)$ on a symbol set $\mathcal{X}$ of size v
2. the **last column** of A contains symbols from a set $\mathcal{Y}$ of size v^{t-s}
3. **any s of the first k columns of A, together with the last column of A**, contain all possible $(s+1)$-tuples from $\mathcal{X}^s \times Y$ exactly once.

Example

- We give an example of an $\mathrm{AOA}(1,3,3,3)$.
- Take $\boldsymbol{\mathcal{X}} = \mathbb{Z}_{\mathbf{3}}$ and $\boldsymbol{\mathcal{Y}} = \mathbb{Z}_{\mathbf{3}} \times \mathbb{Z}_{\mathbf{3}}$.
- The AOA is generated by the following matrix:

$$M = \left(\begin{array}{ccc|c} 1 & 0 & 0 & (1,1) \\ 0 & 1 & 0 & (1,0) \\ 0 & 0 & 1 & (0,1) \end{array}\right).$$

- The first three columns generate all 27 triples over $\mathbb{Z}_3$.
- Any one of the first three columns, together with the last column, generate all 27 ordered pairs from $\mathbb{Z}_3 \times (\mathbb{Z}_3 \times \mathbb{Z}_3)$.

Main Equivalence Theorem

Theorem 3

There exists an ideal (s, t, n)-ramp scheme defined over a set of v shares **if and only if** *there exists an* $\mathrm{AOA}(s, t, n, v)$.

Theorem 4

If *there exists an* $\mathrm{OA}(t, k + t - s, v)$, **then** *there exists an* $\mathrm{AOA}(s, t, k, v)$.

Proof.

Merge the last $t - s$ columns of an $\mathrm{OA}(t, k + t - s, v)$ to form a single column whose entries are $(t - s)$-tuples of symbols. $\square$

Ramp Schemes and (Augmented) Orthogonal Arrays

Summarizing, we have the following equivalences/implications:

$$\begin{array}{ccc}
\textbf{strong ideal } (s,t,n)\textbf{-ramp scheme} & & \\
\textbf{defined over a set of } v \textbf{ shares} & \Longleftrightarrow & \mathbf{OA}(t, n+t-s, v) \\
\Big\Downarrow & & \Big\Downarrow \\
\textbf{ideal } (s,t,n)\textbf{-ramp scheme} & & \\
\textbf{defined over a set of } v \textbf{ shares} & \Longleftrightarrow & \mathbf{AOA}(s,t,n,v)
\end{array}$$

OAs vs AOAs

- The **converse** of Theorem 4 is not always true.
- Consider the $\mathrm{AOA}(1, 3, 3, 3)$ presented earlier.
- Suppose we split the last column into two columns of elements from $\mathbb{Z}_3$.
- We would get an array generated by the following matrix:

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

- The **fourth column** of M is the **sum of the first two columns** of M, so these three corresponding columns generated by M will not contain all possible 3-tuples.
- In fact, there does not exist **any** $\mathrm{OA}(3, 5, 3)$, because the parameters violate the classical **Bush bound** .
- So we get an example of parameters for which an **ideal ramp scheme exists** but a **strong ideal ramp scheme does not exist** .

OAs vs AOAs: Two General Results

Theorem 5

Suppose q is an odd prime power and $3 \leq t \leq q$. Then **there exists** *an* $\mathrm{AOA}(1, t, q, q)$ *but* **there does not exist** *an* $\mathrm{OA}(t, q + t - 1, q)$.

Theorem 6

Suppose q is a prime power and $s \leq q - 1$. Then **there exists** *an* $\mathrm{AOA}(s, q + 1, q + 1, q)$ *but* **there does not exist** *an* $\mathrm{OA}(q + 1, 2(q + 1) - s, q)$.

Example

We take $q = 3$, $s = 2$ in Theorem 6. Let

$$N = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{pmatrix}.$$

This array generates a (linear) $\mathrm{OA}(2, 4, 3)$.

Then the following array generates a (linear) $\mathrm{AOA}(2, 4, 4, 3)$:

$$M = \left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & (1,0) \\ 0 & 1 & 0 & 0 & (1,1) \\ 0 & 0 & 1 & 0 & (1,2) \\ 0 & 0 & 0 & 1 & (0,1) \end{array}\right).$$

However, by the Bush bound, there is no $\mathrm{OA}(4, 6, 3)$.

References

[1] W.A. Jackson and K.M. Martin. **A combinatorial interpretation of ramp schemes.** *Australasian Journal of Combinatorics* **14** (1996), 51–60.

[2] K.M. Martin. **Discrete Structures in the Theory of Secret Sharing** . PhD Thesis, University of London, 1991.

[3] A. Shamir. **How to share a secret.** *Communications of the ACM* **22** (1979), 612–613.

[4] D.R. Stinson. **Optimal ramp schemes and related combinatorial objects.** ArXiv report 1705.06247, May 17, 2017.

Thank You For Your Attention!