SECRET SHARING SCHEMES

- A Secret sharing scheme enables a dealer D to split a secret S among a set \{P_1, \cdots, P_n\} of players, each of whom receives a share B_i.
- In \((k,n)\) threshold schemes, the shares of at least \(k\) players out of \(n\) are required to recover the secret [3]
- Goal: Implement \((2,n)\) schemes using cellular automata (CA) and Latin squares

CELLULAR AUTOMATA (CA)

- A cellular automaton is composed of a lattice of cells, each of which updates its binary state according to a local rule \(f\)

```
\ldots 0 1 1 0 0 \ldots
```

local rule \(\downarrow f\): \(x_1 \oplus x_2 \oplus x_3\)

- The CA evolution is given by the application of the global rule \(F\) on the central cells

```
1 1 0 0 0 0 1 0 1
```

\(\downarrow \text{Global rule } F\)

LATIN SQUARES

- In a Latin square of side \(N\), each number from 1 to \(N\) is contained exactly once in each row and in each column

```
1 2 3 4
4 2 1 3
2 4 3 1
3 1 2 4
```

- Two Latin squares are orthogonal if in their superposition each pair of numbers from 1 to \(N\) occurs exactly once

```
1 3 4 2
4 2 1 3
2 4 3 1
3 1 2 4
```

- Remark: A set of \(n\) mutually orthogonal Latin squares (MOLS) is equivalent to a \((2,n)\) threshold scheme

LATIN SQUARES FROM BIPERMUTIVE CA

- A CA with bipermutive rule of radius \(r\) generates a Latin square of side \(2^r\)

```
\begin{array}{|c|c|}
\hline
\multicolumn{2}{|c|}{L(x,y)} \\
\hline
\end{array}
```

- Example: radius \(r = 1, N = 4\), \(f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3\)

```
\begin{array}{|c|c|c|c|}
\hline
1 & 2 & 3 & 4 \\
2 & 3 & 4 & 1 \\
3 & 4 & 1 & 2 \\
4 & 1 & 2 & 3 \\
\hline
\end{array}
```

Encoding: 00 \(\mapsto\) 1, 10 \(\mapsto\) 2, 01 \(\mapsto\) 3, 11 \(\mapsto\) 4

MAIN RESULT AND FUTURE DEVELOPMENTS

- Two linear CA generate orthogonal Latin squares if and only if their associated polynomials are relatively prime
- Example: Rule 150 \(\mapsto\) 1 + \(X + X^2\), Rule 90 \(\mapsto\) 1 + \(X^2\)

```
\begin{array}{|c|c|c|c|}
\hline
1 & 4 & 3 & 2 \\
2 & 3 & 4 & 1 \\
3 & 4 & 1 & 2 \\
4 & 1 & 2 & 3 \\
\hline
\end{array}
```

Rule 150

```
\begin{array}{|c|c|c|c|}
\hline
1 & 2 & 3 & 4 \\
2 & 1 & 4 & 3 \\
3 & 4 & 1 & 2 \\
4 & 3 & 2 & 1 \\
\hline
\end{array}
```

Rule 90

```
\begin{array}{|c|c|c|c|}
\hline
1 & 4 & 3 & 2 \\
2 & 3 & 4 & 1 \\
3 & 4 & 1 & 2 \\
4 & 1 & 2 & 3 \\
\hline
\end{array}
```

Superposition

- Future development: Count the number of coprime pairs of polynomials with nonzero constant term and degree \(n\)
- This number is related to OEIS sequence A002450 [2], \(a(n) = 0, 1, 5, 21, 85, \ldots\) for \(n = 1, 2, 3, 4, 5, \ldots\)

REFERENCES

[2] The Online Encyclopedia of Integer Sequences (OEIS), Sequence A002450. URL: https://oeis.org/A002450