Secret Sharing
A Cryptographic Application of Finite Geometry

Kiah H.M. ¹ and James Quah²

Department of Mathematics, Faculty of Science, National University of Singapore
10 Kent Ridge Road, Singapore 117546

ABSTRACT

A secret sharing scheme is a protocol to share a secret $X$ among a set of participants in such a way that: participants in specified subsets are able to recover $X$ by pooling their information; while participants in the other subsets are unable recover any information on $X$. In 1979, Blakley constructed secret sharing schemes using structures from finite geometry. Following him, other mathematicians modified his scheme to include other features. In particular, we look at the compartment schemes, multi-level schemes, schemes with vetoing capabilities and schemes capable of identifying cheaters.

FINITE PROJECTIVE GEOMETRY

An incidence structure, or geometry, comprises a set of points, a set of lines and a relation, incidence, between them. A finite geometry would comprise a set of finite points and a set of finite lines.

A projective space is a geometry of a set of points and a set of lines, with an incidence relation, such that the following holds:

1. Any two points lie exactly on a line.
2. (Veblen-Young axiom) Let $A$, $B$, $C$, $D$ be four distinct points such that no three are collinear. If the lines $AB$ and $CD$ intersect each other, then the lines $AD$ and $BC$ also intersect each other.
3. Any line has at least three points.
4. There are at least two lines.

---

¹ Student
² Supervisor
THRESHOLD SCHEMES

A \textit{t}-\textit{threshold scheme} is a secret sharing scheme with the following properties:

- At least \( t \) participants are required to reconstruct the secret.
- Any constellation of \( t - 1 \) or fewer participants is unable to construct the secret.

Blakley constructed a scheme satisfying the above conditions using the following algorithm:

1. In \( \text{PG}(t, q) \), randomly select a point \( X \) to be the secret.
2. Randomly select a public line \( g \) containing \( X \). We call \( g \) a public line, as the dealer will announce to all participants that point \( X \) is on \( g \).
3. Select a hyperplane \( H \) such that \( H \) intersects \( g \) at \( X \).
4. Choose \( n \) points \( X_1, X_2, \ldots, X_n \) in \( H \) such that the points \( X, X_1, X_2, \ldots, X_n \) are in general position in \( H \).
5. To reconstruct the secret, calculate the span \( U \) of the shares and find the intersection of \( U \) and \( g \) and check the intersection is \( X \).

Blakley’s construction also has the characteristic of being \textbf{perfect}: \textit{for any illegal set of participants, the probability of them being able to randomly guess the secret correctly is a constant value.}

MODIFICATIONS OF BLAKLEY’S SCHEME

The threshold scheme is a very simple form of a secret sharing scheme. Certainly, it is not very realistic in the physical world. Blakley’s scheme can be modified into secret sharing schemes which have interesting properties:

- \textbf{Compartment schemes} – the participants are divided into subgroups called \textit{compartments}. To obtain the secret, a quorum of compartments is required. But for a compartment to participate in the quorum, another quorum of shares is required.

- \textbf{Multi-level schemes} – the participants are divided into two ordered levels. To reconstruct the secret, a smaller quorum is required in the higher level. Also, each member of a ‘higher’ level can replace a member of the ‘lower’ level.
• **Schemes with veto-capabilities** – to allow a qualified minority of participants to say ‘no’ and hence disallowing the quorum to obtain the secret.

• **Schemes capable of identifying cheaters** – to allow individual participants to verify that the other participants are honest and are giving their true shares.

**ASSUMPTIONS**

In the report, we have assumed the following:

• **Honest dealer** - The dealer is one who constructs the scheme and distributes the shares to the participants. The dealer is **honest** if he distributes the shares in such a way that the secret can be reconstructed.

• **Machine is trustworthy** - The machine is one which performs the action of combining of the shares and reconstructing the secret. We have also assumed that our machine not only sees all the inputted shares, but also it keeps them secret to the participants.

**ADVANTAGES OF CONSTRUCTING SECRET SHARING SCHEMES OVER FINITE GEOMETRIES**

• **Provable security** - Unlike many public-key cryptosystems, secret sharing schemes do not rely on known NP-complete problems. Hence, while improvements in computer technology by intruders can affect the relative security of public-key systems, they have no effect on Blakley’s scheme. It can be shown, the probability of deception is computable and we can fix the security level at any arbitrary level.

• **Comfortable Participant Management** - Indeed, one can add users to a secret sharing scheme without altering the shares of the other participants. This is provided that the projective space is big enough to accommodate the points. In a projective space of order \( q \), we can have at least \( q + 1 \) points to be in general position in this space. That is, we can have at least \( q +1 \) shares. Hence, a large \( q \) will solve our problem.
REFERENCES


Gustavus J. Simmons, *Prepositioned shared secret and/or shared control schemes*, Eurocrypt 89

A. Beutelspacher, *How to say ‘No’*, Eurocrypt 89