Geometrical contributions to secret sharing theory

Wen-Ai Jackson[1], Keith M. Martin[2*] and Christine M. O'Keefe[1†]

[1]Department of Pure Mathematics
University of Adelaide
Adelaide 5005
Australia

[2]Katholieke Universiteit Leuven
Dept. Elektrotechniek - ESAT
Kardinaal Mercierlaan 94
B-3001 Heverlee
Belgium

Abstract

Finite geometry has found applications in many different fields and practical environments. We consider one such application, to the theory of secret sharing, where finite geometry has proved to be very useful, both as a modelling tool and as a means to establish interesting results. A secret sharing scheme is a means by which some secret data can be shared among a group of entities in such a way that only certain subsets of the entities can jointly compute the secret. Secret sharing schemes are useful for information security protocols, where they can be used to jointly protect cryptographic keys or provide a means of access control. We review the contribution of finite geometry to secret sharing theory, highlighting results and techniques where the use of finite geometry has been of particular significance.

1 Introduction

Finite geometry has been shown to have applications in many different areas. Most recently a number of applications have been found in topics related to information security. This is a subject of great current interest as electronic communication is becoming increasingly important in almost all aspects of life, from personal computing to international commerce. In this context, *information security* includes the study of protocols and procedures for ensuring confidentiality and integrity of communicated data, the main tool for the former being *cryptography* [12, 17]. Finite geometry has played a fundamental role in developing the theory of several information security topics, notably *message authentication*, *key distribution* and *secret sharing*. It has had a particularly important role to play in the latter of these topics and it is this contribution that we hope to outline in this paper.

The aims of this paper are twofold. The first aim is simply to introduce the problems of secret sharing and describe them in a geometrical context. The second aim is to illustrate the significant contribution finite geometry has made to the theory of secret sharing. We pursue these two aims throughout the text.

The paper is arranged as follows. In Section 2 we introduce the terminology and basic concepts required to discuss secret sharing. We also briefly identify a number of applications. In Section 3 we review geometric

*This work was supported by the European Commission under ACTS project AC095 (ASPeCT)
†This work was supported by the Australian Research Council

constructions of secret sharing schemes. The basic secret sharing problem and the related contribution of finite geometry is presented in Section 4. The influence of geometry in the classification of special types of secret sharing scheme is discussed in Section 5 and we describe geometrical roles in some extensions of basic secret sharing in Section 6. Lastly we make some comments as to why finite geometry has proved such a useful tool for developing secret sharing theory.

2 Secret sharing basics

A *secret sharing scheme* is a protocol by which means of which a *secret* can be protected among a group of *participants* in such a way that only certain sets of participants can compute the secret. Each participant is issued with a *share* of the secret by a *dealer* (some trusted party). The *access structure* of the secret sharing scheme specifies which sets of participants can jointly compute the secret from their shares. In this paper all access structures Γ are *monotone* (if $A \in \Gamma$ and $A \subseteq A'$ then $A' \in \Gamma$). A (monotone) access structure is thus uniquely determined by its *minimal* sets (A is minimal in Γ if it does not strictly contain any set in Γ). The most well-known access structures are the (k,n)-*threshold* access structures, which consist of all subsets of an n-participant set of at least size k.

Informally we say that a secret sharing scheme is *perfect* if the joint shares of a set of participants not belonging to the access structure (an *unauthorised* set) do not give away any information about the secret. This idea can be formalised in information theoretic or combinatorial terms (see for example [16]).

Secret sharing has many potential applications within information security. These all involve situations where one entity is not trusted sufficiently with a secret and the trust is thus spread across a number of different entities, those subsets in the access structure being jointly trusted with the secret. This is relevant to problems such as cryptographic key protection (for example a top level *master key* is often initialised manually and secret sharing can be used to avoid having to trust just one person with knowledge of the key), access control (a simple but rather crucial example is the U.S. dual access control over nuclear weapons) and trust delegation (recent proposals for cryptographic systems permitting *key recovery* [11] allow law enforcement agents to obtain cryptographic keys from registered authorities in order to legally intercept private communications - use of secret sharing enhances user privacy by only permitting interception to take place after a delegated group of trusted authorities have approve the warrant).

We conclude this section with a useful notational representation [1] of an access structure. Let Γ be an access structure defined on participant set $\mathcal{P}$ with minimal sets $\{C_1, \ldots, C_n\}$, where each $C_i \subseteq \mathcal{P}$. We can associate Γ with the logical expression $\Gamma = C_1 + \cdots + C_n$, where $+$ represents logical *and* and juxtaposition represents logical *or*. Let $A \subseteq \mathcal{P}$. It follows that $A \in \Gamma$ if and only if the logical expression Γ is *true* when the boolean variables corresponding to A are all set to *true*. This association simply gives us a useful way of describing access structures, where the logical form just described corresponds to the *disjunctive normal form*. By this association we can represent the access structure defined on $\mathcal{P} = \{a, b, c, d\}$ with minimal sets $\{a, b, c\}$, $\{c, d\}$ by $\Gamma = abc + cd$, or equivalently as $\Gamma = (ab + d)c$.

3 Geometric schemes

***This section to contain a review of secret sharing schemes constructed using finite geometry. Should discuss early work of Blakley, Beutelspacher and Simmons. Should define a geometric scheme in our terms and should include the result that there exists a geometric scheme for every access structure - in fact I suggest that the algorithm is provided.*

3.1 The basic geometric model

[insert definition and basic examples]

Note that secret sharing schemes can be defined in more general terms using combinatorial language [] or information theory []. To see that geometric schemes are compatible with these models, see for instance [].

[here? Note that the secret sharing schemes we discuss in this paper are *unconditionally secure*. This means that...]

3.2 A short history

Secret sharing schemes with threshold access structures (*threshold schemes*) were first described independently by Shamir [13] and Blakley [6] in 1979. Both of these schemes can be interpreted as geometric schemes.

Example 1 *(Shamir)*

Example 2 *(Blakley)*

In 1986 Beutelspacher and Vedder [4] gave a number of related constructions for threshold schemes in projective and affine geometries. Each of these constructions is a variant of Example ? These examples were further discussed in [2, 3].

In 1988 Simmons presented a paper [14] (published 1990) which was influential not just because it was the first paper to use the model for geometric schemes discussed here, but also because it was a seminal work on secret sharing in general. In a series of papers [**?**, **?**, **?**] two geometric secret sharing models were presented. [Insert text]

Also in 1989, Brickell [8] discussed constructions for ideal secret sharing schemes. The model used for these schemes was described in terms of vector spaces, and thus was in fact simply a different manifestation of geometric schemes. [Insert text] Note that in particular [14] and [8] proposed geometric constructions for secret sharing schemes with *multilevel* access structures (see also [5]).

In 1991 it was shown by Simmons et al [**?**] that a geometric scheme could be constructed for any monotone access structure and an algorithm based on manipulation of logical expressions was provided [see next subsection].

Since 1991, the model for geometric schemes has been used to prove significant results concerning secret sharing [,] and has been extended in several different ways [,]. We discuss many of these results in this paper. Note also that since the original models of [14] and [8], a number of other models have been proposed in the literature that are equivalent to geometric schemes. [insert text on Bertilsson and Blak+Kabat]. Another version of this model was proposed in 199? by van Dijk [10]. [insert text]. Geometric schemes appear to have been reinvented again by Wu and He [18] in 1995. These later repetitions may partly be due to a lack of familiarity with finite geometry and the varied technical backgrounds of other researchers in the field.

3.3 Existence of geometric schemes

We end this section by providing the construction of [15] for the existence of a geometric scheme for any monotone access structure Γ. [insert construction]

4 The basic secret sharing problem

***This section describes the "basic secret sharing problem" - that of finding schemes with small shares, and of finding optimal rates. In particular*

- *motivate problem, define (geometrically) information rates and randomness coefficient*
- *ad hoc constructions*
- *discuss the duality result*
- *discuss decompositions - perhaps one example, described geometrically (may need restrictions and contractions also)*
- *brief discussion of algorithm(s)*
- *brief summary of some known results*

4.1 Efficiency of geometric schemes

[insert text from old section 2.2 - note that the result about shares being larger than secret will probably have to be quoted]

In the remainder of this section we consider various techniques for finding geometric schemes that perform well against the measures just suggested. Note that the concept of *performing well* is not always clearly defined. In order to gauge how efficient a given geometric scheme is, an upper bound on the measure being used must first be determined. Considerable work has gone into trying to find upper bounds for the measures defined above for certain families of access structures [, , ,]. Such techniques normally use information theoretic arguments, although in some cases combinatorial techniques can also be applied[**?**].

4.2 Ad hoc constructions

[insert text]

4.3 New geometric schemes from old

[insert text from section 4 - except for dual]

4.4 Decomposition constructions

[insert text - include an example]

4.5 Duality of geometric schemes

4.6 Algorithmic approaches

[insert text - but perhaps a strict subset of what is currently in 3.4]

4.7 Summary of known results

[insert text - something based on current 3.5]

5 Classification of secret sharing schemes

***This section to deal with classification of secret sharing schemes - really only two topics worth mentioning. Classification of ideal threshold schemes and classification of ideal schemes and access structures. Probably a fairly short section. Perhaps open problems in this area could be identified..?*

Having defined a series of measures to quantify efficiency of geometric schemes, the natural question of classifying certain (optimal) cases of these measures presents itself. Such classifications can take two different forms, namely:

- classification of access structures which have certain optimal efficiency rates;
- classification of (geometric) schemes which have certain optimal efficiency rates.

The most obvious case of interest is that of ideal geometric schemes. We include two classifications that are relevant, one in each of the above categories.

5.1 Classification of access structures realisable by ideal geometric schemes

[insert result - some stuff in 2.4] [mention more general open problems - cite Delft paper?]

5.2 Classification of ideal geometric threshold schemes

[insert result]

6 Extended capabilities and extensions

***This section to explore some extended capabilities and extensions of basic secret sharing that have had geometric input. Not sure which ones to mention yet. Possibly..*

- *mulitsecret sharing*
- *cheaters*
- *mtafree*
- *schemes that need linearity*
- *???*

7 Concluding remarks

***This section to contain a small philosophical rave on what properties of geometry make it an attractive modelling tool and why secret sharing problems are often particularly suited to geometric interpretation*

It is hoped that the two aims of this paper have now been achieved: most importantly the second aim, of highlighting the contribution that finite geometry has made to the theory of secret sharing. We conclude by making a few suggestions as to why this has proved to be the case.

The first remark is that the requirements for the construction of a secret sharing scheme, particularly one with a complex access structure, clearly suggest the need to study discrete objects with a rich internal structure. In order to be able to meet the specification of any monotone access structure, this structure needs to be both flexible and intricate. It is not such a surprise then that secret sharing schemes can be modelled using finite geometry. But why is it that finite geometry not only seems to be able to provide examples, but also provides desirable examples, that is ones with attractive properties and parameters?

There are several possible answers to this last question. Firstly, the core of the basic secret sharing problem essentially consists of two classical combinatorial problems: determining bounds on the parameters of a discrete object, then searching for optimal constructions. This thus partially explains why at least some answers to the basic secret sharing questions have arisen from the theory of finite geometry. A further advantage is the fact that geometry is an area where people have studied building constructions and classifications over an extensive time period, and much useful theory is already in place.

While clearly of theoretical interest, a last question to ask is how much practical interest there is in the study of secret sharing, and in particular geometric schemes. The answer is a great deal, but this is qualified by noting that to date this interest is largely in threshold schemes. A threshold access structure is the most straightforward to demand, and perhaps thge easiest for potential users to accept among all types of monotone access structure. Threshold schemes that are optimal under all proposed measures are easily constructed [13] and have been known of since 1979. The interesting point to note is that the attractive properties of these threshold schemes, such as the efficiency with which they can be implemented and their linearity (useful for some extended capabilities), carry over into all geometric schemes and so it would seem likely that if more complex access structures become more in demand then, as first suggested by Gus Simmons in 1988 [14], it will be geometric schemes that may be considered as the solutions of choice.

References

[1] J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. *Adv. in Cryptology - CRYPTO'88, Lecture Notes in Comput. Sci.*, 403:27–35, 1990.

[2] A. Beutelspacher. Enciphered geometry: some applications of geometry to cryptography. *Annals Discr. Math.*, 37:59–68, 1988.

[3] A. Beutelspacher. Applications of finite geometry to cryptography. *Geometries, Codes and Cryptography*, CISM Courses and Lecture Notes 313:161–186, Springer-Verlag, 1990.

[4] A. Beutelspacher and K. Vedder. Geometric structures as threshold schemes. *Cryptography and Coding*, 255–268, H.J. Beker and F.C. Piper eds., Oxford University Press, 1989.

[5] A. Beutelspacher and F. Wettl. On 2-level secret sharing. *Des. Codes Cryptogr.*, 3:127–134, 1993.

[6] G.R. Blakley. Safeguarding cryptographic keys. *Proceedings of AFIPS 1979 National Computer Conference*, 48:313–317, 1979.

blakleykabat G.R. Blakley and G.A. Kabatianskii. Linear algebra apparoach to secret sharing schemes. *Error Control, Cryptography and Speech Compression - Lecture Notes in Comput. Sci.*, 829:33–40, 1994.

[7] C. Blundo, A. Giorgio Gaggia and D.R. Stinson. On the dealer's randomness required in secret sharing schemes. *Des. Codes Cryptogr.*, 11:107–122, 1997.

[8] E.F. Brickell. Some ideal secret sharing schemes. *J. Combin. Math. Combin. Comput.*, 9:105–113, 1989.

[9] E.F. Brickell and D.R. Stinson. The detection of cheaters in threshold schemes. *SIAM J. of Disc. Math.*, 4:502–510, 1991.

[10] M. van Dijk. A linear construction for perfect secret sharing schemes. *Adv. in Cryptology - EUROCRYPT '94, Lecture Notes in Comput. Sci.*, 950:23–34, 1995.

[11] EES. A proposed federal information processing standard for an escrowed encryption standard. *U.S. federal register*, July 30, 1993.

[12] A. Menezes, P. van Oorschot and S. Vanstone. *Handbook of Applied Cryptography.* CRC Press, Boca Raton (1996).

[13] A. Shamir. How to share a secret. *Comm. ACM*, 22(11):612–613, 1979.

[14] G.J. Simmons. How to (really) share a secret. *Adv. in Cryptology - CRYPTO '88, Lecture Notes in Comput. Sci.*, 403:390–448, 1990.

[15] G.J. Simmons, W.-A. Jackson and K. Martin. The geometry of shared secret schemes. *Bull. Inst. Combin. Appl.*, 1:71–88, 1991.

[16] D. R. Stinson. An explication of secret sharing schemes. *Des. Codes Cryptogr.*, 2:357–390 (1992).

[17] D.R. Stinson. *Cryptography: theory and practice.* CRC Press, Boca Raton (1995).

[18] T.-C. Wu and W.-H. He. A geometric approach for sharing secrets. *Computers and Security*, 14:135–146, 1995.