SOME NEW CLASSES OF GEOMETRIC THRESHOLD SCHEMES

Marijke De Soete[1] and Klaus Vedder[2]

[1]Seminar of Geometry and Combinatorics
State University of Ghent
Krijgslaan 281
B-9000 Ghent, Belgium

[2]GAO
Gesellschaft für Automation
und Organisation mbH
Euckenstraße 12
D-8000 München 70, West Germany

Abstract We construct and discuss new infinite classes of t-threshold schemes with $t = 2$ and 3 which are based on generalized quadrangles. The paper also contains threshold schemes which deal with the case where the group of trustees is made up of mutually distrusting parties.

1 INTRODUCTION

Any scheme which is to protect information has to be designed with the following three main points in mind: possible loss or destruction of the information or parts thereof, attack from inside or outside to obtain or destroy the information and efficiency.

One obvious way to guard the information against loss or destruction is to make multiple copies of it and distribute them amongst trustworthy parties. This has two obvious drawbacks. Too few copies might cause the loss of the information while too many copies could lead to the information falling into wrong hands. Moreover, each trusted party is in the

C.G. Guenther (Ed.): Advances in Cryptology - EUROCRYPT '88, LNCS 330, pp. 389-401, 1988.

possession of all of the information.

In 1979 Blakley and Shamir independently introduced what is known under the name "threshold schemes". In those schemes pieces of information are distributed amongst "trustees" in such a way that any number of trustees which achieve a quorum or threshold can reconstruct the information.
Clearly "reconstruction of the information" can be replaced by "gaining access", "starting a computer program", "signing a cheque" or anything which is similar to this. A more formal definition reads as follows.

A *t-threshold scheme* consists of $s \geq t$ pieces of information, called *shadows*, such that
(i) a *secret datum* X can be retrieved from any t of the s shadows and
(ii) X cannot be determined from any $t-1$ or fewer of the s shadows.

The second condition needs some explanation. First of all, it means that the knowledge of $t-1$ shadows should suggest every possible datum with about the same probability. If the number of possible data is finite, then one can, of course, guess the correct datum in a finite amount of time and the knowledge of $t-1$ shadows might even reduce the time necessary. It should, however, be beyond any reasonable computing time.

The security considerations depend on the nature of the secret datum X. If the value of X is, for instance, the master key of a cryptosystem ([3], [8]), then a correct guess of X compromises the system. The probability to do this might be different to the probability to cheat the system by entering "made-up" shadows. If the knowledge of X is by itself of no use, X might be a trigger to start a computer program, then this probability determines the security level. The possible difference of these two probabilities is illustrated by the schemes given in Section 3.3.

In the above definition the number s stands for the maximum number of shadows one can hand out to the trustees. If $s = t$, the loss of any one

shadow is, by definition, equivalent to the loss of the secret datum. This is also the case, if $s > t$ but the number of shadows handed out is equal to t. Administrative procedures such as a back-up list of all shadows, of course, prevent such a break down but impair the security.

Hence it is advantageous to the designer of a t-threshold scheme, if he has some room of manoeuvre between t and s. This allows him to fix the number of distributed shadows according to his needs.

In the present paper we discuss a class of threshold schemes with $t = 2$ and 3 which have the property that the level of security and with it the number s can be chosen as high and large as desired. They are based on so-called generalized quadrangles. These finite incidence structures also allow the construction of threshold schemes which cater for the situation where the trustees do not trust each other and a threshold has to be achieved in each one of a number of distrusting parties. This could, for instance, also be useful in a situation which involves not only human beings but say computer programs as well. We conclude this introduction with a definition of such threshold schemes.

A $(t_1, \ldots, t_n)$-*threshold scheme* is a t-threshold scheme with $t = \sum_{i=1}^{n} t_i$ where the set of shadows is partitioned into n subsets B_i $(i = 1, \ldots, n)$, with $|B_i| = s_i$, $\sum_{i=1}^{n} s_i = s$, and a quorum of $t_i \leq s_i$ is needed in each set B_i. If just n thresholds $t_1, \ldots, t_n$ have to be achieved and it does not matter in which one of the sets B_i, we call it a $(t_1, \ldots, t_n)^*$-threshold scheme.

2 GEOMETRIC BACKGROUND

An *incidence structure* is a triple (P, B, I) which consists of two non-empty and disjoint sets P and B and a subset $I \subseteq P \times B$. The elements of P and B are called *points* and *blocks* (or in our context *lines*), respectively. I is called the *incidence relation.* We say that a point x and a

line L are incident with each other and write $x\ I\ L$ if and only if the pair (x, L) is an element of I.

A (finite) *generalized quadrangle* (GQ) of *order* (σ, τ) is an incidence structure which satisfies the following axioms:

(i) Each point is incident with exactly $1 + \tau$ lines ($\tau \geq 1$) and two distinct points are incident with at most one line.

(ii) Each line is incident with exactly $1 + \sigma$ points ($\sigma \geq 1$) and two distict lines are incident with at most one point.

(iii) For every point x and every line L which are not incident with each other, there exists a unique line which is incident with both x and a (unique) point on L.

It follows from this definition that every GQ of order (σ, τ) has associated with it a GQ of order (τ, σ) which is obtained by interchanging the rôles of the points and lines. We call it *the dual GQ*. This implies that in any definition or theorem the words "points" and "lines" and the parameters "σ" and "τ" may be interchanged.

The definition allows us to identify each line with the set of points it is incident with. This and the obvious geometric structure of a GQ are the reasons for expressions such as "x lies on L", "x is contained in L" for $x\ I\ L$ and "L and M intersect each other in the point x" for $L\ I\ x\ I\ M$.

We call two not necessarily distinct points x and y collinear and write $x \sim y$, if there exists a line which contains both of them. If there is no such line we say that they are not collinear and write $x \not\sim y$. The set of points collinear with a point x is denoted by $x^{\perp}$ (note that $x \in x^{\perp}$).

Axiom (iii) is crucial for understanding most of the arguments in this paper. It means that, except for exactly one line, all the remaining τ lines through x do not intersect the line L. So a generalized quadrangle

does not contain a "triangle".

The proof of the following lemma is left to the reader as an easy exercise with the exception of (iii) a proof of which can be found in [7].

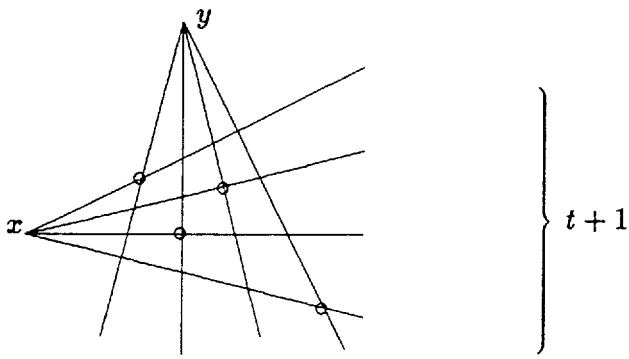
Lemma 1 *Let (P, B, I) be a generalized quadrangle of order (σ, τ), then*

(i) $|P| = (\sigma+1)(\sigma\tau+1)$, $|B| = (\tau+1)(\sigma\tau+1)$

(ii) $|x^\perp| = 1 + (\tau+1)\sigma$ for all points $x \in P$

(iii) $\sigma + \tau$ divides $\sigma\tau(\sigma+1)(\tau+1)$.

The threshold schemes we are going to introduce are based on *the span* of pointsets. The *trace* of a pair (x, y) of distinct points is defined to be the set $x^\perp \cap y^\perp$ and is denoted as $\mathrm{tr}(x,y)=\{x,y\}^\perp$. More generally, one can define for $A \subset P$, the set $A^\perp = \cap\,\{x^\perp \mid x \in A\}$. The span of two distinct points x and y, is defined as $\mathrm{sp}(x,y)=\{x,y\}^{\perp\perp}=\{u \in P \mid u \in z^\perp\ \forall z \in \mathrm{tr}(x,y)\}$. Hence it consists of all points which are collinear with every point in the trace of x and y.



If x and y are collinear, then $\mathrm{sp}(x,y)$ is the unique line through x and y and hence $|\mathrm{sp}(x,y)| = \sigma + 1$.
If x and y are not collinear, then no two of the points of $x^\perp \cap y^\perp$ marked by "o" in the diagram above are collinear. We note that x, y are in $\mathrm{sp}(x,y)$,

no two points of $\mathrm{sp}(x,y)$ are collinear and $|\mathrm{sp}(x,y)| \leq \tau + 1$. The latter follows since the points of $\mathrm{sp}(x,y)$ have to be contained in the $\tau + 1$ lines through any of the points of $x^\perp \cap y^\perp$.

Finally, a *triad* (of points) is a triple of mutually non-collinear points. Given a triad $T = (x,y,z)$, a *centre* of T is just a point of $T^\perp = \mathrm{tr}(x,y,z)$. The reader who is interested in finding out more about the theory of generalized quadrangles is referred to the book by Payne and Thas [7].

3 THE SCHEMES

3.1 The 2-Threshold Schemes

Let G be a generalized quadrangle of order (σ,τ) with $\sigma,\tau > 1$, and let x and y be two non-collinear points of G. Then the points of $\mathrm{sp}(x,y)$ can be used as the shadows of a 2-threshold scheme with the secret datum X being the span of x and y.

For consider two distinct points w and z of $\mathrm{sp}(x,y)$. As points of the span they are not collinear but each one of them is collinear with every point in $x^\perp \cap y^\perp$. Hence $z^\perp \cap w^\perp = x^\perp \cap y^\perp$ and $\mathrm{sp}(z,w) = \mathrm{sp}(x,y) = X$. So the secret datum is determined by any two of the shadows.
The probability to obtain X with the knowledge of no or just one shadow depends on the number of shadows in X. This number is subject to the structure of G and the particular choice of the span. It is however, never greater than $\tau + 1$. We obtain the following expression for the possibility that the secret datum is revealed by entering a valid shadow and some other point.

$$\mathrm{Prob} = \frac{\mathrm{s} - 1}{\sigma^2\tau + \sigma\tau + \sigma} \leq \frac{\tau}{\sigma^2\tau + \sigma\tau + \sigma}. \quad (3.1)$$

When setting the security level one has, however, to take into account that a trustee knows some finite geometry and for some reason or other the lines through his own shadow. This increases his probability of a successful attempt to break the system to

$$\text{Prob} = \frac{s-1}{\sigma^2\tau + \sigma\tau + \sigma - (\sigma\tau + \sigma)} = \frac{s-1}{\sigma^2\tau} \leq \frac{1}{\sigma^2} \quad (3.2)$$

as he can rule out the $\sigma\tau + \sigma$ points which are collinear with his shadow. Equation (3.2) implies that the security level only depends on σ or, in other words, the number of points on a line, if $\text{sp}(x, y)$ contains $\tau + 1$ points. If this is the case, the pair (x, y) is called *regular*. A point x is said to be regular, if for every y, $y \not\sim x$, the pair (x, y) is regular.

So far we have not said anything about the existence of generalized quadrangles. If a point of a GQ is regular then $\sigma \geq \tau$ (see [7]). So the smallest case is $\sigma = \tau$. Such generalized quadrangles exist indeed. The ones in which all the points are regular are derived from the projective geometry $PG(3, q)$. The points of the GQ are just the points of $PG(3, q)$ while the lines are the totally isotropic lines with respect to a symplectic polarity. For the necessary background in finite geometry the reader is referred to [1], [6]. As these geometries exist for every prime power q, we have obtained an infinite class of 2-threshold schemes which admit $q + 1$ shadows at a security level of $1/q^2$ and have an implementation size of $q^3 + q^2 + q + 1$ points and lines. Since these generalized quadrangles are coordinatized (see [7]), they can be implemented on a computer.

Using a regular pair of points for an implementation supplies us with at least $\tau + 1 \geq \sqrt{\sigma} + 1$ shadows at a security level of $1/\sigma^2$ since the inequalities $\tau^2 \geq \sigma \geq \tau$ hold (see [7]). Such a number is in nearly all cases far beyond anything needed. So the question arises whether one should use a non-regular pair of points whose span is sufficiently large. A span containing s points increases the security level to $(s-1)/\tau\sigma^2$ at the same order (σ, τ). For instance, the generalized quadrangles derived from a non-singular hermitian variety in $PG(4, q^2)$ have order (q^2, q^3). Here the spans consist of $q + 1$ points. Hence the probability to cheat is approximately $1/q^6$ while the above examples attain a security level of only $1/q^4$ at the same line-size. This is, however, not the only criterion for the magnitude of the implementation.

It should be mentioned that regular pairs have a non-negligible advantage when it comes to the actual implementation, since we can make use of the following observation. Two points x' and y' belong to $\mathrm{sp}(x,y)$ if and only if they are collinear with every one of the points in $x^{\perp} \cap y^{\perp}$. Checking this is clearly not feasible. If the pair (x,y) is regular, it suffices to show that x' and y' are collinear with just two of those points. Since in this case the trace of a span is equal to the span of the trace. So we just have to store two points of the trace and check whether x' and y' are collinear with both of them. The amount of computation needed for this depends on the number of coordinates and the particular field used for the coordinatization.

3.2 The 3-Threshold Schemes

The threshold schemes constructed in the preceding section were based on pairs of non-collinear points. Now we are going to use triads of points. We will see that, when assessing the security of the new systems, it is not sufficient to just transfer the considerations made for the 2-threshold schemes. The "extension" will provide an attacker with new possibilities.

Let (x,y,z) form a triad, and let $\mathrm{sp}(x,y,z) = \{x,y,z\}^{\perp\perp}$ be the secret datum X. It is easy to see that any three points of X uniquely determine X. So condition (i) for a 3-threshold scheme is satisfied.
Two disloyal trustees with respective shadows x', y' have a success rate of

$$(s-2)/(\sigma^2\tau + \sigma\tau + \sigma - 1) \quad (3.3)$$

in a staight forward attack. If they can rule out the $2\sigma(\tau+1)-(\tau+1) = 2\sigma\tau+2\sigma-\tau-1$ points which are collinear with x', y', then their probability to break the system is

$$\mathrm{Prob} = \frac{s-2}{\sigma^2\tau - \sigma\tau - \sigma + \tau}. \quad (3.4)$$

So far everything is similar to the case of two non-collinear points. Being able to rule out the points of $\mathrm{tr}(x',y')$, however, opens up new ways of

breaking the system in this situation as we will see later.

The number of shadows depends on the underlying GQ. If this is of order (σ, σ^2) with $\sigma > 1$, then $\mathrm{tr}(x,y,z) = \{x,y,z\}^\perp$ always consists of $\sigma+1$ points and hence $\mathrm{sp}(x,y,z)$ contains at most $\sigma+1$ points. The point x is 3-regular, if $|\mathrm{sp}(x,y,z)| = \sigma+1$ for any triad (x,y,z) through x in G. Hence X contains $s = \sigma+1$ shadows.

Examples of such generalized quadrangles are $Q(5,q)$, the elliptic quadrics in $PG(5,q)$, for every prime power q. These give rise to 3-threshold schemes with $q+1$ shadows. We will discuss the security using the generalized quadrangles of order (σ, σ^2). For these Equation (3.4) reads

$$\mathrm{Prob} = \frac{\sigma-1}{\sigma^4-\sigma^3+\sigma^2-\sigma} = \frac{1}{\sigma^3+\sigma}. \quad (3.5)$$

If the two trustees x' and y' can work out the points of $\mathrm{tr}(x',y')$ they could make use of this knowledge and the relationship between a trace and its span. They take any point u in $\mathrm{tr}(x,y)$, choose a line L through this point and a point $g \neq u$ on L. The probability that u is in $\mathrm{tr}(x,y,z)$ is $(\sigma+1)/(\sigma^2+1)$, the one for L to intersect $\mathrm{sp}(x,y,z)$ in a point different to x and y is $(\sigma-1)/(\sigma^2-1)$, while the probability that g is indeed this point is $1/\sigma$. Assuming that the three events are independent the two disloyal trustees succeed in breaking the system with a probability of

$$\frac{\sigma+1}{\sigma^2+1} \cdot \frac{\sigma-1}{\sigma^2-1} \cdot \frac{1}{\sigma} = \frac{1}{\sigma^3+\sigma}. \quad (3.6)$$

So all this effort has not increased their chances. An improvement of this attack can be made if one knows conditions under which a line L through z does or does not intersect $\mathrm{sp}(x,y,z)$ and the checking of these conditions could be done without the system knowing it. Being able to determine a correct line raises the "success rate" to $(\sigma+1)/(\sigma^3+\sigma)$.

Clearly a lot of computing would have to go into such an attack. Any decrease in the security level given by (3.4) was based on the assumption that the trustees know not only their coordinates but also enough about the implementation to work out $\mathrm{tr}(x',y')$. If they can do this it is also

fair to assume that they can determine a point of $\mathrm{sp}(x', y')$ and feed the system this point. As $\mathrm{sp}(x, y, z)$ is contained in $\mathrm{sp}(x', y')$ the security now depends only on the size of $\mathrm{sp}(x', y')$ which is bounded above by $\sigma^2 + 1$. This yields a probability of

$$\mathrm{Prob} = \frac{\sigma - 1}{|\mathrm{sp(x', y')}|} \geq \frac{\sigma - 1}{\sigma^2 - 1} = \frac{1}{\sigma + 1}. \quad (3.7)$$

Hence, if the trustees know the underlying implementation, the security level depends only on the span of x' and y' and might be unacceptable.

There is clearly no need for a trustee to know "his" shadow but one cannot rule out the possibility that he does. There is, however, in this scheme a way to prevent the trustee from making use of his knowledge. Before the system checks the shadows for their validity it does apply a secret coordinate transformation to them. So the secret datum X is not the span of the points x,y and z but of their transforms. This renders the knowledge of both $\mathrm{tr}(x', y')$ and $\mathrm{sp}(x', y')$ a useless information and increases the security level to the security level given in (3.4).

3.3 Combined Schemes

Distinct threshold schemes defined on the same underlying GQ obviously give rise to $(t_1, \ldots, t_n)$-threshold schemes. Using the geometry of the GQ allows the construction of more sophisticated schemes.

Let G be a generalized quadrangle with $\sigma > \tau$ in which every point is regular. To construct a $(1, 2)^*$-threshold scheme we choose a triad (x, y, z) where z is not collinear with any point in $\mathrm{sp}(x, y)$. The condition $\sigma > \tau$ guarantees the existence of such triads since there are $\tau(\sigma - \tau)(\sigma - 1)$ points z for every pair (x, y) of non-collinear points. As the secret datum X we select an arbitrary point of $\mathrm{tr}(x, y)$. Putting $B_1 = \mathrm{sp(x, y)}$ and $B_2 = \mathrm{tr(X, z)}$ we obtain a $(1, 2)^*$-threshold scheme.

To verify this we note that z is not collinear with X as (x, y) is a regular pair. The regularity of all points also implies that every triad has

exactly 0,1, or $\tau + 1$ centres (see [7]).

Let x', y' be two shadows of B_1 and z' a shadow of B_2. If they form a triad, then, in view of Axiom(iii), X is the unique centre of this triad. If z' and, say x' are collinear, then X is the unique point on the line through z' and x' which is collinear with y'. Now consider the case that two shadows are in B_2 and one is in B_1. The trace T of the two points in B_2 has exactly one point in common with $\mathrm{tr}(x, y)$, namely the point X. This is the only point of T which is collinear with the shadow in B_1.

Two non-collinear shadows, whether or not they belong to the same class, determine a trace which contains X and τ further points. Hence their probability to guess X is

$$\frac{1}{\tau + 1} \quad (3.8).$$

Even if all the trustees of one class join their forces they cannot improve this probability. If the two shadows are collinear, then X is one of the $\sigma - 1 \geq \tau$ points on their common line. So this case gives a probability of

$$\frac{1}{\sigma - 1} \leq \frac{1}{\tau} \quad (3.9).$$

We note that there are no non-trivial examples known of generalized quadrangles with $\sigma = \tau + 1$. Examples which can be used are the duals of those mentioned in the preceding section. They are of order (q^2, q), where q is any prime power.

Using the same kind of implementation as before one can check that the shadows belong to the correct classes. We store three points X, z and w, where w is in $\mathrm{tr}(x, y)$. When three points together with their respective "class numbers" are entered, the system checks that they are collinear with the appropiate pair of the three stored points.
So we have joined two 2-threshold schemes to form a $(1, 2)^*$-threshold scheme.

Since the system checks the entered values for the correct class, the probability to break the system is smaller then the ones given above, if the knowledge of X in itself is not equivalent to a compromise of the system.
There are several ways to construct a possible third shadow. None of these yields a better probability than trying to figure out X first and then a "correct" shadow. So the probability in (3.8) has to be multiplied by $1/(\sigma - 1)$ and the one given in (3.9) by $1/\sigma$. So the chances to enter a correct third shadow are about $1/\tau^2$.
It should be mentioned that a coordinate transformation will reduce all these probabilities to about 1 over the number of points of the GQ. So two trustees stand no better chance than two outsiders who just know the underlying GQ.

We conclude this section with an example involving a "supershadow". Let (x, y, z) be a triad such that z is not in $\mathrm{sp}(x, y)$. Then $\mathrm{sp}(x, y)$ and $\mathrm{sp}(x, z)$ have just the point x in common. We define three classes $B_1 = \{x\}$, $B_2 = \mathrm{sp(x,y)}\backslash\{\mathrm{x}\}$ and $B_3 = \mathrm{sp(x,z)}\backslash\{\mathrm{x}\}$, and let $X = \mathrm{tr(x,y)} \cup \mathrm{tr(x,z)}$. This yields both a (1,1,1)- and a (0,2,2)-threshold scheme with the shadow x being more powerful than the other shadows. We note that $\mathrm{tr}(x, y)$ and $\mathrm{tr}(x, z)$ intersect in a unique point u, say. So, if every point is regular, we only need to store u and a further point in each trace. We leave it to the reader to work out the various probabilities to cheat the system.

Acknowledgement

The first author is indebted to the Philips Research Laboratory Brussels for the facilities they offered during the preparation of this paper.

References

[1] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Wissenschaftsverlag Bibliographisches Institut Mannheim, 1985.

[2] A. Beutelspacher and K. Vedder, *Geometric Structures as Threshold Schemes.* Proc. of the IMA Conference on Cryptography and Coding Theory, Cirencester, Oxford Univ. Press (to appear).

[3] G. R. Blakley, *Safeguarding cryptographic keys.* Proceedings NCC, AFIPS Press, Montvale, N.J., Vol. 48 (1979), 313-317.

[4] M. De Soete and J. A. Thas, *A coordinatization of the generalized quadrangles of order* $(s, s+2)$, to appear in J. C. T. (A).

[5] G. Hanssens and H. Van Maldeghem, *Coordinatization of Generalized Quadrangles*, Annals of Discr. Math. 37 (1988), 195–208.

[6] D. R. Hughes and F. C. Piper, *Design Theory*, Cambridge University Press, 1985.

[7] S. E. Payne and J. A. Thas, *Finite generalzed quadrangles*, Research Notes in Math. #110, Pitman Publ. Inc. 1984.

[8] A. Shamir, *How to share a secret*, Communications ACM, Vol. 22 nr.11 (1979), 612–613.