HOW TO SAY "NO"

Albrecht Beutelspacher
Mathematisches Institut
Justus-Liebig-Universität Gießen
Arndtstr. 2, D-6300 Gießen
Federal Republic of Germany

ABSTRACT

We pose the question whether there exist threshold schemes with positive and negative votes (shadows), that is threshold schemes in which any qualified minority can prohibit the intended action. Using classical projective geometry, the existence of such systems is proved. Finally, possible attacks on such systems are discussed.

1. INTRODUCTION

Threshold schemes have been introduced in order to control the access to secret data: The secret is divided into n "shadows" such that from any t shadows the secret can be reconstructed, but it is not feasable to retrieve the secret by knowing only t–1 shadows. So, only if a certain numbers t of participants say "yes", the secret will be disclosed. (Threshold schemes have been introduced by Shamir [4]; for an excellent survey on threshold schemes which emphasizes in particular the connections to geometry see [5].)

In many practical situations it is desirable that a qualified minority should also be able to "close" the secret. Think for example of the serious (usually not solved) problem of deactivating a master key after a certain time. Here one would like to have a system which allows a qualified "no". The aim of this note is to introduce such systems. These will be "ordinary threshold schemes" with an additional negative feature. Typically, every user will get a "positive" and a "negative" vote.

First we will introduce some notation and then study several examples. Since we look for constructions using geometry we shall call the shadows *points*.

A (t;s)-*threshold scheme* consists of a collection $P \cup N$ of points such that the following conditions are satisfied.

- Any t points of P together with at most s–1 points of N determine a secret X uniquely;
- if less than t points of P are "active", then the secret X cannot be retrieved (independent how many points of N are active).

J.J. Quisquater and J. Vandewalle (Eds.): Advances in Cryptology - EUROCRYPT '89, LNCS 434, pp. 491-496, 1990.

- if at least s points of N are active, then it is impossible to determine the secret.

One can think of the points-of P as *positive* votes, whereas the points of N represent *negative* votes.

2. EXAMPLES

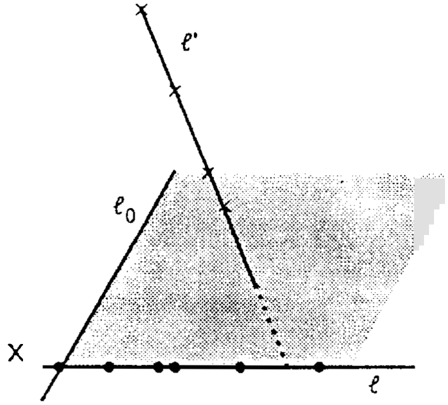
2.1 Basic Example

Consider a 3-dimensional geometry. We shall restrict ourselves to the 3-dimensional projective space $\mathbf{P} = PG(3,q)$ of order q. (For the geometric background see [2] and [3].) Fix a point X of $\mathbf{P}$ which will be identified with the secret. Choose a line ℓ_0 of $\mathbf{P}$ through X. Now we define

P to be a set of points on a line ℓ intersecting ℓ_0 in X and

N as a set of points distinct from $\ell' \cap <\ell,\ell_0>$ on a line ℓ' skew to ℓ.

Protocol: If a set U of (positive and negative) points is *active*, then the system computes $<U>$ and intersects it with ℓ_0. If $<U> \cap \ell_0$ is a point, the system takes it as the secret.



Analysis of the Basic Example:

- If at least two points of P are active, but no point of N, then the system computes ℓ and $\ell \cap \ell_0 = X$.

- If at least two points of P and exactly one point Y of N is active, then the system computes the plane $E = <\ell,Y>$; since $Y \notin <\ell,\ell_0>$, we have $E \neq <\ell,\ell_0>$; so, E intersects ℓ_0 only in X.

- If at least two points of P and at least two points of N are active, then the system computes $<\ell,\ell'> = \mathbf{P}$, intersects it with ℓ_0 and gets ℓ_0. The probability of choosing the correct secret point is only $1/(q+1)$. So, the secret cannot be retrieved.

- If at most one point of P and at least two points of N are active, then the system gets a point different from X of ℓ_0 – if any.

Conclusion: The Basic Example provides a (2;2)-*threshold scheme.*

2.2 A general construction

The above construction can be generalized in the following way.

Consider $\mathbf{P} = PG(d,q)$ and sets P and N of subspaces of $\mathbf{P}$. If a subset $U \subseteq P \cup N$ is active, the the system computes $\mathbf{R} = <U>$ and intersects $\mathbf{R}$ with a prefixed subspace $\mathbf{M}$ containing the secret X. If $\mathbf{R} \cap \mathbf{M} = X$, then the system says "yes".

The trick is the following: If enough elements of P are active, then $\mathbf{R}$ will contain X; but if in addition enough elements of N are active, then $\mathbf{R}$ will contain all points of $\mathbf{M}$. In this case, for an attacker, all point of $\mathbf{M}$ is equally likely; so, he can reconstruct the secret only with the (a priori !) probability $1/(q+1)$.

In the following *example* we will deal only with the situation in which all elements of $P \cup N$ are points.

Let $d = t+s-1$. Fix a $(t-1)$-dimensional subspace $\mathbf{T}$, an $(s-1)$-dimensional subspace $\mathbf{S}$ which is skew to $\mathbf{T}$ and a line $\mathbf{M}$ which intersects $\mathbf{T}$ in a unique point X and is skew to $\mathbf{S}$. Let $\mathbf{M}$ be spanned by the points X and Y. Now choose a set P of points in $\mathbf{T}$, a set N of points of $\mathbf{S}$ in such a way that the set $P \cup N \cup \{X,Y\}$ is an *arc*, which means that any $d+1$ of them generate the whole space. This implies:

- Let U be a subset of $P \cup N$. If U contains at most t-1 points of P, then $X \notin <U>$, so the secret cannot be reconstructed.
- If in a subset U of $P \cup N$ there are at most s-1 points of N, then $Y \notin <U>$, so the secret may be retrieved - if there are enough points of P in U.
- If U contains at least s points of N and at least t points of P, then $<X,Y> \subseteq U$, so the secret cannot be retrieved.

Hence we get a (t;s)-*threshold scheme.*

3. GENERALIZATION

Let G be a *geometry* consisting of *subspaces* (the empty set, points, lines, planes,..., i-dimensional subspaces,..., hyperplanes, the whole space) satisfying the following condition: For any set of subspaces $U_1,\ldots,U_a$, there is a unique subspace $<U_1,\ldots,U_a>$ of smallest dimension containing them. Such a geometry is often called a *matroid* [6] and most of the considered geometries are matroids (for instance projective and affine spaces, vector spaces,...)

Fix a point X in the geometry G and a line ℓ through it. Furthermore, fix two non-negative integers t and s. Now consider sets P and N of subspaces of G satisfying the following properties. For any subspaces $V_1,...,V_a$ of P and $W_1,...,W_b$ of N it holds

- If $\dim V_1 + ... + \dim V_a < t$, then $X \notin <V_1,...,V_a,W_1,...,W_b>$.
- If $\dim V_1 + ... + \dim V_a \geqq t$ and $\dim W_1 + ... + \dim W_b < s$, then $<V_1,...,V_a,W_1,...,W_b> \cap \ell = \{X\}$.
- If $\dim V_1 + ... + \dim V_a \geqq t$ and $\dim W_1 + ... + \dim W_b \geqq s$, then $\ell \subseteq <V_1,...,V_a,W_1,...,W_b>$.

Clearly, such an arrangement fulfills our initial requirements. *Namely:* The first condition says that if $V_1,...,V_a$ are too small alltogether, then the secret cannot be reached. The second condition guarantees that if $<V_1,...,V_a>$ is big enough, but $<W_1,...,W_b>$ is not too spacious, then the secret will be retrieved automatically. Finally, the last condition says that a great portion $<W_1,...,W_b>$ of subspaces of N can obstruct the system.

We note that this system is very flexible in as much as the elements of P and N may have different dimensions. This corresponds to real-world requirements, since in reality not all men are equal: User i gets subspaces $V_i \in P$ and $W_i \in N$ whose dimensions correspond to the (positive, resp. negative) power (importance, level in the hierarchy,...) of i. In other words, this is a $(t;s)$-threshold scheme only if the subspaces in $P \cup N$ are just points.

On the other hand, there is an abundance of geometries with the above properties. In section 2 we have indicated that one can use flats for the construction of such systems. But many other objects do the job, for instance curves of a certain degree, surfaces, and so on. In such a way one can generalize also Shamir's original construction [4].

We remark that for ordinary threshold schemes a similar approach has been undertaken in [1].

4. ATTACKS

There is an obvious attack against our models of $(t;s)$-threshold schemes: Sombody who knows a set $P' \cup N'$ of active positive and negative points (with $|P'| \geqq t$) has a good chance to forge the system. If he knows P', he can directly determine the secret. If, on the other hand, he knows 'only' $P' \cup N'$, then he can form all t-element subsets of this set and try each possibility; since the number of all t-element subsets of $P' \cup N'$ is much smaller than the number of points per line, also this is a reasonable attack.

These attacks imply strong restrictions on the machine which evaluates the incoming votes (points). Firstly, the machine must keep all inputs secret. Furthermore, the machine must operate trustworthy: It must not be possible to misuse it in order to obtain the positive or negative votes.

Therefore, there seem to be strong restrictions in using such a system. This is true. But it is only fair to mention that similar restrictions apply to all kinds of threshold schemes.

1. In any threshold scheme, the machine evaluating the shadows has to keep these shadows secret. (Otherwise, everybody who has access to the machine could obtain a sufficient number of shadows.) So, although the machine is not supposed to keep secrets for a long time, it must be able to keep secrets for a short time and then destroying them reliably.

2. Let us look at another example, namely Simmon's [5] realization of *robust shared secret systems.* In its simplest form, the shadows are points on a line ℓ and any two shadows are sufficient to determine the secret $X = \ell \cap \ell_0$. As a guarantee that the points are correct, the system wants a third point; if all three points lie on the same line, the system is convinced that all points are correct.

Of course, such a procedure makes only sense if the machine works trustworthy: Otherwise, given any two shadows, the machine could easily compute a third point on the line given by the two shadows and could so 'convince' itself that the points are correct.

To sum up, the restrictions on the machine, namely secrecy for short-term secrets and trustworthy operation are shared by many, if not all threshold schemes. But of course, there might exist systems (with or without negative votes) which have these properties only to a certain extend or not at all.

5. CONCLUSION

We present an extension of threshold schemes which allows negative votes. The philosophy behind the construction of these new schemes is the following. In an (ordinary) threshold scheme, the secret cannot be reconstructed, if there is too little information. With negative votes, the secret may also not be retrieved, if there is too much information. Using geometric structures we construct several infinite families of such threshold schemes.

REFERENCES

[1] A. Beutelspacher and K. Vedder, *Geometric structures as threshold schemes.* The Institute of Mathematics and its Applications, Conference Series **20**, Cryptography and Coding (ed. by H.J. Beker and F.C. Piper), 1989, 255-268.

[2] A. Beutelspacher, *Einführung in die endliche Geometrie I. Blockpläne.* B.I.-Wissenschaftsverlag, Mannheim - Wien - Zürich, 1982.

[3] P. Dembowski, *Finite Geometries.* Springer-Verlag, 1968.

[4] A. Shamir, *How to share a secret*. Comm. ACM Vol. 22 (1), 612-613 (1979).

[5] G.J. Simmons, *How to (really) share a secret*. To appear in Proc. of Crypto '88.

[6] D.J.A. Welsh, *Matroid theory*. Academic Press, London, New York, San Francisco, 1976.