A signature with shared verification scheme

Marijke De Soete[1], *Jean-Jacques Quisquater*[2] and *Klaus Vedder*[3]

(1)*MBLE-I.S.G.*, Rue des Deux Gares 82, B–1070 Brussels, Belgium
(2)*PRLB*, Avenue Van Becelaere 2, B–1170 Brussels, Belgium
(3)*GAO*, Euckenstraße 12, D–8000 München 70, Federal Republic of Germany

Abstract This paper presents a signature scheme for a single user or a group of users. The shared verification of such a signature uses the principle of threshold schemes. The constructions are based on a special class of finite incidence structures, so called generalised quadrangles.

1 Introduction

The schemes generate a signature for a single user X, denoted by $sign_x$, or for a group of users G, denoted by $sign_G$. The verification system, knowing the identity of X or G, can check the validity of the signature using the principle of threshold schemes (see Simmons [5]). This means that there exists a group of verifiers and the scheme only needs a certain number of them for the verification of the signature. We will call this a *shared verification scheme*, for which a more formal definition reads as follows:

A t-shared verification scheme consists of $s \geq t$ classes called *verifiers* such that

- any t of the s verifiers can execute the verification
- the verification cannot be done by any $t-1$ or fewer of the s classes.

The construction of the schemes is based on a special class of geometric incidence structures, so called generalised quadrangles. Generalised quadrangles have been used before to construct threshold schemes (see [3]) which are closely related to the topic of this paper.

G. Brassard (Ed.): Advances in Cryptology - CRYPTO '89, LNCS 435, pp. 253-262, 1990.

A typical environment where these schemes could be employed is described by Simmons in [4]. Here they could serve the purpose of checking the signature on data transmitted by a seismic station. The verification could be done by a central body which also selects, possibly randomly, the required number of verifiers from the group of all verifiers.

Another field of application might be any system where a central institution supervises its member bodies. The signing of a document by one of the member bodies has to be verified by the central institution. This can use therefore a shared verification scheme where the classes of verifiers consist of delegates of the various member bodies.

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) *generalised quadrangle* (GQ) of order σ, $\sigma \geq 1$, is an incidence structure $S=(P, B, I)$ which satisfies the following axioms:

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

(ii) Each line is incident with exactly $\sigma + 1$ points and two distinct 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.

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 $L\ I\ x\ I\ M$.

Axiom (iii) is crucial for understanding most of the arguments in this paper. It means that, with the exception of one line, all the remaining σ lines through x do not intersect the line L. So a generalised quadrangle does not contain a "triangle".

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 $x \in x^\perp$).

The proof of the following lemma is left as an easy exercise to the reader.

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

(i) $|P| = |B| = (\sigma + 1)(\sigma^2 + 1)$

(ii) $|x^\perp| = \sigma^2 + \sigma + 1$, for all points $x \in P$.

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 trace(x, y). Notice that $|\text{trace}(x, y)| = \sigma + 1$. The span of two distinct points x and y, is defined as span(x, y)=$\{u \in P \mid u \in z^\perp, \forall z \in \text{trace}(x, y)\}$. Hence it consists of all points which are collinear with every point in the trace of x and y. More generally, one can define for $A \subset P$, the set $A^\perp = \cap_{x \in A} x^\perp$. In this notation trace$(x, y)$= $\{x, y\}^\perp$ and span(x, y)=$\{x, y\}^{\perp\perp}$.
If x and y are collinear, then trace(x, y)=span(x, y) is the unique line through x and y having $\sigma + 1$ points. If x and y are not collinear, then no two distinct points of trace(x, y) are collinear. We note that x, y are in span(x, y), no two distinct points of span(x, y) are collinear and $|\text{span}(x, y)| \leq \sigma + 1$. The upper bound follows from the fact that the points of span(x, y) are contained in the $\sigma + 1$ lines through any of the points of $x^\perp \cap y^\perp$. Furthermore, two spans intersecting in at least two points define the same trace and hence coincide.
A pair (x, y) is called *regular* if $|\text{span}(x, y)| = \sigma + 1$. The point x is regular if and only if (x, y) is regular, for all $y \neq x$.

An *ovoid* of a generalised quadrangle S is a set θ of points of S such that each line is incident with a unique point of θ. One verifies easily that $|\theta| = \sigma^2 + 1$.

The following property of quadrangles of order σ (see [8] p. 21) is fundamental for the construction of the schemes.

Theorem *Let (x, y) be a regular pair of non-collinear points in a GQ of order σ. Then any ovoid contains exactly two points of trace(x, y) and none of span(x, y) or exactly two points of span(x, y) and none of trace(x, y).*

As an example of a generalised quadrangle satisfying these properties we consider a non-degenerate quadric Q in a finite projective space $PG(4, q)$. The points of Q together with the lines (which are the subspaces of maximal dimension on Q) define a generalised quadrangle $Q(4, q)$ of order σ.
If q is even this quadrangle contains ovoids and all its points are regular. The sheme may be implemented on a computer using the coordinatisation of these quadrangles given by Payne [7]. Note that this coordinatisation is based on a finite field $GF(q)$. For further information on generalised quadrangles we refer to the book by Payne and Thas [8].

3 Signature for a single user

3.1 The scheme

We consider a generalised quadrangle S of order σ containing an ovoid θ and a regular point $y \in \theta$.
The *individual users* correspond to the points of $\theta \setminus \{y\}$ while the *verifiers* correspond to the lines through y. Hence we have at most σ^2 users and up to $\sigma + 1$ verifiers.

The general signature of user X is defined to be the set

$$sign_x = \text{span}(x, y) \setminus \theta.$$

In view of the preceding theorem and the regularity of y, we have $sign_x = \text{span}(x, y) \setminus \{x, y\}$ and therefore $|sign_x| = \sigma - 1$. Since different spans can have at most one point in common (here the point y), it follows that different users have different signatures.

Due to the fact that y is regular, the span (x, y) and thus $sign_x$ are uniquely determined by any two of its points. So we may represent a specific signature of

the user X by two distinct points in $sign_x$, say x_1 and x_2, where one of these points could be x depending on the specific implementation.

To check a signature we need at least two verifiers, say V_1 and V_2. Let L_1 and L_2 be their corresponding lines. Verifier V_i constructs the respective unique lines through x, x_1 and x_2 which intersect L_i, $i = 1, 2$. The points x_1 and x_2 are elements of $sign_x$ if and only if the lines constructed by V_1 are concurrent in the same point u_1 on L_1 and those constructed by V_2 are concurrent in the same point u_2 on L_2. Indeed, x_1 and x_2 are in $sign_x$=span$(x, y) \setminus \theta$ if and only if they are collinear with the two points u_1 and u_2 of trace(x, y) on the lines L_1 and L_2, respectively.

3.2 Implementation and security

The security of the scheme will clearly depend on the particular implementation. First of all we have to make the assumption that the computer producing the signature (host) has a high security module for this purpose which also contains y. Anybody knowing y can produce "authentic" verifiers and stands a good chance of totally compromising the system by guessing the correct ovoid through y. Therefore care has to be taken that nobody can compute y from information such as a line L_i or a span(x_1, x_2). Each user has a personal IC card with his distinguished name and his secret identification number (SIN) which could be the coordinates of x. Having a SIN distinct from x can be of an advantage in certain environments. When a user wants to produce his signature, he enters his IC card and the host reads its information. Clearly, for the welfare of X, its SIN should be kept secret. Hence the SIN should go neither in clear nor encrypted with a constant key over the interface since this could lead to replay attacks. SIN has to be transmitted as a dynamic (time-variant) variable. One way would be that the host supplies the IC card with a true random number which is used to derive the key for the algorithm which encrypts the SIN.

The host checks that the SIN belongs to the distinguished name and derives, if necessary, the point x from SIN by means of a cryptographic algorithm, a coordinate transformation, or just by looking it up in a secret table. This last possibility has the disadvantage that the table need to be updated when a new user joins the system.
The host then produces $sign_x$ and the two points x_1 and x_2.

The verifying system can be laid out in such a way that it checks a signature with respect to a specific signatory or that it just proves that someone has presented a valid signature. The requirements for the individual verifiers are very similar except that in the first case it has to derive x from SIN. In either case a verifier need not know anything about the underlying geometry. It just has to be capable of constructing and intersecting lines. This also means that verifiers can be added to the system without any problem by a trusted third party which has to know y, a list of existing verifiers together with their lines and the means which protect the communication between the entities.
Hence the verifying system can consist of secure boxes. Each verifier V_i receives a box which can make the necessary calculations and contains information about the lines L_i so that when a point is entered, the box can check the collinearity with points on L_i. Depending on the outcome of this process the box gives the message "YES" or "NO" and, if required, the distinguished name of X. So we consider the following two scenarios.

- User X presents his SIN and the two points x_1 and x_2 to the verifying system. Two verifiers enter this information into their secure box. Each box derives x from SIN and checks for collinearity. A box gives the message YES if x, x_1 and x_2 are collinear with the same point on its line. If the two verifiers have received a YES from their respective boxes for the same distinguished name, the signature is accepted. We should point out that it is sufficient for the verification of the signature $sign_x$ to use SIN and one further point x_1, say. This would however give an attacker a better chance to cheat in certain cases as we will see in the next section.

- User X presents two points of his signature x_1 and x_2 to the verifying system. Two verifiers enter this information into their secure box and each box checks that the two points are collinear with the same point on its line. If two verifiers obtain a positive answer, they know that a user X presented a valid signature. Indeed, the collinearity of the two points with the same point on the respective lines means that $y \in \text{span}(x_1, x_2)$. It follows from the theorem that $\text{span}(x_1, x_2)$ contains a second point of the ovoid θ, i.e. a user. However, the verifiers do not know if this point is x. In other words they cannot check that the valid signature is indeed the one corresponding to X.

To conclude this section we summarize the different steps necessary for producing

and verifying a signature. It is assumed that all communication between entities is done in a secure way. For an eavesdropper can derive y from two pairs x_1, x_2 and z_1, z_2 belonging to different spans, if he knows the coordinatisation of the underlying geometry.

I. Signature process

Step 1. User X feeds his SIN to the host in a secure way.

Step 2. The host constructs $sign_x$.

Step 3. The host picks two distinct points x_1, x_2 of $sign_x$.

Step 4. The host feeds the two points x_1 and x_2 to the user X.

II. Verification of the signature

Step 1. User X presents his SIN and the two points to the verifying system.

Step 2. At least two verifiers feed the information to their boxes.

Step 3. Each box checks the necessary collinearity with a point on its line.

Step 4. The boxes give the message YES or NO and, possibly, the distinguished name of X.

Step 5. The signature (of X) is accepted if and only if all verifiers obtained a YES (and the distinguished names are the same).

3.3 Attacks

For running a successful attack it is not sufficient to find the correct values for the points. They also have to be accepted by the sytem as such. This means that a potential attacker has also to overcome the secure communication system between the entities. As this is up to a specific implementation we will make our considerations on the assumption that this can be done.

The first case we consider is that the verifying box requires SIN and the attacker knows SIN but not x. Then he has to guess two correct points in $sign_x$. This probability is approximately $1/\sigma^4$. For the probability to find a first correct point is given by

$$\frac{\sigma-1}{(\sigma^2+1)(\sigma+1)} \approx \frac{1}{\sigma^2}$$

since $sign_x$ contains $\sigma-1$ points and the quadrangle has $\sigma^3+\sigma^2+\sigma+1$ points in total. The probability to choose a matching second point is given by

$$\frac{\sigma-2}{\sigma^3} \approx \frac{1}{\sigma^2}$$

for the opponent can rule out all the points collinear with his first one. This gives him a probability of $\approx 1/\sigma^4$ to find two points of a specific signature.

If he also knows x, then he can rule out for his choice of x_1 all $\sigma^2+\sigma+1$ points collinear with x. He has therefore a probability to guess a point in $sign_x$ of $(\sigma-1)/(\sigma^3) \approx 1/\sigma^2$. The second point he can construct by considering $\mathrm{span}(x, x_1)$.

In our second scenario the verifying system just checks that the points entered are in $\mathrm{span}(y, x) \setminus \{y, x\}$ for some point x on the ovoid. In this case the attacker picks an arbitrary point for x_1 not on the ovoid and for x_2 one which is not collinear with x_1. The probability that x_1, x_2 get accepted as a signature is

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

The situation is completely different if the attacker knows y. In the second scenario he can produce "valid" signatures with a probability of 1. He picks two lines L_1 and L_2 through y and a 4-gon $u_1x_1u_2x_2$ where u_1 is on L_1, u_2 on L_2 and x_1, x_2 are not on L_i, $i = 1, 2$. The points x_1, x_2 will get accepted as a valid signature.

Next one can ask for the probability to break the whole system by determining the ovoid θ. Suppose an opponent knows two points x_1 and x_2 of a valid signature. Then he has to consider all ovoids intersecting $\mathrm{span}(x_1, x_2)$ in two points. This depends now on the particular generalised quadrangle used and we cannot say anything in the general case. For $Q(4, q)$, q even, it follows from papers due to Bagchi and Sastry (see [1], [2]) who studied the intersection of ovoids in $PG(3, q)$ in detail that there are sufficiently many ovoids through two points to guarantee the security

of the system.

Similarly, the probability of two verifiers to construct "genuine" signatures depends on the number of ovoids through the point y their corresponding lines have in common. As a verifier need not know his line, only the verifying box should be in possession of the coordinates of the line to make it more difficult for two verifiers to cooperate.

4 Signature for a group of users

We consider again the same geometric structure as before with an ovoid θ and a regular point y on θ. The *groups of users* are defined to be the sets $G = \text{span}(x, y) \setminus \theta$, $x \in P$, $x \not\sim y$. By the theorem we have $|\text{span}(x, y) \cap \theta| = 2$ (since $y \in \text{span}(x, y) \cap \theta$) and hence $|G| = \sigma - 1$. These spans partition the set of points not collinear with y of the GQ. It follows that we have at most σ^2 groups each consisting of $\sigma - 1$ users. Again we let the *verifiers* correspond to the lines through y, so we have up to $\sigma + 1$ of them.

The signature of a group G is defined to be the unique point of G which lies in the set $\theta \setminus \{y\}$, i.e.

$$sign_G = G \cap (\theta \setminus \{y\}).$$

The uniqueness of this point is guaranteed by the theorem. Different groups have necessarily different signatures since the spans we consider only have the regular point y in common.

To verify the signature of a member X_G of a certain group G, two verifiers are sufficient. If the two points X_G and $sign_G$ are presented to the verifying system, at least two verifiers V_1 and V_2 check if the two given points are collinear with the same point on each of their corresponding lines L_1 and L_2. If and only if this is the case for both, $sign_G$ is accepted.

The implementation can be done by installing a similar system as the one described for a single user. The detailed description of it as well as an overview of the possible attacks in this case are left to the reader.

References

[1] B. Bagchi and N. S. Sastry, *Even order inversive planes, generalised quadrangles and codes*, Geom. Ded. 22 (1987), 137–147.

[2] B. Bagchi and N. S. Sastry, *Intersection pattern of the classical ovoids in symplectic 3-space of even order*, Preprint.

[3] M. De Soete and K. Vedder, *Some new classes of geometric threshold schemes*, Proceedings of Eurocrypt '88, ed. G. Günther, L.N.C.S. 330 (1988), Springer Verlag, 389–401.

[4] G. J. Simmons, *A Natural Taxonomy for Digital Information Authentication Schemes*, Proceedings of Crypto '87, ed. C. Pomerance, L.N.C.S. 293 (1988), Springer Verlag, 269–288.

[5] G. J. Simmons, *How to really share a secret*, Proceedings of Crypto '88, L.N.C.S., Springer Verlag, to appear.

[6] G. J. Simmons, *Shared Secret and / or Shared Control Schemes*, Eurocrypt '89 Houthalen (Belgium), April 10–13, extended abstract.

[7] S. E. Payne, *Generalised quadrangles of even order*, J. Algebra 31 (1974), 367–391.

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