Authentication codes from generalized quadrangles

Jeroen Schillewaert and Koen Thas*
Department of Pure Mathematics and Computer Algebra
Ghent University
Krijgslaan 281, S22, B-9000 Ghent, Belgium
jschille@cage.Ugent.be; kthas@cage.UGent.be

Abstract

Authentication codes were introduced by Simmons in [3]. Many combinatorial structures can be used to construct authentication codes, and interesting combinatorial bounds can be obtained, see e.g. [7], [8] and [9]. We investigate authentication codes arising from generalized quadrangles (GQs), which was first done in [1]. The use of intricated techniques and constructions from the theory of GQs allows us to obtain several systems of authentication codes, each with their own advantages.

1 Introduction and notation

This introduction is strongly based on the reference work [4], and a lot more can be found there.

Authentication is very important in information security, when e.g. Alice and Bob try to exchange messages. It provides protection against malicious persons trying to change messages or to impersonate the sender of these messages. There are two main models:

- one where Alice and Bob trust each other, called *A-codes*;
- one where they do not, called A^2*-codes*.

*This author is a Postdoctoral Fellow of the Fund for Scientific Research — Flanders (Belgium).

In the latter case, an *arbiter* is needed.

We denote the set of all source states by $\mathcal{S}$, the set of keys by $\mathcal{K}$, the set of encoding rules by $\mathcal{E}$ and the set of all possible encoded messages by $\mathcal{M}$.

In the A-model, sender Alice and receiver Bob agree upon a secret private key k. With each key there is associated a unique encoding rule e. Alice selects a source state s and encodes s into a message m using the encoding rule e corresponding with the chosen key k. After having received the message Bob checks whether it lies in the range $e(\mathcal{S})$. If it does, then the message is accepted as authentic. Bob can recover the possible source states as the preimage of the message under e. If this preimage is always unique, then we say the code is *Cartesian*. So once the message is observed, one can retrack the corresponding source state. Whence there is no secrecy involved here.

An opponent can try to construct a message lying in $e(\mathcal{S})$ after observing r valid messages. The probability of success of such a spoofing attack will be denoted by P_r.

In the A^2-model, we assume that Alice and Bob do not trust each other. In this case, they do not agree upon an encoding rule. Instead, a trusted person, the *arbiter*, is also involved in the scheme. Now Alice has a set of encoding rules $\mathcal{E}_T$, and Bob a set of decoding rules $\mathcal{E}_R$. If Alice and Bob want to communicate, Bob chooses a decoding rule $f \in \mathcal{E}_R$ and sends it to the arbiter. For every given f and given source state s there is a set of valid messages $\mathcal{M}(s, f)$. On receipt of f the arbiter selects one message out of $\mathcal{M}(s, f)$, hereby forming an encoding rule $e \in \mathcal{E}_T$, which he secretly sends to Alice. In this case, the encoding rule e is valid for the decoding rule f. When Bob receives a message he checks whether it is in some subset $\mathcal{M}(s, f)$. If so he accepts it as a valid one and he can retreive the corresponding source state. If there is a dispute between Alice and Bob about a message m, the arbiter checks if m is valid for the encoding rule given to the transmitter.

Below, we define this attack probability more formal. As in [4] we will use the "worst case definition". Denote a set of r observed messages as m^r. Let $P(m^r)$ be the probability that one has observed m^r after r messages. Furthermore, let $P(m|m^r)$ be the probability that the message m is valid given that m^r has been observed. Then we define the *attack probability* of the opponent P_{O_r} as follows.

$$P_{O_r} = \sum_{m^r \in \mathcal{M}_r} P(m^r) \max_{m \in \mathcal{M}} P(m|m^r).$$

If we assume a uniform probability distribution for the messages, then we get

$$P_{O_r} = \max_{m \in \mathcal{M}} P(m|m^r).$$

Introduce the following notation:

$$\mathcal{E}(m^r) = \{e \in \mathcal{E} \parallel m_i \in e(\mathcal{S}), 1 \leq i \leq r\}.$$

Denote by m'^r the set of $r+1$ messages m^r and m'. Then

$$P_{O_r} = \frac{|\mathcal{E}(m^r)|}{|\mathcal{E}(m'^r)|}.$$

In the A^2-model, three types of attacks have to be considered. The first one is the spoofing attack by the opponent such as in the A-model. The other two attacks are the spoofing attack T by Alice, sending a message and then claiming not to have sent it, and the spoofing attack by Bob, claiming to have received a message from Alice while this is not the case. One denotes the corresponding probabilities by P_{O_r}, P_{R_r} and P_T respectively.

The opponent's *attack probability* P_{O_r} is defined as in the A-model.

Let $P(f)$ denote the probability of a decoding rule f, and let $P(m|f, m^r)$ denote the probability of the event that the message m could be valid for the encoding rule used by the transmitter, given the decoding rule f and the first r messages $m^r = (m_1, \ldots, m_r)$. The *spoofing attack probability* of the receiver is then defined as

$$P_{R_r} = \sum_{f \in \mathcal{E}_R} P(f) \sum_{m^r \in \mathcal{M}^r} P(m^r|f) \max_{m \in \mathcal{M}} P(m|f, m^r).$$

Let $P(e)$ denote the probability of an encoding rule e, and let $P(m'|e)$ denote the probability of the event that the message $m' \in \mathcal{M}'(e)$ is acceptable by the receiver, given the encoding rule e. The *spoofing attack probability* of the transmitter is then defined as

$$P_T = \sum_{e \in \mathcal{E}_T} P(e) \max_{m' \in \mathcal{M}'(e)} P(m'|e).$$

If we assume a uniform probability distribution on the messages, the formulas reduce in the same way as for the A-codes.

2 Some combinatorics of generalized quadrangles

Finite Generalized Quadrangles. A (finite) *generalized quadrangle* (GQ) *of order* (s, t) is a point-line incidence structure $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathbf{I})$ in which $\mathcal{P}$ and $\mathcal{B}$ are disjoint (non-empty) sets of objects called *points* and *lines* respectively, and for which $\mathbf{I}$ is a symmetric point-line incidence relation satisfying the following axioms:

(i) each point is incident with $t + 1$ lines ($t \geq 1$) and two distinct points are incident with at most one line;

(ii) each line is incident with $s + 1$ points ($s \geq 1$) and two distinct lines are incident with at most one point;

(iii) if p is a point and L is a line not incident with p, then there is a unique point-line pair (q, M) such that $p\ \mathbf{I}\ M\ \mathbf{I}\ q\ \mathbf{I}\ L$.

If $s = t$, then $\mathcal{S}$ is also said to be *of order* s. If $s, t > 1$, $\mathcal{S}$ is *thick*.

Point-Line Duality. There is a *point-line duality* for GQs of order (s, t) for which in any definition or theorem the words "point" and "line" are interchanged and also the parameters. (If $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathbf{I})$ is a GQ of order (s, t), $\mathcal{S}^D = (\mathcal{B}, \mathcal{P}, \mathbf{I})$ is a GQ of order (t, s).)

Collinearity/Concurrency/Regularity. Let p and q be (not necessarily distinct) points of the GQ $\mathcal{S}$; we write $p \sim q$ and call these points *collinear*, provided that there is some line L such that $p\ \mathbf{I}\ L\ \mathbf{I}\ q$. Dually, for $L, M \in \mathcal{B}$, we write $L \sim M$ when L and M are *concurrent*.
For $p \in \mathcal{P}$, put

$$p^\perp = \{q \in \mathcal{P} \parallel q \sim p\}$$

(and note that $p \in p^\perp$). For a pair of distinct points $\{p, q\}$, we denote $p^\perp \cap q^\perp$ also by $\{p, q\}^\perp$. Then $|\{p, q\}^\perp| = s + 1$ or $t + 1$, according as $p \sim q$ or $p \not\sim q$, respectively. For $p \neq q$, we define

$$\{p, q\}^{\perp\perp} = \{r \in \mathcal{P} \parallel r \in s^\perp \text{ for all } s \in \{p, q\}^\perp\}.$$

Automorphisms. An *automorphism* of a GQ $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathbf{I})$ is a permutation of $\mathcal{P} \cup \mathcal{B}$ which preserves P, B and I. The set of automorphisms of a GQ $\mathcal{S}$ is a group, called the *automorphism group* of $\mathcal{S}$, which is denoted by $\mathrm{Aut}(\mathcal{S})$.

SubGQs. A *subquadrangle*, or also *subGQ*, $\mathcal{S}' = (\mathcal{P}', \mathcal{B}', \mathbf{I}')$ of a GQ $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathbf{I})$ is a GQ for which $\mathcal{P}' \subseteq \mathcal{P}$, $\mathcal{B}' \subseteq \mathcal{B}$, and where $\mathbf{I}'$ is the restriction of $\mathbf{I}$ to $(\mathcal{P}' \times \mathcal{B}') \cup (\mathcal{B}' \times \mathcal{P}')$.

The following results will sometimes be used without further reference.

Theorem 2.1 ([5], 2.2.1) *Let $\mathcal{S}'$ be a proper subquadrangle of order (s', t') of the GQ $\mathcal{S}$ of order (s, t). Then either $s = s'$ or $s \geq s't'$. If $s = s'$, then each external point of $\mathcal{S}'$ is collinear with the $st' + 1$ points of an ovoid of $\mathcal{S}'$; if $s = s't'$, then each external point of $\mathcal{S}'$ is collinear with exactly $1 + s'$ points of $\mathcal{S}'$.*

Theorem 2.2 ([5], 2.2.2) *Let $\mathcal{S}'$ be a proper subquadrangle of the GQ $\mathcal{S}$, where $\mathcal{S}$ has order (s, t) and $\mathcal{S}'$ has order (s, t') (so $t > t'$). Then we have*

(1) *$t \geq s$; if $s = t$, then $t' = 1$.*

(2) *If $s > 1$, then $t' \leq s$; if $t' = s \geq 2$, then $t = s^2$.*

(3) *If $s = 1$, then $1 \leq t' < t$ is the only restriction on t'.*

(4) *If $s > 1$ and $t' > 1$, then $\sqrt{s} \leq t' \leq s$ and $s^{3/2} \leq t \leq s^2$.*

(5) *If $t = s^{3/2} > 1$ and $t' > 1$, then $t' = \sqrt{s}$.*

(6) *Let $\mathcal{S}'$ have a proper subquadrangle $\mathcal{S}''$ of order (s, t''), $s > 1$. Then $t'' = 1$, $t' = s$ and $t = s^2$.*

3 Previously known results

Combinatorial Bounds. If we denote $|\mathcal{S}| = k$, $|\mathcal{M}| = v$, and by $\overline{\mathcal{M}^r}$ the set of r-tuples of elements of $\mathcal{M}$ and if we have observed r messages, then we have the following theorem [4, Proposition 3.3, pp. 36].

Theorem 3.1 *We have*

$$P_{O_r} \geq \frac{k-r}{v-r}.$$

Equality holds if and only if

$$P(m|m^r) = \frac{k-r}{v-r}$$

is satisfied for any $m^r = (m_1, \ldots, m_r) \in \overline{\mathcal{M}^r}$ and any $m \in \mathcal{M}$ with $m \neq m_i, 1 \leq i \leq r$.

Naturally, the number of encoding and decoding rules is lower bounded if one wants to construct good schemes.

For authentication without arbitration we have.

Theorem 3.2 *If an authentication code has attack probabilities for the opponent $P_{O_r} = 1/n_i$ $(0 \leq i \leq l)$ then $|\mathcal{E}| \geq n_0 \cdot \cdots \cdot n_l$.*

If equality holds, the authentication code is called *perfect*.

We have the following lower bounds for the number of encoding and decoding rules for a scheme with arbitration.

Theorem 3.3

$$|\mathcal{E}_R| \geq (P_{O_0} P_{O_1} \cdots P_{O_{t-1}} P_T)^{-1},$$
$$|\mathcal{E}_T| \geq (P_{O_0} P_{O_1} \cdots P_{O_{t-1}} P_{R_0} P_{R_1} \cdots P_{R_{t-1}})^{-1}.$$

If equality holds in both inequalities above, then we call the arbitration scheme *t-fold perfect*.

A Scheme using GQs. The scheme below is due to De Soete [1]. Take a fixed point p in a GQ of order (s,t). Let the source states be the $t+1$ lines of the GQ passing through p, the encoding rules the points not collinear with p, and the messages the points collinear with p but different from p. The third axiom of GQs makes this scheme work. In this way, we get a Cartesian authentication code with $|\mathcal{S}| = t+1$, $|\mathcal{M}| = (t+1)s$, $|\mathcal{E}| = ts^2$, and $P_0 = P_1 = 1/s$.

Remark 3.4 It is due to the projection property that this scheme works well. Our schemes below will exploit other more sophisticated projection properties of generalized quadrangles.

A garden of examples exists, using GQ theory, which all have comparable strength as the construction of De Soete. We are interested in stronger schemes, leading us to use more intricated techniques in order to pursue our goal.

4 Construction

Suppose $\mathcal{S}$ is a GQ of order (s,t). Suppose $\mathcal{S}'$ is a subGQ of $\mathcal{S}$ of order $(s,t/s)$; then an easy counting exercise shows that each line of $\mathcal{S}$ meets $\mathcal{S}'$ in either 1 or $s+1$ points.

Let x be a point of $\mathcal{S} \setminus \mathcal{S}'$; then the $t+1$ points of $\mathcal{S}'$ which are collinear with x (and which respectively correspond to the lines incident with x by the previous property) are two by two non-collinear; since $t+1 = s \cdot t/s + 1$, this means that these points form an "ovoid", $\mathcal{O}_x$, of $\mathcal{S}'$. An ovoid is a point set meeting each line precisely once. This ovoid is "subtended" by x.

Now suppose $\{\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_r\}$ is a set of $r > 0$ distinct subGQs of order $(s,t/s)$ of the GQ $\mathcal{S}$ of order (s,t), where $s \neq 1 \neq t$ but we allow $t/s = 1$. Let Σ be the number of points in

$$\bigcup_{i=1}^{r} \mathcal{S}_i,$$

so that the number of points outside this union is

$$(s+1)(st+1) - \Sigma.$$

The $\mathcal{S}_j$'s are the source states. The keys are the points of $\mathcal{S} \setminus \bigcup_{i=1}^{r} \mathcal{S}_i$, and the messages are the ovoids in the GQs $\mathcal{S}_j$ which are subtended by a point

outside their union.

Let k be the maximal number of points outside $\bigcup_{i=1}^{r} \mathcal{S}_i$ that subtend the same ovoid of some $\mathcal{S}_j$. Then

$$P_0 = \frac{|\mathcal{E}(m)|}{|\mathcal{E}|} = \frac{k}{(s+1)(st+1)-\Sigma}.$$

By [5, 1.4.1], we have

$$k \leq \frac{s^2}{t} + 1$$

so that

$$P_0 \leq \frac{s^2/t+1}{(s+1)(st+1)-\Sigma}.$$

We want to focus on two particular situations that appear to yield satisfying results.

(1) Let $t = s^2$ so that $t/s = s$. Then

$$P_0 \leq \frac{2}{(s+1)(s^3+1)-\Sigma}.$$

Suppose now that in $\mathcal{S}$ we have the following situation: Γ is an $(s+1) \times (s+1)$-grid (that is, a subGQ of order $(s,1)$), and all the $\mathcal{S}_j$'s contain Γ — it follows easily then that Γ is precisely the pairwise intersection of any two distinct $\mathcal{S}_j$'s. Moreover, if z is a point outside the subGQ union, and $\mathcal{S}_g, \mathcal{S}_h \neq \mathcal{S}_g$ are elements of $\{\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_r\}$, then z obviously subtends different ovoids in $\mathcal{S}_g$ and $\mathcal{S}_h$.

Whence

$$P_0 \leq \frac{2}{(s+1)(s^3+1)-(s+1)^2-r(s^3-s)} = \frac{2}{(s+1)(s^2-s)(s+1-r)}.$$

Note that we can choose the subGQs in such a way that the inequality becomes strict.

(2) Let $t = s$, so that $t/s = 1$ and

$$P_0 \leq \frac{s+1}{(s+1)(s^2+1)-\Sigma}.$$

Also, let Γ be two distinct lines, and let all the $\mathcal{S}_j$'s contain Γ — it follows (again) that Γ is precisely the pairwise intersection of any two distinct $\mathcal{S}_j$'s. If

z is a point outside the union, and $\mathcal{S}_g, \mathcal{S}_h \neq \mathcal{S}_g$ are elements of $\{\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_r\}$, then z subtends different ovoids in $\mathcal{S}_g$ and $\mathcal{S}_h$.

Whence

$$P_0 \leq \frac{s+1}{s(s^2+(1-r)s-1)}.$$

Remark 4.1 The schemes described in this section are *Cartesian*. Furthermore, the scheme is *perfect* if every ovoid is subtended by the same number of points. Examples of this situation are given below.

5 Examples

We first describe all known generalized quadrangles of order (s, s^2) (for some natural number s) that have at least one subGQ of order s.

First, we recall the description of some classical examples of GQs which we will use further on.

Consider a nonsingular quadric $\mathbf{Q}$ of Witt index 2, that is, of projective index 1, in $\mathbf{PG}(n, q)$, $n \in \{4, 5\}$. The points and lines of the quadric form a generalized quadrangle which is denoted by $\mathbf{Q}(n, q)$ and has order (q, q^{n-3}). Next, let $\mathbf{H}$ be a nonsingular Hermitian variety in $\mathbf{PG}(3, q^2)$. The points and lines of $\mathbf{H}$ form a generalized quadrangle $\mathbf{H}(3, q^2)$, which has order (q^2, q).

Note that the variety $\mathbf{H}$ has the following canonical form:

$$X_0^{q+1} + X_1^{q+1} + \cdots + X_d^{q+1} = 0.$$

Suppose $\mathcal{O}$ is an ovoid of $\mathbf{PG}(3, q)$, q any prime power. Then from $\mathcal{O}$ one can construct a GQ of order (q, q^2), denoted $\mathbf{T}_3(\mathcal{O})$, always containing subGQs of order q.

A *flock* of the quadratic cone in $\mathbf{PG}(3, q)$, the 3-dimensional projective space over the finite field $\mathbb{F}_q$, is a partition of the cone without its vertex into q disjoint irreducible conics. The planes generated by the conics are the *flock planes*. From any such flock $\mathcal{F}$ in even characteristic one can construct a GQ $\mathcal{S}(\mathcal{F})$ of order (q^2, q) whose dual always contains subGQs of order q.

Let $\mathcal{F}$ be a flock, derived [10, §4.8] from a semifield flock [10, §4.5] of the quadratic cone in $\mathbf{PG}(3, q)$, q any prime power. Then a GQ $\mathcal{S}(\mathcal{F})$ of order (q^2, q) can be constructed from $\mathcal{F}$ which has the property that its dual $\mathcal{S}(\mathcal{F})^D$ has a point (∞) such that there exists an elementary abelian automorphism group of $\mathcal{S}(\mathcal{F})^D$ that fixes (∞) linewise while acting sharply transitively on the points not collinear with (∞). This property has the advantage that from $\mathcal{S}(\mathcal{F})^D$ one can construct another GQ, the "translation dual" [10, §3.10], of

the same order, which has an automorphism group with similar properties as the original one.

Consider the following sequence:

$$\mathcal{S}(\mathcal{F}) \xrightarrow{D} \mathcal{S}(\mathcal{F})^D \xrightarrow{*} (\mathcal{S}(\mathcal{F})^D)^* \xrightarrow{D} [(\mathcal{S}(\mathcal{F})^D)^*]^D.$$

(Here, the operation "$*$" means that we take the translation dual.) Then $(\mathcal{S}(\mathcal{F})^*)^D$ is a GQ of order (q, q^2) which has $\mathbf{Q}(4, q)$-subGQs, with the following features.

Classical/Even case. If $\mathcal{F}$ is classical ("linear" — the flock planes share a line), then we have

$$\mathbf{H}(3, q^2) \cong \mathcal{S}(\mathcal{F}) \xrightarrow{D} \mathbf{Q}(5, q) \cong \mathcal{S}(\mathcal{F})^D \xrightarrow{*} \mathbf{Q}(5, q) \cong (\mathcal{S}(\mathcal{F})^D)^* \xrightarrow{D}$$

$$\mathbf{H}(3, q^2) \cong [(\mathcal{S}(\mathcal{F})^D)^*]^D.$$

In $\mathbf{Q}(5, q)$, any $\mathbf{Q}(4, q)$-subGQ has the property that each subtended ovoid is subtended by *precisely* two distinct points (see, for instance, [12]). For q even, we are necessary in the classical case.

Nonclassical case. Then q is odd. We distinguish two subcases.

- KANTOR-KNUTH. If $\mathcal{F}$ is nonlinear and derived from a Kantor-Knuth flock (note that the term "derived" is abundant here, since all derived flocks are isomorphic to the original semifield one [11]), $(\mathcal{S}(\mathcal{F})^D)^* \cong \mathcal{S}(\mathcal{F})^D$, and the latter contains two classes of $\mathbf{Q}(4, q)$-subGQs of order q, the union of which has size $q^3 + q^2$. In one class, each subtended ovoid is subtended by two distinct points, in the other class this is not the case.
- NOT KANTOR-KNUTH. A result of the second author [13] states that no $\mathbf{Q}(4, q)$-subGQ in $(\mathcal{S}(\mathcal{F})^D)^*$ can be doubly subtended. As in the Kantor-Knuth case, each such example contains q^3+q^2 subGQs of $\mathbf{Q}(4, q)$ type.

As for the second specific scheme we described, we now introduce a class of generalized quadrangles that contains all known GQs of order s (for some natural number s) which have $(s + 1) \times (s + 1)$-grids.

Suppose $H = \mathbf{PG}(3n - 1, q)$ is the finite projective $(3n - 1)$-space over $\mathbb{F}_q$, and let H be embedded in a $\mathbf{PG}(3n, q)$, say H'. Now consider a set $\mathcal{O} = \mathcal{O}(n, n, q)$ of $q^n + 1$ distinguished $(n - 1)$-dimensional subspaces of H, denoted $\mathbf{PG}(n - 1, q)^{(i)}$, so that (1) every three generate H; (2) for every

$i = 0, 1, \ldots, q^m$, there is a subspace $\mathbf{PG}(2n-1,q)^{(i)}$ of H of dimension $2n-1$, which contains $\mathbf{PG}(n-1,q)^{(i)}$ and which is disjoint from any $\mathbf{PG}(n-1,q)^{(j)}$ if $j \neq i$.

Then $\mathcal{O}$ is called a *pseudo-oval* or an $[n-1]$-*oval* of $\mathbf{PG}(3n-1,q)$. (Note that a [0]-oval of $\mathbf{PG}(2,q)$ is an *oval* of $\mathbf{PG}(2,q)$.)

From any such $\mathcal{O} = \mathcal{O}(n,n,q)$ there arises a GQ $\mathbf{T}(n,m,q) = \mathbf{T}(\mathcal{O})$, as follows.

- The POINTS are of three types.

  (1) A symbol (∞).

  (2) The subspaces $\mathbf{PG}(2n,q)$ of H' which intersect H in a $\mathbf{PG}(2n-1,q)^{(i)}$.

  (3) The points of $H' \setminus H$.

- The LINES are of two types.

  (a) The elements of $\mathcal{O}(n,n,q)$.

  (b) The subspaces $\mathbf{PG}(n,q)$ of $\mathbf{PG}(3n,q)$ which intersect H in an element of $\mathcal{O}$.

- INCIDENCE is defined as follows: the point (∞) is incident with all the lines of Type (a) and with no other lines; a point of Type (2) is incident with the unique line of Type (a) contained in it and with all the lines of Type (b) which it contains (as subspaces); finally, a point of Type (3) is incident with the lines of Type (b) that contain it.

Define

$$\mathcal{C}^+ = \{\mathbf{T}(\mathcal{O}) \parallel \quad \mathcal{O} \text{ is a pseudo-oval in even characteristic}\} \cup$$

$$\{\mathbf{T}(\mathcal{O})^D \parallel \quad \mathcal{O} \text{ is a pseudo-oval in even characteristic}\},$$

and

$$\mathcal{C}^- = \{\mathbf{T}(\mathcal{O}) \parallel \quad \mathcal{O} \text{ is a pseudo-oval in odd characteristic}\}.$$

Then every element of $\mathcal{C}^+ \cup \mathcal{C}^-$ is a GQ of order s for some natural s which has an $(s+1) \times (s+1)$-grid, and each known GQ with these properties belongs to $\mathcal{C}^+ \cup \mathcal{C}^-$.

6 Authentication with arbitration: H-schemes

Consider the following situation. $\{\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_r\}$ is a set of distinct $\mathbf{Q}(4,q)$-subGQs in a $\mathbf{Q}(5,q)$ (which, as above, can be chosen in a suitable position), and let those subGQs be source states. Let x be a point of $\mathbf{Q}(5,q)$ outside the union of the subGQs, which is chosen by Bob. For such a point x and for each source state $\mathcal{S}_j$, let $\mathcal{O}_x$ be the ovoid of $\mathcal{S}_j$ which is subtended by x. The arbiter chooses a point c_j of $\mathcal{S}_j$ on $\mathcal{O}_x$.

We can now make a scheme with arbitration as follows. For the system we choose a list $\mathbf{H}$ of subgroups of $\mathrm{Aut}(\mathbf{Q}(5,q))$, being $\mathbf{O}^-(6,q) \rtimes \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_p)$ (q is a power of the prime p). Bob chooses a fixed subgroup H in $\mathbf{H}$. Bob hands H and his chosen point x to the arbiter. The subgroup H has different orbits on $\mathbf{Q}(5,q)$. The arbiter hands c_j and the H-orbit c_j, denoted by c_j^H, as encoding rule to Alice for a given source state S_j. If Alice transmits a message to Bob, then she picks a source state S_j and sends the triple (S_j, c_j, c_j^H) to Bob.

When receiving a triple (a,b,c) Bob accepts it as valid if b is on the ovoid of a and c is the H-orbit of b.

In case of a dispute concerning a triple (a,b,c), the arbiter checks if b is the point he handed to Alice for the subGQ a and if c is the orbit under H of b. If this is the case, then he decides Alice sent the message, otherwise that she has not.

If Bob wants to cheat, he has to make a guess about the point c_j.

If Alice wants to cheat, she has to make sure she gets the right orbit. It is almost impossible for Alice to guess H from the orbits she sees, except possibly by exhaustive search through all subgroups of $\mathrm{Aut}(\mathbf{Q}(5,q))$ if there are only very few groups producing an orbit she observes. But the arbiter can avoid this by choosing the appropriate points.

An opponent has to guess both c_j and the group H, an even harder task.

We do not make calculations in detail, but once one has chosen the list of allowed subgroups one can adapt the scheme to one's own needs.

This scheme depends largely on the list $\mathbf{H}$ of subgroups we allow. By choosing them appropriately, one can control the length of the orbits.

Remark 6.1 (i) Similar schemes can be built from other incidence geometries, such as the natural embedding of Hermitian quadrangles $\mathbf{H}(3,q^2) \subset \mathbf{H}(4,q^2)$.

(ii) We always assume that the points outside the union of subGQs are chosen with equal probability. One could define a natural probability

$$P : \mathcal{S} \setminus \cup_i \mathcal{S}_i \mapsto]0,1[$$

on this set by comparing, for a pre-chosen subgroup G of $\mathrm{Aut}(\mathcal{S})_{\cup_i \mathcal{S}_i}$, the size of the G-orbit $G(x)$ that contains x, to $|\mathcal{S} \setminus \cup_i \mathcal{S}_i|$.

7 Conclusion

In this paper, we have shown that using projection properties of GQs, one gets a bunch of schemes, strongly dependent on parameters, such that the user has some control to optimize the schemes to his own needs. Our goal was not to give a complete overview of possible schemes based on GQs (since there are an overwhelming number of possibilities), but rather to give the reader an idea which ideas are behind such schemes.

The authors are preparing a paper [6] on construction theory of "algebraic" authentication code schemes, based on finite group theory.

Acknowledgement. The research of the first author is carried out within the project "Linear codes and cryptography" of the Fund for Scientific Research Flanders (FWO-Vlaanderen) (Project nr. G.0317.06), and the Interuniversitary Attraction Poles Programme-Belgian State-Belgian Science Policy: project P6/26-Bcrypt.

References

[1] M. Desoete. Some construction for authentication-secrecy codes, in: Advances in cryptology—EUROCRYPT '88 (Davos, 1988), Springer, Berlin, 1988, pp 57-75.

[2] B. Huppert. *Endliche Gruppen I*, Springer-Verlag, Berlin, 1967.

[3] G. L. Simmons. Authentication theory/coding theory, Advances in Cryptology-Crypto '84, in: Lecture notes in computer science **196**, Springer Verlag, Berlin, 1985, pp 411-431.

[4] D. Pei. *Authentication Codes and Combinatorial Designs*, Discrete Mathematics and its applications, Chapman & Hall/CRC, Boca Raton, FL, 2006.

[5] S. E. Payne and J. A. Thas. *Finite Generalized Quadrangles*, Research Notes in Mathematics **110**, Pitman Advanced Publishing Program, Boston/London/Melbourne, 1984.

[6] J. Schillewaert and K. Thas. Algebraic authentication, Manuscript in preparation.

[7] D.R. Stinson. Some constructions and bounds for authentication codes, *J. Cryptology*, **1** (1988), 37-52.

[8] D.R. Stinson. A construction for authentication and secrecy codes, *J. Cryptology*, **2** (1988), 199-127.

[9] D.R. Stinson. The combinatorics of authentication and secrecy codes, *J. Cryptology*, **2**, (1990), 23–49.

[10] J. A. Thas, K. Thas and H. Van Maldeghem. *Translation Generalized Quadrangles*, Series in Pure Mathematics **26**, World Scientific, Singapore, 2006.

[11] K. Thas. Translation generalized quadrangles for which the translation dual arises from a flock, *Glasgow Math. J.* **45** (2003), 457–474.

[12] K. Thas. *Symmetry in Finite Generalized Quadrangles*, Monograph, Frontiers in Mathematics **1**, Birkhäuser, 2004.

[13] K. Thas. A stabilizer lemma for translation generalized quadrangles, *European J. Combin.* **28** (2007), 1–16.