

Geometric authentication codes

J. Schillewaert

Department of Pure Mathematics and Computer Algebra
Ghent University

September 21, 2007 / Contact forum

What is authentication?

- Alice and Bob share a secret private Key K .
- Alice sends to Bob: Source state S and $M=e(S,K)$.
- Bob receives S and M and checks if $M=e(S,K)$.
- Goal for an opponent: Produce a pair $(S,e(S,K))$.

Message authentication codes

A message authentication code (MAC) is a 4-tuple $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$ with

- 1 \mathcal{S} a finite set of source states.
- 2 \mathcal{M} a finite set of messages.
- 3 \mathcal{K} a finite set of keys.
- 4 For each $K \in \mathcal{K}$, we have an authentication rule $e_K \in \mathcal{E}$ with $e_K : \mathcal{S} \rightarrow \mathcal{M}$.

Security of a MAC-Perfect MAC

- Let p_i denote the probability of an attacker to construct a pair $(s, e_K(s))$ without knowledge of the key K , if he only knows i different pairs $(s_j, e_K(s_j))$.
- If a MAC has attack probabilities $p_i = 1/n_i$ ($0 \leq i \leq l$) then $|\mathcal{K}| \geq n_0 \cdots n_l$. If equality holds, the MAC is called perfect.
- For perfect MAC's: $|\mathcal{S}| \leq \frac{n_{l-1}n_l-1}{n_l-1} + l - 1$.

Important issues of MAC's

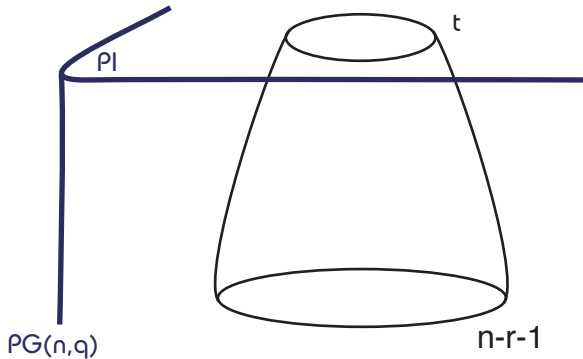
- We assume a uniform distribution for the encoding rules.
- Cartesian: $\mathcal{M}(s_1) \cap \mathcal{M}(s_2) = \emptyset$.
- Perfect authentication schemes are in 1-1 correspondence with certain designs.
- Impersonation and substitution attack.
- Replay attack.

Gilbert-MacWilliams-Sloane

Fix an r -space Π in $PG(n, q)$.

- Source states: t -spaces in Π .
- Encoding rules: $(n - r - 1)$ -spaces skew from Π .
- Messages: $(n - r + t)$ -subspaces intersecting Π in a t -space.

Gilbert-MacWilliams-Sloane II



A problem with MAC's

- Stockbroker and customer.
- Disputes about orders.
- How to decide in case of such a dispute?

What are arbitration schemes?

- Alice and Bob don't trust each other.
- A trusted arbiter is needed.
- Bob gives a decoding rule to the arbiter.
- The arbiter gives an encoding rule to Alice.

Arbitration codes

A message authentication code with arbitration A^2 -code consists of

- \mathcal{S} : a set of source states.
- \mathcal{M} : a set of encoded messages.
- $\mathcal{E}_{\mathcal{T}}$, a set of encoding rules : 1-1 mappings from \mathcal{S} to \mathcal{M} .
- $\mathcal{E}_{\mathcal{R}}$, a set of decoding rules: mappings from \mathcal{M} to \mathcal{S} or reject.

Security of a MAC with arbitration

- Probabilities for the opponent P_{O_i} .
- If dispute between Alice and Bob, then arbiter takes a decision.
- Probability for the sender P_T .
- Probabilities for the receiver P_{R_i} .

Combinatorial bounds

Theorem

We have the following lower bounds for the number of encoding and decoding rules.

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

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

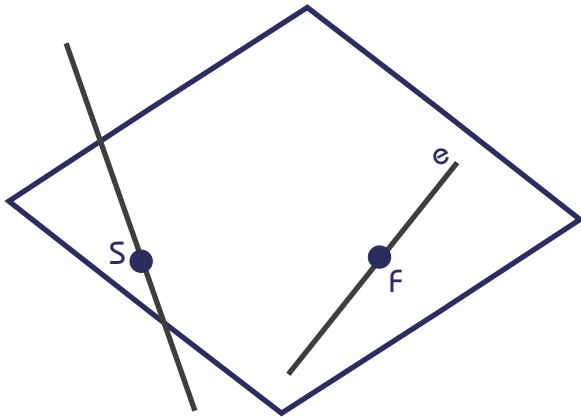
If equality holds in both inequalities above, then we call the arbitration scheme *t-fold perfect*.

A first scheme with arbitration I (T. Johansson)

Fix a line L_0 in $PG(3, q)$.

- Source states: Points on L_0 .
- Receiver's decoding rule: Point F not on L_0 .
- Transmitter's encoding rule: A line e not intersecting L_0 .
- Messages: planes spanned by a source state S and an encoding rule e .
- e valid under F if F on e .

A first scheme with arbitration II



Generalized dual arcs

- A generalised dual arc \mathcal{D} of order l with dimensions $d_1 > d_2 > \dots > d_{l+1}$ of $PG(n, q)$ is a set of subspaces of dimension d_1 such that:
 - 1 each j of these subspaces intersect in a subspace of dimension d_j , $1 \leq j \leq l + 1$,
 - 2 each $l + 2$ of these subspaces have no common intersection.

Definition

A generalised dual arc of order l with parameters $(n = d_0, \dots, d_{l+1})$ is *regular* if, in addition, it satisfies the property that if π is the intersection of j elements of \mathcal{D} , $j \leq l$, then π is spanned by the subspaces of dimension d_{j+1} which are the intersections of π with the remaining elements of \mathcal{D} .

Use of a GDA to construct a MAC

Theorem

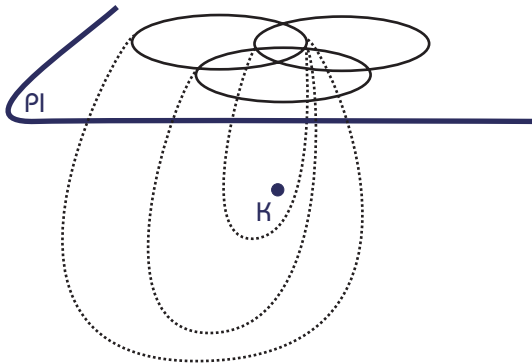
(A. Klein, J.S., L. Storme) Let Π be a hyperplane of $PG(n + 1, q)$ and let \mathcal{D} be a generalised dual arc of order l in Π with parameters (n, d_1, \dots, d_{l+1}) .

The elements of \mathcal{D} are the source states and the points of $PG(n + 1, q)$ not in Π are the keys. The message that belongs to a source state and a key is the generated $(d_1 + 1)$ -dimensional subspace.

This defines a perfect MAC with attack probabilities

$$p_i = q^{d_{i+1} - d_i}.$$

Use of a GDA to construct a MAC



Use of a GDA to construct a MAC with arbitration

Theorem

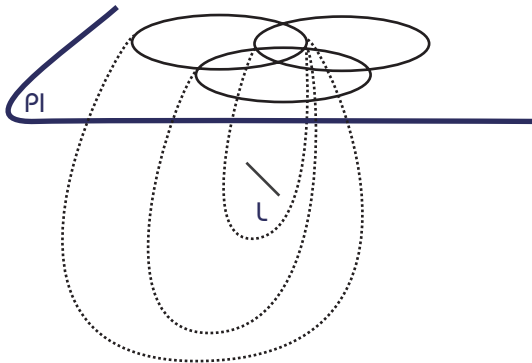
(A. Klein, J.S., L. Storme) Let Π be a codimension 2 space of $PG(n+2, q)$ and let \mathcal{D} be a generalised dual arc of order l in Π with parameters (n, d_1, \dots, d_{l+1}) .

The elements of \mathcal{D} are the source states and the lines of $PG(n+2, q)$ skew to Π are the keys. The message that belongs to a source state and a key is the generated $(d_1 + 2)$ -dimensional subspace.

This defines a perfect MAC with attack probabilities

$$p_{O_i} = q^{d_{i+1} - d_i}, \quad p_T = \frac{1}{q+1}, \quad p_{R_i} = q^{d_{i+1} - d_i}.$$

Use of a GDA to construct a MAC with arbitration



Examples of a GDA I

- The mapping $\zeta : PG(2, q) \rightarrow PG(5, q)$ with

$$\zeta([x_0, x_1, x_2]) = [x_0^2, x_1^2, x_2^2, x_0x_1, x_0x_2, x_1x_2]$$

defines the quadratic Veronesean V_2^4 .

- This defines a configuration of $q^2 + q + 1$ planes in $PG(5, q)$ such that
 - They generate $PG(5, q)$.
 - Each two intersect in a point.
 - Each three are skew.

Examples of a GDA II

- Consider the map $\zeta : PG(2, q) \rightarrow PG(9, q)$ with

$$\zeta([x_0, x_1, x_2]) = [x_0^3, x_1^3, x_2^3, x_0^2 x_1, x_0^2 x_2, \dots, x_2^2 x_1, x_0 x_1 x_2]$$

- This defines a configuration of $q^2 + q + 1$ 5-dimensional spaces in $PG(9, q)$ such that
 - Each two intersect in a plane
 - Each three in a point
 - Each four are skew.

Construction of a GDA I

- $PG(V)$ resp. $PG(W)$ a d -dimensional resp. $\binom{d+l+1}{l+1} - 1$ -dimensional space.
- We define $\zeta : PG(V) \rightarrow PG(W)$ by

$$\zeta : \left[\sum_{i=0}^d x_i e_i \right] \mapsto \left[\sum_{0 \leq i_0 \leq \dots \leq i_l \leq d} x_{i_0} \cdot \dots \cdot x_{i_l} e_{i_0, \dots, i_l} \right].$$

- For each $x \in V$, we denote by x^\perp the subspace of V perpendicular to x with respect to b . So

$$x^\perp = \{y \in V \mid b(x, y) = 0\}.$$

Construction of a GDA II

- For each point $P = [x]$ of $PG(V)$, we define a subspace $D(P)$ of $PG(W)$ by

$$D(P) = \{[z] \in W \mid B(z, \zeta(y)) = 0 \text{ for all } y \in x^\perp\}. \quad (1)$$

Theorem

The set $\mathcal{D} = \{D(P) \mid P \in PG(V)\}$ is a regular generalised dual arc with dimensions $d_i = \binom{d+l+1-i}{l+1-i} - 1$.

A characterization of Veronesean surfaces

Theorem

(J. A. Thas-H. Van Maldeghem) Let \mathcal{F} be a set of $\frac{q^{n+1}-1}{q-1}$ n -dimensional spaces generating $PG(N = \frac{n(n+3)}{2}, q)$, such that

- 1 two distinct elements of \mathcal{F} intersect in a point,
- 2 three distinct elements of \mathcal{F} have an empty intersection.
- 3 Two technical conditions which can be dropped in some cases.

Then \mathcal{F} consists of V_{n-1} subspaces to a Veronesean surface $V_n^{2^n}$ if q is odd, if q is even there is also an exception with the nucleus subspace.

Extension result on Veronesean surfaces

Theorem

(A. Klein, J.S., L. Storme) A set of $\frac{q^{n+1}-1}{q-1} - \delta$ n -dimensional spaces in $PG(N = \frac{n(n+3)}{2}, q)$ satisfying the above properties can always be extended if $\delta \leq \frac{q}{2} - 1$.

Algebraic characterisation of the GDA $(9, 5, 2, 0)$

Theorem

Every regular generalised dual arc \mathcal{D} with parameters $(9, 5, 2, 0)$ in $PG(9, q)$, $q > 3$, q odd, which contains $q^2 + q + 1$ elements, is isomorphic to the one given in the construction.

Corollary

A regular generalised dual arc in $PG(9, q)$, $q > 3$, q odd, with parameters $(9, 5, 2, 0)$ contains at most $q^2 + q + 1$ elements.

More general algebraic characterisation

We work inductively.

- Basic step: Theorem of Thas-Van Maldeghem.
- We get generalised dual arcs with missing elements in the subspaces.
- Find the remaining elements in these subspaces using our result.

Generalized quadrangles

A GQ of order (s, t) is an incidence structure $S = (P, B, I)$ for which I is a symmetric point-line incidence relation satisfying the following axioms.

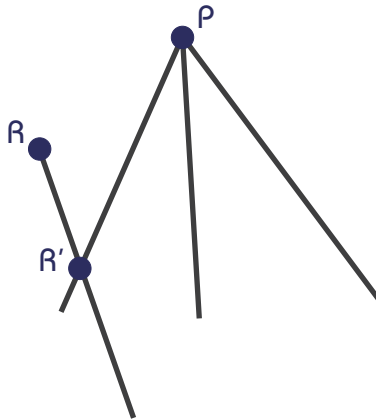
- (GQ1) Each point is incident with $t + 1$ lines ($t \geq 1$) and two distinct points are incident with at most one line.
- (GQ2) Each line is incident with $s + 1$ points ($s \geq 1$) and two distinct lines are incident with at most one point.
- (GQ3) If p is a point and L is a line not incident with p , then there is a unique point-line pair (q, M) such that $pIMlqL$.

A scheme by Desoete using GQ's

Take a fixed point p in a GQ.

- Source states: Lines through p .
- Encoding rules: Points not collinear with p .
- Messages: The points of $p^\perp \setminus \{p\}$.

A scheme by Desoete



An A-scheme using ovoids in subGQ's (JS-K.Thas)

Consider a set $\{S_1, \dots, S_r\}$ of $r > 0$ distinct subGQs of order $(s, \frac{t}{s})$ of the GQ S of order $(s > 1, t > 1)$

- Source states: subGQs S_j .
- Keys: Points in $S \setminus \cup_{i=1}^r S_i$.
- Messages: Ovoids in the GQs S_j subtended by a point outside their union.
- This yields 1-fold perfect schemes with very good p_0 .

Several schemes

All kinds of geometries and combinatorial structures can be used.

- Unitary and symplectic space.
- Latin squares.
- Rational normal curves.
- ...