Essentially ℓ-fold secure authentication systems

Albrecht Beutelspacher
Justus Liebig-Universität Gießen
Mathematisches Institut
Arndtstr. 2
D-6300 Gießen

Ute Rosenbaum
Siemens AG
ZFE IS SOF 4
Otto Hahn-Ring 6
D-8000 München 83

Abstract

In this paper we first introduce the notion of essentially ℓ-fold secure authentication systems; these are authentication systems in which the Bad Guy's chance to cheat after having observed ℓ messages is – up to a constant – best possible. Then we shall construct classes of essentially ℓ-fold secure authentication systems; these systems are based on finite geometries, in particular spreads and quadrics in finite projective spaces.

1. Introduction

An **authentication system A** consists of an set **S** of **source states**, a set **K** of **keys**, and a set **M** of authenticated **messages** along with a mapping e: $\mathbf{S} \times \mathbf{K} \to \mathbf{M}$. The mapping e together with the keys defines a set E of different **encoding rules**.
For a subset **M'** of **M** we denote by E(**M'**) the set of encoding rules which have all $m \in \mathbf{M}'$ as possible messages.

In the authentication systems which we are going to deal with every message uniquely determines its source state. These authentication systems offer no secrecy. They were first studied by Gilbert, MacWilliams and Sloane [5].

In this paper we investigate the security of authentication system with respect to spoofing attacks of order ℓ. This means that a Bad Guy has observed ℓ messages authenticated with the same key. He is looking for the maximum probability in order to substitute another message.

I.B. Damgard (Ed.): Advances in Cryptology - EUROCRYPT '90, LNCS 473, pp. 294-305, 1991.

We define p to be the maximum of the probabilities $p_0, \ldots, p_\ell$, where p_i is the probability of success when the Bad Guy has observed i different messages. Furthermore, we define the real number n by $n = 1/p$. We call n the **ℓ-order** of the authentication system **A**.

We assume throughout that the source states and the keys are equally distributed and independent.

Fåk [5] has proved the following result. *Let* **A** *be an authentication system without secrecy, in which the source states are uniformly distributed. If* ℓ *messages are observed, then*

$$p := \max\{p_0, \ldots, p_\ell\} \geqq |E|^{-1/(\ell+1)};$$

equality holds if and only if

$$|E(M')| = |E|^{(\ell+1-i)/(\ell+1)}$$

for any $M' \subset M$, $|M'| = i$, $i = 0, \ldots, \ell+1$, *where the* $m \in M'$ *belong to different source states.*

Definition. The authentication system **A** is called **ℓ-fold secure** if equality holds in the above result. A 1-fold secure system is also called **perfect** according to Simmons [8] (see also [4]).

In an ℓ-fold secure authentication system one has $p = |E|^{-1/(\ell+1)}$ and so its ℓ-order can be computed as $n = |E|^{1/(\ell+1)}$. Moreover, it follows that n is an integer. (*In fact,* $n = |E|^{1/(\ell+1)} = |E(M')|$ for any ℓ-subset M' of M.)

Definition. Let **A** be an authentication system and m be a fixed message. Then the **derivation A_m** of **A** with respect to m is defined as:
The set S_m of *source states* of A_m consists of the source states of **A** except for the source state belonging to m. The set E_m of *encoding rules* consists of the encoding rules of **A** under which m is a possible message, i.e. $E_m = E(m)$. The set M_m of *messages* consists of the messages of **A** which are possible under an encoding rule of E_m and a source state of S_m.

1.1 Lemma. *If* m *is a message in an* ℓ*-fold secure authentication system* **A**, *then* A_m *is an* $(\ell-1)$*-fold secure authentication system.*

The proof is a direct consequence of the definition.□

1.2 Lemma. *The number* σ *of source states in a* ℓ*-fold secure authentication system of* ℓ*-order* n *is at most* $n+\ell$.

Proof. In [2] it was proved that the number of source states in a 1-fold secure authentication system is at most $1/\sqrt{|E|}+1 = n+1$. Thus, the assertion follows in view of Lemma 1.□

For $\ell = 1$ and $\ell = 2$ there exist examples satisfying $\sigma = n+\ell$. We shall show that equality in the case $\ell = 2$ implies that n is an *even* integer. Consequently, if in an ℓ-fold secure authentication system one has $\sigma = n+\ell$ and $\ell \geqq 2$, then n must be an even integer. For $\ell > 2$ one can construct examples with $\sigma = n+1$. Recently Mitchell, Walker and Wild [7] have investigated ℓ-fold secure authentication systems with maximum number of source states.

ℓ-fold secure authentication systems have two disadvantages: They have very few source states compared to the number of keys. Also they seem to be very rare. For this reasons we introduce the notion of an essentially ℓ-fold authentication system.

Definition. Let C be a class of infinitely many authentication systems such that any two members of C have a different number of keys. Thus we can use the number of keys as index for the elements of C:

$$C = \{\mathbf{A}_k \mid k = \text{number of keys in } \mathbf{A}_k\}.$$

We say that C consists of **essentially ℓ-fold secure authentication systems,** if there is a constant c such that

$$p \leqq c \cdot k^{-1/(\ell+1)}$$

for any authentication system $\mathbf{A}_k$ in C. We shall call a single authentication system **essentially ℓ-fold secure** if it is clear from the context in which essentially ℓ-fold secure class it is contained.

We believe that the above definition is quite useful, since it covers classes of authentication systems which are still unconditional secure, but for which there is a much larger flexiblity to construct them than ℓ-fold secure authentication systems in the strong sense.

Note, that we use the term "essentially secure" in a stronger sense as in [1,2,3].

3.1 Lemma. *Let* $C = \{A_q \mid q \text{ some index}\}$ *be a class of essentially* ℓ*-fold secure authentication systems with* $p \leqq c^* \cdot 1/q$ *for any authentication system* A_q. *Then for each* A_q *we have for the number of keys* k

$$k \geqq a \cdot q^{\ell+1}$$

with a constant a *independent from* q *and* k.

Proof. By Fåk [5] the probability of deception p is larger than $k^{-1/(\ell+1)}$ Hence

$$k^{-1/(\ell+1)} \leqq p \leqq c^{*} \cdot 1/q .$$

So, $k \geqq c^{*-(\ell+1)} \cdot q^{\ell+1}$.□

We present three classes of examples for essentially secure authentication systems. These examples are based on partial spreads and quadrics in finite projective spaces. Finally we shall deal with implementational aspects.

2. The maximum number of source states in a 2-fold secure authentication system

2.1 Theorem. *Let* A *be a 2-fold secure authentication system, denote by* σ *its number of source states. Then* $\sigma \leqq n+2$. *If* $\sigma = n+2$, *then* n *must be even.*

Sketch of the proof. It is easy to see that $\sigma \leqq n+2$. Suppose therefore that $\sigma = n+2$. One first shows certain regularity conditions: Every source state is on exactly n messages, every message is on exactly n^2 keys, etc.. Then it is possible to prove that any two keys share either 0 or exactly 2 messages. Using this, it follows that n must be even. □

Example of a 2-fold secure authentication system with n + 2 messages (cf. [2]). Fix a point P_0 in a 3-dimensional projective space **P** of even order n. Since n is even, there is a set S of n + 2 lines through P_0 such that no three of which are in a common plane. Define S to be the source states, where the keys are the n^3 planes not through P_0 and the messages are the points $\neq P_0$ on the lines of S. This yields a 2-fold secure authentication system.

Remark. If, in the above example, we choose *all* lines through P_0 as source states, then the resulting authentication system is not essentially 2-fold secure. Indeed, if the Bad Guy has observed two messages P, Q (belonging to the source states P_0P and P_0Q), he knows that the key is a plane through the line PQ. Thus he is able to authenticate any source state L which is a line through P_0 intersecting PQ in a point $R \neq P, Q$. Then R is the message belonging to the source state L.

3. Some classes of essentially ℓ-fold secure authentication systems

Example 1 (cf. [2]). Consider a hyperbolic quadric Q (ruled quadric) in **P** = PG(3,q), the 3-dimensional projective space of odd order q. The following facts are well known (cf. [6]):

- Q is covered by two sets R and R', each consisting of q + 1 skew lines. The set R is called a **regulus**.

- Every plane of **P** intersects Q either in two lines or in an **oval** (that is a set of $q+1$ points no three of which are collinear).
- There are sets S of q^2-q skew lines such that $S \cup R$ is a **spread** that is a set of skew lines covering all points of **P**.

We shall construct an authentication system **A**(q) for any prime power q. Denote by $S \cup R$ a spread in **P** = PG(3,q), where R is a regulus. The *source states* are the lines of S, the *keys* are the points on the lines of R, and the *messages* are the planes through the source states.

3.1 Theorem. *Let* **A**(q) *be the above defined authentication system.*
(a) **A**(q) *has* q^2-q *source states and* $(q+1)^2$ *keys.*
(b) $p_0 = 1/(q+1)$, $p_1 = 2/(q+1)$.
(c) **A**(q) *is essentially* 1*-fold secure.*

Proof. (b) Since each of the $q+1$ planes through a source state contains the same number $q+1$ of keys, we have $p_0 = 1/(q+1)$. Assume that the Bad Guy knows a message m, that is a plane through a source state S_m. This plane intersects the set of keys in an oval, and the actual key is one point of the oval. Assume now that the Bad Guy wants to authenticate a source state $S^* \neq S_m$. The line S^* intersects m in a point X. For the Bad Guy it is sufficient to find a line L through X in m containing the actual key. (Then $<S^*,L>$ is the message.) Since any line of m through X contains at most two keys, his chance p_1 of success is at most $2/(q+1)$.

(c) follows with $c = 2$. □

Note, that in **A**(q) the number of source states has the same order of magnitude as the number of keys.

Now we change roles. Let Q be as above. Define **A'**(q) as follows. The *source states* are the lines of R, the *keys* are the points outside R, and the *messages* are the planes containing a line of Q.

3.2 Theorem. *Let* **A'**(q) *be the above defined authentication system.*
(a) **A'**(q) *has* $q+1$ *source states and* q^3-q *keys.*
(b) $p_0 = 1/(q+1)$, $p_1 = 1/q$, $p_2 = 1/(q-1)$.
(c) **A'**(q) *is essentially* 2*-fold secure.*

Proof. (b) The fact that $p_0 = 1/(q+1)$ follows as above. Assume now that the Bad Guy knows a message m, that is a plane through a line S_m of R. This plane intersects the points of the lines of R in two lines S_m and T. The line T contains exactly one point of any source state. Suppose that the Bad Guy wants to authenticate $S^* \neq S_m$, which intersects m in a point $X \neq S_m \cap T$ of T. Observe, that T contains no key, but any of the q lines $\neq T$ through X contains exactly $q-1$ keys. Thus, $p_1 = 1/q$.

Finally, assume that the Bad Guy has observed two messages m and m' with source states S_m and $S_{m'}$. The planes m and m' intersect in a line L. Since the actual key is a point of L, L must contain at least one, hence exactly $q-1$ keys. The remaining two points of L are points of S_m and $S_{m'}$, respectively. It follows that any other source state S^* is a line skew to L. Thus, in order to authenticate S^*, the Bad Guy has to choose one of the $q-1$ keys on L, which gives $q-1$ distinct planes through S^*. Hence $p_2 = 1/(q-1)$.

(c) For $c \geqq 6^{1/3}$ it follows

$$1/(q-1) \leqq c \cdot (q^3-q)^{-1/3}$$

for any $q \geqq 2$. □

Remark. We have not only proved that $A'(q)$ is essentially 2-fold secure; it satisfies the following stronger condition: Given *any* two messages, the Bad Guy has only a chance of $1/(q-1)$ to authenticate any third source state. (Note that "essentially 2-fold secure" only means, that, given a *randomly chosen* pair of messages, the Bad Guy has a certain chance to cheat.)

We will review the examples constructed in [3] using quadrics. It will turn out that these examples are essentially ℓ-fold secure authentication systems with large ℓ.

Example 2 (cf. [3]). Consider the quadrics Q in $P = PG(d,q)$, q even, with the following properties:

- Q does not contain the point $N = (1,0,\ldots,0)$,
- any line through N intersects Q in exactly one point.

It is easy to check that these are exactly those quadrics satisfying an equation of the following type

$$f(x) = x_0^{\,2} + \sum_{1 \leq i \leq j \leq d} a_{ij} \cdot x_i \cdot x_j = 0$$

with $a_{ij} \in GF(q)$.

Now we can define an authentication system $A_d(q)$ as follows. The *source states* are all lines through N and the *keys* are all quadrics of the above defined form. The *message* belonging to a source state S and a key K is the unique point of intersection of the line S with the quadric K. This authentication system contains $q^{d(d+1)/2}$ keys and $q^{d-1} + q^{d-2} + \ldots + q + 1$ source states; it is essentially $[d(d+1)/2-1]$-fold secure. We shall first deal with the case $d = 2$.

3.3 Theorem. *Let* $\mathbf{A_2(q)}$ *be the above defined authentication system for* $d = 2$. *Then* $\mathbf{A_2(q)}$ *has* $q + 1$ *source states and* $k = q^3$ *keys. It is 2-fold secure.*

Proof. Since $d = 2$ these quadrics have the equation

$$f(x) = x_0^2 + a_{11} \cdot x_1^2 + a_{22} \cdot x_2^2 + a_{12} \cdot x_1 \cdot x_2 = 0, \text{ where } a_{ij} \in GF(q).$$

Each of the a_{ij} could be any of the q elements of GF(q), so the number of keys (which are all possible quadrics of the above form) is q^3. The message, belonging to a source state S, could be any of the q points $\neq$ N on S. This is also true, if one message, that is a point $\neq$ N of **P**, is known. Thus, $p_0 = 1/q$ and $p_1 = 1/q$. Suppose, two messages P and Q, belonging to the source states S_P and S_Q, are known. If S^* is an arbitrary source state different from S_P and S_Q, then there exists exactly one quadric through each point $\neq$ N of S^*, which yields $p_2 = 1/q$.

We have $p := \max\{p_0, p_1, p_2\} = 1/q = k^{-1/3}$, so $\mathbf{A_2(q)}$ is 2-fold secure in the strong sense.

3.4 Theorem. *Let* $\mathbf{A_d(q)}$ *be the above defined authentication system.*
(a) $\mathbf{A_d(q)}$ *has* $q^{d-1} + q^{d-2} + \ldots + q + 1$ *source states and* $q^{(d+1)d/2}$ *keys.*
(b) $\mathbf{A_d(q)}$ *is essentially* $[d(d+1)/2-1]$*-fold secure.*

Proof. (a) Each set of different a_{ij}'s, $1 \leqq i \leqq j \leqq d$, yields different quadrics of the type

$$f(x) = x_0^2 + \sum_{1 \leq i \leq j \leq d} a_{ij} \cdot x_i \cdot x_j = 0 .$$

Since the number of points i,j with $1 \geqq i \leqq j \leqq d$ is $(d+1)d/2$ and each a_{ij} can take q different values, the number of keys of $\mathbf{A_d(q)}$ is $q^{(d+1)d/2}$.

In $\mathbf{P} = PG(d,q)$ there are $q^{d-1} + q^{d-2} + \ldots + q + 1$ lines through a point, so the number of source states is $q^{d-1} + q^{d-2} + \ldots + q + 1$.

(b) As for $\mathbf{A_2(q)}$ it follows that $p_0 = 1/q$, $p_1 = 1/q$ and $p_2 = 1/q$. Let us first compute p_3.

Suppose that two messages P and Q belonging to the source states S_P and S_Q are known. Denote by E the plane through S_P and S_Q. It intersects $\mathcal{Q}$ in a quadric $\mathcal{Q}'$. Since in E the quadric $\mathcal{Q}'$ has similar properties as $\mathcal{Q}$ in **P**, $\mathcal{Q}'$ is determined by any three of its points. If the Bad Guy happens to observe three messages P, Q and R, where the associated source states are in one plane, he can authenticate each of the other $q-2$ other source states in this plane.

To calculate p_3, we have to look at the definition of p_i. The probability p_i is defined as the probability that the Bad Guy succeeds in substituting a message belonging to a source state, which wasn't sent, given that he has observed i different messages. Thus

$$p_i = \sum_{M'\subseteq M, |M'|=i} p(M') \cdot \text{payoff}(M'),$$

where M is the set of messages, M' a subset of order i, and payoff(M') the probability that the Bad Guy succeeds given that he has observed the messages in M'.

The probabilty to observe a set of messages depends only on the probability of the set of source states. Also payoff(M') is constant for all M' that belong to the same set of source states S'. Hence in $A_d(q)$,

$$p_i = \sum_{S'\subseteq S, |S'|=i} p(S') \cdot \text{payoff}(S').$$

With this, we can calculate p_3. If the Bad Guy observes the messages P, Q, and R, where the corresponding source states are in a common plane, he can cheat with probability 1. In all other cases, his probability of success is only 1/q. Thus

$$\begin{aligned} p_3 &= p(S_R \subseteq <S_P,S_Q>)\cdot 1 + p(S_R \not\subseteq <S_P,S_Q>)\cdot 1/q \\ &= (q-1)/(q^{d-1}+\ldots+q-1) + (q^{d-1}+\ldots+q-1-(q-1))/(q^{d-1}+\ldots+q-1)\cdot 1/q \\ &= (q^{d-2}+\ldots+2q-1)/(q^{d-1}+\ldots+q-1) \\ &\leqq 2\cdot 1/q. \end{aligned}$$

Now we proceed to the general case and show that $p_i \leqq c\cdot 1/q$ for $i \leqq d(d+1)/2$.

If the Bad Guy can determine the intersection of the key (quadric) Q with some subspace U of PG(d,q), then each point of the quadric $Q \cap U$ is a valid authenticator. If $Q \cap U$ contains at least one message not already observed he can cheat with probability 1. In all other case the probability of cheating is 1/q.

Hence, if p^* denotes the probability that the Bad Guy cannot determine the intersection of the key with some subspace containing unobserved messages, then

$$p_i = (1-p^*)\cdot 1 + p^*\cdot 1/q \leqq (1-p^*) + 1/q.$$

It remains to show that

$$(*) \qquad p^* \geq \frac{q^n + \sum_{i=0}^{n-1} b_i q^i}{q^n + \sum_{i=0}^{n-1} a_i q^i}$$

for $a_i, b_i \in N_0$, $n \in N$, all independent from q.

(Then

$$p^* \geq \frac{q^n + \sum\limits_{i=0}^{n-1} b_i\, q^i}{q^n + \sum\limits_{i=0}^{n-1} a_i\, q^i} \geq 1 - \frac{\sum\limits_{i=0}^{n-1} (a_i - b_i)\, q^i}{q^n + \sum\limits_{i=0}^{n-1} a_i\, q^i} \geq 1 - c \cdot \frac{1}{q}$$

for a suitable c independent of q. So $p_i \leqq (1 - p^*) + 1/q \leqq (c+1) \cdot 1/q$.)

We have to calculate the probability p^* that the Bad Guy cannot determine the intersection of the quadric $\mathcal{Q}$ with some subspace U of $PG(d,q)$ containing at least one unobserved message.

The Bad Guy knows i different messages m_j, $1 \leqq j \leqq i$, i.e. points of the quadric $\mathcal{Q}$. In a t-dimensional subspace U, $t \geqq 1$, of $<m_1,\dots,m_i>$ he can determine the quadric $\mathcal{Q} \cap U$ if he knows at least n_u messages contained in U, where $n_u = (t+2) \cdot (t+1)/2 - 1$ if $N \notin U$ and $n_u = (t+1)t/2$ if $N \in U$. For this he needs at least $(t+2) \cdot (t+1)/2 - 1$ source states in a $(t+1)$-dimensional subspace or $(t+1)t/2$ source states in a t-dimensional subspace. For cheating with probability 1 the quadric $\mathcal{Q} \cap U$ must contain at least one unobserved message, in particular we must have $t \geqq 2$.

Thus,

p^* = prob (Bad Guy cannot determine the intersection of the quadric $\mathcal{Q}$ with some subspace U of $PG(d,q)$ such that $\mathcal{Q} \cap U$ contains at least one unobserved message)

$\geqq$ prob (no $(t+1)t/2$ source states are in a t-dimensional and no $(t+2)(t+1)/1-1$ source states are in a $(t+1)$-dimensional subspace of $PG(d,q)$, $t \geqq 2$)

= prob (among i points of $PG(d-1,q)$ there are no $(t+1)t/2$ in a $(t-1)$-dimensional and no $(t+2)(t+1)/2-1$ in a t-dimensional subspace for all t, $2 \leqq t < d$)

$\geqq$ prob (among i points of $PG(d-1,q)$ there are no $(t+1)$ in a $(t-1)$-dimensional subspace for all t, $2 \leqq t \leqq d$)

=: p'

because $t + 1 \leqq (t+1)t/2$ and $t + 2 \leqq (t+2)(t+1)/2 - 1$ for $t \geqq 2$.

Denote by s the minimum of $d-1$ and i. Then

$$p' = \prod_{j=2}^{s} \text{prob (the } (j+1)\text{−th point is not contained in the subspace generated by the first } j \text{ points)}$$

$$\cdot \prod_{j=s+1}^{i-1} \text{prob (the } (j+1)\text{−th point is not contained in any of the } \binom{j}{d-1}$$

$$(d-2)\text{−dimensional subspaces generated by the first } j \text{ points)}$$

$$= \prod_{j=2}^{s} \frac{\#\text{points in } PG(d-1,q) - \#\text{points in a } j-\text{dimensional space}}{\#\text{points in } PG(d-1,q) - j}$$

$$\cdot \prod_{j=s+1}^{i-1} \frac{\#\text{points in } PG(d-1,q) - \#\text{points on the} \binom{j}{d-1} (d-2)-\text{dimensional subspace}}{\#\text{points in } PG(d-1,q)}$$

$$\geqq \prod_{j=2}^{i-1} \frac{\#\text{points in } PG(d-1,q) - \binom{j}{d-1} \#\text{points in } PG(d-2,q)}{\#\text{points in } PG(d-1,q)}$$

$$= \prod_{j=2}^{i-1} \frac{q^{d-1}+q^{d-2}+\ldots+1 - \binom{j}{d-1}(q^{d-2}+q^{d-3}+\ldots+1)}{q^{d-1}+q^{d-2}+\ldots+1}$$

Because i is independent of q, we have shown (*).

So, $\mathbf{A}_d(q)$ is essentially $[d(d+1)/2-1]$-fold secure. □

Example 3 (cf. [3]). Consider the quadrics Q in $\mathbf{P} = PG(d,q)$, with the following properties:

- Q contains the point $N = (1,0,\ldots,0)$,
- $x_1 = 0$ is tangential hyperplane in N.

It is easy to verify that these are exactly those quadrics satisfying an equation of the following type

$$f(x) = x_0 \cdot x_1 + \sum_{1 \le i \le j \le d} a_{ij} \cdot x_i \cdot x_j = 0$$

with $a_{ij} \in GF(q)$.

Now we can define the authentication system $\mathbf{A'}_d(q)$ as follows. The *source states* are all lines through N not in the hyperplane $x_1 = 0$ and the *keys* are all quadrics of the above defined form. The *message* belonging to a source state S and a key K is the unique point of intersection of the line S with the quadric K different from N.

3.5 Theorem. *Let* $\mathbf{A'}_d(q)$ *be the above defined authentication system.*

(a) $\mathbf{A'}_d(q)$ *has* q^{d-1} *source states and* $q^{(d+1)d/2}$ *keys.*

(b) $\mathbf{A'}_d(q)$ *is essentially* $[d(d+1)/2-1]$-*fold secure.*

The *proof* is similar to the proof of Theorem 3.4. □

This example can be generalized in the following way.

In PG(d,q) the equation

$$f(x) = x_0 \cdot x_1^{n-1} + \phi^n(x_1,\ldots,x_d) = 0,$$

where ϕ^n is a homogeneous polynomial of degree n, represents a hypersurface T.

T has multiplicity $n-1$ at $N=(1,0,\dots,0)$. The tangent cone in N has the equation $x_1{}^{n-1} = 0$, and the number of undetermined coefficients of the above equation is $\binom{d+n-1}{n}$.

Now the authentication system can be defined as follows. The *source states* are the q^{d-1} lines of $PG(d,q)$ through N, which do not lie on the hyperplane $x_1=0$. The *keys* are the hypersurfaces with an equation of the above form. The *message* belonging to a source state S and a key K is the unique point of intersection different from N of the line S with the hypersurface K.

The authentication system is essentially ℓ-fold secure with $\ell = \binom{d+n-1}{n} - 1$.

For $n=2$ the hypersurfaces are the quadrics of Theorem 3.5.

4. Implementation

We discuss a possible implementation of the example 1 in section 3.

We represent a *point* of $P = PG(3,q)$ by its homogeneous coordinates $(x_0,x_1,x_2,x_3) \neq (0,0,0,0)$, where the x_i are in $GF(q)$, the field with q elements. Two such 4-tuples (x_0,x_1,x_2,x_3), (y_0,y_1,y_2,y_3) represent the same point if there exists an $h \in GF(q)$ with $(x_0,x_1,x_2,x_3) = h\cdot(y_0,y_1,y_2,y_3)$.

The *planes* are the sets of all points (x_0,x_1,x_2,x_3) satisfying an equation

$$a_0\cdot x_0 + a_1\cdot x_1 + a_2\cdot x_2 + a_3\cdot x_3 = 0 \ (a_i \in GF(q), \text{not all } a_i = 0).$$

Thus, we can represent any plane by a 4-tuple $[a_0,a_1,a_2,a_3]$, this 4-tuple being unique up to a factor $k \neq 0$.

The *lines* of P through the distinct points (x_0,x_1,x_2,x_3) and (y_0,y_1,y_2,y_3) consist of all the points with homogeneous coordinates

$$a\cdot(x_0,x_1,x_2,x_3) + b\cdot(y_0,y_1,y_2,y_3), \text{ with } a,b \in GF(q);$$

We represent this line by $<(x_0,x_1,x_2,x_3), (y_0,y_1,y_2,y_3)>$.

Given a line g through the points (a_0,a_1,a_2,a_3) and (b_0,b_1,b_2,b_3), and a point $P = (x_0,x_1,x_2,x_3)$ not on g, then the plane $m = [m_0,m_1,m_2,m_3]$ through g and P is obtained by solving the following system of linear equations:

$$\begin{aligned} a_0\cdot m_0 + a_1\cdot m_1 + a_2\cdot m_2 + a_3\cdot m_3 &= 0 \\ b_0\cdot m_0 + b_1\cdot m_1 + b_2\cdot m_2 + b_3\cdot m_3 &= 0 \\ p_0\cdot m_0 + p_1\cdot m_1 + p_2\cdot m_2 + p_3\cdot m_3 &= 0 \end{aligned}$$

As the set S of source states we shall take a "regular spread" in PG(3,q) with $q \equiv 3 \bmod 4$. This has the advantage that the coding of the "real" source states into the lines of S is easily performed:

Such a regular spread S can be described as follows. It consists of the lines

$$g_{h,k} = <(h,k,1,0),(-k,h,0,1)> \quad h,k \in GF(q)$$

and the line

$$g_\infty = <(1,0,0,0),(0,1,0,0)>.$$

Moreover

$$R = \{g_\infty\} \cup \{g_{k,0} | k \in GF(q)\}$$

is a regulus contained in S.

Now, if q is a prime, we can represent the source states by a tuple (h,k) of integers with $0 \leqq h < q, 0 < k < q$. The tuple (h,k) is will be encoded by the source state $g_{h,k}$. The keys are represented by a tuple (k_1,k_2) with $0 \leqq k_1, k_2 \leqq q$, where k_1 identifies the line of R and k_2 is a point of this line. A message is represented by the homogeneous coordinates of the plane, i.e. a tuple (m_0,m_1,m_2,m_3) with $0 \leqq m_i < q$, $i = 0,\ldots,3$.

To authenticate a source state with a key and to determine the source state from a message, one has only to solve a system of three linear equations.

References

[1] Beutelspacher, A., Perfect and essentially perfect authentication systems. Proc. Eurocrypt 87, Lecture notes in Computer Science **304**, p. 167-170, 1988.

[2] Beutelspacher, A., Rosenbaum U., Geometric Authentication Systems. Ratio Math. **1** (1990), 39-50.

[3] Beutelspacher, A.,Tallini, G., Zanella C., Examples of essentially s-fold secure geometric authentication systems with large s. To appear in Rend. mat. Roma.

[4] Gilbert, E.N., MacWilliams, F.J., Sloane, N.J.A., Codes which detect Deception. The Bell System Technical Journal, vol. **53**, no. 3, pp. 405-424, March 1974.

[5] Fåk, V., Repeated use of Codes which Detect Deception. IEEE Transactions in Information Theory, vol. IT-25, no. 2, pp. 233-234, March 1979.

[6] J.W.P. Hirschfeld, Finite projective spaces of three dimensions. Clarendon Press, Oxford 1985.

[7] Mitchell, C., Walker, M., Wild, P., The combinatorics of perfect authentication schemes. To appear.

[8] Simmons, G.J., Authentication Theory / Coding Theory. Proc. of Crypto 84, Lecture Notes in Computer Science **196**, pp. 411-432, 1985.