RATIO MATH. 1.
(1990), 39 - 50

Geometric Authentication Systems

Albrecht Beutelspacher(*) and Ute Rosenbaum(**)
(*) Universität Giessen-Mathematisches Institut-West Germany
(**) Siemens AG-Otto Hahn-Ring 6 - München-West Germany

1. INTRODUCTION

Suppose that Caesar wants to send a message M ("Ti amo") to Cleopatra. It is important that Cleopatra receives the message without any alteration. On the other hand, a bad guy X looks for his chance to alter M in his favour. In order to make the bad guy's life difficult, Caesar **authenticates** the message M.

For this, Caesar and Cleopatra have to agree on an authentication function f and a secret key K. The function f has M and K as its input, and the **authenticator** (also called **message authentication code**) f(M,K) as its output.

Now the procedure is as follows. Caesar sends the message M along with the authenticator A = f(M,K). Cleopatra receives a message, say M' and an "authenticator" A'. She computes $A^* = f(M',K)$. Only if $A^* = A'$ she accepts the received message as it stands.

What can a bad guy do? He wants to delete M and to insert another message M^* ("Ti odio"). Since he does not know the secret key K, he has no method to forge M, he can only try. But the bad guy's chances of success are not as bad as it may seem. Gilbert, MacWilliams and Sloane [9] have proved the following

Theorem. *Suppose that any authenticator has just one message. Assume furthermore that all messages and all keys occur with the same probability. Denote by k the total number of keys. Then, in any authentication system, the bad guy's chance of success is at least* $1/\sqrt{k}$.

An authentication system in which the bad guy's chance is exactly $1/\sqrt{k}$ is called **perfect.** In other words, in a perfect system the chance of success for a bad guy is as small as one can hope for. Gilbert, MacWilliams and Sloane [9] have constructed perfect authentication systems using projective planes (cf. sect. 2). These examples lack on the fact that there are very few messages (compared with the number of keys).

Apart from the above example, there are many other serious instances (in particular in the banking area), where authentication (and data integrity) is a necessity. So it is very important to have many good authentication systems available which enable the user to authenticate many messages. (See for instance [4] and [5].) The aim of this paper is to construct authentication systems, in particular those with 'many' messages. Some of our schemes are not perfect in a strong sense, but **essentially perfect.** By this we mean that the bad guy's chance of success is only $O(1/\sqrt{k})$. Our constructions are based on geometric structures, in particular finite projective spaces. Definitions and results can be found in [6] and [10].

In an other context, similar constructions can be found in [1]. Some of the results of this paper have shortly been described in [3].

2. Perfect systems allow only few messages

Throughout this paper we shall suppose that *any authenticator belongs to only one message.* Such systems are also called **cartesian.**

The aim of this section is to show that the example given in [8] is best possible in the sense that it has as many messages as possible.

The example (which we shall call **fundamental example**) is constructed as follows. Let P be a projective plane of order q. Fix a line l of P. Define the authentication system A as follows:

> The *messages* of A are the $q+1$ points on l,
>
> the *keys* of A are the q^2 points of P outside l,
>
> the *authenticator* belonging to message M and key K is the line of P through M and K.

It is easily shown (cf. also sect. 3) that A is a perfect system.

Consider now an arbitrary perfect authentication system A. Then the

number k of keys of A is a square number, say $k = k_1^2$ for a natural number k_1. We recall the following result (see [9], p.412).

2.1 Lemma. *Assume that* A *is a perfect authentication scheme with exactly* $k = k_1^2$ *keys. Then*

(i) *Every authenticator belongs to exactly* k_1 *keys.*

(ii) *Every message is on exactly* k_1 *authenticators.*

(iii) *Any two authenticators which belong to distinct messages have exactly one key in common.*

Now we are able to prove the following

2.2 Theorem. *Let* A *be a perfect authentication system with* $k = k_1^2$ *keys. Denote the number of messages by* m *and the number of authenticators by* a. *Then* $m \leq k_1 + 1$ *with equality if and only if* A *is the fundamental example.*

Proof. We define the incidence structure S in the following way.

The *points* of S are the messages and the keys of A,

the *lines* of S are the authenticators of A and a "special line" l.

The *incidence rules* are as follows. Any message is on the line l. A message M is on the authenticator A if there is a key K such that A is the authenticator of M under the key K. Similarly, a key K is on the authenticator A if there is a message M such that A authenticates M under the key K.

Then any two lines intersect in exactly one common point. [By our general hypothesis, any authenticator meets l uniquely. If two authenticators belong to different messages, then, by 2.1(iii), they have exactly one key in common. If they belong to the same message (but different keys), then they intersect in a unique message.] In other words, S is the dual of a "linear space". By a fundamental theorem due to de Bruijn and Erdös [7], the number b of lines of S is at least as big as the number v of points; equality holds if and only if S is a projective plane.

In our situation, this reads $a + 1 = b \leq v = k + m$. Since $a = k_1 \cdot m$ and $k = k_1^2$ it follows $k_1 . m + 1 \leq \kappa_1^2 + m$, hence

$$(k_1 - 1) \cdot m \leq k_1^2 - 1$$

Therefore $m \leq k_1 + 1$ with equality if and only if S is a projective plane.

Remark. Recently, in [12] perfect autentication schemes have been classified from a combinatorial point of view.

3. Geometric authentication systems

Definition. Let $\mathbf{P} = PG(d,q)$ be the finite projective space of dimension d and order q. Denote by **M** and **K** sets of (certain) s- and t-dimensional subspaces, respectively, with the property that any element of **K** is skew to any element of **M**.

We define the **geometric authentication system** $A = A(K, M)$ as follows:

The *keys* of A are the elements of **K**;

the *messages* are the elements of **M**;

the *authenticator* belonging to the key **K** and the message **M** is the subspace $<K,M>$ generated by **K** and **M**.

So, any authenticator is a subspace of dimension $s + t + 1$. We always denote by A the set of all authenticators, by k the total number of keys and by m the number of messages.

The maximal possible number of keys in an authenticator is computed in the following

3.1 Lemma. *Let* A *be a subspace of dimension* $s+t+1$ *and let* M *be an s-dimensional subspace of* A. *Then the number* a_t *of t-dimensional subspaces in* A *which are skew to* M *is* $q^{(s+1)(t+1)}$.

Proof. We proceed by induction on t.

If $t = 0$, then $\mathbf{P} = PG(s+1,q)$, and a_t is the number of points outside the hyperplane M of A. Hence $a_t = q^{s+1}$.

Now we assume that $t > 0$ and that the assertion is correct for t-1.

First we compute the number b_{t-1} of (t-1)-dimensional subspaces which are skew to M. Since any hyperplane contains exactly a_{t-1} of them and no distinct hyperplanes through M intersect in a (t-1)-dimensional subspace which is skew to M, we have

$$b_{t-1} = a_{t-1}(q^{s+t+1-s-1} + ... + 1) = a_{t-1}(q^t + ... + 1).$$

On the other hand, fix a (t-1)-dimensional subspace W skew to M. Through W there are $q^{s+t+1-(t-1)-1} + ... + 1$ subspaces of dimension t, $q^s + ... + 1$ of which are not skew to M. It follows

$$(q^t + ... + 1)a_t = a_{t-1}(q^t + ... + 1)q^{s+1},$$

so

$$a_t = a_{t-1}n^{s+1} = q^{(s+1)(t+1)}.$$

Now we define a very big class of geometric authentication systems.

Definition. Let W be a w-dimensional subspace of $\mathbf{P} = PG(d,q)$. Let M be a set of s-dimensional subspaces of W and denote by K the set of all t-dimensional subspaces of P skew to W.

Denote by $\mathbf{A} = A(d,w,s,t;M) = A(K,M)$ the corresponding geometric authentication system.

We shall compute the parameters of A and study the case when A is perfect.

3.2 Lemma. *Let* $\mathbf{A} = A(d,w,s,t;M)$ *be the above defined authentication system.*

(a) *The number of keys of* A *equals*

$$k_t = \frac{q^{(t+1)(w+1)} \cdot \theta_{d-w-1} \cdot ... \cdot \theta_{d-w-t-1}}{\theta_t \cdot ... \cdot \theta_0}$$

where $\theta_r = q^r + ... + q + 1$ *is the number of points in an r-dimensional projective space of order* q.

(b) *Any authenticator contains just one message and precisely* $q^{(s+1)(t+1)}$ *keys.*

Proof. (a) We proceed by induction on t.

For t = 0 we get

k_0 = number of points in P not in W = $q^{w+1}\cdot(q^{d-w-1}+\ldots+1)$.

Suppose now that the assertion is true for $t \geq 0$ and $d \geq w+t+2$. Consider the incidence structure whose points are t-dimensional subspaces skew to W and whose blocks are the $(t+1)$-dimensional subspaces skew to W. Double counting yields

$$k_{t+1}\cdot(q^{t+1}+\ldots+1) = k_t\cdot(q^{d-t-1}+\ldots+q^{w+1}).$$

Thus, the assertion follows.

(b) follows from the definition of A and in view of 3.1.

3.3 Theorem. *Suppose that* $A = A(d,w,s,t;M)$ *is a perfect authentication system. Then any two elements of* M *are disjoint. Moreover,* $w = 2s+1$ *and* $d = w+t+1 = 2s+t+2$.

Proof. Let M and M^* be two elements of M intersecting each other in a subspace of dimension $i \geq -1$.

The bad guy knows M and the corresponding valid authenticator A, which is a $(s+t+1)$-dimensional subspace through M. In order to obtain the valid authenticator for M^* he has to try all $(s+t+1)$-dimensional subspaces which are generated by M^* and a t-dimensional subspace T of A skew to M. The number of these subspaces can be computed using 3.1 as $q^{(s+1)(t+1)}/q^{(i+1)(t+1)} = q^{(s-i)(t+1)}$.

If A is perfect, then, by definition

$$k_t = q^{2(s-i)(t+1)}.$$

On the other hand, by 3.2 we have

$$k_t = q^{(t+1)(w+1)}\cdot f,$$

where $f \geq 1$ is the number of t-dimensional subspaces in a (d-w-1)-dimensional space. Therefore,

$$q^{2(s-i)(t+1)} = q^{(t+1)(w+1)}\cdot f \geq q^{(t+1)(w+1)},$$

so

$$2(s-i)(t+1) \geq (t+1)(w+1),$$

or

$$2s\text{-}2i \geq w+1 \geq 2s\text{-}i+1,$$

since $<M,M^*>$ is a subspace of W.

It follows that $i \leq -1$, so $i = -1$, which means that M and M^* are skew.

Moreover,

$$2(s+1) = 2(s\text{-}i) \geq w+1 \geq 2s+1+1,$$

and so $w = 2s+1$.

Finally, from

$$q^{2(s+1)(t+1)} = q^{2(s-i)(t+1)} = q^{(t+1)(2s+2)} \cdot f$$

it follows that $f = 1$. This means that the number of t-dimensional subspaces in a (d-w-1)-dimensional space equals 1, which implies $t = d\text{-}w\text{-}1$.

Remark. A particular important case of the above theorem is obtained when $s = 0$. We get the following example. The *messages* are the points on a line l in a $(t+2)$-dimensional projective space and the *keys* are the t-dimensional subspaces skew to l. If $t = 0$, we obtain again the fundamental example.

Another example of a geometric authentication system is obtained as follows.

Definition. Let **P** be a d-dimensional finite projective space of order q and fix a hyperplane **H** of **P**. We define the geometric authentication system $\mathbf{A_1} = \mathbf{A_1}(t,d)$ as follows:

The *messages* are the t-dimensional subspaces of **H** ($t \leq d\text{-}1$),

the *keys* are the points of **P-H.**

3.4 Theorem. *The authentication system* $\mathbf{A_1}(t,d)$ *is essentially perfect if and only if* $d = 2t+2$; *it is perfect if and only if* $d = 2, t = 0$.

Proof. In any case, the number of keys is $k = q^d$. Assume that the bad guy wants to forge an authenticated message. For this, we may assume that he has a valid authenticator A (which is a $(t+1)$-dimensional subspace of **P**), which intersects **H** in the message M. He wants to substitute M by the message M^*,

which is also a t-dimensional subspace of **H**. Since almost all t-dimensional subspaces of H are skew to M, we may assume for the moment that M and M^* are disjoint.

In the worst case, the bad guy is clever. He observes that he has not to check all keys, but only those which are points of A-H. Since there are only q^{t+1} such points, his chance of success is at least $1/(q^{t+1})$.

If our system is essentially perfect, we have therefore

$$O(1/\sqrt{q^d}) = O(1/q^{t+1}),$$

that is $d = 2t+2$.

Suppose now $d = 2t+2 > 2$. Then there are messages $M^* \neq M$ which intersect M in a subspace W of dimension $i \geq 0$. Then any hypothetical (but reasonable) authenticator A^* of M^* intersects A in a subspace of dimension $i+1$, the bad guy's chance of success is

$$1/q^{t-i} > 1/q^{t+1}.$$

So, the system is essentially perfect, not perfect in the strong sense.

Remark. The system $A_1(0,2)$ is exactly the fundamental example.

4. Partial spreads

Throughout this section, we denote by $\mathbf{P} = PG(d,q)$ the finite projective space of dimension d and order q. A **partial t-spread** of **P** is a set S of mutually skew t-dimensional subspaces of **P**. A **t-spread** of **P** is a partial t-spread S with the property that every point of **P** lies on (precisely) one element of S. It is well known that **P** has a t-spread if and only if $t+1$ divides $d+1$. Any t-spread in $PG(2t+1,q)$ has $q^{t+1}+1$ elements; a partial t-spread S of $PG(2t+1,q)$ has **deficiency** $\delta = q^{t+1}+1-|S|$. The set of points of **P** not covered by the partial t-spread S is denoted by D(S).

4.1 Theorem. *Let* S *be a partial t-spread of* $\mathbf{P} = PG(2t+1,q)$ *with* $|S| \geq 2$. *Define the authentication system* $\mathbf{A} = \mathbf{A}(S)$ *as follows:*

The **messages** *are the elements of* S;

the **keys** *are the points in* D(S);

the **authenticator** *for the message* M *under the key* K *is the* (t + 1)*-dimensional subspace* <M,K>.

If the deficiency δ of S *equals*

$$\delta = q^t + ... + q + 1,$$

then the number of messages is q^{t+1}-$q(q^{t-1} + ... + 1)$, *the total number of keys is* $(q^t + ... + 1)^2$ *and* A(S) *is essentially perfect.*

Proof. The number k of keys equals $k = \delta(q^t + ... + 1) = (q^t + ... + 1)^2$. On the other hand, any (t + 1)-dimensional subspace through an element of S has exactly δ points in common with D(S). So, the bad guy can forge a message with probability $1/\delta = 1/(q^t + ... + q + 1)$.

So, the assertion follows.

Remarks.

1. The case t = 1 is of particular interest. In the essentially perfect case, we have q^2-q messages, but only $(q + 1)^2$ keys. One example of such a system is obtained if a regulus is removed from a "regular spread" (alias an "elliptic congruence").

2. The authentication systems A(S) are only perfect if the order of P is 2. (Assume that A(S) is perfect. Then, by 2.1 (iii) any two distinct authenticators must intersect in a unique key. This means that any two (t + 1)-dimensional subspaces through distinct elements of S intersect each other in at most one point of D(S). Therefore any line joining two points of D(S) intersects at most one element of S. In other words, any such line contains at most one point of P(S), where P(S) denotes the set of points on the elements of S.

So, for a fixed point $Q \in D(S)$ we have

$q^{2t} + ... + q + 1$ = number of lines through $Q \geq |P(S)| = q^{2t+1} + ... + 1 - |D(S)|$,

therefore

$$|D(S)| \geq q^{2t+1}.$$

On the other hand, any line connecting two points on different elements on S contains at most one point of D(S). Since any point of P lies on such a line, it follows

$$| D(S) | \leq (q^t + \ldots + 1)^2.$$

Together it follows

$$q^{2t+1} \leq | D(S) | \leq (q^t + \ldots + 1)^2.$$

Consequently,

$$q^{2t+1}(q-1)^2 \leq (q^{t+1}-1)^2,$$

$$q^{2t+1}(q^2-3q+1) \leq -2q^{t+1}+1 < 0,$$

so $q = 2$.

5. The Lucky Bad Guy

In this last section we address the problem of the lucky bad guy. So far we considered our systems under the unspoken hypothesis that the same key was used only once. In other words, we assumed that a change of keys takes place after every message. Now we would like to discuss a more realistic situation in which there are several messages authenticated with the same key. Is there any security, if the bad guy knows two or more valid authenticators belonging to the same key? For most of the above discussed authentication schemes the answer is "no". (This is called a spoofing attack of order s [11]). For most of the above discussed authentication schemes the answer is "no". For instance, in the fundamental example two different authenticators determine the key uniquely.

Let us consider authentication systems in which all messages have the same number n of authenticators. Then the bad guy's chance of success is at least 1/n, since for his favourite message he simply has to choose one of the n authenticators at random. What we would like to have is that after the observation of s messages beloinging to the same key the chances of the bad guy become not better.

Under the same conditions for authentication system in [9] Fåk has shown the following:

Theoreme. *Suppose that any authenticator has just one message. Assume furthermore that all messages and all keys occur with the same probability. Denote by* k *the total number of keys. Then, in any authentication system, the bud guy's chance of succes for a spoofing attack of order* s *is at least* $1/k^{1/(s+1)}$.

For $s = 1$ this is the bound proven in [9].

An authentication system **A** in which this theoretical bound is hold is said to be **s-fold perfect.** In a s-fold perfect authentication system given any $i, 0 \leq i \leq s$ messages $m_1, ..., m_i$ authenticated by the same key, the bud guy's chance of successfully falsificating any messages $m \neq m_1, ..., m_i$ is only $1/k^{1/(s+1)}$.

A is called essentially **s-fold perfect,** if knowledge of any s authenticators belonging to the same key gives the bad guy a chance of success of $O(1/k^{1/(s+1)})$ for falsificating an authenticator of a message choosen at random out of the remaing messages.

We conclude by presenting the following authentication systems.

5.1 Theorem. *Let* $\mathbf{P} = PG(s+1,q)$ *be the* $(s+1)$*-dimensional projective space of order* q. *Fix a point* P_0 of **P**. *Define the following authentication system* **A.**

Messages are the $q^s + ... + q + 1$ lines of **P** through P_0,

keys are the q^{s+1} hyperplanes of **P** not through P_0,

the **authenticator** belonging to the message l and the key H is the point $l \cap H$. In other words, the authenticators are precisely the points $\neq P_0$ of **P**.

Then **A** is essentially s-fold perfect.

Proof. Suppose that the bad guy has observed $t \leq s$ messages $m_1, ..., m_t$ with corresponding authenticators $a_1, ..., a_t$. then the bad guy knows that the key hyperplane H interscts $< m_1, ..., m_t >$ in $< a_1, ..., a_t >$, which is a hyperplane of $< m_1, ..., m_t >$. therefore he knows that a message in $< m_1, ..., m_t >$ has as its authenticator the point $m \cap < a_1, ..., a_t >$. So, for those $\leq q^{t+1} + ... + q + 1$ messages the chance of falsificating is 1, whereas for any of the other $\geq q^s + ... + q^t$ messages the probability is only 1/q.

So, the mean probability of guessing the correct authenticator is $O(1/k^{1/(s+1)})$.

Hence **A** is essentially s-fold perfect.

5.2 Theorem. *Let* $\mathbf{P} = PG(s+1, q)$ *be the* $(s+1)$*-dimensional projective space of order* q. *Fix a point* P_0 of **P**. *Define the following authentication system* **A**.

> **Messages** *are lines of* **P** *throught* P_0 *which are in general position, that is, no* t *of them are contained in a common* (t-1)*-dimensional subspace* $(t \leq s+1)$
>
> **keys** are the q^{s+1} hyperplanes of **P** not through P_0,
>
> the **authenticator** belonging to the message l and the key H is the point $l \cap H$. In other words, the authenticators are precisely the points $\neq P_0$ of **P**.

Then **A** *is* s*-fold perfect.*

Proof.. It is clear that under the present hypotheses the situation described above cannot occur.

References

[1] A. Beutelspacher: Partial spreads in finite projective spaces and partial designs. Math. Z. 145 (1975), 211-229.

[2] A. Beutelspacher: Enciphered Geometry. Some Applications of Geometry to Cryptography. Annals of Discrete Math. 37 (1988), 59-68.

[3] A. Beutelspacher: Perfect and essentially perfect authentication systems. Extended abstract. Advances in Cryptology: Proceedings of EUROCRYPT 87 (Lecture Notes in Computer Science 304), D. Chaum and W.L. Price, Eds., Springer-Verlag 1988, 167-170.

[4] A. Beutelspacher: Kryptologie. Vieweg-Verlag, Braunschweig und Wiesbaden 1987.

[5] D.W. Davies and W.L. Price: Security for Computer Networks. John Wiley & Sons, 1984.

[6] P. Dembowski: Finite Geometries, Springer-Verlag, 1968.

[7] N.G. de Bruijn and P. Erdös: On a combinatorial problem. Indag. Math. 10 (1948), 421-423.

[8] V. Fåk: Repeated use of des which Detected Deception, IEEE Transactions in Information Theory, vol. IT-25, no. 2, pp. 233-234, March 1979.

[9] E.N. Gilbert, F.J. MacWilliams, N.J.A. Sloane: Codes which detect deception. Bell. Syst. Tech. J. 53 (1974), 405-424.

[10] J.W.P. Hirschfeld: Geometries over finite fields. Clarendon Press, Oxford 1979.

[11] J. L. Massey: Cryptography - A Selective Survey, Proc of Int. Tirrenia Workshop on Digital Communications, Tirrenia, Italy, Sept. 1985.

[12] de Soete, M. Vedder, K. Walker, M. : Cartesian Authentication schemes. To appear in Procedings of EUROCRYPT'89.