PERFECT AND ESSENTIALLY PERFECT AUTHENTICATION SCHEMES

Extended Abstract

Albrecht Beutelspacher

Siemens AG
ZT ZTI SYS 4,
D-8000 München 83
Federal Republic of Germany

Suppose that *A* wants to send a message M to *B*. It is important that *B* 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, *A authenticates* the message M.

For this, **A** and **B** 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. *A* sends the message M along with the authenticator A = f(M,K). *B* receives a message, say M'. Then *B* computes A' = f(M',K); only if A' = A, *B* accepts the received message as it stands.

What can a bad guy do? He wants to delete M and to insert another message M*. 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 are not as bad as it may seem. Gilbert, MacWilliams and Sloane [2] have proved the following

Result. Assume 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*. Gilbert, MacWilliams and Sloane [2] have constructed perfect authentication systems using projective planes (see below). These examples lack on the fact that there are very few messages (compared with the number of keys). The aim of this paper is to present many 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 projectivce spaces. Definitions and results can be found for instance in in [1].

Construction 1. Let **P** be a d-dimensional finite projective space of order n and fix a hyperplane **H** of **P**. We define the authentication system **A** = **A**(t,d) as follows:

D. Chaum and W.L. Price (Eds.): Advances in Cryptology - EUROCRYPT '87, LNCS 304, pp. 167-170, 1988.

The *messages* are the t-dimensional subspaces of **H** ($t \leqq d-1$),

the *keys* are the points of **P–H**,

the *authenticator* belonging to message M and key K is the $(t+1)$-dimensional subspace $<M,K>$.

Theorem 1. The authentication system **A**(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 $k = n^d$. 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–H**), 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 n^{t+1} such points, his chance of success is at least $1/(n^{t+1})$.

If our system is essentially perfect, we have therefore

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

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 $i \geqq 0$. 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

$$1/(n^{t-i}) > 1/(n^{t+1}).$$

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

Remark. The systems **A**(0,2) are exactly the systems constructed by Gilbert, MacWilliams and Sloane [2].

Another construction, which also yields perfect authentication systems is as follows.

Construction 2. Denote by $P = PG(s+t+1,q)$ the projective space of dimension $s+t+1$ ($s,t \geqq 0$) and order q. Fix an s-dimensional subspace U of **P**. Define the system **A**(s,t) as follows:

The *messages* are the points on U,

the *keys* are the t-dimensional subspaces of **P** which are skew to U,

the *authenticator* of the message M corresponding to the key W is the subspace $<M,W>$ of dimension $t+1$.

Theorem 2. *Let be the above defined authentication system.*

(a) *The probability of forging is* $1/(q^{t+1})$.

(b) *The system is perfect if and only* if $s = 1$.

Proof. (a) Let A be an authenticator, that is a $(t+1)$-*dimensional* subspace which intersects U in just one point M. The assertion follows since there are exactly q^{t+1} hyperplanes of A which do not contain M, that is are skew to U.

(b) It is sufficient to prove the following assertion: The number a_t of t-dimensional subspaces disjoint to U equals

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

This formula is not difficult to prove.□

Construction 3. Denote by $\mathbf{P} = PG(d,q)$ the finite projective space of dimension d and order q. A *partial* t-*spread* of $\mathbf{P}$ is a set S of mutually skew t-dimensional subspaces of P. A t-*spread* of $\mathbf{P}$ is a partial t-spread S with the property that every point of $\mathbf{P}$ lies on (precisely) one element of S. It is well known that $\mathbf{P}$ 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 $\mathbf{P}$ not covered by the partial t-spread S is denoted by $D(S)$.

Theorem 3. *Let* S *be a partial* t-*spread of* $\mathbf{P} = PG(2t+1,q)$. *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 $<M,K>$.

Claim: This authentication system is essentially perfect if and only if the definciency δ *of* S *equals* $\delta = q^t + \ldots + q + 1$. *In this case, the number of messages is* $q^{t+1} - q(q^{t-1} + \ldots + 1)$ *and the total number of keys is* $(q^t + \ldots + 1)^2$.

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

Remark. The case $t = 1$ is of particular interest. In the 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").

Construction 4. Here, we would like to 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 gay knows two or more valid authenticators belonging to the same key? For most of the above discussed authentications schemes the answer is "no". For instance, in the fundamental example [2] 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.

Such an authentication system A is said to be *s-fold secure*, if

– knowledge of any s authenticators belonging to the same key gives the bad guy only a chance of sucess of $1/n$;

– knowledge of some $s+1$ authenticators gives the bad guy a considerably better chance.

We conclude by presenting the following s-fold secure authentication system, which generalizes the (dual version) of the example constructed in [2].

Let $\mathbf{P} = PG(s+1,n)$ be the $(s+1)$-dimensional projective space of order n. Fix a point P_0 of $\mathbf{P}$.

Messages are the $n^s + \ldots + n + 1$ lines of $\mathbf{P}$ through P_0,

keys are the n^{s+1} hyperplanes of $\mathbf{P}$ not through P_0,

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

We claim that this system is s-fold secure. In fact, even if the bad guy knows s authenticators, i.e. s points $\neq P_0$, then through these points there are at least n hyperplanes which do not pass through P_0. So his chance to guess the correct key is still not better than $1/n$. On the other hand, $s+1$ points in general position uniquely determine a hyperplane.□

References

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

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