Rendiconti di Matematica, Serie VII
Volume 11 , Roma (1991), 23-29

Smart Cards and Authentication Schemes

L. BERARDI - F. EUGENI[(*)]

To Professor Giuseppe Tallini in occasion of his 60^{th} birthday

> *La prova fondamentale del valore di un Maestro è quella sorta di convincimento che Egli crea in altri uomini ai fini di proseguire ed ampliare la Sua opera.*
>
> *(Walter Lippmann, 1945)*

RIASSUNTO – *Molti sistemi crittografici attuali sono usati per l'autenticazione di messaggi elettronici, quali i trasferimenti elettronici di denaro. Ciò accade ad esempio nei sistemi che fanno ricorso alle Smart Cards. Nel 1974 Gilbert, Mac Williams e Sloane introdussero il concetto di schema di autenticazione e tra questi chiamarono "perfetti" quelli per cui la probabilità che un intruso forzi il sistema è minima. I pochi schemi perfetti noti sono stati costruiti "via Geometrie Finite". Presentiamo una nuova classe di schemi di autenticazione, tra cui vi sono schemi perfetti, ottenuti utilizzando certe strutture d'incidenze note in letteratura con il nome di disegni divisibili.*

ABSTRACT – *In this paper we construct a new class of authentication schemes based on divisible designs. Some of them are perfect.*

KEY WORDS – *Criptography - Authentication - Designs.*

A.M.S. CLASSIFICATION: 94B05

[(*)]Communicated at V Meeting "Euro Working Group on Financial Modelling", Acireale (CT) - 1989.

1 – Introduction: the idea of authentication schemes

Today many original ideas have been developed in cryptology. One of the most pervasive problems in military and in commercial communications systems is the need to authenticate digital messages [3], [4], [6], [7], [11]. For example many secure Electronic Fund Transfer nets need cryptographic systems which are connected with their protection and security against unauthorized intrusion of a bad guy. This occurs, for example, in the Smart Card's systems. According to the International Organization of Standard a Smart Card is a card, similar to a magnetic stripe card (Bancomat), but containing a micro-processor. Usually connection with the circuit is ensured through a round printed goldered patch divided in eight zones. One of these zones, the so-called secret zone, is impossible to read from outside the chip and its physical protection is assured by tecnology.

The use of smart cards for payment applications offers a very high level of security. There is a previous authentication of the cardholder using a Personal Identification Number (so called PIN) and the identification card-system, via a cryptographic algorithm.

In Italy there are not many of these Smart Cards. Recently two Italian University, namely the University of Roma "La Sapienza" and the University of Bologna introduced a Smart Card system for confidential data of their students. The design and the hardware has been studied by "ENIDATA".

Consider a transmitter who wants to send a confidential message to a remote receiver along an imperfect channel of communication. Two things can happen:

– the transmitted message can be received in error, since there is noise in the channel. This problem can be solved by the theory of error correcting codes;

– the channel may be in the hands of a bad guy who can either listen to the message during transmission and simply read it (a passive attack), or deliberately alter message in his favour introducing fraudolent ones, in such a way that the messages seem to be legitimate (an active attack). The first problem can be solved by using a cryptographic scheme, the second one can be solved by using authentication schemes.

The procedure of an authentication system runs as follows. The transmitter A and the receivėr B fix an alghoritm f and a secret key K. Then

- A sends the message M together with the authenticator $a = f(K, M)$.
- B receives a message M' and an authenticator a'.
- B computes $a^* := f(K, M')$.
- Only if $a^* = a'$, B does accept the message M' as the original.

Suppose that we have to change M and a in an illegal way. We want to delete M and to insert another message M'. Since we do not known the secret key K and $a' = f(K, M)$ is different by a we can only try! Our chances of success are not as bad as it may seem. In fact, there is the following

THEOREM (GILBERT-MAC WILLIAMS-SLOANE [11]). *Suppose that any authenticator has only one message and that all messages and all keys occur with the same probability. Denote by t the total number of keys. Then, in any authentication scheme, the chances of guessing the correct authenticator are at least $1/\sqrt{t}$.*

An authentication system in which the above chances are precisely $1/\sqrt{t}$ is called a *perfect authentication system*. Some schemes are not perfect but their chances are only $0(1/t)$. These systems are called *essentially perfect*.

A perfect geometric authentication scheme is the following. Fix a finite projective plane, for example a projective plane P over a Galois field $GF(q)$. Fix a line L. The messages are the points of L, the keys are the points of P out of L (in number of q^2). For a message M and a key K the authenticator is the line through M and K. It is easy to prove that one can try with the points of line $MK \setminus \{M\}$. So, the bad guy has to do q proves.

The next section is devoted to construct a new class of authentication systems which contains perfect authentication systems using Divisible Designs.

2 – A new authentication system via divisible designs

A *divisible design* D is a pair (S, B) where (cf. [8]):

a) S is a set of elements, called *points*, partitioned into m n-subsets $G_1, G_2, \ldots, G_m$, said *generators*.
b) B is a family of k-subsets of S.
c) Any two points x and y of S are contained in precisely s blocks if and only if they are in two different generators.

Particular cases of such a structure are the following:

- If $n = 1$ the generators are singleton and the structure is a so-called $2-(m, k, s)$ design (cf. [10]).
- Suppose $k = n$ and $s = 1$. Then the new family containing blocks and generators is a Steiner system $2-(nm, k, 1)$, (cf. [10], [12]). If b is the number of blocks of B and then r the number of blocks containing a fixed point x, then it follows:

$$r \geq sn\,, \; m \geq k\,. \tag{2.1}$$

Note that $r = sn$ if and only if $m = k$. In this case D is said to be a *transversal design*. If we count the pair (x, B) and (T, B) where T is a 2-set contained in the block B and x is a point of B we obtain:

$$b = \frac{m(m-1)n^2s}{k(k-1)} \tag{2.2}$$

$$r = \frac{n(m-1)s}{(k-1)} \tag{2.3}$$

The dual structure of the pair (S, B) is obtained by interchanging points with blocks. A divisible design D is called *symmetric* if its dual structure is a divisible design with the same parameters. Examples of divisible designs can be found in [8], [9] and [13]. Some of them are the following, which are embedded in projective spaces.

In a projective space $PG(d, q)$ over Galois field $GF(q)$ choose a point x and an hyperplane H. Removing H with all its points and point x together with all the hyperplanes containing it, we obtain two examples of symmetric divisible designs, according to whether x lies in H or not, which are of course square. The parameters are the following

$$n = q\,,\; n = q^{d-1}\,,\; k = q^{d-1}\,,\; s = q^{d-2} \text{ (if } x \text{ lies in} H)$$

or

$$n = q - 1\,,\ m = q^{d-1} + \ldots + 1\,,\ k = q^{d-1}\,,\ s = q^{d-2}\,.$$

So, if $d = 2$, we have square divisible designs with $s = 1$. We shall prove that using such designs some new perfect authentication schemes can be constructed.

Now we construct a new authentication system.

DEFINITION. *Let D be a divisible design with $s = 1$. Let the messages be the points of a fixed block M of D.*

For each message m of M let $G(m)$ be the generator through m. We define the set of keys of m as $S \setminus (MUG(m))$.

Finally for each message m and for each related key c the authenticator $a(m,c)$ is the unique block containing m and c.

REMARK. A and B fix the key K. This is a point of design D outside of the line M of the messages. If $g = G(m_0)$ is the generator containing K, we remark that A cannot send the message m_0. So, if A and B use the key K, then the possible messages are the points of $M \setminus \{m_0\}$.

Now we prove the following

THEOREM. *The geometric authentication system defined above is perfect if and only if D is a square divisible design with $s = 1$.*

PROOF. Let D be a divisible design with $s = 1$.

The total number of keys, related to a fixed message m, is:

$$t(m) = nm - (k + n - 1)$$

According to the Gilbert-Mac Williams-Sloane theorem we suppose that all messages and all keys occur with the same probability.

So, the bad guy's chances of success is at least $1/t(m)$.

On the other hand, suppose that the pair $(m, a(m,c))$ has been altered in $(m^*, a^*(m^*,c))$. The bad guy's chance of success in this case is $1/(k-1)$. It follows that $1/\sqrt{t(m)} \leq 1/(k-1)$, from which

$$t(m) \geq (k-1)^2\,.$$

This implies

$$n(m-1) \geq k(k-1),$$

where equality holds if and only if the authentication system is perfect. In this case (2.2) can be written:

$$\frac{b}{mm} = \frac{n(m-1)}{k(k-1)}.$$

Then the authentication system is perfect if and only if $b = mn$ i.e. the design is square. So, the assertion is proved.

It remains to do a more detailed study of such designs and a systematic collection of known examples.

REFERENCES

[1] L. BERARDI: *Constructing 3-designs from spreads and lines*, Discrete Math., 71 (1988), 1-2.

[2] L. BERARDI: *Some remarks about an electronic signature derived from a generalized RSA-code*, J. of Information & Opti. Sci., 1 (1990), 189-194.

[3] L. BERARDI - A. BEUTELSPACHER: *I buoni angeli custodi, ovvero i protettori di un messaggio*, Archimede 2-3 (1988), 6-16.

[4] L. BERARDI - F. EUGENI: *Strutture geometriche, crittografia e sistemi di sicurezza richiedenti un quorum*, Atti del I Simposio su "Stato e Prospettive della Ricerca Crittografica in Italia", Roma, Fondaz. Bordoni, 1987.

[5] A. BEUTELSPACHER - T. HUESKE: *Payment application with multifunctional smart cards*, Smart Card 2000 (1989), 95-101. (D. Chaum et alt. editors, North-Holland)

[6] A. BEUTELSPACHER - U. ROSENBAUM: *Geometric authentication systems*, Ratio Math., 1 (1990), 39-50.

[7] A. BEUTELSPACHER - G. TALLINI - C. ZANELLA: *Examples of essentially s-fold secure geometric authentication systems with large s*, Rend. di Mat. e appl. (Roma), to appear.

[8] R.C. BOSE: *Symmetric group divisible design with the dual property*, J. Statist. Plann. Inference, 1 (1977), 87-101.

[9] R. BOSE - W.S. CONNOR: *Combinatorial property of group divisible incomplete block design*, Ann. Math. Stat. 23 (1952), 367-383.

[10] M. CERASOLI - F. EUGENI - M. PROTASI: *Elementi di Matematica Discreta*, Zanichelli, Bologna, 1988.

[11] E.N. GILBERT - F.J. MAC WILLIAMS - N.J. SLOANE: *Codes which detect deception*, Bell Syst. Tech. J. 53 (1974), 405-424.

[12] M. GIONFRIDDO: *Sui Sistemi di Steiner*, Sem. Geom. Combin. Univ. L'Aquila, Quad. 9 (1986), 1-18.

[13] D. JUNGNICKEL - K. VEDDER: *Square divisible design with $k = (n+1)s$*, Arch. Math., 43 (1984), 275-284.

Lavoro pervenuto alla redazione il 27 gennaio 1990
ed accettato per la pubblicazione il 21 aprile 1990
su parere favorevole di A. Bichara e di R. Scozzafava

INDIRIZZO DEGLI AUTORI:

Luigia Berardi - Franco Eugeni - Dipartimento di Ingegneria Elettrica - Facoltà di Ingegneria - Università degli Studi - 67040 Poggio di Roio - L'Aquila - Italia