SOME CONSTRUCTIONS FOR AUTHENTICATION - SECRECY CODES

Marijke De Soete

Seminar of Geometry and Combinatorics
State University of Ghent
Krijgslaan, 281
B–9000 Ghent, Belgium

ABSTRACT

We deal with authentication / secrecy codes having unconditional security. Besides some new results for a "spoofing attack of order L", we give several constructions using finite incidence structures (designs, generalized quadrangles).

1 AUTHENTICATION-SECRECY

It is the aim to deal in this paper with codes having unconditional security, which means that the security is independent of the computing power. Analogously to the theory of unconditional secrecy due to Shannon [12], Simmons developed a theory of unconditional authentication [14].

Consider a transmitter who wants to communicate a source to a remote receiver by sending messages through an imperfect communication channel. Then there are two fundamentally different ways in which the receiver can be deceived. The channel may be noisy so that the symbols in the transmitted message can be received in error, or the channel may be under control of an opponent who can either deliberately modify legitimate messages or else introduce fraudulent ones. Simmons [14] showed that both problems could be modeled in complete generality by replacing the classical noisy communications channel of coding theory with a

C.G. Guenther (Ed.): Advances in Cryptology - EUROCRYPT '88, LNCS 330, pp. 57-75, 1988.

game - theoretic noiseless channel in which an intelligent opponent, who knows the system and can observe the channel, plays so as to optimize his chances of deceiving the receiver. To provide some degree of immunity to deception (of the receiver), the transmitter also introduces redundancy in this case, but does so in such a way that, for any message the transmitter may send, the altered messages that the opponent would introduce using his optimal strategy, are spread randomly. Authentication is concerned with devising and analyzing schemes (codes) to achieve this "spreading".

In the model some simplifying assumptions are made. We suppose that the transmitter and receiver trust each other completely and that neither acts to deceive the other. We also assume that only the receiver need be convinced of the authenticity of a message, so there is no third party (arbiter) involved here. In addition, we also agree that all successful deceptions of the receiver are of equal value to the opponent. We have to distinguish the authentication schemes in which the opponent knows the state of source (message authentication without secrecy) from the message authentication in situations in which the opponent is ignorant of the information being communicated to the receiver by the transmitter.

2 A MATHEMATICAL AUTHENTICATION MODEL

In this model (see [14], [15], [16], [17], [18]) there are three participants: a *transmitter*, a *receiver* and an *opponent*. The transmitter wants to communicate some information to the receiver. The opponent wanting to deceive the receiver, can either impersonate the receiver, making him accept a fraudulent message as authentic, or, modify a message which has been sent by the transmitter.

Let S denote the set of k source states, M the set of v messages and E the set of b encoding rules.

A *source state* $s \in S$ is the information that the transmitter wishes to communicate to the receiver. The transmitter and receiver will have secretly chosen an *encoding rule* $e \in E$ beforehand. An encoding rule will

be used to determine the message $e(s)$ to be sent to communicate any source state s. In a model with *splitting*, several messages can be used to determine a particular source state. However, in order for a receiver to be able to uniquely determine the source state from the message sent, there can be at most one source state which is encoded by any given message $m \in M$, for a given encoding rule $e \in E$ (this means: $e(s) \neq e(s')$ if $s \neq s'$).

An opponent will play *impersonation* or *substitution*. When the opponent plays impersonation, he sends a message to the receiver, attempting to have the receiver accept the message as authentic. When the opponent plays substitution, he waits until a message m has been sent, and then replaces m with another message m', so that the receiver is misled as to the state of source. More generally, an opponent can observe i (≥ 0) distinct messages being sent over the channel knowing that the same key is used to transmit them, but ignoring this key. If we consider the code as a secrecy system, then we make the assumption that the opponent can only observe the messages being sent. Our goal is that the opponent be unable to determine any information regarding the i source states from the i messages he has observed.

The following scenario for authentication is investigated. After the observation of i messages $M' \subset M$, the opponent sends a message m' to the receiver, $m' \notin M'$, hoping to have it accepted as authentic. This is called a *spoofing attack of order* i [9], with the special cases $i = 0$ and $i = 1$ corresponding respectively to the impersonation and substitution game. The last games have been studied extensively by several authors (see [4], [6], [13], [14], [16]).

For any i, there will be a probability on the set of i source states which occur. We ignore the order in which the i source states occur, and assume that no source state occurs more than once. Also, we assume that any set of i source states has a non-zero probability of occurring. Given a set of i source states, we define $p(S)$ to be the probability that the source

states in S occur.

Given the probability distributions on the source states described above, the receiver and transmitter will choose a probability distribution for E, called an *encoding strategy.* If splitting occurs, then they will also determine a *splitting strategy* to determine $m \in M$, given $s \in S$ and $e \in E$ (this corresponds to non-deterministic encoding). The transmitter/receiver will determine these strategies to minimize the chance that an opponent can deceive them.

Once the transmitter/receiver have chosen encoding and splitting strategies, we can define for each $i \geq 0$ a probability denoted P_{d_i}, which is the probability that the opponent can deceive the transmitter/receiver with a spoofing attack of order i.

In this paper, we consider only codes without splitting. We shall use the following notation. Given an encoding rule e, we define $M(e) = \{e(s) \mid s \in S\}$, i.e. the set of messages permitted by encoding rule e. For a set M' of distinct messages, and an encoding rule e, define $f_e(M') = \{s \mid e(s) \in M'\}$, i.e. the set of source states which will be encoded under encoding rule e by a message in M'. Define also $E(M') = \{e \in E \mid M' \subseteq M(e)\}$, i.e. the set of encoding rules under which all the messages in M' are permitted. It is useful to think of a code as being represented by a $b \times k$ matrix A, where the rows are indexed by encoding rules, the columns are indexed by source states and the entry in row e and column s is $e(s)$. We can also define a $b \times v$ incidence matrix X in which the rows represent the encoding rules, the columns the messages and the entry on row e and column m is 0 or 1 according $m \notin M(e)$ or $m \in M(e)$.
Finally we denote by $AC(k, v, b)$ an authentication system with k source states, v messages and b encoding rules.

Example. Consider the following code on 2 source states using 4 encoding rules given by:

$$A = \begin{pmatrix} s_1 & s_3 \\ s_2 & s_4 \\ s_1 & s_4 \\ s_2 & s_3 \end{pmatrix} \text{ and } X = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

This is the "best" authentication system possible for $k = 2$, $b = 4$, since we have $P_{d_0} = P_{d_1} = 1/2 = 1/\sqrt{b}$.

3 BOUNDS ON P_{d_i}

Many of the bounds on P_{d_i} depend on entropies of the various probability distributions. For a probability distribution on a set X, we define the *entropy* of X, $H(X)$ as follows:

$$H(X) = -\sum_{x \in X} p(x) \cdot log\, p(x).$$

As well, the conditional entropy $H(X/Y)$ is defined to be

$$H(X/Y) = \sum_{y \in Y} \sum_{x \in X} p(y) \cdot p(x) \cdot log\, p(x/y).$$

Theorem 3.1 (Simmons [14]) *In an authentication system without splitting $P_{d_0} \geq k/v$.*

Theorem 3.2 (Simmons [14]) *In any authentication system $P_{d_0} \geq 2^{H(MES)-H(E)-H(M)} = 2^{H(M/ES)+H(S)-H(M)}$. In an authentication system without splitting $H(M/ES) = 0$, so $P_{d_0} \geq 2^{H(S)-H(M)}$.*

An authentication system which satisfies the bound of this theorem with equality is said to be *perfect.*

In a perfect authentication code without splitting, the following properties hold (Brickell [4]):

1. for all messages m, $P_{d_0} = \Sigma_{\{e \in E(m)\}}\, p(e) = k/v$
2. for any message m, $p(s)$ is constant for all s such that there is an e such that $e_s = m$.

The following bound is for substitution with secrecy.

Theorem 3.3 (Brickell [4], Simmons [14]) *In any authentication system* $P_{d_1} \geq 2^{-H(E/M)} = 2^{H(M)-H(E)-H(S)+H(M/ES)}$. *In an authentication system without splitting* $H(M/ES) = 0$, *so* $P_{d_1} \geq 2^{H(M)-H(E)-H(S)}$.

Theorem 3.4 (Schöbi [11], Stinson [17]) *In an authentication system without splitting*

$$P_{d_i} \geq \frac{k-i}{v-i} \quad (i \geq 0).$$

Following Massey [9], an authentication system is *L-fold secure against spoofing* if

$$P_{d_i} = \frac{k-i}{v-i}, \quad \text{for all } i,\ 0 \leq i \leq L.$$

Remarks. An authentication code which is perfect (in the sense of 3.1) is 0-fold secure against spoofing (see [4]).

The first bound for P_{d_1}, found by Gilbert, MacWilliams and Sloane [6] using an uniform source distribution, is given by

$$P_{d_i} \geq \frac{1}{\sqrt{b}}.$$

They called a system with this bound *perfect.* Examples of such a systems are included in [6], [2].

Afterwards this bound was proven under general conditions by Simmons and Brickell. They obtained

$$v_G = max\{P_{d_0}, P_{d_1}\} \geq 2^{-\frac{1}{2}H(E)}$$

and if equality holds, then $v_G = 2^{H(E/M)-H(E)}$ and $v_G = 2^{H(S)-H(M)}$ (in a system without splitting). They called a system with this bound *doubly perfect.* Hence doubly perfect implies perfect (in the sense defined in 3.2).

4 SECRECY

Considering the secrecy properties of a code, we desire that no information be conveyed by the observation of the messages. A code has *perfect L-fold secrecy* (Stinson [17]) if, for every set M_1 of at most L messages observed in the channel, and for every set S_1 of at most $|M_1|$ source states, we have $p(S_1/M_1) = p(S_1)$. This means that observing a set of at most L messages in the channel does not help the opponent to determine the L source states.
On the other hand, a code is said to be *Cartesian* ([4], [16]) if any message uniquely determines the source state, independent of the particular encoding rule being used.
In terms of entropy, this is expressed by $H(S/M) = 0$. Hence in a Cartesian authentication code there is no secrecy (it has 0-fold secrecy).

5 BOUNDS ON THE NUMBER OF KEYS b

The first example of an authentication code with $P_{d_1} = 1/\sqrt{b}$ was given by Gilbert, MacWilliams and Sloane [6] using a finite projective plane $PG(2, q)$. However it has the disadvantage that the number of keys q^2 is much larger then the number of source states $q + 1$. Codes with $k \gg b$ have more interest.

The number of keys is basically influenced by the following two aspects:

- the distribution on the source states
- the secrecy of the code.

To illustrate this we mention the following theorems.

Theorem 5.1 (Massey [9], Schöbi [11]) *For an authentication system which is L-fold secure against spoofing there holds*

$$b \geq \frac{\binom{v}{L+1}}{\binom{k}{L+1}}.$$

Theorem 5.2 (Stinson [17]) *If a code achieves perfect L-fold secrecy and is $(L-1)$-fold secure against spoofing, then*

$$b \geq \binom{v}{L}.$$

Theorem 5.3 *If an authentication system without splitting achieves perfect L'-fold secrecy and if it is L-fold secure against spoofing, $L' \leq L+1$, then*

$$b \geq \frac{\binom{v}{L+1}}{\binom{k}{L+1}} \cdot \binom{k}{L'}.$$

Proof. Let M_1 be a set of $i \leq L$ messages which are permitted under a particular encoding rule. Let x be any message not in M_1. Let us suppose there is no encoding rule under which all messages in $M_1 \cup \{x\}$ are valid. Then it follows from the proof of 3.4 in [17] that we would obtain $P_{d_i} > (k-i)/(v-i)$, a contradiction. Hence, it follows that every $(L+1)$-subset of messages is valid under at least one encoding rule.

Now pick any L'-subset M_2, such that $M_2 \subset M_1$. In order to achieve perfect L'-fold secrecy, the messages in M_2 must encode every possible L'-subset of source states. Hence every L'-subset M_2 is a valid set of messages under at least $\binom{k}{L'}$ encoding rules. We remark that the same L'-subset occurs in exactly $\binom{k-L'}{L+1-L'}$ $(L+1)$-subsets. Hence counting L'-subsets of messages we obtain:

$$b \cdot \binom{k}{L'} \geq \frac{\binom{v}{L+1} \cdot \binom{L+1}{L'}}{\binom{k-L'}{L+1-L'}} \cdot \binom{k}{L'}$$

or

$$b \geq \frac{\binom{v}{L+1}}{\binom{k}{L+1}} \cdot \binom{k}{L'} . \blacksquare$$

We define an *optimal* (L', L)*-code*, $0 \leq L' \leq L+1$, to be a code which achieves perfect L'-fold secrecy and is L-fold secure against spoofing and for which b meets the bound given in 5.3. According to Stinson [17], for $L' = L+1$, we call it an *optimal* $(L+1)$*-code*.

6 CONSTRUCTIONS OF AUTHENTICATION CODES FOR AN ARBITRARY SOURCE DISTRIBUTION

6.1 Authentication codes derived from generalized quadrangles

A (finite) *generalized quadrangle* (GQ) is an incidence structure $\mathcal{G} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ in which P and B are disjoint (nonempty) sets of objects called *points* and *lines* resp., and for which I is a symmetric point-line incidence relation satisfying the following axioms:

1. Each point is incident with $1+t$ lines ($t \geq 1$) and two distinct points are incident with at most one line.

2. Each line is incident with $1+s$ points ($s \geq 1$) and two distinct lines are incident with at most one point.

3. If x is a point and L a line not incident with x, then there is a unique pair $(y, M) \in P \times B$ for which $x \; I \; M \; I \; y \; I \; L$.

The integers s and t are the *parameters* of the GQ and $\mathcal{G}$ is said to have *order* (s,t). There is a point-line duality for GQ (of order (s,t)) for which in any definition or theorem the words "point" and "line" are interchanged and the parameters s and t are interchanged. There holds $|P| = (s+1)(st+1)$, $|B| = (t+1)(st+1)$ and $s+t$ divides $st(s+1)(t+1)$.

Let $x, y \in P$, we write $x \sim y$ and say that x and y are *collinear*, provided that there is some line L for which $x \; I \; L \; I \; y$. And $x \not\sim y$ means that x and y are not collinear. For $x \in P$, put $x^\perp = \{y \in P | y \sim x\}$, and note that $x \in x^\perp$. For x, $y \in P$, $x \neq y$, the *trace* of the pair (x,y) is the set $\{x,y\}^\perp = x^\perp \cap y^\perp$. We have $|\{x,y\}^\perp| = s+1$ or $t+1$ according as $x \sim y$ or $x \not\sim y$. The span of the pair (x,y) is the set $\{x,y\}^{\perp\perp} = \{u \in P | u \in z^\perp \; \forall z \in \{x,y\}^\perp\}$. For $x \sim y$, this is the set of points of the line xy, while for $x \not\sim y$, $|\{x,y\}^{\perp\perp}| \leq t+1$.
A *spread* of a GQ $\mathcal{G}$ is a set $\mathcal{R}$ of lines of $\mathcal{G}$ such that each point of $\mathcal{G}$ is incident with a unique line of $\mathcal{R}$. Hence there holds $|\mathcal{R}| = st+1$.
Further information about GQ can be found in [10].

Let $\mathcal{G}$ be a GQ of order (s,t), $s,t > 1$. Take an arbitrary point x. Let the sources be defined by the $t+1$ lines which are incident with x, the messages are the points of $x^\perp \backslash \{x\}$ and the encoding rules are the points of $P \backslash x^\perp$.

Theorem 6.1 *If there exists a GQ of order (s,t) then there is a cartesian $AC(t+1,(t+1)s,ts^2)$ which is 0-fold secure against spoofing.*

Proof. It is easy to verify that $k = t+1$, $v = (t+1)s$ and $b = (s+1)(st+1) - (t+1)s - 1 = s^2t$. We define an encoding rule in the following way. Given a point $y \notin x^\perp$, we define for a source state L, xIL, the message $e_y(L) = z$ with z the unique point on L such that $y \sim z \; I \; L$. We use each encoding rule with probability $1/s^2t$. We verify that $P_{d_0} = k/v$. For an arbitrary message m, there exists st encoding rules containing m. Hence payoff(m), the probability that the message m is accepted by the receiver is given by

$$\text{payoff}(m) = \sum_{e \in E(m)} p(e) = \frac{st}{s^2 t} = \frac{1}{s} = \frac{k}{v}.$$

We also remark that $P_{d_1} = 1/s > (k-1)/(v-1)$.
Indeed, let m, m' be two distinct messages. We obtain

$$\text{payoff}(m, m') = \frac{\Sigma_{\{e \in E(m,m')\}}\ p(e) \cdot p(S = f_e(m))}{\Sigma_{\{e \in E(m')\}}\ p(e) \cdot p(S = f_e(m'))} =$$

$$\frac{\Sigma_{\{e \in E(m,m')\}}\ p(S = f_e(m'))}{\Sigma_{\{e \in E(m')\}}\ p(S = f_e(m'))} = \frac{t}{st} = \frac{1}{s},$$

since there are t encoding rules for which both m, m' occur. Hence payoff(m, m')=1/s. ∎

Remarks 1. Using the same set of source states and messages we can define an
$AC(t+1, (t+1)s, ts^2(t+1))$ with $P_{d_0} = 1/s$, $P_{d_1} = 1/s$, which is 0-fold secure against spoofing and which has perfect 1-fold secrecy. From each encoding rule of the preceding theorem we define $t+1$ new encoding rules in the following way. Let $M(e_y) = M_y = \{z_1, ..., z_{t+1}\}$, then we define for each $0 \leq i \leq t$

$$e(M_y, i) = (e_j \mid 1 \leq j \leq t+1) \text{ where } e_j = z_{j+i \pmod{t+1}}.$$

This illustrates the influence of the secrecy of the code on the number of encoding rules b.

2. If the point x is *regular*, this means that $|\{x, y\}^{\perp\perp}| = t+1$, $\forall y \in P$, $y \not\sim x$ (see [10]), the foregoing code can be improved to an $AC(t+1, (t+1)s, (t+1)s^2)$ with $P_{d_0} = 1/s$, $P_{d_1} = 1/s$, which is 0-fold secure against spoofing and which has perfect 1-fold secrecy. Therefore we take $M(e_y) = \{x, y\}^{\perp}$, $\forall y \in P$, $y \not\sim x$. Since we have s^2 different sets M_{e_y} the number of encoding rules (using the same procedure as in 1.) now equals $s^2(t+1)$.

3. A complete description of the "known" GQ of order (s, t) is given in [10].

Consider again a GQ $\mathcal{G}$ of order (s,t) which contains a spread $\mathcal{R}=\{L_1,\ldots,L_{st+1}\}$. Define the source states as the lines of $\mathcal{R}$ ($k=st+1$) and the messages as the points of $\mathcal{G}$ ($v=(st+1)(s+1)$). Denote the points as $x_{1,1},x_{1,2},\ldots,x_{i,j},\ldots,x_{st+1,s+1}$, with $x_{i,j}\ I\ L_i$, $1\leq j\leq s+1$, $1\leq i\leq st+1$.
Then we define an encoding rule in the following way. We associate with each point $x_{i,j}$ an encoding rule

$$e_{x_{i,j}}(L_k)\ =\ x_{i+k,l'},$$

with $x_{i+k,l'}$ the unique point on the line L_{i+k} which is collinear with $x_{i,j}$ (where $i+k$ is taken (mod $st+1$)). In this way we obtain $b=(1+s)(1+st)$ encoding rules.

Theorem 6.2 *If there exists a GQ of order (s,t) containing a spread $\mathcal{R}$, then there is an optimal 1-code for $st+1$ source states and $(st+1)(s+1)$ messages.*

Proof. We shall use each encoding rule with probability $1/(s+1)(st+1)$. Let us first verify that $P_{d_0}=k/v$. Consider a message m. Then m occurs in $st+1$ encoding rules (since there are st points collinear with m, not on the line of the spread incident with m). Hence payoff(m) is given by

$$\text{payoff}(m)\ =\ \sum_{e\in E(M)}p(e)\ =\ \frac{st+1}{(s+1)(st+1)}\ =\ \frac{1}{s+1}\ =\ \frac{k}{v}.$$

So the system is 0-fold secure against spoofing. The code has perfect 1-fold secrecy since each message occurs exactly once in each column of the $b\times k$ matrix. Since $b=v$, equality is valid in 5.2 and we have an optimal 1-code. ∎

Remark. For the known spreads in GQ of order (s,t) we refer again to [10].

Implementation of the optimal 1-code.

We implement the optimal 1-code derived from the GQ $T_2^*(O)$ of order $(q-1,q+1)$, $q=2^h$ (see [10]). Therefore we use the coordinatization of

this quadrangle given in [5].

Consider an automorphism α of $GF(q)$, $q = 2^h$, such that $0^\alpha = 0$, $1^\alpha = 1$ and $\{(1, x, x^\alpha), x \in GF(q)\} \cup \{(0, 0, 1)\}$ defines an oval in $PG(2, q)$.

The source states are the lines of the spread $[[m, k]]$, $m, k \in GF(q)$. Denote them by L_{k+mq}.
The messages are the points (m, g, k), $m, g, k \in GF(q)$, which will be denoted by $x_{k+mq,g}$.
The encoding rules are given by

$$e_{k+mq,g}(L_j) = x_{k+k'+(m+m')q,g'}$$

with $j = k' + m'q$ and $g' = g + (k'm'^{-1})^\alpha m$.
Hereby is $x_{k+k'+(m+m')q,g'}$ the unique point $(m + m', g + (k'm'^{-1})^\alpha, k + k')$ on the line $L_{k+k'+(m+m')q}$ collinear with (m, g, k).

6.2 Authentication codes derived from Steiner systems

Consider a t-(v, k, λ) design $\mathcal{D}$. For $\lambda = 1$, these are the so called *Steiner systems* (see [1], [3], [8]).

Theorem 6.3 *A Steiner system $\mathcal{D}$ defines an $AC(k, v, v!(k-t)!/(v-t)!)$ which has perfect t-fold secrecy and $(t-1)$-fold security against spoofing.*

Proof. In a t-$(v, k, 1)$ design $\mathcal{D}$, each element occurs in $r = (v-1)\cdots(v-t+1)/(k-1)\cdots(k-t+1)$ blocks and the total number of blocks is given by $v\cdot(v-1)\cdots(v-t+1)/k\cdot(k-1)\cdots(k-t+1)$. We construct $k!$ encoding rules from every block of $\mathcal{D}$, since for each block $A = \{x_1, \ldots, x_k\}$ this is the number of keys required to do a perfect enciphering on the k points. Denote the keys, derived from the block A by $e_{A_1}, \ldots, e_{A_{k!}}$. Hence we obtain

$$b = \frac{v \cdot (v-1)\cdots(v-t+1)}{k \cdot (k-1)\cdots(k-t+1)} \cdot k! = \frac{v!(k-t)!}{(v-t)!}$$

encoding rules, which we shall use with probability $1/b$.
We first verify that the code is $(t-1)$-fold secure against spoofing.
Let $M' \subset M$, $|M'| = i$, $i \leq t-1$, $m \in M \backslash M'$, then we obtain:

$$P_{d_i} = \text{payoff}(m, M') = \frac{\sum_{\{e \in E(M' \cup \{m\})\}} p(e) \cdot p(S = f_e(M'))}{\sum_{\{e \in E(M')\}} p(e) \cdot p(S = f_e(M'))}$$
$$= \frac{\sum_{\{e \in E(M' \cup \{m\})\}} p(S = f_e(M'))}{\sum_{\{e \in E(M')\}} p(S = f_e(M'))},$$

since we use the uniform encoding strategy.

First we remark that the messages of M', resp. $M' \cup \{m\}$, occur in $\lambda' = (v-i)\cdots(v-t+1)/(k-i)\cdots(k-t+1)$, resp. $\lambda'_m = (v-(i+1))\cdots(v-t+1)/(k-(i+1))\cdots(k-t+1)$ blocks. For each such block there are exactly (k-i)! encoding rules e_{A_i} such that $M' \subset M(e_{A_i})$, resp. $M' \cup \{m\} \subset M(e_{A_i})$ and $f_e(M') = S' \subset S$ with $|S'| = i$.

There results

$$P_{d_i} = \frac{\lambda'_m}{\lambda'} = \frac{k-i}{v-i}.$$

The authentication code has perfect t-fold secrecy since $p(S'/M') = p(S')$, for every $S' \subset S$, $M' \subset M$ with $|S'| = |M'| = t$.■

Remark. The foregoing construction of an optimal t-code can be applied to a more general structure, nl. a group-divisible t-design.

A *group-divisible t-design* $GD(k, \lambda, n, t, v)$ is a triple (X, G, A) satisfying:

1. X is a set of v elements called *points*
2. G is a partition of X into v/n subsets of n points, called *groups*
3. A is a set of subsets of X (called *blocks*), each of size k, such that a group and a block contain at most one common point
4. every t points of distinct groups occur in exactly λ blocks.

Note that a $GD(k, \lambda, n, t, k \cdot n)$ is equivalent with a *transversal t-design* (see [7]).

Applying the same construction as in 6.3 a $GD(k, \lambda, n, t, v)$ defines an

$$\text{AC}(\text{k}, \text{v}, \frac{\lambda \cdot \text{v} \cdot (\text{v}-\text{n})\cdots(\text{v}-(\text{t}-1)\text{n})}{\text{k} \cdot (\text{k}-1)\cdots(\text{k}-\text{t}+1)}\text{k!})$$

which has perfect t-fold secrecy and for which $P_{d_i} = (k-i)/(v-i \cdot n)$, for $0 \leq i \leq t-1$.

Moreover the code is $(t-1)$-fold secure against spoofing if and only if $n = 1$, in which case we have a t-(v, k, λ) design.

7 AUTHENTICATION CODES FOR UNIFORM SOURCE DISTRIBUTION

We consider the construction of authentication codes for uniform source distributions ($p(s) = 1/k$, for any source state s). As before we are dealing only with codes without splitting. We know that the best bound is given by $P_{d_i} = (k-i)/(v-i)$, for a spoofing attack of order i.

Theorem 7.1 *An authentication system is L-fold secure against spoofing w.r.t. the uniform probability distribution on the source states if and only if, for every i, $0 \leq i \leq L$ and for every $M' \subset M$, $|M'| = i+1$,*

$$\sum_{e \in E(M')} p(e) = \frac{k}{v} \cdot \frac{k-1}{v-1} \cdots \frac{k-i}{v-i}.$$

Proof. Stinson [18] proved the theorem for $L = 0, 1$. We procede by induction.

Suppose that the system is $(L-1)$-fold secure against spoofing, then for every i, $0 \leq i \leq L-1$, and for every $M' \subset M$, $|M'| = i+1$,

$$\sum_{e \in E(M')} p(e) = \frac{k}{v} \cdot \frac{k-1}{v-1} \cdots \frac{k-i}{v-i}.$$

There holds $P_{d_L} = (k-L)/(v-L)$ if and only if, for every $M'' \subset M$, $|M''| = L$, $m \in M \backslash M''$, we have

$$\text{payoff}(m, M') = \frac{\sum_{e \in E(M'' \cup \{m\})} p(e) \cdot p(S = f_e(M''))}{\sum_{\{e \in E(M'')\}} p(e) \cdot p(S = f_e(M''))} = \frac{k-L}{v-L}.$$

Since the source distribution is uniform, this is equivalent to:

$$\frac{\sum_{\{e \in E(M'' \cup \{m\})\}} p(e)}{\sum_{\{e \in E(M'')\}} p(e)} = \frac{k-L}{v-L}.$$

Taking account of the induction hypothesis,

$$\sum_{e \in E(M'')} p(e) = \frac{k}{v} \cdot \frac{k-1}{v-1} \cdots \frac{k-(L-1)}{v-(L-1)},$$

and hence

$$\sum_{e \in E(M'' \cup \{m\})} p(e) = \frac{k}{v} \cdot \frac{k-1}{v-1} \cdots \frac{k-L}{v-L} \cdot \blacksquare$$

Remarks. In many authentication codes, the encoding strategy is to choose every encoding rule with probability $1/b$. If we assume that this encoding strategy is in fact optimal, then the properties of the foregoing theorem are of purely combinatorial nature. We can formulate the following theorem.

Theorem 7.2 *An authentication system is L-fold secure against spoofing with respect to a uniform encoding strategy and a uniform probability distribution on the source states if and only if the following property is valid for every i, $0 \leq i \leq L$ and every $M' \subset M$, $|M'| = i + 1$,*

$$|E(M')| = b \cdot \frac{k}{v} \cdots \frac{k-i}{v-i}.$$

Example. *A t-(v, k, λ) design (see* [1], [3], [8]*) defines an authentication system for a uniform source distribution and a uniform encoding strategy $AC(k, v, b)$ which is $(t-1)$-fold secure against spoofing.*

Indeed, let $\mathcal{D}$ be a t-(v, k, λ) design. Then $\mathcal{D}$ is also a t'-$(v, k, \lambda'_{t'})$ design, $0 \leq t' \leq t$, with

$$\lambda'_{t'} = \lambda \cdot \frac{(v-t') \cdot (v-t'+1) \cdots (v-t+1)}{(k-t') \cdot (k-t'+1) \cdots (k-t+1)}.$$

Since for a 2-design $v \cdot r = b \cdot k$ and $(k-1) \cdot r = (v-1) \cdot \lambda'_2$, we obtain

$$b = \frac{v \cdot r}{k} = \lambda \cdot \frac{v \cdot (v-1) \cdots (v-t+1)}{k \cdot (k-1) \cdots (k-t+1)}.$$

Using the uniform encoding strategy and uniform source probability, we define a code, identifying blocks with keys and points with messages. Any t' messages occur in λ' blocks and hence for $M' \subset M$, $|M'| = t'$, $1 \leq t' \leq t$,

$$|E(M')| = \lambda'_{t'} = \lambda \cdot \frac{(v-t') \cdots (v-t+1)}{(k-t') \cdots (k-t+1)} =$$

$$b \cdot \frac{k \cdot (k-1) \cdots (k-t'+1)}{v \cdot (v-1) \cdots (v-t'+1)}$$

and theorem 7.2 is satisfied.

Using known families of t-(v, k, λ) designs we can define many authentication codes for uniform source distributions.

Consider the symmetric *Hadamard 2-(n-1,$\frac{1}{2}$n-1,$\frac{1}{4}$n-1) design* and the *Hadamard 3-(n,$\frac{1}{2}$n,$\frac{1}{4}$n-1) design*, derived from a *Hadamard matrix* of order n. We remark that there exist Hadamard matrices for each power 2^k, $k \geq 2$ (see [8], [3], [1]).
Hence we can derive 1-fold secure $AC(2^{k-1}-1, 2^k-1, 2^k-1)$ and 2-fold secure
$AC(2^{k-1}, 2^k, 2(2^k-1))$ authentication systems.
A *Hadamard matrix* of order $4k^2$, $k > 1$, defines a symmetric 2-$(4k^2, 2k^2-k, k^2-k)$ design and hence a 1-fold secure $AC(2k^2-k, 4k^2, 4k^2)$.
Note that it is a conjecture that Hadamard matrices exist for all $n \equiv 0$ (mod4), $n > 0$. (the smallest unsettled case at the present is $n = 188$).
We also want to mention the following nice property of Hadamard matrices. If there exist Hadamard matrices of order m, resp. n, then there exists a Hadamard matrix of order $m \cdot n$. This unables us to define new authentication systems derived from those systems which are associated with Hadamard designs.

Acknowledgement

We would like to thank D. Stinson and J. J. Quisquater for the interesting suggestions and valuable discussions on the subject. We are also mostly indebted to the Philips Research Laboratory Brussels for the facilities they offered during the preparation of this paper.

References

[1] T. Beth, D. Jungnickel, H. Lenz, *Design Theory*, Wissenschaftsverlag Bibliografisches Institut Mannheim, 1985.

[2] A. Beutelspacher, *Perfect and essentially perfect authentication schemes*, Extended abstract, Eurocrypt 1987, Amsterdam.

[3] P. J. Cameron, J. H. Van Lint, *Graph Theory, Coding Theory and Block Designs*, Lond. Math. Soc. Lect. Notes 19, Camb. Univ. Press, 1975.

[4] E. F. Brickell, *A few results in message authentication*, Proc. of the 15th Southeastern Conf. on Combinatorics, Graph theory and Computing, Boca Raton LA (1984), 141–154.

[5] M. De Soete, J. A. Thas, *A coordinatization of the generalized quadrangles of order* $(s, s+2)$, to appear in J. C. T. (A).

[6] E. N. Gilbert, F. J. MacWilliams, N. J. A. Sloane, *Codes which detect deception*, Bell Sys. Techn. J., Vol.53–3 (1974), 405–424.

[7] Hanani H., *A Class of Three-Designs*. J.C.T.(A) 26 (1979), 1–19.

[8] D. R. Hughes, F. C. Piper, *Design theory*, Cambridge University Press, 1985.

[9] J. L. Massey, *Cryptography - A Selective Survey*, Proc. of 1985 Int. Tirrenia Workshop on Digital Communications, Tirrenia, Italy, 1985, Digital Communications, ed. E. Biglieri and G. Prati, Elsevier Science Publ., 1986, 3–25.

[10] S. E. Payne, J. A. Thas, *Finite generalized quadrangles*, Research Notes in Math. #110, Pitman Publ. Inc. 1984.

[11] P. Schöbi, *Perfect authentication systems for data sources with arbitrary statistics*, Eurocrypt 1986, Preprint.

[12] C. E. Shannon, *Communication Theory of Secrecy Systems*. Bell Technical Journal, Vol.28 (1949), 656–715.

[13] G. J. Simmons, *Message Authentication: A Game on Hypergraphs*, Proc. of the 15th Southeastern Conf. on Combinatorics, Graph Theory and Computing, Baton Rouge LA Mar 5–8 1984, Cong. Num. 45 (1984), 161– 192.

[14] G. J. Simmons, *Authentication theory / Coding theory*, Proc. of Crypto'84, Santa Barbara, CA, Aug 19–22, 1984, Advances in Cryptology, ed. R. Blakley, Lect. Notes Comp. Science 196, Springer 1985, 411–432.

[15] G. J. Simmons, *A natural taxonomy for digital information authentication schemes*, Proc. of Crypto '87, Santa Barbara, CA, Aug 16–20, 1987, to appear in Advances in Cryptology, ed. C. Pomerance, Springer-Verlag, Berlin.

[16] D. R. Stinson, *Some constructions and bounds for authentication codes*, Crypto'86, Santa Barbara, CA, Aug 12–15, 1986, Advances in Cryptology, ed. A. M. Odlyzko, Springer-Verlag, Berlin, 1987, 418–425.

[17] D. R. Stinson, *A construction for authentication / secrecy codes from certain combinatorial designs*, Crypto '87, Santa Barbara, CA, Aug 16–20, 1987, to appear in Journal of Cryptology.

[18] D. R. Stinson, *Some constructions and bounds for authentication codes*, J. Cryptology, Vol.1 nr1 (1988), 37–51.