# Cartesian Authentication Schemes

M. De Soete[(1)] K. Vedder[(2)] M. Walker[(3)]

[(1)]*MBLE-I.S.G.*, Rue des Deux Gares 82, 1070 Brussel, Belgium
[(2)]*GAO*, Euckenstraße 12, 8000 München 70, Federal Republic of Germany
[(3)]*Racal Research Ltd.*, Worton Drive, Reading Berkshire RG2 OSB, England

**Abstract.** This paper gives a characterisation of perfect Cartersian authentication schemes. It is shown that their existence is equivalent to the existence of nets. Furthermore the paper presents constructions of new authentication schemes derived from generalised $n$-gons which take on the lowest combinatorial bound for the impersonation attack. They include, as special cases, those based on projective planes and generalised quadrangles which are described in [5] and [3] respectively. It investigates the properties of the encoding rules and contains a brief discussion of questions in connection with key management.

## 1 A Mathematical Authentication Model

There are three participants in the authentication model introduced by Simmons [7]: a *transmitter*, a *receiver* and an *opponent*. The transmitter wants to communicate certain information to the receiver, whereas the opponent tries to deceive the receiver.
More formally, we have a set of *source states* $S$, a set of *authenticators* or *authenticated messages* $M$ and a set of *keys* $K$. A source state $s \in S$ is the information which the transmitter wishes to communicate to the receiver. This is done under a common secret key $l \in K$ which defines the encoding rule $e_l$ used to determine the authenticated message $m = e_l(s)$ sent to the receiver (this means that $e_l$ is a mapping from $S$ to $M$ and hence we investigate codes without splitting). In order for the receiver to be able to uniquely determine the source state from the obtained message, there can be at most one source state which is encoded by any given authenticated message $m \in M$ (i.e. $e_l(s) \neq e_l(s')$ if $s \neq s'$). This means that the encoding rules $e_l$, $l \in K$, are one-to-one mappings from $S$ to $M$.

In the authentication codes we are going to construct every message uniquely determines the source state, independently of the key used. Such codes which offer no secrecy are called *Cartesian*. Another way of expressing the property of a scheme which is Cartesian is to say that there exists a map from $M$ to $S$ the restriction of which to $e_l(S) \subseteq M$ is the inverse of the map $e_l$ for every key $l$.
We shall henceforth assume that every authenticated message is the image of at least

J.J. Quisquater and J. Vandewalle (Eds.): Advances in Cryptology - EUROCRYPT '89, LNCS 434, pp. 476-490, 1990.

one source state under at least one encoding rule. This is no restriction, since the deceiver knows the encoding rules and can thus rule out all other elements in $M$.

The receiver verifies the validity of a received authenticated message $m^*$ by checking that $m^*$ is contained in $e_l(S)$. If this is the case, then the unique source state $s^*$ with $e_l(s^*) = m^*$ will be accepted. A message $m^*$ not in $e_l(S)$ is rejected as fraudulent. Our definition of the acceptance rule implies that the probability of every source state is nonzero and that the receiver accepts a verified source state independent of its probability.

## 2 Perfect Authentication Codes

We consider two situations in which an opponent can launch an attack. In the first one he / she tries to make the receiver accept an authenticated message without having intercepted one. This is called *impersonation*. The other one is *substitution*. Here the opponent replaces an intercepted authenticated message by a different one.

We assume that there is a given probability distribution on the set of source states. The transmitter and receiver will determine a probability distribution on $K$, called an *encoding strategy*. We will denote by $P_i$ the probabilities that the opponent can deceive the transmitter / receiver with an impersonation ($i = 0$) or a substitution ($i = 1$) attack.

Simmons [7] defined a code to be *perfect* if

$$\max(P_0, P_1) = \frac{1}{\sqrt{|E|}},$$

with $E$ ($\subset K$) the set of "distinct" encoding rules or transformations (since different keys can define the same encoding transformation).
Perfect authentication codes were investigated by several authors [5], [7]. In [5] it was shown that for uniform source distribution $P_1 \geq 1/\sqrt{|E|}$. So the best such a scheme can achieve for the transmitter and receiver is $1/\sqrt{|E|}$. We prove the following theorem in this paper.

**Theorem 1** *There exists a perfect Cartesian authentication code on $r$ source states, $r \cdot k$ authenticated messages and $k^2$ encoding rules if and only if there exists a net of degree $r$ and order $k$ (see* [1], [2]).

We remark that this equivalence is implicitly contained in the paper by Gilbert, MacWilliams and Sloane [5] but the proof given here is the first direct approach for arbitrary source distribution.

# 3 Properties of the encoding rules

When substituting a fraudulent message for an intercepted one, the opponent may have one of the following three aims in mind

(i) to "disturb" the system,

(ii) to have any fraudulent message accepted,

(iii) to have a particular fraudulent message accepted.

In the schemes we consider he can always achieve (i), while (ii) and (iii) have the same probabilities attached.

The probability that the opponent can successfully deceive the receiver depends on the way the sets $e_l(S)$ are related to each other for the various encoding rules. We have to assume that the opponent has complete knowledge not only of the source states and authenticated messages but also of all the encoding rules. That is to say that the security of the scheme depends on the particular choice of $e_l$ (or $l$) being kept secret. If, for instance, $e_l(S) \cap e_{l'}(S) = \phi$ for any two distinct encoding rules, then the opponent can derive the encoding rule $e_l$, say, from every intercepted authenticated message $m$. He could thus replace $m$ by $m' \neq m$, $m' \in e_l(S)$, and he can deceive the receiver with a probability of 1. The opponent's probability to impersonate successfully the transmitter, that is to plant a message without having observed one, is just $|e_l(S)|/|M| = 1/|E|$. In the other extreme we have $|M| = |e_l(S)| = |S|$ for one and hence for all keys. In this situation the opponent can deceive the receiver in either case with a probability of 1.

An intercepted message $m$ provides the opponent with some information about the encoding rule. It has to lie in the set $E^m$ of all those encoding rules which take on $m$ as an image of a source state, that is $E^m = \{e_l \mid e_l \in E \text{ and } m \in e_l(S)\}$. Assuming that all encoding rules are equally likely, the opponent has a probability of $1/|E^m|$ of guessing the correct rule. He can deceive the receiver with a probability of 1 if $\cap e_l(S)$, over all $e_l$ in $E^m$, contains an authenticated message $m' \neq m$. For a replacement of $m$ by $m'$ would not be noticed by the receiver. This yields the following requirements

(i) $|E^m| \neq 1$ for all $m \in M$, and

(ii) $\cap_{E^m} e_l(S) = \{m\}$ for all $m \in M$.

Let us illustrate this by an example. We take $S = \{A, B, C\}$, $E = \{e_1, \ldots, e_4\}$ and $M$ the entries of the matrix below which define the encoding rules. The only case where the opponent cannot deceive the receiver with a probability of 1 is when he intercepts $b_1$.

| | $A$ | $B$ | $C$ |
|---|---|---|---|
| $e_1$ | $a_1$ | $b_1$ | $c_1$ |
| $e_2$ | $a_2$ | $b_1$ | $c_2$ |
| $e_3$ | $a_1$ | $b_2$ | $c_1$ |
| $e_4$ | $a_2$ | $b_3$ | $c_2$ |

Example 1

Let $e_K(s)$ denote the set of images of the source state $s$ under all encoding rules, that is $e_K(s) = \{e_l(s) \mid l \in K\} \subseteq M$. Since, for Cartesian authentication schemes, distinct encoding rules never map distinct source states to the same authenticated message, distinct source states give rise to disjoint sets. It follows that the sets $e_K(s)$, $s \in S$, partition the set of authenticated messages and that there is a natural 1-1 correspondence between $S$ and $\{e_K(s) \mid s \in S\}$. The knowledge of this property gives an opponent a sure way of disturbing the system. Say he intercepts the message $m = e_l(s)$. He then replaces $m$ by a message $m' \in e_K(s)$, $m' \neq m$. Though $m'$ corresponds to the same source state $s$ as the correct message $m$ the receiver cannot decide whether this type of substitution was played or whether $m'$ was substituted for a message $m_1 = e_l(s_1)$ authenticating a source state $s_1 \neq s$.

If the opponent wants to deceive the receiver, then he has to choose a message $m' = e_l(s')$ in the set $e_l(S)$ with $s' \neq s$. Which set he chooses and which message in this set depends primarily on the way the encoding rules "distribute" the source states among the authenticated messages. We will from now on assume that there is a uniform probability distribution on the set of encoding rules, that is all encoding rules are equally likely.

For a message $m$ let $n_m$ denote the number of encoding rules which take on $m$ as an image, that is $n_m = |E^m|$. If the opponent runs an impersonation attack, then he is not restricted in his choice by any message sent by the transmitter. Thus his probability to succeed depends solely on the distribution of the values $n_m$ in $M$. If he does not mind which fraudulent message gets accepted he picks the message $m$ with $n_m = \max\{n_m \mid m \in M\}$. If he wants to run a *chosen* attack, that is he wants a specific source state $s$ to be accepted, then he chooses the message $m$ with the largest value $n_m$ among $e_K(s)$. Since all encoding rules are equally likely his chances to succeed is $P_0 = n_m/|E|$. This yields the following inequality $n_m/|E| \geq |S|/|M|$. We also note that, if $n_m$ is a constant $n$, both the chosen and the non-specific attack have the same probability. Counting pairs $(e_l, m)$ with $e_l(s) = m$ for some $s \in S$ we obtain $n \cdot |M| = |E| \cdot |S|$. Hence $n/|E| = |S|/|M|$, which is the lowest possible bound. The situation is different in the case of substitution. Firstly, the opponent, who has intercepted a message $m$, $m \in e_K(s)$, " cannot" choose a message in the "intercepted" class $e_K(s)$. Secondly, he has obtained some knowledge about the set $E^m$ of encoding rules which might have been used. Let us illustrate this again by giving an example.

| | $A$ | $B$ | $C$ | $A'$ | $D$ |
|---|---|---|---|---|---|
| $e_1$ | $a_1$ | $b_1$ | $c_1$ | $a_1$ | $d_1$ |
| $e_2$ | $a_1$ | $b_2$ | $c_2$ | $a_2$ | $d_1$ |
| $e_3$ | $a_1$ | $b_3$ | $c_3$ | $a_3$ | $d_1$ |
| $e_4$ | $a_2$ | $b_1$ | $c_2$ | $a_3$ | $d_2$ |
| $e_5$ | $a_2$ | $b_2$ | $c_3$ | $a_1$ | $d_2$ |
| $e_6$ | $a_2$ | $b_3$ | $c_1$ | $a_2$ | $d_2$ |

Example 2

Suppose that we have a probability distribution on the set of source states which reads as follows:

$$\text{prob}(A) = 0.6,\ \text{prob}(B) = \text{prob}(C) = 0.2.$$

Given this distribution the opponent has a success rate of 1/2 in 40% of all transmissions, that is when $B$ or $C$ is authenticated. In the remaining 60% of all transmissions his success rate is just 1/3.

The probability distribution on the source sates can be counteracted by using column $A'$ instead of $A$ which requires one extra authenticated message. In this scheme all transmissions supply the opponent with a success rate of $1/2 > 1/\sqrt{6} = 1/\sqrt{|E|}$. Furthermore, $P_0 = 1/3$ and $P_1 = 1/2$ since $n_m = 2$ for all messages $m$. The reader should convince himself that this is the best possible value one can achieve on three source states with six encoding rules.

The transmission of a message rules out not only certain encoding rules but also certain messages. Say message $m = b_1$ was sent by the transmitter, then an opponent knows that the receiver will not accept $a_2$ or $c_3$ as they are not in $E^m(S)$. So the condition which should be imposed on the encoding rules is that $E^m(S) = M$ and that $E^m$ gives a uniform distribution on all messages not in $e_K(s)$. It is easily seen that this cannot be achieved in a scheme with just three source states. An example of such a scheme can be constructed from columns $B$, $C$, $A'$ and $D$ extending them in the obvious way. We note that this is an affine plane of order 3.

Now let all messages in $M \setminus e_K(s)$ lie on the same number $n'$ of encoding rules in $E^m$. Then by counting pairs $(m', e_l)$ with $m' \notin e_K(s)$ and $e_l(s') = m'$ for some $s' \in S$ and $e_l \in E^m$ we obtain

$$n' \cdot (|M| - |e_K(s)|) = |E^m| \cdot (|S| - 1).$$

We note that

$$\frac{n'}{|E^m|} = \frac{|S|}{|M|} = \frac{n}{|E|}$$

and $P_1 = P_0$ in such a system if and only if

$$|M| = |S| \cdot |e_K(s)|.$$

The last equation holds, by the way, for the perfect schemes described in [5]. They are constructed from projective planes which are the projective closure of affine planes. These are nets of maximal degree.

# 4 Perfect Schemes and Nets

## 4.1 Nets

A *finite incidence strucuture* $\mathcal{P}$ is a triple $(P, B, I)$ which consists of two finite, non-empty and disjoint sets $P$ and $B$ and a subset $I \subseteq P \times B$. The elements of $I$ are called *flags* while those of $P$ and $B$ are referred to as *points* and *lines* respectively. $I$ is called the *incidence relation*. We say that a point $x$ and a line $L$ are incident with each other and write $x \in L$ if and only if $(x, L)$ is a flag.

Throughout this paper we shall only be concerned with *linear* incidence structures, which are characterised by the property that distinct points are incident with at most one line. As furthermore every line is incident with at least two points we can identify each line with the set of points it is incident with.

An incidence structure is *tactical* if it has the property that every point is incident with the same number $r$ of lines and every line is incident with the same number $k$ of points. Using $|P| = v$ and $|B| = b$ it is easily seen by counting flags in two different ways that

$$v \cdot r = b \cdot k = |I|.$$

A *net* of degree $r$ and order $k$ (see Bose [1]) is an incidence structure $\mathcal{P}{=}(P, B, I)$ which satisfies the following axioms

(i) the lines can be partitioned into exactly $r$ disjoint, non-empty "parallel classes" such that

(a) each point is on exactly one line of each class

(b) two lines of distinct classes intersect in exactly one point;

(ii) each line is incident with $k$ points.

Then it can be proved that the incidence structure is tactical, so each line of the net contains exactly $k$ distinct points and each point of the net lies on exactly $r$ distinct lines. Furthermore the net has exactly $r \cdot k$ distinct lines and $k^2$ distinct points.

It is easy to see that $r \leq k+1$ and $r = k+1$ if and only if $\mathcal{P}$ is an affine plane. An affine plane is known to exist for every prime power $k$. Nets with (at least) $r = 4$ parallel classes exist for all values of $k$.

## 4.2 Proof of the Theorem

We will first prove that an authentication scheme constructed from a net is perfect. Let $(P, B, I)$ be a net of degree $r$ and order $k$, and let $\mathcal{P}$ be its set of parallel classes. The construction closely resembles the one given in [5] for projective planes. Let

$$S = \mathcal{P}$$

be the set of source states,

$$M = B$$

the set of authenticated messages and

$$K = P$$

the set of keys. The encoding rule $e_l$ defined by the key $l$ maps a source $s$ to the authenticated message $m$ which is the unique line in the parallel class $s$ which is incident with $l$. This is well defined since every point of the net is incident with exactly one line of each parallel class. Observe also that, since each line of a net is contained in exactly one parallel class, this authentication scheme is Cartesian.

We now prove that the schemes constructed above are perfect. We show that $P_0 = P_1 = 1/\sqrt{|E|}$ under the assumption that there is a uniform distribution on the set of keys, so $p(l) = 1/|K| = 1/|P|$. Let $q_0(m)$ be the opponents optimal impersonation strategy. Then

$$P_0 = \sum_{m \in M} q_0(m) \cdot \sum_{l\, I\, m} p(l).$$

Setting $p(l) = 1/|K|$ and noting that $\sum_{x\, I\, m} 1 = k$, gives

$$P_0 = \frac{k}{|P|} = \frac{1}{\sqrt{|K|}},$$

where the last equality follows from $|P| = k^2$ for a net.

Suppose now that the opponent has observed the sender's authenticated message $m$, and let $q_1(m^*|m)$ be his optimal strategy. Clearly, we have $q_1(x|m) = 0$, whenever $x||m$, because parallel messages always correspond to the same source state, and the opponent usually is not interested in substituting $m$ by a message corresponding to the same source state. Then

$$P_1 = \sum_{m \in M} p(m) \cdot \sum_{m^* \in M, m^* \not\parallel m} q_1(m^*|m) \cdot \sum_{l\,I\,m,\, l\,I\,m^*} p(l|m).$$

Since $m$ and $m*$ are not parallel they intersect in exactly one point. Furthermore $p(l|m) = 1/k$, since there are $k$ points per line and $p(l)$ is uniform. This gives

$$P_1 = \frac{1}{k} = \frac{1}{\sqrt{|K|}}.$$

Now we will prove that every perfect authentication system defines a net. Suppose we are given a Cartesian authentication scheme with a set of source states $S$, a set of authenticated messages $M$, a set of keys $K$ and a set of encoding rules $\{e_l : S \to M \mid l \in K\}$. We associate with our authentication scheme an incidence structure $N{=}(K, M, I)$, with points set $K$, line set $M$ and an incidence relation defined in the following way:

if $l \in K$ and $m \in M$, then $l\,I\,m \Longleftrightarrow$ there exists an $s \in S$ such that $e_l(s) = m$.

Note that the term line above is an abuse of terminology since two "lines" may have more than one point in common.

For each $m \in M$ we denote by $\sigma(m)$ the unique source state which encodes to $m$. This is well defined for our authentication scheme is Cartesian. The function $\sigma :\ M \to S$ gives rise to an equivalence relation "||" on $M$, defined by

$m||m'$ if and only if $\sigma(m) = \sigma(m')$.

For each $s \in S$ let $\mathcal{P}_s{=}\{m \in M \mid \sigma(m) = s\}$ denote the equivalence class of "parallel" lines corresponding to $s$. Two distinct parallel lines $m$ and $m^*$ in $\mathcal{P}_s$ have no point in common. For otherwise there exists a point (key) $l$ such that $e_l(s') = m$ and $e_l(s^*) = m^*$. As $m||m^*$ it follows that $s = s' = s^*$ and, since $e_l$ is a mapping, $m = m^*$ contradicting $m \neq m^*$. It also follows that for each point $l$ of our incidence structure $N$ there is a unique line $e_l(s)$ in $\mathcal{P}_s$ which is incident with $l$. So the lines of $\mathcal{P}_s$ partition the points of $N$ and all the lines form a "parallelism".

The above discussion indicates that $N$ has a net-like structure. It remains to show that each line is incident with the same number of points and that two distinct non-parallel lines intersect in a unique point. We denote by $[m]$ the number of points on a line $m$ and by $[m, m^*]$ the number of points the lines $m$ and $m^*$ have in common.

We assume that the key is chosen according to the uniform distribution $p(l) = 1/|K|$. Let $q_0'(m)$ be any impersonation strategy selected by the opponent. Then, since the authentication scheme is perfect, we have

$$P_0' = \sum_{m\in M} q_0'(m) \cdot \sum_{\{l \mid e_l(\sigma(m))=m\}} p(l) \leq \frac{1}{\sqrt{|K|}}$$

where $P_0'$ denotes the probability of a succesful impersonation. Substituting $p(l) = 1/|K|$, and $|\{l \mid e_l(\sigma((m)) = m\}| = [m]$, gives

$$P_0' = \frac{1}{|K|} \sum_{m\in M} q_0'(m) \cdot [m] \leq \frac{1}{\sqrt{|K|}}.$$

Since this inequality holds for every strategy $q_0'(m)$, it follows that

$$[m] \leq \sqrt{|K|},$$

for all $m \in M$. As a consequence we obtain

$$|S| \cdot |K| = \sum_{m\in M} [m] \leq |M|\sqrt{|K|},$$

with equality if and only if $[m] = \sqrt{|K|}$ for each $m$. In this expression $|S|$ is the number of parallel classes (i.e., the number of source states). The equality in the expression follows because both sides of the equation count the number of flags of the incidence structure.

Suppose now that $q_1'(m)$ is an opponent's substitution strategy, and let $q_1'(m^*|m)$ be the strategy given that $m$ has been intercepted. We shall assume that $q_1'(x|m) = 0$ for all messages $x$ which are parallel to $m$. Since the authentication scheme is perfect we have

$$P_1' = \sum_{m\in M} p(m) \cdot \sum_{m^*\in M, m \nparallel m^*} q_1'(m^*|m) \cdot \sum_{\{l \mid e_l(\sigma(m))=m,\ e_l(\sigma(m^*))=m^*\}} p(l|m) \leq \frac{1}{\sqrt{|K|}},$$

where $P_1'$ is the expected probability of a succesful substitution.
However

$$p(m) = p(\sigma(m)) \sum_{l\, I\, m} p(l)$$

so that substituting for $p(l) = 1/|K|$, $p(l|m) = 1/[m]$ and noting that $|\{l \mid e_l(\sigma(m)) = m,\ e_l(\sigma(m^*)) = m^*\}| = [m, m^*]$, we obtain

$$P_1' = \sum_{m\in M} p(\sigma(m)) \cdot \frac{[m]}{|K|} \cdot \sum_{m^*\in M, m \nparallel m^*} q_1'(m^*|m) \cdot \frac{[m, m^*]}{[m]} \leq \frac{1}{\sqrt{|K|}}.$$

This holds for all choices of $q_1'(m^*|m)$. For each $m$, choose an $m'$ with

$$[m, m'] \geq [m, m^*], \text{ all } m^* \nparallel m$$

and define $q_1'(x|m) = 1$ if $x = m'$ and 0 otherwise (i.e. the strategy is to substitute a message which has the maximum number of points in common with $m$). Then we obtain

$$\sum_{m \in M} p(\sigma(m)) \cdot [m, m'] \leq \sqrt{|K|}.$$

But

$$\sum_{m \in M} p(\sigma(m)) \leq \sum_{m \in M} p(\sigma(m)) \cdot [m, m'],$$

since $[m, m'] \geq 1$.
On the other hand

$$\sum_{m \in M} p(\sigma(m)) \geq \frac{|M|}{|S|}.$$

Hence there results

$$\frac{|M|}{|S|} \leq \sum_{m \in M} p(\sigma(m)) \leq \sum_{m \in M} p(\sigma(m)) \cdot [m, m'] \leq \frac{|M|}{|S|}$$

which gives $[m, m'] = 1$ for all $m$ and $|M| = \sqrt{|K|} \cdot |S|$. The first of these equalities means that $[m, m^*] \leq 1$ for all $m$, $m^*$ whilst the second equality tells us that $[m] = \sqrt{|K|}$ for all $m$.
It remains to argue that if $m \not| m^*$, then $[m, m^*] = 1$. This is trivial. Each line $\sigma(m^*)$ which meets $m$ does so in precisely one point. There are $[m] = \sqrt{|K|}$ such lines, and each is incident with $\sqrt{|K|}$ distinct points. Thus each of the $|K|$ points of the incidence structure lies on precisely one of these lines.

# 5 Authentication Schemes Constructed from Generalised Polygons

## 5.1 Generalised Polygons

Given an incidence structure $P$, in the sense of [2] (see also Section 4.1), we denote by $\Delta(P)$ the flag graph of $P$. Thus $\Delta(P)$ is the bipartite graph having vertex set the collection of points and blocks of $P$ and edges the totality of flags (unordered incident point–block) pairs of $P$.

A *(thick) generalised polygon* ($n \in N$, $n \geq 2$) is an incidence structure $P$ with the property that $\Delta(P)$ satisfies the following three conditions:

(i) each vertex has valency at least 3;

(ii) each pair of edges is contained in a circuit of length $2n$;

(iii) there is no circuit of length less than $2n$.

In this paper we deal with $n \geq 3$ and use the term "line" instead of block. Examples of generalised 3- and 4-gons are projective planes and generalised quadrangles which were used in [5] and [3], respectively to construct authentication schemes. The finite generalised $n$-gons, with which we shall be dealing exclusively, were studied by Feit and Higman [4]. They proved that $n = 3, 4, 6$ or 8. These structures are tactical configurations (which means that every point is incident with the same number of lines) and we follow the convention of denoting the number of points on a line by $s+1$, $s > 1$, and the number of lines through a point by $t+1$, $t > 1$.

In discussing generalised $n$-gons the following notation and observations prove to be useful.

Condition (ii) implies that $\Delta = \Delta(P)$ is connected and that the distance $\delta(X,Y)$ between two vertices $X$ and $Y$ is at most $n$. If $\delta(X,Y) = n$, then $X$ and $Y$ are called *opposite*. If vertices $X$ and $Y$ are such that $\delta(X,Y) < n$, then there is, by condition (iii), a unique path of length $\delta(X,Y)$ which joins $X$ and $Y$. This path is denoted by $< X, Y >$.

Now, let $X$ be a vertex of $\Delta$, and let $\Delta_d(X) = \{Y \in \Delta \mid \delta(X,Y) = d\}$, the set of all vertices which are at distance $d$ from $X$. We can interprete $\Delta$ as a graph with root $X$ and $n+1$ levels $0, \ldots, n$, where the vertices at level $d$ are the elements of $\Delta_d(X)$. It is easily seen that a vertex $Y$ at level $d \neq 0, n$ is joined to exactly one vertex at level $d-1$ and $s$ or $t$ vertices at level $d+1$, depending on it being a line or a point. We denote those at level $d+i$ from $X$ and level $i$ from $Y$ by $\Delta_{+i}(Y)$. The vertices at level $n$ are joined only to vertices at level $n-1$. This means that the subgraph with vertex set $\cup_{d \neq n} \Delta_d(X)$ forms a tree (see [6]).

So the number of vertices in $\Delta_d(X)$, $d < n$, is equal to the number of distinct paths of length $d$ which start in $X$. Hence, if $X$ is a point, then

$$|\Delta_d(X)| = \begin{cases} (t+1)(st)^{(d-1)/2} & d \text{ odd} \\ (t+1)s^{d/2}t^{d/2-1} & d \text{ even.} \end{cases}$$

To obtain $\Delta_n(X)$ we have to divide $\Delta_{n-1}(X)$ by $t+1$ or $s+1$, whichever is the degree of the vertices opposite to $X$. Here it is important to observe that $s = t$ for $n$ odd. For, if $X$ is a point, then an opposite vertex $Z$ is a line and hence there are precisely $s+1$ distinct paths from $Z$ to $X$. Thinking of $Z$ as the root there are $t+1$ paths from $X$ to $Z$. But the number of paths has to be the same. These observations yield the expressions (2) and (3) given below.

## 5.2 The Schemes

For every finite generalised $n$-gon of order $n \geq 3$ with parameters $s$ and $t$ we can define, making use of an arbitrary point $X$, a Cartesian authentication scheme with the set of source states

$$|S| = |\Delta_1(X)| = t+1, \tag{1}$$

the set of authenticated messages

$$|M| = |\Delta_d(X)| = \begin{cases} (t+1)t^{d-1} & d \text{ odd} \\ (t+1)s^{d/2}t^{d/2-1} & d \text{ even} \end{cases} \tag{2}$$

and the set of keys

$$|K| = |\Delta_n(X)| = \begin{cases} t^2 & n=3 \\ s^{n/2}t^{n/2-1} & n \text{ even.} \end{cases} \tag{3}$$

The encoding rule $e_Z$ determined by the key $Z$ maps a source $Y$ to

$$e_Z(Y) = Z_d$$

where $Z_d$ is the vertex at distance $d$ from $X$ in the unique path $< Y, Z >$. A receiver with knowledge of the key $Z$ authenticates $Z_d$ by checking that it is at distance $n-d$ from $Z$. The corresponding source state $Y$ is simply the vertex adjacent to $X$ in the path $< X, Z_d >$.

Starting with a line instead of a point results in an interchange of the parameters $s$ and $t$ in the above expressions. Note that $s = t$ for $n = 3$. We remark that such a scheme can be constructed from any tree by introducing an extra level $n+1$ and joining vertices of level $n$ with new ones at level $n+1$.

## 5.3 Implementation and Security

When implementing a scheme it is important to strike the right balance between security and the problem of handling. Keeping in mind that security is a relative term one may say that the more secure a system becomes the less managable it will be. Furthermore, one should take into account that the security gained by keeping certain additional information secret could be short lived. In our case, a potentional attacker can deduce at least part of this information from intercepted authenticated messages.

In the extreme one could keep everything but the underlying scheme secret, that is not only the key $Z$ but also the level $d$ and the root $X$ could be part of the keying information. This is certainly interesting from a theoretical point of view. It would, however, make the system extremely difficult to handle since the receiver needs to know how the source states are labelled in order to pick the correct authenticated message. Thus all the information about the source states becomes part of the key and the system becomes unmanagable.

As $d$ can be derived from the knowledge of $X$ and an intercepted authenticated message, keeping $d$ secret has no effect on the probability of a successful substitution by an interceptor. It does, however, increase the likelihood of detecting an impersonation attack. For any vertex not equal to $X$ or at distance $n$ from $X$ could be an authenticated message and not only $|S|$ messages at distance $d$. So the security gained by making $d$ part of the key might well justify the additional overhead.

We will now assume that both $X$ and $d$ are known and that all keys are equally likely. The probability to guess the correct key is $1/|K|$ if no message is intercepted, and $1/|\Delta_{n-d}(m) \cap \Delta_n(X)|$ if one message $m$ is intercepted.
For $d > n/2$ any two authenticated messages uniquely determine the key since there is no circuit of length less than $2n$. This has two important consequences. Firstly, the key has to be changed after each transmission. Secondly, distinct keys define distinct encoding rules since their "corresponding" set of authenticated messages have at most one element in common.
For $d \leq n/2$ the situation depends on the structure of the underlying geometry. We will highlight this in Section 5.4.

## 5.4 Impersonation and substitution

Obviously, for $d = 1$ every source state is encoded by itself and this encoding is independent of the key. This implies that $P_0 = P_1 = 1$. We will henceforth assume that $d > 1$ and that $X$ is a point. If $X$ is a line, then the values of $s$ and $t$ have to be interchanged in all the following formulas.

We have the following probabilities for the impersonation attack.

$$P_0 = \begin{cases} 1/(st)^{(d-1)/2} & d \text{ odd} \\ 1/s^{d/2}t^{d/2-1} & d \text{ even.} \end{cases}$$

The sets $\Delta_{+(d-1)}(s)$, $s \in S$, partition the set of vertices at level $d$. For a given key $k$ each of them contains exactly one authenticated message.
We note that $P_0 = |S|/|M|$ which is the lowest possible combinatorial bound for an impersonation attack (see [7]).

For the substitution attack we obtain

$$P_1 = P_0 \text{ for } d \leq n/2$$

whilst for $d > n/2$, we have

$$P_1 = \begin{cases} 1/(st)^{(n-d)/2} & n \text{ even, } d \text{ even} \\ 1/s(st)^{(n-d-1)/2} & n \text{ even, } d \text{ odd} \\ 1/t & n = 3,\ d = 2. \end{cases}$$

For $d > n/2$ any two authenticated messages uniquely determine the key $k$. This means that a successful substitution attack is equivalent to determining the key. Let $m$ be the intercepted message. Then choose any vertex in $\Delta_{n-d}(m) \cap \Delta_n(X)$, say $k'$.
If $k' = k$, then every vertex in $\Delta_{n-d}(k')$ is an authenticated message. Pick your favourite one.
If $k' \neq k$, then except for $m$ no vertex in $\Delta_{n-d}(k')$ is an authenticator.
For $d < n/2$ it follows from Axioms (ii) and (iii) that for every source state $s$ exactly one vertex in $\Delta_{+(d-1)}(s)$ is an authenticated message. We note that in all cases the probability to have one's favourite source state accepted is the same as having any odd source state accepted and that the probabilities are independent of the distribution on the source states (assuming that all of them have non-zero probability).

We conclude this section with a complete list of the schemes for all possible values of $n$. An entry * in the tables below means that the value depends, as already mentioned, upon the structure of the generalised $n$-gon.

$n = 3$: projective planes
$|S| = t + 1$, $|K| = t^2$

| d | 2 |
|---|---|
| $\lvert M\rvert$ | $t(t+1)$ |
| $P_0$ | $1/t$ |
| $P_1$ | $1/t$ |
| $\lvert E\rvert$ | $t^2$ |

$n = 4$: generalised quadrangles
$|S| = t + 1$, $|K| = s^2t$

| d | 2 | 3 |
|---|---|---|
| $\lvert M\rvert$ | $s(t+1)$ | $st(t+1)$ |
| $P_0$ | $1/s$ | $1/st$ |
| $P_1$ | $1/s$ | $1/s$ |
| $\lvert E\rvert$ | * | $s^2t$ |

$n = 6$: generalised hexagon
$|S| = t + 1$, $|K| = s^3t^2$

| d | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| $\|M\|$ | $s(t+1)$ | $st(t+1)$ | $s^2t(t+1)$ | $(st)^2(t+1)$ |
| $P_0$ | $1/s$ | $1/st$ | $1/s^2t$ | $1/(st)^2$ |
| $P_1$ | $1/s$ | $1/st$ | $1/st$ | $1/s$ |
| $\|E\|$ | * | * | $s^3t^2$ | $s^3t^2$ |

$n = 8$: generalised octagon
$|S| = t + 1$, $|K| = s^4t^3$

| d | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| $\|M\|$ | $s(t+1)$ | $st(t+1)$ | $s^2t(t+1)$ | $(st)^2(t+1)$ | $s^3t^2(t+1)$ | $(st)^3(t+1)$ |
| $P_0$ | $1/s$ | $1/st$ | $1/s^2t$ | $1/(st)^2$ | $1/s^3t^2$ | $1/(st)^3$ |
| $P_1$ | $1/s$ | $1/st$ | $1/s^2t$ | $1/s^2t$ | $1/st$ | $1/s$ |
| $\|E\|$ | * | * | * | $s^4t^3$ | $s^4t^3$ | $s^4t^3$ |

**Remark** For $n$ even, i.e. $n = 2m$, it is possible to construct perfect schemes when using as root a regular vertex $X$ with $d = m$.

# References

[1] R. C. Bose, *Graphs and designs*, in: Finite geometric structures and their applications, ed. A. Barlotti, Ed. Cremonese Roma (1973), 1-104.

[2] P. Dembowski, *Finite Geometries*, Springer Verlag, 1968.

[3] M. De Soete, *Some Constructions for Authentication / Secrecy Codes*, Advances in Cryptology–Proceedings of Eurocrypt '88, Lect. Notes Comp. Science 330, Springer 1988, 57–75.

[4] W. Feit and G. Higman, *The non-existence of certain generalised polygons*, J. Algebra 1 (1964), 114–131.

[5] E. N. Gilbert, F. J. MacWilliams and N. J. Sloane, *Codes which detect deception*, Bell System Technical Journal, Vol. 53-3 (1974), 405–424.

[6] D. Jungnickel, *Graphen, Netzwerke und Algorithmen*, Wissenschaftsverlag Bib. Inst. Zürich, 1987.

[7] G. J. Simmons, *Authentication Theory / Coding Theory*, Advances in Cryptology–Proceedings of Crypto'84, Lect. Notes Comp. Science 196, Springer 1985, 411–432.