1990

Some remarks on authentication systems

Martin HG Anthony

Keith M. Martin

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

Peter Wild

Some remarks on authentication systems

Abstract

Brickell, Simmons and others have discussed doubly perfect authentication systems in which an opponent's chance of deceiving the receiver is a minimum for a given number of encoding rules. Brickell has shown that in some instances to achieve this minimum the system needs to have splitting. Such a system uses a larger message space. Motivated by Brickell's ideas we consider authentication systems with splitting and the problems of reducing the message space.

Disciplines

Physical Sciences and Mathematics

Publication Details

Anthony, MHG, Martin, KM, Seberry, J & Wild, P, Some remarks on authentication systems, (Josef Pieprzyk and Jennifer Seberry, (Eds.)), Auscrypt'90 – Advances in Cryptography, 453, Lecture Notes in Computer Science, Springer-Verlag, 1990, 122-139.

Some Remarks on Authentication Systems

Martin H.G. Anthony*, Keith M. Martin*,
Jennifer Seberry**, Peter Wild*

Abstract

Brickell, Simmons and others have discussed doubly perfect authentication systems in which an opponent's chance of deceiving the receiver is a minimum for a given number of encoding rules. Brickell has shown that in some instances to achieve this minimum the system needs to have splitting. Such a system uses a larger message space. Motivated by Brickell's ideas we consider authentication systems with splitting and the problems of reducing the message space.

1 Authentication

We use the model of authentication described by Simmons [9, 10] and Brickell [1]. There are three participants involved in this model; a transmitter T, a receiver R and an opponent O. T wants to communicate some information to R. It is not necessary that the information be kept secret, but R wants to be sure that the information did indeed come from T.

An item of information that the transmitter might want to send to the receiver is called a source state, and we denote by S the set of source states. We assume that there is some fixed probability distribution P_S on S ($P_S(s)$ is the probability that $s \in S$ is to be communicated on any given occasion).

In order to relay a source state $s \in S$ to R, T encodes it (using some encoding rule chosen from a set I of encoding rules) as a message m and sends m to R.

In order for R to be able to determine which source state is being relayed it is necessary that for any given encoding rule a message m can relay at most once source state under that rule. T and R agree on which encoding rule they will use before communication starts.

Let M be the set of messages that T can send to R. Let 0 be an element not belonging to S. Associated with an encoding rule i is a mapping $f_i : M \to S \cup \{0\}$ given by $f_i(m) = s$ if T can encode $s \in S$ as m under encoding rule i and $f_i(m) = 0$ if no source state can be encoded as m under i. R accepts a message m as authentic (relaying source state s) if $f_i(m) = s$. R rejects m if $f_i(m) = 0$.

We call the triple (I, M, S) an authentication system and if $|I| = b$, $|M| = v$ and $|S| = k$ we denote it by $AS(b, v, k)$. It may be represented by a matrix whose rows are indexed by the set I of encoding rules and whose columns are indexed by the set M of messages with entry $f_i(m)$ in row i, column m. Alternatively it may be represented by a $b \times k$ array $A = (a_{is})$ where $a_{is} = \{m \in M | f_i(m) = s\}$ for $i \in I$, $s \in S$. We call this $b \times k$ array A an authentication array corresponding to the authentication system.

Example 1: Authentication array for $AS(9, 9, 3)$ with $M = \{a, b, c, d, e, f, g, h\}$, is

$$
\begin{array}{ccc}
a & d & g \\
a & e & h \\
a & f & i \\
b & d & h \\
b & e & i \\
b & f & g \\
c & d & i \\
c & e & g \\
c & f & h
\end{array}
$$

The opponent O attempts to get R to accept some information that did not

come from T. If O knows which encoding rule T and R have agreed upon then O may succeed with probability 1. We assume that T and R share an encoding rule in secret for each transmission and that the encoding rule is chosen according to a probability distribution P_I on the set I of encoding rules. O may deceive R by impersonation or substitution. O impersonates T by sending a message when in fact T has not sent a message. O is successful if R accepts the message as authentic. If T sends a message m, relaying source state s, then O may intercept it and substitute a different message m'. O is sucessful if R accepts the substituted message m' and this message relays a source state different form s.

If $i \in I$ and there exists $m_1 \neq m_2$ such that $f_i(m_1) = f_i(m_2) \neq 0$ then we say splitting occurs in encoding rule i. If splitting occurs then two or more messages may relay the same source state for some encoding rule. In this case T also chooses a splitting strategy. Given that encoding rule $i \in I$ and the source state $s \in S$ are used, a splitting strategy determines the probability that T sends message m for each message m with may relay s under i.

An optimal strategy for T is a probability distribution P_I on the set I of encoding rules and a splitting strategy which minimizes the probability that O may successfully deceive R. This probability is denoted by V_G and is a measure of the security afforded by the authentication system.

2 Cartesian Doubly Perfect Authentication Systems

Simmons and Brickell [1] have given a bound on V_G in terms of the size of the set I of encoding rules. They show that $V_G \leq b^{-\frac{1}{2}}$. This result was also obtained by

Gilbert, MacWilliams and Sloane [5] for a slightly different situation.

An authentication system for which $V_G = b^{-\frac{1}{2}}$ is called doubly perfect.

In an authentication system (I, M, S), for each $m \in M$, let $I(m)$ denote the set $\{i \in I | f_i(m) \in S\}$. The proof of the following result is contained in the proof of Theorem 6 of Brickell [1].

Lemma 1 *Let (I, M, S) be a doubly perfect authentication system $AS(b,\ v,\ k)$ with $V_G = \alpha$. Then $n = 1/\alpha$ is an integer, $b = n^2$ and $|I(m)| = n$ for all $m \in M$.*

The bound of the following lemma is given by Simmons [11]. Simmons also shows that if equality holds then splitting does not occur in any encoding rule of an optimal strategy. In an optimal strategy for a doubly perfect authentication system all encoding rules are equally likely.

Hence we have

Lemma 2 *Let (I, M, S) be an authentication system $AS(b, v, k)$. Write $n = 1/V_G$. Then $v \geq kn$. If the system is doubly perfect then equality holds if and only if there is no splitting.*

An authentication system is called cartesian if whenever $f_i(m) \neq 0$ and $f_j(m) \neq 0$ for $i, j \in I$ and $m \in M$ then $f_i(m) = f_j(m)$. In a cartesian authentication system a message relays the same source state whichever encoding rule is being used. The sets $M(s) = \{m \in M | f_i(m) = s \text{ for some } i \in I\}$ for $s \in S$ then partition M. In the $b \times k$ array A representing a cartesian authentication system the entry a_{is} is a subset of $M(s)$ which is the set of messages relaying source state s.

Suppose that, for each $s \in S$, ϕ_s is a bijection from $M(s)$ to the set of integers $\{1, 2, \ldots, |M(s)|\}$. Thus ϕ_s labels the messages of $M(s)$ with the integers 1 to

$|M(s)|$. Then $A' = (a_{is})$ where $a_{is} = \phi_s(a_{is})$ is a $b \times k$ array with integer entries. We refer to A' as a cartesian authentication array.

Example 2: Cartesian authentication array corresponding to $AS(9,9,3)$ of Example 1.

Source States			
1	1	1	
1	2	2	
1	3	3	
2	1	2	Encoding
2	2	3	Rules
2	3	1	
3	1	3	
3	2	1	
3	3	2	

Brickell [1] has constructed cartesian doubly perfect authentication systems using cartesian authentication arrays which he has called orthogonal multi-arrays. An orthogonal multi-array $OMA(k, n; r_1, \ldots, r_k)$ is a $n^2 \times k$ array $A = (a_{ij})$ satisfying (i) a_{ij} is a r_j-subset of the set $\{ 1, 2, \ldots, r_j\}$ and (ii) given integers x, y with $1 \leq x < y \leq k$ and integers m_1, m_2 with $1 \leq m_1 \leq r_x n$ and $1 \leq m_2 \leq r_y n$ there exists exactly one i such that $m_1 \in a_{ix}$ and $m_2 \in a_{iy}$. An $OMA(k, n; r_1, \ldots, r_k)$ corresponds to a cartesian doubly perfect authentication system with $b = n^2$, $v = n \sum r_j$ and $V_G = 1/n$. This system has splitting if and only if $r_j > 1$ for some j.

An $OMA(k, n;\ 1, \ldots, 1)$ is called an orthogonal array and denoted $OA(k, n)$. An $OA(k, n)$ is equivalent to a set of $k - 2$ mutually orthogonal latin squares of order n. The maximum number of mutually orthogonal latin squares of order n is $n - 1$. A set of $n - 1$ mutually orthogonal latin squares of order n is called a

complete set. Complete sets of mutually orthogonal latin squares are known to exist when n is a prime power.

$A' = (\phi_s(a_{is})) =$

1	1	1	1,7
1	2	2	2
1	3	3	5
1	4	4	6
1	5	5	3
1	6	6	4,8
2	1	2	6
2	2	3	1,8
2	3	6	3
2	4	1	2
2	5	4	4,7
2	6	5	5
3	1	3	3
3	2	6	6
3	3	2	4,7
3	4	5	1,8
3	5	1	5
3	6	4	2
4	1	4	8
4	2	1	4
4	3	5	2,6
4	4	2	3,5
4	5	6	1
4	6	3	7
5	1	5	4
5	2	4	3,5
5	3	1	8
5	4	6	7
5	5	3	2,6
5	6	2	1
6	1	6	2,5
6	2	5	7
6	3	4	1
6	4	3	4
6	5	2	8
6	6	1	3,6

Encoding Rules

(the numbers represent messages)
Table 1.

If there do not exist $k-2$ mutual orthogonal latin squares of order n then a cartesian doubly perfect authentication system with $V_G = 1/n$ and $|S| = k$ must

have splitting. For example, since there does not exist a pair of orthogonal latin squares of order 6, a cartesian doubly perfect authentication system with $V_G = 1/6$ and $|S| = 4$ must have splitting. In such a case $v > 24$. Brickell [1] gives an example of an $OMA(4, 6; 1, 1, 1, 2)$. This example corresponds to an authentication system with $v = 30$. This is the minimum size of M that such a system arising from an OMA can have. The following example shows that it is possible for a cartesian doubly perfect authentication system with $V_G = 1/6$ and $|S| = 4$ to have fewer than 30 messages.

This example is a cartesian authentication array corresponding to a cartesian doubly perfect authentication system with $V_G = 1/6$, $|S| = 4$ and $v = 26$.

Stinson [11] has used transversal designs to construct a cartesian authentication system with $V_G = 1/6$, $|S| = 7$ and $v = 42$. (This system has a subsystem with 4 source states and 24 messages). However this example has $b = 72$ and is not doubly perfect. In the light of the above example we may state a result in a slightly more general form that that given in theorems 5 and 6 of Brickell [1].

Theorem 1 *Let $S = \{s_1, \ldots, s_k\}$ and let $M(s_1), \ldots, M(s_k)$ be disjoint sets. Put $M = M(s_1) \cup \ldots \cup M(s_k)$. An $n^2 \times k$ array $A = (a_{is})$ where $a_{is} \subseteq M(s)$ for $1 \leq i \leq n^2$, $s \in S$ is an authentication array corresponding to a cartesian doubly perfect authentication system with $V_G = 1/n$ and $|S| = k$ if and only if*

(i) $a_{is} \neq \phi$ for all $1 \leq i \leq n^2$, $s \in S$

(ii) for all $s \in S$ and $m \in M(s)$, $I(m) = \{i | m \in A_{is}\}$ has n elements

(iii) for any s_i, $s_j \in S$, $s_i \neq s_j$, $|I(m_1) \cap I(m_2)| \leq 1$ for all $m_1 \in M(s_1)$ and $m_2 \in M(s_2)$.

3 Incidence Structures

An incidence structure is a triple $(\mathbf{P}, \mathbf{B}, I)$ where $\mathbf{P}$ and $\mathbf{B}$ are non-empty disjoints sets and $\mathbf{I} \subseteq \mathbf{P} \times \mathbf{B}$. The elements of $\mathbf{P}$ are called points and the elements of B are called blocks. We say $P \in \mathbf{P}$ is incident with $x \in B$ if and only if $(P, x) \in \mathbf{I}$.

Let (I, M, S) be a cartesian doubly perfect authentication system $AS(n^2, v, k)$. We may define an incidence structure $(I, M, \mathbf{I})$ by $(i, m) \in \mathbf{I}$ if and only if $f_i(m) \neq 0$. We note that each block $m \in M$ is incident with n points. We also note that if two blocks m, $m' \in M$ are incident with the same set of points then $(I, M \backslash \{m'\}, S)$ would also be a cartesian doubly perfect authentication system. We therefore assume throughout that no two blocks of $(I, M, \mathbf{I})$ are incident with the same set of points. An incidence structure with these two properties is called a design.

The design $(I, M, \mathbf{I})$ has the property that there is a partition of blocks into classes $M(s_1), \ldots M(s_k)$ such that

(i) every point belongs to at least one block of every class,

(ii) any two blocks, belonging to distinct classes, have at most one point in common.

Indeed the existence of a cartesian doubly perfect authentication system with $V_G = 1/n$ and $|S| = k$ is equivalent to the existence of a design with n^2 points, block size n and such a partition.

If the authentication system (I, M, S) has been constructed from an orthogonal multi-array then the partition $M(s_1), \ldots, M(S_k)$ of the design $(I, M, \mathbf{I})$ has the property that each point is incident with a constant number of blocks from each

class. Such a partition is called a resolution. Moreover any two blocks from distinct classes are incident with exactly one common point. Such a resolution is called an *outer resolution.* If the orthogonal multi-array is in fact an orthogonal array, so that there is no splitting in the authentication system, then the blocks of a class are disjoint and the design is a net (See Hughes and Piper [6]). A net with k classes is equivalent to $k-2$ mutually orthogonal Latin squares.

There are two problems:

(1) for a given n find the largest integer k such that there exists a cartesian doubly perfect authentication system with $V_G = 1/n$ and $|S| = k$.

(2) for given n and k find a cartesian doubly perfect authentication system with the minimum number of messages.

These problems correspond to constructing designs admitting partitions of the blocks having the properties described above with the maximum number of blocks. The largest value of k is $n+1$ and the minimum number of blocks is kn. These solutions correspond to orthogonal arrays. See Stinson [11] for a description of these systems in terms of transversal designs.

Theorem 2 *Let (I, M, S) be a cartesian doubly perfect authentication system with $V_G = 1/n$. Let A be a cartesian authentication array for it.*

Then

(i) $|S| \leq n+1$ with equality if and only if A is an orthogonal array

(ii) $|M| \geq n|S|$ with equality if and only if A is an orthogonal array.

Proof: (i) Let $|S| = k$. Let $i \in I$. There exist $m_1, \ldots, m_k \in M$ such that $f_i(m_1)$, $\ldots$, $f_i(m_k)$ are the k elements of S. Then $I(m_1), \ldots I(m_k)$ are k n-subsets of I which intersect pairwise in $\{i\}$. Thus $1 + k(n-1) \leq |I| = n^2$, Hence $k \leq n+1$.

If $k = n+1$ then $I(m_1), \ldots, I(m_k)$ cover the $n^2 - 1$ points of I distinct from i exactly once. Suppose $m \in M$ and $f_i(m) \neq 0$. Then $f_i(m) = f_i(m_j)$ for some j. Now $|I(m) \cap I(m_h)| \leq 1$ for $h \neq j$, so $I(m) \cap I(m_h) = \{i\}$ and we must have $I(m) = I(m_j)$. Hence $m = m_j$.

It follows that there is no splitting, blocks within a class are disjoint and blocks from distinct classes meet in exactly one point. Thus $(I, M, \mathbf{I})$ is a net, and A is an orthogonal array, (ii) follows by lemma 2 and Brickell [1] theorem 6.

When n is a prime power constructions of appropriate nets in the case of equality in theorem 2 are well known for any $k = |S| \leq n+1$.

4 Mutually Orthogonal F-squares

By lemmas 1 and 2 an authentication system (I, M, S) with $|S| = k$, $|I| = n^2$ and $|M| < nk$ cannot be doubly perfect. That is if $|M| \leq nk$ then $V_G \geq 1/n$.

However, for some applications, it may be important that the size of the message space is kept small. In this section we use F-squares which are generalizations of latin squares to construct cartesian authentication systems $AS(n^2, v, k)$ with $v < nk$. By theorem 1 of Simmons [9], which asserts that $V_G \geq |S|/|M|$ it follows that for these systems $V_G > 1/n$, and they are not doubly perfect.

Let n be a positive integer and let $(\lambda_1, \ldots, \lambda_m)$ be a vector of positive integers such that $\lambda_1 + \ldots + \lambda_m = n$. An F-square of order n with frequency vector $(\lambda_1, \ldots, \lambda_m)$ is an $n \times n$ matrix $X = (x_{ij})$ with entries x_{ij} from a set

$U = \{u_1, \ldots, u_n\}$ of m symbols such that each element $u_i \in U$ appears exactly λ_i times in each row and in each column of X. The F-square X is denoted $F(n; \lambda_1, \lambda_2, \ldots, \lambda_m)$. An $F(n; 1, \ldots, 1)$ (also denoted $F(n; 1^n)$) is a latin square. The integers $\lambda_1, \ldots, \lambda_m$ are called the frequencies of the symbols in the square. Two F-squares $F_1(n; \lambda_1, \ldots, \lambda_m)$ and $F_2(n; \mu_1, \ldots \mu_p)$ are called orthogonal if for all $1 \leq i \leq m$ and $1 \leq j \leq p$ the pair (i, j) occurs exactly $\lambda_i \mu_j$ times when F_1 and F_2 are superimposed. (See Denes and Keedwell [4]).

Theorem 3 *Suppose* $F_1 = (x_{ij}^1) = F_1(n; \lambda_{11}, \ldots, \lambda_{1m}), \ldots, F_{k-2} = (x_{ij}^{k-2}) = F_{k-2}(n; \lambda_{(k-2),1}, \ldots, \lambda_{(k-2),m_{(k-2)}})$ *are a set of* $k-2$ *mutually orthogonal* F*-squares. Put* $\lambda = max(\lambda_{ij})$ *and* $t = min(m_i)$. *Then there is a cartesian authentication system* $AS(b, v, k)$ *with* $b = n^2$, $v = 2n + \sum m_i$ *and* $1/n \leq V_G \leq \lambda/n$.

Proof: The $k-2$ mutually orthogonal F-squares determine a $b \times k$ array, $A' = (a_{ij})$ where, for $1 \leq i, j \leq n$,

$$\begin{aligned} a_{n(i-1)+j,h} &= x_{ij}^{h-2} \quad h = 3, \ldots, k \\ a_{n(i-1)+j,1} &= i \\ a_{n(i-1)+j,2} &= j \end{aligned}$$

Corresponding to A' is a cartesian authentication system $(I, M, S) = AS(n^2, v, k)$ where $v = 2n + \sum M_i$. Let $S = \{s_i, \ldots, s_k\}$ and let the partition of M be

$$M_{s_i} = \{m_{i1}, \ldots, m_{i_{p_i}}\}.$$

Suppose $p_h = t$, and suppose O impersonates T using message m_h with probability $1/t$ for $j = 1, \ldots, t$. Since there is, for each encoding rule, exactly one message in M_s which is valid under that rule the probability that O is successful is $\sum p(i) 1/t = 1/t$. Hence $V_G \geq 1/t$.

Now suppose that T uses a strategy with the uniform probability distribution on the encoding rules. Suppose O impersonates T by sending m_{ij}. Then there are $n\lambda_{ij}$ encoding rules under which m_{ij} is valid and the probability that O succeeds is

$$\frac{n\lambda_{ij}}{n^2} = \frac{\lambda_{ij}}{n} \leq \frac{\lambda}{n}.$$

Suppose O observes the message m_{ij} and substitutes m_{ab} for it. There are $n\lambda_{ij}$ encoding rules under which m_{ij} is valid and of these there are $\lambda_{ij}\lambda_{ab}$ under which m_{ab} is also valid. Hence O succeeds in deceiving R with a substitution attack with probability

$$\frac{\lambda_{ij}\lambda_{ab}}{n\lambda_{ij}} = \frac{\lambda_{ab}}{n} \leq \frac{\lambda}{n}.$$

It follows that $V_G \leq \lambda/n$.

Remark: If we identify some symbols in any column of A' so that the total number of occurrences of this combined symbol is at most λn then we obtain an $AS(n^2, v', k)$ which still satisfies $(1/n) \leq V_G \leq \lambda/n$ but for which $v' \leq v$. By making suitable identifications of symbols in an array arising from mutually orthogonal F-squares, we obtain the following result.

Corollary 1 *Suppose there exist $k-2$ mutually orthogonal $F(n, \lambda^t)$-squares (necessarily $n = \lambda t$). Then there exists a cartesian authentication system $AS(n^2, kn/\lambda, k)$ with $V_G = \lambda/n$.*

Example 3: Table 2 is a cartesian authentication array corresponding to an $AS(36, 16, 6)$ with $1/2 \leq V_G \leq 2/3$ constructed as above from four mutually orthogonal F-squares: $F_1(6; 1^6)$, $F_2(6; 1^4, 2)$; $F_3(6; 2^3)$, $F_4(6; 2^1, 4^1)$,

1	2	3	4	5	6
2	3	6	1	4	5
3	6	2	5	1	4
4	1	5	2	6	3
5	4	1	6	3	2
6	5	4	3	2	1

$F_1(6;1^6)$

1	2	5	5	3	4
5	1	3	2	4	5
3	5	4	1	5	2
5	4	2	3	1	5
4	3	5	5	2	1
2	4	1	4	5	3

$F_2(6;1^42)$

1	2	3	3	2	1
1	2	3	3	2	1
3	1	2	2	1	3
2	3	1	1	3	2
3	1	2	2	1	3
2	3	1	1	3	2

$F_3(6;2^3)$

1	2	2	2	2	1
2	1	2	2	1	2
1	2	2	2	2	1
2	2	1	1	2	2
2	2	1	1	2	2
2	1	2	2	1	2

$F_4(6;2^1,4^1)$

Seberry [8] has shown how to construct a set of $n-1$ mutually orthogonal $F(n;\lambda^t)$-squares using a generalized Hadamard matrix of size $n=\lambda t$ with entries from a group G of order t.

Several families of generalized Hadamard matrices $GH(n;G)$ of size n with entries from G are known to exist including the families: $n=2p^\alpha$, $G=Z_p^\alpha$ (Jungnickel [7], Street [12]); $n=4p^\alpha$, $G=Z_p^\alpha$ (Dawson [2]; and $n=(p^\alpha-1)p^\alpha$, $G=\mathbf{Z}_p^\alpha$ (Seberry [8]) (where p is a prime and α is a positive integer). These give families of cartesian authentication systems $AS(b,v,k)$ with $b=n^2$, $v=p^\alpha(n-1)$, $k=n-1$ and $V_G=1/p^\alpha$.

5 Cyclotomy and Mutually Orthogonal F-squares.

In this section we use sets of mutually orthogonal F-squares and cyclotomy to construct authentication systems. This construction is based on a method of Parker (see [4]) for constructing sets of mutually orthogonal latin squares. It

produces authentication schemes $AS(b, v, k)$ with similar properties to those of the previous section: $b = (q+f)^2$, $v < (q+f)k$ and $V_G \leq \lambda/(q+f)$ where q is a prime power and f is the order of the F-squares of some set of $k-2$ mutually orthogonal F-squares.

	Source States					
	1	1	1	1	1	1
	1	2	2	2	2	2
	1	3	3	5	3	2
	1	4	4	5	3	1
	1	5	5	3	2	2
	1	6	6	4	1	2
	2	1	2	5	1	2
	2	2	3	1	2	2
	2	3	6	3	3	1
	2	4	1	2	3	2
	2	5	4	4	2	2
	2	6	5	5	1	1
	3	1	3	3	3	2
	3	2	6	5	1	2
	3	3	2	4	2	1
Encoding Rules	3	4	5	1	2	1
	3	5	1	5	1	2
	3	6	4	2	3	2
	4	1	4	5	2	2
	4	2	1	4	3	1
	4	3	5	2	1	2
	4	4	2	3	1	2
	4	5	6	1	3	2
	4	6	3	5	2	1
	5	1	5	4	3	2
	5	2	4	3	1	1
	5	3	1	5	2	2
	5	4	6	5	2	2
	5	5	3	2	1	1
	5	6	2	1	3	2
	6	1	6	2	2	1
	6	2	5	5	3	2
	6	3	4	1	1	2
	6	4	3	4	1	2
	6	5	2	5	3	1
	6	6	1	3	2	2

(the numbers represent messages)

Table 2.

Let $q = mf + 1$ be a prime power. The multiplicative group of $GF(q)$ is cyclic of order $q - 1$ and has a unique subgroup H of order f. The cyclotomic classes of index m of $GF(q)$ are the cosets of H in the multiplicative group of $GF(q)$.

Suppose $F_1 = (x_{ij}^1)$, $F_2 = (x_{ij}^2)$, ..., $F_m = (x_{ij}^m)$ are m mutually orthogonal F-squares of order f. Suppose that the rows and columns for these F-squares are indexed by an F-set U. Suppose that U_i is the set of symbols appearing in F_i, $i = 1, \ldots, m$. Let $\psi : H \to U$ be a bijection and, for $i = 1, \ldots, m$ let $\phi_i : H \to U_i$ be a function such that for each $u \in U$ there are exactly λ elements $h \in H$ with $\phi_i(h) = u$ where u appears λ times and each row (and column) of F_i.

Let $D = \{(a_1, 1), (a_2, 2), \ldots, (a_{m+1}, m+1)\} \subseteq GF(q) \times \mathbf{Z}_{m+2}$ such that $a_i \neq a_j$ for $i \neq j$. We define a $(q + f)^2 \times m + 2$ array A in the following way:

(1) the f^2 rows of the $f^2 \times (m + 2)$ array B obtained as in the previous section from $F_1, \ldots, F_m$ are rows of A

(2) for each $a \in GF(q)$ the row $aa \ldots a$ is a row of A

(3) for each $(h, j, a) \in H \times \mathbf{Z}_{m+2} \times GF(q)$ there is a row whose dth entry ($1 \leq d \leq m + 2$) is

$$ha_i + a \text{ where } i + j \equiv d (\mathrm{mod} m + 2) \text{ if } j \not\equiv d (\mathrm{mod} m + 2)$$

$$\phi_{d-2}(h) \text{ if } j \equiv d (\mathrm{mod} m + 2), \quad d \neq 1, 2$$

$$\psi(h) \text{ if } j \equiv d (\mathrm{mod} m + 2), \quad d = 1, 2$$

We note that the array A has the following properties: each symbol appearing in columns 1 and 2 appears $q + f$ times; each element of $GF(q)$ appears $q + f$

times in each of the columns 3 to $m+2$; if a symbol appears λ times in each row (and column) of F_i then it appears $\lambda(q+f)$ times in column $i+2$ of A.

Two symbols, neither of which belongs to $GF(q)$, appear together in the same row only in rows of B. The number of times this happens is given by the product of the frequencies of the two symbols (symbols in columns 1 and 2 have frequency 1). A symbol not in $GF(q)$ and an element of $GF(q)$ occur together in λ rows where λ is the frequency of the symbol. Two elements $a, b \in GF(q)$, $a \neq b$, occur together in the same row if and only if there exist $a_i, a_j \in D$ such that $a-b$ or $b-a$ and $a_i - a_j$ belong to the same cyclotomic class.

Put $D_k = \{a_i - a_j | a_i, a_j \in D, i-j = k(\mathrm{mod}\, m+2)\}$, $k = 1, \ldots, m+1$.

Suppose μ_k is the maximum number of representatives of any one cyclotomic class which belong to D_k. Then for $i - j \equiv k(\mathrm{mod}(m+2))$, μ_k is the maximum number of rows of A in which any pair $a, b \in GF(q)$ appear together in columns i, j (respectively). Let μ be the maximum of $\mu_1, \ldots, \mu_{m+1}$. The following theorem may be proved in a similar fashion to theorem 3.

Theorem 1 *Let $q = mf+1$ be a prime-power. Suppose $F_1, \ldots F_m$ are mutually orthogonal F-squares of order f. Let λ be the maximum of the frequencies occurring in $F_1, \ldots F_m$. Suppose $D = \{(a_1, 1), \ldots, (a_{m+1}, m+1)\} \subseteq GF(q) \times \mathbf{Z}_{m+2}$ is such that $a_i \neq a_j$ for $i \neq j$. Let μ be as described above. Then the array A as defined above is a cartesian authentication array corresponding to a cartesian authentication system $AS(b, v, k)$ with $b = (q+f)^2$, $v \leq (q+f)k$ and $V_G \leq max(\lambda, \mu)/(q+f)$.*

By making identifications of symbols we may obtain other cartesian authentication systems $AS(b, v', k)$ with $V_G \leq \max(\lambda, \mu)/(q+f)$ and $v' < v$.

We remark that the construction may be generalized by using a cartesian authentication array of size $f^2 \times (m+2)$ in place of B in D above.

Example 1: Consider $m = 4$. Let $q = 4f + 1$ be a prime power. Suppose there exist four mutually orthogonal F-squares of order f such that each symbol in these squares has frequency 1 or 2. Let α be a primitive element of $GF(q)$ and put $D = \{$ (0,1), (1,2), $(1+\alpha, 3)$, $(1+\alpha+\alpha^2, 4)$, $(1+\alpha+\alpha^2+\alpha^3, 5)\}$. Then if f is odd D_k contains at most 2 elements from any cyclotomic class of index 4 for $k = 1, 2, 3, 4, 5$. Hence in this case the above construction yields an $AS((q+f)^2, 6(q+5), 6)$ with $V_G \leq 2/(q+f)$. For example with $f = 9$, $q = 37$, since there exist four mutually orthogonal latin orders of order 9 we obtain an $AS(46^2, 6.46, 6)$ with $V_G \leq 2/46$.

Ackowledgement: Professor Jennifer Seberry received support under SERC Visiting Fellow Research Grant GR/E83870. The work of Martin H.G. Anthony was supported by an SERC Studentship and the work of Keith M. Martin was supported by a SERC CASE award.

References

[1] Brickell, E.F. A few results in message authentication. *Congressus Numerantium*, **43**, (1984), 141-154.

[2] Dawson, J.E. A construction for generalized hadamard matrices $GH(4q, EA(q))$, *J. Stat. Planning and Inference*, **11**, (1985), 103-110.

[3] de Launey, W. A survey of generalized Hadamard matrices and difference matrices $D(k, \lambda, G)$ with large k, *Utilitas Math.*, **30** (1986), 5-29.

[4] Denes, J. and Keedwell, A.D. *Latin Squares and their Applications*, English

Universities Press, London, 1974.

[5] Gilbert, E.N., MacWilliams, F.J. and Slone, N.J.A. Codes which detect deception. *The Bell Sys. Tech Journal*, **53**, (1974), 405-414.

[6] Hughes, D.R. and Piper, F.C. *Design Theory*, Cambridge University Press, Cambridge, 1985.

[7] Jungnickel, D. On difference matrices, resolvable TD's and generalized Hadamard matrices, *Math. Z*, **167**, (1979), 49-60.

[8] Seberry, J. A construction for generalized Hadamard matrices, *J. Stat. Planning and Inference*, **4**, (1980), 365-368.

[9] Simmons, G.J. Message authentication: a game on hypergraphs, *Congressus Numerantium*, **45**, (1984), 161-192.

[10] Simmons, G.J. Authentication theory / coding theory, in *"Advances in Cryptology: Proceedings of Cryto '84"*, Lecture Notes in Computer Science, vol. 196, 411-432, Springer Verlag, Berlin, 1985.

[11] Stinson, D.R. Some constructions and bounds for authentication codes, *J. of Cryptology*, **1**, (1988), 37-51.

[12] Street, D.J. Generalized Hadamard matrices, orthogonal arrays and F-squares, *Ars Combinatoria*, **8**, (1979), 131-141.

*Department of Mathematics
RHBNC
University of London
Egham, Surrey TW20 0EX,
U.K.

**Department of Computer Science
University College
University of New South Wales
Australian Defence Force Academy
Canberra, A.C.T. 2600
Australia