A Construction for Authentication/secrecy Codes from 3-homogeneous Permutation Groups

D. R. Stinson and L. Teirlinck

In this paper, we construct codes which provide both secrecy and authentication using 3-homogeneous groups. We construct an infinite family of codes which provide perfect secrecy even if the same encoding rule is used three times in succession; and provide optimal protection against deception by an opponent who observes up to two authentic messages and then substitutes a message of his own choosing.

1. Authentication and Secrecy

This paper is a continuation of [19], in which we studied the properties of codes with respect to secrecy and authentication. We are interested in the *unconditional,* or *theoretical,* security provided by such codes: that is, we assume that any opponents have unlimited computational resources. The theory of unconditional secrecy is due to Shannon [14]. More recently, Simmons has developed an analogous theory of unconditional authentication.

We shall use the model of authentication theory as described by Simmons in [15], [16] and [17]. In this model, there are three participants: a transmitter, a receiver and an opponent. The *transmitter* wants to communicate some information to the *receiver,* whereas the *opponent* wants to deceive the receiver. The opponent can either impersonate the receiver, or, modify a message which has been sent by the transmitter, in each case attempting to make him accept a fraudulent message as authentic.

More formally, we have a set of k source states $\mathcal{S}$, a set of v messages $\mathcal{M}$, and a set of b encoding rules $\mathcal{E}$. A *source state* $s \in \mathcal{S}$ is the information that the transmitter wishes to communicate to the receiver (i.e. the *plaintext*). The transmitter and receiver will have secretly chosen an *encoding rule* (or *key*) $e \in \mathcal{E}$ beforehand. An encoding rule e will be used to determine the *message* (or *ciphertext*) $e(s)$ to be sent to communicate any source state s. It is possible that more than one message can be used to determine a particular source state (this is called *splitting*). However, in order for the 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 $m \in \mathcal{M}$ (i.e. $e(s) \neq e(s')$ if $s \neq s'$). It is useful to think of a code as being represented by a $b \times k$ matrix, 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 are interested in the security of such a code with respect to both *secrecy* and *authentication.* Suppose an opponent observes i ($\geqslant 0$) distinct messages being sent over the communication channel using the same encoding rule. Although he knows that the same encoding rule is being used to transmit the i messages, he does not know what that encoding rule is. 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.

In [10] and [13], the following scenario for authentication is investigated. As before, an opponent observes i distinct messages sent using the same encoding rule. The

0195-6698/90/010073 + 07 $02.00/0

opponent then sends a message m' to the receiver, hoping to have it accepted as authentic (this message m' must be distinct from the i messages already sent). In [10], Massey calls this a *spoofing attack* of order i. We remark that the special cases $i = 0$ and $i = 1$ have been studied extensively by Simmons and other people (see [2], [4], [15], [16], [17], [18] and [19]). The case $i = 0$ is called the *impersonation* game, and the case $i = 1$ is called the *substitution* game.

For any i, there will be some probability distribution 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 S, 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 $\mathscr{E}$, called an *encoding strategy*. If splitting occurs, then they will also determine a *splitting strategy* to determine $m \in \mathscr{M}$, given $s \in \mathscr{S}$ and $e \in \mathscr{E}$. In this paper, however, we consider only codes without splitting. Once the transmitter/receiver have chosen encoding strategies, we can define for each $i \geqslant 0$ a probability denoted Pd_i, which is the probability that the opponent can deceive the transmitter/receiver with a spoofing attack of order i.

THEOREM 1.1 [10, p. 12]. *In an authentication code without splitting,* $Pd_i \geqslant (k - i)/(v - i)$.

Following Massey [10], we say that the authentication code is *L-fold secure against spoofing* if $Pd_i = (k - i)/(v - i)$ for $0 \leqslant i \leqslant L$.

When we consider the secrecy properties of a code, we desire that no information be conveyed by the observation of the messages which are transmitted. We say that a code has *perfect L-fold secrecy* if, for every $L' \leqslant L$, for every set M_1 of L' messages observed in the channel, and for every set S_1 of L' source states, we have $p(S_1 \mid M_1) = p(S_1)$. That is, observing a set of L' messages in the channel gives no information to the opponent regarding the L' source states.

Define an *L-code* to be a code which achieves perfect L-fold secrecy and is $(L - 1)$-fold secure against spoofing. A lower bound on the number of encoding rules required in any L-code is given by the following theorem, proved in [19].

THEOREM 1.2. *If a code achieves perfect L-fold secrecy and is $(L - 1)$-fold secure against spoofing, then* $b \geqslant \binom{v}{L}$.

An L-code is *optimal* if the number of encoding rules is $\binom{v}{L}$. A construction for optimal 2-codes was given in [19]. In this note, we give a construction for an infinite class of 3-codes in which the number of encoding rules is $v(v - 1)(v - 2)/2$, or three times the optimal value. We also give some examples of optimal 3-codes.

2. A Construction for Optimal L-codes Using Perpendicular Arrays

Our interest in this paper is in constructing L-codes. We can do this using a type of combinatorial design known as a perpendicular array. A *perpendicular array* $PA_\lambda(t, k, v)$ is a $\lambda \cdot \binom{v}{t}$ by k array, A, of the symbols $\{1, \ldots, v\}$, which satisfies the following properties:

(i) every row of A contains k distinct symbols;

(ii) for any t columns of A, and for any t distinct symbols, there are precisely λ rows r of A such that the t given symbols all occur in row r in the given t columns.

For $t \geqslant 2$, it is easy to see that property (i) is implied by the other assumptions.

Some necessary conditions for the existence of a $PA_\lambda(t, k, v)$ are given in [8], as follows.

THEOREM 2.1. *Suppose that* $0 \leqslant t' \leqslant t$ *and* $\binom{k}{r} \geqslant \binom{k}{t'}$. *Then a* $PA_\lambda(t, k, v)$ *is also a* $PA_{\lambda(t')}(t', k, v)$, *where*

$$\lambda(t') = \lambda \cdot \binom{v-t'}{t-t'} \Big/ \binom{t}{t'}.$$

Hence,

$$\lambda \cdot \binom{v-t'}{t-t'} \equiv 0 \text{ modulo } \binom{t}{t'}.$$

We have the following construction for secrecy codes using perpendicular arrays.

THEOREM 2.2. *If there exists a* $PA_\lambda(t, k, v)$ *which at the same time is a* $PA_{\lambda(t')}(t', k, v)$ *for all* $t' \leqslant t$, *then there is a code for k source states with v messages and* $\lambda \cdot \binom{v}{t}$ *encoding rules, which achieves perfect t-fold secrecy.*

PROOF. Let A be a $PA_\lambda(t, k, v)$, which at the same time is a $PA_{\lambda(t')}(t', k, v)$ for all $t' \leqslant t$. We construct an encoding rule from each row r of A: for each row $r = (x_1, \ldots, x_k)$, and for each source state s $(1 \leqslant s \leqslant k)$, define $e_r(s) = x_s$. Use each encoding rule with probability $1/\lambda \cdot \binom{v}{t}$. It is easy to see that we have perfect t'-fold secrecy for all $t' \leqslant t$, since any set of t' messages corresponds equally often (namely $\lambda(t')$ times) to every possible set of t' source states. □

Note that if $k \geqslant 2t - 1$, then $\binom{k}{t} \geqslant \binom{k}{t'}$ for all $t' \leqslant t$. Thus, by Theorem 2.1, any $PA_\lambda(t, k, v)$ with $k \geqslant 2t - 1$ satisfies the conditions of Theorem 2.2.

In order for a code constructed by means of Theorem 2.2 to be $(t-1)$-fold secure against spoofing, our PA must enjoy an extra property. A $PA_\lambda(t, k, v)$, A, is said to be an *authentication PA* (and is denoted $APA_\lambda(t, k, v)$) if the following property holds:

> For any $t' \leqslant t - 1$, and for any $t' + 1$ distinct symbols x_i $(1 \leqslant i \leqslant t' + 1)$, we have that among all the rows of A which contain all the symbols x_i $(1 \leqslant i \leqslant t' + 1)$, the t' symbols x_i $(1 \leqslant i \leqslant t')$ occur in all possible subsets of t' columns equally often.

The following theorem shows that an $APA_\lambda(t, k, v)$ always satisfies the condition required in Theorem 2.2.

THEOREM 2.3. *An* $APA_\lambda(t, k, v)$ *is also an* $APA_{\lambda(t')}(t', k, v)$ *for all* $t' \leqslant t$.

PROOF. Let A be an $APA_\lambda(t, k, v)$. If $t = t'$, there is nothing to prove. Hence, assume that $t' < t$ and that we have already proved that A is an $APA_{\lambda(t'+1)}(t'+1, k, v)$. Let C be a set of t' columns of A and let x_i $(1 \leqslant i \leqslant t')$ be t' distinct symbols. For each symbol $a \notin \{x_i\colon 1 \leqslant i \leqslant t'\}$, there are $\lambda(t'+1) \cdot \binom{k}{t'+1}$ rows containing $\{a\} \cup \{x_i\colon 1 \leqslant i \leqslant t'\}$. Of these, $\lambda(t'+1) \cdot \binom{k}{t'+1}/\binom{k}{t'}$ will contain $\{x_i\colon 1 \leqslant i \leqslant t'\}$ in the columns in C. Let λ_0 denote the total number of rows containing $\{x_i\colon 1 \leqslant i \leqslant t'\}$ in the columns in C. We count ordered triples $(c, x_{t'+1}, r)$, where $c \notin C$, $x_{t'+1} \notin \{x_i\colon 1 \leqslant i \leqslant t'\}$, and row r contains $\{x_i\colon 1 \leqslant i \leqslant t'\}$ in the columns in C and $x_{t'+1}$ in column c. This yields

$$(k - t') \cdot \lambda_0 = (v - t') \cdot \lambda(t'+1) \cdot \binom{k}{t'+1} \Big/ \binom{k}{t'}.$$

Simplifying this equation yields $\lambda_0 = \lambda(t')$. Thus, A is a $PA_{\lambda(t')}(t', k, v)$. The fact that A is an APA is obvious. □

Obviously, a necessary condition for the existence of an $APA_\lambda(t, k, v)$ is that

$$\lambda(t'+1)\cdot\binom{k}{t'+1}\equiv 0 \text{ modulo } \binom{k}{t'}$$

for all t', $0\leqslant t'\leqslant t-1$. In the case $t=3$ and $\lambda=1$, we see that $k\equiv 2$ modulo 3 is necessary.

Theorem 2.4. *If there exists an $APA_\lambda(t, k, v)$, then there is a t-code for k source states with v messages and $\lambda\cdot\binom{v}{t}$ encoding rules.*

Proof. This is a modification of [19, Theorem 4]. Let A be an $APA_\lambda(t, k, v)$. Construct the code as in Theorem 2.2. We need only verify that $Pd_i=(k-i)/(v-i)$, $0\leqslant i\leqslant t-1$. Let x_i $(1\leqslant i\leqslant t'+1)$ be distinct messages $(0\leqslant t'\leqslant t-1)$. Define $E(x_1, \ldots, x_j)=\{e: x_i\in\{e(s): s\in\mathcal{S}\}, 1\leqslant i\leqslant j\}$, and define $f_e(m)=s$ if $e(s)=m$. Suppose an opponent observes the t' messages x_i $(1\leqslant i\leqslant t')$ in the channel, and then sends $x_{t'+1}$. His chance of successful deception is calculated to be:

$$\frac{\sum_{e\in E(x_1,\ldots,x_{t'+1})} p(e)\cdot p(\{s_1,\ldots,s_{t'}\}=\{f_e(x_1),\ldots,f_e(x_{t'})\})}{\sum_{e\in E(x_1,\ldots,x_{t'})} p(e)\cdot p(\{s_1,\ldots,s_{t'}\}=\{f_e(x_1),\ldots,f_e(x_{t'})\})}$$

$$=\frac{\sum_{e\in E(x_1,\ldots,x_{t'+1})} p(\{s_1,\ldots,s_{t'}\}=\{f_e(x_1),\ldots,f_e(x_{t'})\})}{\sum_{e\in E(x_1,\ldots,x_{t'})} p(\{s_1,\ldots,s_{t'}\}=\{f_e(x_1),\ldots,f_e(x_{t'})\})} \qquad \text{(since } p(e) \text{ is constant)}$$

$$=\frac{\lambda(t'+1)\cdot\binom{k}{t'+1}}{\lambda(t')\cdot\binom{k}{t'}}=\frac{\binom{t'+1}{t'}\cdot\binom{k}{t'+1}}{(v-t')\cdot\binom{k}{t'}} \qquad \text{(Theorem 2.1)}$$

$$=(k-t')/(v-t').$$

Hence, $Pd_{t'}=(k-t')/(v-t')$, as desired. □

In [19], the existence of $APA_1(2, k, v)$ was studied (in that paper, they were referred to as pair-column balanced PAs). The following theorem summarizes known results.

Theorem 2.5. *There exists an $APA_1(2, 3, v)$ iff $v\geqslant 7$ is odd* ([19] *and Example* 1). *There exists an $APA_1(2, 5, v)$ if $v\equiv 1$ or* 5 modulo 10, *$v\geqslant 11$, $v\neq 15$* ([9]). *There exists an $APA_1(2, k, v)$ if k is odd and $v\equiv 1$* modulo 2*k is a prime power* ([6]).

We present an $APA_1(2, 3, 17)$.

Example 1. An $APA_1(2, 3, 17)$ (private communication from Bert den Boer). Let the π be the permutation (0 1 2 3 4 5 6 7 8 9)(10 11 12 13 14)(15 16). Let π act on the following starting rows, obtaining 10 rows from each of them:

15	0	1	0	1	15
3	15	0	11	9	2
11	1	3	9	2	11
1	3	11	2	11	1
3	11	9	0	4	8

Next, take the images of each of the following three rows under π^i, $i=0, 1, 2, 3, 4$:

0	5	11	5	11	0
11	0	5			

Finally, take the 21 rows of an $APA_1(2, 3, 7)$ on the symbols 10–16.

In the next section, we prove some results concerning $APA_1(3, v, v)$ and $APA_3(3, v, v)$ using 3-homogeneous groups. Then, recursive constructions lead to $APA_1(3, k, v)$ and $APA_3(3, k, v)$, where $v > k$.

3. 3-Homogeneous Groups and Authentication Perpendicular Arrays

In a $PA_\lambda(t, k, k)$, every subset of $\{1, 2, \ldots, k\}$ appears in all rows. Hence, if A is a $PA_\lambda(t, k, k)$, then A is an $APA_\lambda(t, k, k)$ iff A is a $PA_{\lambda(t')}(t', k, k)$ for all $t' \leq t$. Combining this with Theorem 2.1, we obtain:

Theorem 3.1. *Every $PA_\lambda(t, k, k)$ with $k \geq 2t-1$ is an $APA_\lambda(t, k, k)$.*

A permutation group G is said to have *degree n* if it acts on a set, say S, of n symbols. G is defined to be *t-homogeneous* if for all t-subsets $S_1, S_2 \subseteq S$, there are the same number of permutations $\pi \in G$ such that $(S_1)^\pi = S_2$. The number of such π must be $|G|/\binom{n}{t}$. It is clear that if we write down the permutations in a t-homogeneous group of degree n as the rows of an array, then we obtain a $PA_\lambda(t, n, n)$, where $\lambda = |G|/\binom{n}{t}$. If $2 \leq t \leq (n+1)/2$, then by Theorem 3.1, the PA will be an APA.

Of course, codes in which the number of messages equals the number of source states are of no use for authentication, since the probability of deception is 1. We build codes with more messages than source states by means of a recursive construction using t-designs. A t-design $S(t, k, v)$ is a set of k-subsets (called *blocks*) of a v-set, such that every t-subset occurs in a unique block.

Theorem 3.2. *Suppose that there is a t-design $S(t, k, v)$, and an $APA_\lambda(t, k, k)$. Then, there is an $APA_\lambda(t, k, v)$.*

Proof. For each block in the $S(t, k, v)$, construct an $APA_\lambda(t, k, k)$. The union of all these $APA_\lambda(t, k, k)$ is an $APA_\lambda(t, k, v)$. □

In the case $t = 3$, we have the necessary ingredients for Theorems 3.1 and 3.2. First, let us consider examples of 3-homogeneous groups. If $q \equiv 3$ modulo 4 is a prime power, then the group $PSL(2, q)$ is a 3-homogeneous group of degree $q+1$ (see, for example, [1, Prop. III.6.12]). Since $|PSL(2, q)| = (q^3 - q)/2$, then $\lambda = 3$. Hence, we have

Lemma 3.3. *For any prime power $q \equiv 3$ modulo 4, there is an $APA_3(3, q+1, q+1)$.*

Kantor [7] has shown that there are only two examples of *sharply* 3-homogeneous groups (i.e. where $\lambda = 1$) of degree $n \geq 6$. These are $AGL(1, 8)$ and $A\Gamma L(1, 32)$ (see, for example, [1, III.5.7]). The resulting APAs are as follows:

Lemma 3.4. *There is an $APA_1(3, 8, 8)$ and an $APA_1(3, 32, 32)$.*

Example 2. An $APA_1(3, 8, 8)$. Develop the following rows modulo 7.

$$\begin{array}{cccccccc}
x & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\
0 & x & 3 & 6 & 1 & 5 & 4 & 2 \\
1 & 3 & x & 4 & 0 & 2 & 6 & 5 \\
2 & 6 & 4 & x & 5 & 1 & 3 & 0 \\
3 & 1 & 0 & 5 & x & 6 & 2 & 4 \\
4 & 5 & 2 & 1 & 6 & x & 0 & 3 \\
5 & 4 & 6 & 3 & 2 & 0 & x & 1 \\
6 & 2 & 5 & 0 & 4 & 3 & 1 & x
\end{array}$$

There is no sharply 3-homogeneous permutation group of degree 5. However, as noted in [8], a $PA_1(3, 5, 5)$ can be obtained by developing the rows 0 1 2 3 4 and 0 2 4 1 3 modulo 5. By Theorem 3.1, this is an $APA_1(3, 5, 5)$.

We use a class of 3-designs known as inversive geometries in our recursive construction for all prime powers q and for all $d \geqslant 1$, there is an $S(3, q+1, q^d+1)$ (see [23]). Hence, we obtain:

THEOREM 3.5. *For any prime power* $q \equiv 3$ modulo 4, *and for any* $d \geqslant 1$, *there exists an* $APA_3(3, q+1, q^d+1)$.

THEOREM 3.6. *For any* $d \geqslant 1$, *there exists an* $APA_1(3, 5, 4^d+1)$, *an* $APA_1(3, 8, 7^d+1)$ *and an* $APA_1(3, 32, 31^d+1)$.

Theorem 3.5 allows us to construct a 3-code for as many source states as desired (by taking q large enough), and incorporating any desired level of authentication security. For, the resulting code has Pd_i approximately equal to $1/q^{d-1}$ ($i = 0, 1, 2$), which can be made arbitrarily small by taking d large enough.

4. CONCLUDING REMARKS

Two very interesting open problems are whether there are $APA_1(3, k, v)$ for arbitrarily large k, and whether there are any $APA_1(t, k, v)$ with $t \geqslant 4$.

Some other examples of $APA_\lambda(t, k, v)$ with $\lambda > 1$ exist, as follows. The designs $OD_\lambda(t, k, v)$ defined in [20] are $APA_{\lambda \cdot t!}(t, k, v)$. For any t, there exist $OD_1(t, t+1, v)$ for infinitely many values of v by [20]; hence $APA_{t!}(t, t+1, v)$ exist as well. However, the only known $OD_1(t, k, v)$ with $k > t+1$ and $t \geqslant 6$ are the $OD_1(t, t+2, t+2)$ constructed from the alternating group A_{t+2}. These yield $APA_{t!}(t, t+2, t+2)$ and $APA_{(t+1)!/2}(t+1, t+2, t+2)$. Other constructions for $OD_\lambda(t, k, v)$ are given in [21].

The following $APA_\lambda(t, k, k)$ with $1 < \lambda < t!$ and $t \geqslant 4$ can be obtained. $APA_4(4, 9, 9)$, $APA_4(5, 9, 9)$, $APA_6(6, 9, 9)$, $APA_{14}(7, 9, 9)$ and $APA_{56}(8, 9, 9)$ can be constructed from $PGL(2, 8)$; and $APA_4(4, 33, 33)$ can be constructed from $P\Gamma L(2, 32)$ (see [1] for a description of these groups). We are using here the fact that a $PA_\lambda(t, k, k)$ is also a $PA_\lambda(k-t, k, k)$.

From the $PA_3(3, 6, 6)$ constructed in [8], we obtain an $APA_3(3, 6, 6)$, $APA_4(4, 6, 6)$ and $APA_{10}(5, 6, 6)$. Moreover, the $APA_1(3, 5, 5)$ mentioned in Section 3 is also an $APA_2(4, 5, 5)$.

Using t-designs constructed by Witt [22], Denniston [3] and Mills [11], together with Theorem 3.2 we obtain $APA_2(4, 5, v)$ for $v = 11$, 23, 47 and 83; $APA_4(4, 6, 27)$; and $APA_{10}(5, 6, v)$ for $v = 12$, 24, 48 and 84.

Finally, let us mention that designs $OD_\lambda(t, k, v)$ and $APA_\lambda(t, k, v)$ can be constructed recursively using t-wise balanced designs, in a manner similar to Construction 2.1 of [8].

ACKNOWLEDGMENTS

This research was supported in part by the Institute for Mathematics and its Applications, with funds provided by the National Science Foundation. The research of the first author was supported by NSERC grant A9287, and the research of the second author was supported by NSA grant MDA 904-88-H-2005.

References

1. Th. Beth, D. Jungnickel and H. Lenz, *Design Theory,* Bibliographisches Institut, Zurich, 1985.
2. E. F. Brickell, A few results in message authentication, *Congressus Numer.* **43** (1984), 141–154.
3. R. H. F. Denniston, Some new 5-designs, *Bull. London Math. Soc.,* **8** (1976), 263–267.
4. M. De Soete, Some constructions for authentication-secrecy codes, in: *Advances in Cryptology: Proceedings of Eurocrypt '88,* Lecture Notes in Computer Science, vol. 330 Springer-Verlag, Berlin, 1988, pp. 57–76.
5. E. Gilbert, F. J. MacWilliams and N. J. A. Sloane, Codes which detect deception, *Bell System Tech. J.,* **53** (1974), 405–424.
6. A. Granville, A. Moisiadis and R. Rees, Nested Steiner n-gon systems and perpendicular arrays, *J. Comb. Math. Comb. Comput.,* **3** (1988), 163–167.
7. W. M. Kantor, k-homogeneous groups, *Math. Z.,* **124** (1972), 261–265.
8. E. S. Kramer, D. L. Kreher, R. Rees and D. R. Stinson, On perpendicular arrays with $t \geq 3$, *Ars Combin.,* to appear.
9. C. C. Lindner and D. R. Stinson, Steiner pentagon systems, *Discr. Math.,* **52** (1984), 67–74.
10. J. L. Massey, Cryptography—a selective survey, in: *Digital Communications,* 1986, pp. 3–21.
11. W. H. Mills, A new 5-design, *Ars Combin.,* **6** (1978), 193–195.
12. R. C. Mullin, P. J. Schellenberg, G. H. J. van Rees and S. A. Vanstone, On the construction of perpendicular arrays, *Utilitas Math.,* **18** (1980), 141–160.
13. P. Schobi, Perfect authentication systems for data sources with arbitrary statistics, presented at Eurocrypt '86.
14. C. E. Shannon, Communication theory of secrecy systems, *Bell System Tech. J.,* **28** (1949), 656–715.
15. G. J. Simmons, A game theory model of digital message authentication, *Congressus Numer.,* **34** (1982), 413–424.
16. G. J. Simmons, Message authentication: a game on hypergraphs, *Congressus Numer.,* **45** (1984), 161–192.
17. G. J. Simmons, Authentication theory/coding theory, in: *Advances in Cryptology: Proceedings of CRYPTO 84,* Lecture Notes in Computer Science, vol. 196, Springer-Verlag, Berlin, 1985, pp. 411–432.
18. D. R. Stinson, Some constructions and bounds for authentication codes, *J. Cryptol.,* **1** (1988), 37–51.
19. D. R. Stinson, A construction for authentication/secrecy codes from certain combinatorial designs, *J. Cryptol.,* **1** (1988), 119–127.
20. L. Teirlinck, On large sets of disjoint ordered designs, *Ars Combin.,* **25** (1988), 31–37.
21. L. Teirlinck, Generalized idempotent orthogonal arrays, to appear.
22. E. Witt, Die funffach transitiven Gruppen von Mathieu, *Abh. Math. Sem. Hamburg,* **12** (1938), 256–264.
23. E. Witt, Uber Steinersche Systeme, *Abh. Math. Sem. Hamburg,* **12** (1938), 265–275.

Received 24 October 1988 and accepted in revised form 20 June 1989

D. R. Stinson
Department of Computer Science,
University of Manitoba,
Winnipeg, Manitoba R3T 2N2, Canada

L. Teirlinck
Department of Algebra, Combinatorics and Analysis,
Auburn University, Auburn, Alabama 36849, U.S.A.