J. Cryptology (1990) 3: 1–25

Journal of Cryptology

Key-Minimal Cryptosystems for Unconditional Secrecy[1]

Philippe Godlewski
Département réseaux, Ecole Nationale Supérieure des Télécommunications, 46 rue Barrault, 75634 Paris Cedex 13, France

Chris Mitchell
Computer Science Department, Royal Holloway and Bedford New College, Egham Hill, Egham, Surrey TW20 0EX, England

Abstract. This paper is concerned with cryptosystems offering perfect or unconditional secrecy. For those perfect-secrecy systems which involve using keys just once, the theory is well established; however, this is not the case for those systems which involve using a key several times. This paper takes a rigorous approach to the definition of such systems, and exhibits some new families of examples of systems providing perfect secrecy for which the number of keys is minimal.

Key words. Unconditional secrecy, Secrecy code, Perpendicular array, Latin square.

1. Scope and Purpose

Two of the main applications of cryptography are the provision of secrecy and/or authentication for messages. In 1949 Shannon [14] showed how to construct systems offering unconditional secrecy, i.e., theoretically perfect-secrecy systems, at the expense of the use of very large key spaces. Following this work on secrecy, Simmons [15] and others [3], [6] have considered systems which offer unconditional authentication, again at the expense of requiring very large numbers of keys.

In fact, most practical security systems are not theoretically secure, and could be broken given unlimited computational resources. Such practical security systems are based on reasonable assumptions about the difficulty of certain computational problems, and have the advantage of using manageable numbers of keys.

Nevertheless, unconditionally secure systems do find a use in certain special applications, e.g., the Washington–Moscow "Hot Line" [10]. It is also interesting to note that, although such "perfectly-secure" systems have been studied for nearly 40 years, the theory is not fully developed, at least in the public domain. It is the purpose of this paper to contribute to the development of this theory.

In particular, it attempts to classify a number of different definitions of perfect secrecy. Developing from this discussion of definitions, lower bounds are given for

[1] Date received: April 27, 1989. Date revised: May 7, 1990.

the number of keys in such perfect systems, and theorems characterizing systems meeting these lower bounds ("key-minimal systems") are obtained. The last part of the paper is concerned with discussing examples of key-minimal systems providing unconditional secrecy.

2. Notation

In this section we develop the notation and list the assumptions used throughout this paper. We use the basic model for a security code developed by Simmons [15] and used by Brickell [3], De Soete [4], [5], and Stinson [16], [17].

In this model there are three parties: the Transmitter, T, the Receiver, R, and an opponent, O. T wishes to send R one or more pieces of information in such a way that they cannot be read (secrecy) and/or modified/impersonated (authentication) by O. T and R achieve this by using a *security code* in conjunction with a secret, preagreed *encoding rule* from this security code; this encoding rule may be regarded as the cryptographic transformation corresponding to a secret key. It is always assumed that O knows the security code completely, the only secret is the encoding rule (i.e., the key) in use.

More formally, a security code consists of three sets: a set S of *source states*, a set M of *encoded messages*, and a set E of *encoding rules*. Each encoding rule e is an injective function from S into M. Note that in the general case e may map a single element of S onto more than one message; this situation is usually called *splitting* and we do not allow it here (note that splitting is implicitly ruled out by our assumption that each encoding rule is a function). We write k for $|S|$, v for $|M|$, and b for $|E|$ throughout, and, following De Soete [4], [5], write SC(k, v, b) for a security code with k source states, v encoded messages, and b encoding rules.

In this notation the set of source states corresponds to the set of different pieces on information T may wish to send to R. The set of encoded messages corresponds to what is actually transmitted and, perhaps, intercepted by O. The objective is to design the SC(k, v, b) so that the scheme protects T and R from O.

We write $p_M(m)$, $p_S(s)$, and $p_E(e)$ for the *a priori* probabilities of occurrence of message $m \in M$, source state $s \in S$, and encoding rule $e \in E$. We assume that encoding rules and source states are chosen independently, and hence

$$p_{S,E}(s, e) = p_S(s) \cdot p_E(e).$$

We also assume that if two or more source states are to be encoded and sent using the same encoding rule, then the probabilities of occurrence of these source states are independent.

Note that, since the probability of a message occurring is completely dependent on the associated probabilities for encoding rules and source states, we always have

$$p_M(m) = \sum_{*} p_S(s) \cdot p_E(e),$$

where $\sum_*$ denotes the sum over all pairs (s, e) of source states s and encoding rules e such that $e(s) = m$.

We write $p_{S|M}(s|m)$, $p_{M|S}(m|s)$, $p_{E|M}(e|m)$, and $p_{M|E}(m|e)$ for the conditional probabilities that source state s was intended if it is known that message m was sent, etc.

So far we have considered the probabilities of occurrence of single source states, encoding rules, and messages. In fact, for the majority of this paper we are concerned with the situation where L distinct source states are to be communicated from T to R (using the same encoding rule), and hence L distinct messages are sent from T to R. In this context, if S' is any L'-subset of S ($L' \leq L$), then we write $p_S(S' : L)$ for the probability that the intended set of L source states includes S'. The probability $p_M(M' : L)$ is defined in a similar way (where M' is a subset of M of cardinality at most L).

We drop the subscripts in our probability notation if it is clear what probability space is being used. We also drop the value L if it is clear how many source states are to be communicated. We abuse the notation slightly by writing $p_S(\mathbf{s})$ where $\mathbf{s}$ is an i-tuple of distinct source states, instead of something like $p_{S(i)}(\mathbf{s} : i)$ where $S(i)$ denotes the set of all i-tuples of distinct source states. We also write $p(\mathbf{s} : i)$ where $\mathbf{s}$ is a j-tuple of distinct source states, $j \leq i$. By this we mean the probability that the source states in $\mathbf{s}$ are the first j of the i sent. In this context observe that

$$p(\mathbf{s} : i) = p(\mathbf{s} : j),$$

although a similar result would not be true if $\mathbf{s}$ was replaced by a j-subset of S. Minor abuses like these should be clear from the context, and have been done for the sake of clarity of exposition.

The only restrictions we place on the probability distributions are as follows. We require that for every encoding rule e

$$p_E(e) > 0,$$

for every message m

$$p_M(m) > 0,$$

and for every source state s

$$p_S(s) > 0.$$

This can easily be achieved by simply removing from the sets under consideration those source states, messages, and encoding rules with probability 0 of occurrence.

If M' is some subset of M, i.e., M' is a set of encoded messages, then M' is said to be an *allowable* set if and only if there exists an encoding rule e and a subset S' of S such that

$$e(S') = M'.$$

In other words, M' is allowable iff M' could correspond to a set of messages encoded under a single encoding rule. An equivalent definition is as follows. M' is allowable iff

$$p_M(M') > 0.$$

Note that this probabilistic definition is only equivalent to the original one under the above assumptions that all encoding rules and source states have nonzero probabilities of occurrence. Note also that, since every message is assumed to have a nonzero probability of occurrence, every singleton message set $\{m\}$ is allowable. We denote the set of all allowable i-subsets of M by X_i.

We define allowable tuples of messages in the same way. If $\mathbf{m}$ is an i-tuple of distinct encoded messages, then $\mathbf{m}$ is *allowable* if and only if there exists an encoding rule e and an i-tuple of distinct source states $\mathbf{s}$ such that

$$e(\mathbf{s}) = \mathbf{m}.$$

Note that here, as throughout this paper, if

$$\mathbf{s} = (s_1, s_2, \ldots, s_i)$$

is an i-tuple of source states, then by $e(\mathbf{s})$ we mean $(e(s_1), e(s_2), \ldots, e(s_i))$. We denote the set of allowable i-tuples of distinct encoded messages by Y_i.

3. Definitions of "Perfect" Secrecy

The initial problem that needs to be overcome in a formal study of cryptosystems providing unconditional or "perfect" secrecy is the fact that existing definitions vary. Therefore, before attempting to study such systems we review the existing definitions, and indicate the relationships between them.

The first definition we give is a slightly modified version of a definition due to Stinson [16], [17].

Definition. Give $L \geq 1$, an SC(k, v, b) is said to provide *Unordered Perfect L-fold secrecy* (U(L)-*secrecy*) if, for every allowable L-subset M' of M and for every L-subset S' of S,

$$p_{S|M}(S'|M' : L) = p_S(S' : L).$$

The second definition we give is the unmodified form of Stinson's definition [16], [17].

Definition. Given $L \geq 1$, an SC(k, v, b) is said to provide *Stinson Perfect L-fold secrecy* (S(L)-*secrecy*) if, for every allowable L'-subset M' of M ($L' \leq L$) and for every L''-subset S' of S ($L'' \leq L'$),

$$p_{S|M}(S'|M' : L') = p_S(S' : L').$$

Note that the requirement that M' be an *allowable* L'-subset is not explicitly present in Stinson's definition [16], [17]. However, it is implicitly present, since otherwise $p_{S|M}(S'|M' : L')$ is undefined.

The following result follows without difficulty from the above definitions:

Lemma 3.1. *An* SC(k, v, b) *provides* S(L)-*secrecy if and only if it provides* U(L')-*secrecy for every* L' *satisfying* $1 \leq L' \leq L$.

However, U(L)-secrecy by itself is not sufficient to guarantee S(L)-secrecy. For example, any SC(k, v, b) provides U(k)-secrecy, but will not necessarily provide S(k)-secrecy. Note that both these definitions are concerned with unordered sets of messages. A scheme providing S(L)-secrecy protects its users against the opponent O gaining any information about the content of a set of L intercepted messages. However, such a scheme will not necessarily prevent O gaining information about the possible orderings of source states corresponding to observed messages. To provide this stronger notion of secrecy requires the use of a scheme satisfying our third definition, as follows:

Definition. Given $L \geq 1$, an SC(k, v, b) is said to provide *Ordered Perfect L-fold secrecy* (O(L)-*secrecy*) if, for every allowable L-tuple $\mathbf{m}$ of distinct messages from M and for every L-tuple $\mathbf{s}$ of distinct source states from S,

$$p_{S|M}(\mathbf{s}|\mathbf{m} : L) = p_S(\mathbf{s} : L).$$

It is then straightforward to establish:

Lemma 3.2. *If an* SC(k, v, b) *provides* O(L)-*secrecy, then it also provides* O(L')-*secrecy for every L' satisfying $1 \leq L' \leq L$.*

Proof. Suppose $\mathbf{s}$ is an $(L-1)$-tuple of distinct source states, and suppose $\mathbf{m}$ is an allowable $(L-1)$-tuple of distinct messages. In addition let $X(\mathbf{s})$ be the set of L-tuples of distinct source states which "agree" with $\mathbf{s}$ in the first $(L-1)$ positions. Similarly, let $X(\mathbf{m})$ be the set of allowable L-tuples of distinct messages which "agree" with $\mathbf{m}$ in the first $(L-1)$ positions. Then

$$\begin{aligned}
&p_{S|M}(\mathbf{s}|\mathbf{m} : L-1)\\
&\quad = \sum_{\mathbf{s}' \in X(\mathbf{s})} p_{S|M}(\mathbf{s}'|\mathbf{m} : L)\\
&\quad = \sum_{\mathbf{s}' \in X(\mathbf{s})} p_{M|S}(\mathbf{m}|\mathbf{s}' : L) \cdot p_S(\mathbf{s}' : L)/p_M(\mathbf{m} : L)\\
&\quad = \sum_{\mathbf{s}' \in X(\mathbf{s})} \left(\sum_{\mathbf{m}' \in X(\mathbf{m})} p_{M|S}(\mathbf{m}'|\mathbf{s}' : L) \cdot p_S(\mathbf{s}' : L) \right) \Big/ \left(\sum_{\mathbf{m}' \in X(\mathbf{m})} p_M(\mathbf{m}' : L) \right)\\
&\quad = \sum_{\mathbf{s}' \in X(\mathbf{s})} \left(\sum_{\mathbf{m}' \in X(\mathbf{m})} p_{S|M}(\mathbf{s}'|\mathbf{m}' : L) \cdot p_M(\mathbf{m}' : L) \right) \Big/ \left(\sum_{\mathbf{m}' \in X(\mathbf{m})} p_M(\mathbf{m}' : L) \right)\\
&\quad = \sum_{\mathbf{s}' \in X(\mathbf{s})} \left(\sum_{\mathbf{m}' \in X(\mathbf{m})} p_S(\mathbf{s}' : L) \cdot p_M(\mathbf{m}' : L) \right) \Big/ \left(\sum_{\mathbf{m}' \in X(\mathbf{m})} p_M(\mathbf{m}' : L) \right)\\
&\qquad \text{(by O}(L)\text{-secrecy)}\\
&\quad = \sum_{\mathbf{s}' \in X(\mathbf{s})} p_S(\mathbf{s}' : L)\\
&\quad = p_S(\mathbf{s} : L-1).
\end{aligned}$$

The result then follows. □

We also have:

Lemma 3.3. *If an* SC(k, v, b) *provides* O(L)*-secrecy, then it also provides* S(L)*-secrecy.*

Proof. Suppose M^* is any element of X_i and S^* is any j-set of source states, where $j \leq i \leq L$. Let $T_L(M^*)$ denote the subset of Y_L consisting of those L-tuples containing all the elements of M^*. Similarly, let $T_L(S^*)$ denote the set of L-tuples of distinct source states which contain all elements of S^*. Then

$$\begin{aligned}
p_{S|M}(S^*|M^*) &= \sum_{\mathbf{s} \in T_L(S^*)} p_{S|M}(\mathbf{s}|M^*) \\
&= \sum_{\mathbf{s} \in T_L(S^*)} (1/D) \sum_{\mathbf{m} \in T_L(M^*)} p_M(\mathbf{m}) \cdot p_{S|M}(\mathbf{s}|\mathbf{m}) \\
&\quad \left(\text{where } D = \sum_{\mathbf{m} \in T_L(M^*)} p_M(\mathbf{m}) \right) \\
&= \sum_{\mathbf{s} \in T_L(S^*)} (1/D) \sum_{\mathbf{m} \in T_L(M^*)} p_M(\mathbf{m}) \cdot p_S(\mathbf{s}) \qquad \text{(by O}(L)\text{-secrecy)} \\
&= \sum_{\mathbf{s} \in T_L(S^*)} p_S(\mathbf{s}) \\
&= p_S(S^*).
\end{aligned}$$

The result then follows. □

It is straightforward to see why the converse is not true; consider the following example:

Example. Let $E = \{e_0, e_1, e_2\}$, $S = \{s_0, s_1, s_2\}$, $M = \{m_0, m_1, m_2\}$, and suppose $e_i(s_j) = m_k$, where $k = i + j \pmod 3$. Suppose also that $p(e_i) = \frac{1}{3}$ for every i.

This example provides S(2)-secrecy and U(2)-secrecy. However, it only provides $O(1)$-secrecy and not $O(2)$-secrecy.

Before proceeding to our fourth (and final) definition it is important to note that all the above definitions relate to "ciphertext-only" attacks. Essentially, they are all concerned with the situation where the opponent O has intercepted L encoded messages and wishes to deduce information about the corresponding set of L source states. We now consider a definition of perfect security (due to Massey [10]) based on the concept of a "known-plaintext" attack.

Massey defines a known-plaintext attack of order i to be an attack where the opponent O has intercepted i valid and distinct plaintext/ciphertext pairs (i.e., source state/encoded message pairs) all encrypted using the same encoding rule, e say. O is also assumed to have a further encoded message, m say, produced using e and distinct from the messages in the i pairs, for which he wishes to obtain information about the corresponding source state. Then the attack will be said to "succeed" if there exists some source state s, distinct from the states in the i pairs, such that the probability that s corresponds to m given the knowledge of the i pairs is different from the *a priori* probability of s (given that it is known that it differs from the source states contained in the i pairs).

Definition. An SC(k, v, b) is said to provide *Massey Perfect L-fold secrecy* (M(L)-*secrecy*) if, for any $i < L$, the scheme is secure against an order i known-plaintext attack.

Note that the above definition is intended to be precisely the same as Massey's except that what we call M(L)-secrecy is what Massey calls Perfect $(L-1)$-fold secrecy. We have modified the definition so that it corresponds more closely with the other definitions given here. An equivalent definition of M(L)-secrecy, and one that fits more naturally with the other definitions, is as follows:

Definition. Consider any SC(k, v, b). Let $\mathbf{s}$ be any i-tuple of distinct source states and let $\mathbf{s}'$ be the unique $(i-1)$-tuple derived from $\mathbf{s}$ by deleting its last entry. Let $\mathbf{m}$ be any allowable i-tuple of distinct messages with the property that there exists an encoding rule e and an i-tuple of distinct source states $\mathbf{s}^*$ with $e(\mathbf{s}^*) = \mathbf{m}$ and $\mathbf{s}^*$ agreeing with $\mathbf{s}$ in all the first $i-1$ positions. Then, the SC(k, v, b) provides M(L)-secrecy if and only if, for every $i \leq L$ and for every $\mathbf{s}$, $\mathbf{s}'$, $\mathbf{m}$ as above,

$$p(\mathbf{s}|\mathbf{m}, \mathbf{s}' : i) = p(\mathbf{s}|\mathbf{s}' : i).$$

Note that, by definition, M(L)-secrecy implies M(L')-secrecy for every $L' \leq L$. It is perhaps surprising to discover that Massey's definition is no stronger than the previous one. In fact we have:

Theorem 3.4. *If an* SC(k, v, b) *provides* O(L)*-secrecy, then it also provides* M(L)*-secrecy.*

Proof. Suppose $i \leq L$ and that $\mathbf{m}$, $\mathbf{s}$, $\mathbf{s}'$ are as in the definition immediately above; in addition let $X(\mathbf{s}')$ denote the set of all i-tuples of distinct elements of S which agree with $\mathbf{s}'$ in the first $i-1$ positions. Moreover, suppose that the system provides O(L)-secrecy and hence O(i)-secrecy (by Lemma 3.2). Then

$$\begin{aligned} p(\mathbf{s}|\mathbf{m}, \mathbf{s}' : i) &= p(\mathbf{s}, \mathbf{m}, \mathbf{s}' : i)/p(\mathbf{s}', \mathbf{m} : i) \\ &= p(\mathbf{s}, \mathbf{m} : i)/p(\mathbf{s}', \mathbf{m} : i) \\ &= p(\mathbf{s}|\mathbf{m} : i) \cdot p(\mathbf{m} : i)/p(\mathbf{s}'|\mathbf{m} : i) \cdot p(\mathbf{m} : i) \\ &= p(\mathbf{s} : i)/p(\mathbf{s}'|\mathbf{m} : i) \qquad \text{(by O}(i)\text{-secrecy).} \end{aligned}$$

Now

$$\begin{aligned} p(\mathbf{s}'|\mathbf{m} : i) &= \sum_{\mathbf{t} \in X(\mathbf{s}')} p(\mathbf{t}|\mathbf{m} : i) \\ &= \sum_{\mathbf{t} \in X(\mathbf{s}')} p(\mathbf{t} : i) \qquad \text{(by O}(i)\text{-secrecy)} \\ &= p(\mathbf{s}' : i). \end{aligned}$$

Hence

$$\begin{aligned} p(\mathbf{s}|\mathbf{m}, \mathbf{s}' : i) &= p(\mathbf{s} : i)/p(\mathbf{s}' : i) \\ &= p(\mathbf{s}|\mathbf{s}' : i). \end{aligned}$$

□

It is also rather surprising to discover that the converse to Theorem 3.4 is not true. Consider the following example:

Example. Let $E = \{e_0, e_1, e_2\}$, $S = \{s_0, s_1\}$, $M = \{m_0, m_1, m_2\}$, and suppose $e_i(s_j) = m_k$, where $k = i + j \pmod 3$. Moreover, suppose that $p(e_i) = \frac{1}{3}$ for every i,

Then it is straightforward to see that this example gives O(1)-secrecy, M(2)-secrecy, S(2)-secrecy, and U(2)-secrecy, but does not give O(2)-secrecy. Note also that the example following Lemma 3.3 provides S(2)-secrecy and U(2)-secrecy but only M(1)-secrecy and O(1)-secrecy.

From now on, although it is a little more powerful, we use the definition of O(L)-secrecy rather than that of M(L)-secrecy, since it appears to be easier to handle. Before proceeding note also that, for $L = 1$, all the above definitions coincide and in fact equate to Shannon's notion of perfect secrecy [14].

4. Bounds for L-Secrecy Systems

We now consider a variety of bounds which can be established for L-secrecy systems of various types. We start by considering the weakest form of L-secrecy, namely U(L)-secrecy.

Lemma 4.1. *If an* SC(k, v, b) *provides* U(L)*-secrecy, then for every allowable L-set of messages M' and for every L-set of source states S' there exists an encoding rule e such that*

$$e(S') = M'.$$

Proof. Suppose not, i.e., suppose there exists a pair of L-sets M', S' (M' allowable) such that there is no encoding rule which maps S' onto M'. Then, clearly

$$p_{S|M}(S'|M') = 0,$$

which contradicts the assumption of U(L)-secrecy since

$$p_S(S') > 0. \qquad \square$$

It is also straightforward to show:

Lemma 4.2. *If an* SC(k, v, b) *provides* U(L)*-secrecy, then*

$$b \geq |X_L|,$$

where, as before, X_L is the set of allowable L-subsets of M. Moreover, if

$$b = |X_L|,$$

then:

(i) *If S^* is any L-subset of S and M^* is any element of X_L, there exists a unique encoding rule e such that*

$$e(S^*) = M^*.$$

(ii) *For every encoding rule e, if M^* is any element of X_L which is also a subset of $e(S)$, then*

$$p_E(e) = p_M(M^*).$$

Proof. Let S^* be any L-subset of S. Then, by Lemma 4.1, if M^* is any allowable L-subset of M, there exists an encoding rule e with

$$e(S^*) = M^*.$$

Therefore, if we fix S^* and let M^* range over all elements of X_L, we obtain a set of $|X_L|$ different encoding rules. The bound follows.

Now suppose $b = |X_L|$. Following the above argument, it is clear that fixing S^* and letting M^* range over all the elements of X_L exhausts the set of encoding rules. Statement (i) then follows immediately.

To establish (ii) suppose S^* is any L-set of source states and let M^* be any element of X_L. In addition let e be the unique encoding rule which maps S^* onto M^*. Then

$$\begin{aligned} p_{S|M}(S^*|M^*) &= p_{E|M}(e|M^*) \\ &= p_{M|E}(M^*|e) \cdot p_E(e)/p_M(M^*) \\ &= p_S(S^*) \cdot p_E(e)/p_M(M^*). \end{aligned}$$

But, by the definition of U(L)-secrecy,

$$p_{S|M}(S^*|M^*) = p_S(S^*).$$

Hence

$$p_E(e) = p_M(M^*)$$

and (ii) follows immediately. □

Using these lemmas we can now establish the following theorem, the bound of which was previously obtained in the two cases of greatest interest by De Soete [4], and a special case of which is also given by Stinson [18, Theorem 2.1].

Theorem 4.3. *If an* SC(k, v, b) *provides* U(L)*-secrecy, then*

$$b \geq (v/k) \cdot \binom{k}{L}.$$

Moreover, if

$$b = (v/k) \cdot \binom{k}{L},$$

then:

(i) *If $L > 1$, for any pair of encoding rules e_1, e_2 either*

$$e_1(S) = e_2(S)$$

or $e_1(S)$ and $e_2(S)$ are disjoint.

(ii) *If e_1 and e_2 are encoding rules satisfying*

$$e_1(S) = e_2(S),$$

then

$$p_E(e_1) = p_E(e_2) = p_M(M^*)$$

for every M^* in X_L which is also a subset of $e_1(S)$.

Proof. By Lemma 4.2, to establish the bound we need only show that

$$|X_L| \geq (v/k) \cdot \binom{k}{L}.$$

Choose any message m; then, since we assume throughout that $p_M(m) > 0$, there exists a source state s and an encoding rule e with

$$e(s) = m.$$

Now, it is clear that

$$|e(S)| = k,$$

and hence there are at least $\binom{k-1}{L-1}$ allowable L-subsets of M which include m. Since there are precisely v choices for m this gives us a total of $v \cdot \binom{k-1}{L-1}$ (not necessarily distinct) allowable L-subsets of M. Each such allowable L-subset cannot have been counted more than L times, giving us

$$|X_L| \geq v \cdot \binom{k-1}{L-1}/L.$$

The bound follows.

Now suppose that

$$b = (v/k) \cdot \binom{k}{L},$$

and hence

$$(b=) \qquad |X_L| = v \cdot \binom{k-1}{L-1}/L.$$

Suppose also that $L > 1$. We know that each message m is included in at least $\binom{k-1}{L-1}$ allowable L-sets; hence, since there are only $(v/L) \cdot \binom{k-1}{L-1}$ allowable L-sets in total, each message m is contained in precisely $\binom{k-1}{L-1}$ allowable L-sets. Now, if e is any encoding rule for which $m \in e(S)$, then since $|e(S)| = k$, e itself will immediately yield $\binom{k-1}{L-1}$ allowable L-sets containing m. Hence, if e' is any

other encoding rule for which $m \in e'(S)$, then $e(S) = e'(S)$, since there are no more allowable L-sets containing m. Note that the above argument is only valid if $L > 1$. The above applies for all messages m and (i) follows.

Statement (ii) is immediate on application of Lemma 4.2(ii). □

We consider examples of schemes possessing U(L)-secrecy in Section 5 below. Note that, because S(L)-secrecy implies U(L)-secrecy, the results of Theorem 4.3 also apply to S(L)-secrecy systems. Before proceeding observe that Theorem 4.3(i) does not hold for the case $L = 1$. Counterexamples are provided by any latin rectangle scheme (see Section 5 below).

If we now consider O(L)-secrecy, then we get a similar set of results as follows:

Lemma 4.4. *If an* SC(k, v, b) *provides* O(L)*-secrecy and* t *satisfies* $1 \leq t \leq L$, *then for every allowable* t*-tuple of distinct messages* $\mathbf{m}$ *and for every* t*-tuple of distinct source states* $\mathbf{s}$ *there exists an encoding rule* e *such that*

$$e(\mathbf{s}) = \mathbf{m}.$$

Proof. Suppose not, i.e., suppose there exists a pair of t-tuples $\mathbf{m}$, $\mathbf{s}$ ($\mathbf{m}$ allowable) such that there is no encoding rule which maps $\mathbf{s}$ onto $\mathbf{m}$. Then, clearly

$$p_{S|M}(\mathbf{s}|\mathbf{m}) = 0,$$

which, by Lemma 3.2 contradicts the assumption of O(L)-secrecy since

$$p_S(\mathbf{s}) > 0.$$ □

It is also straightforward to show:

Lemma 4.5. *If an* SC(k, v, b) *provides* O(L)*-secrecy, then*

$$b \geq |Y_L|,$$

where, as before, Y_L *is the set of allowable* L*-tuples of distinct elements of* M. *Moreover, if*

$$b = |Y_L|,$$

then:

(i) *If* $\mathbf{s}$ *is any* L*-tuple of distinct elements of* S *and* $\mathbf{m}$ *is any element of* Y_L, *there exists a unique encoding rule* e *such that*

$$e(\mathbf{s}) = \mathbf{m}.$$

(ii) *For every encoding rule* e, *if* $\mathbf{m}$ *is any element of* Y_L *for which the elements of* $\mathbf{m}$ *are all contained in* $e(S)$, *then*

$$p_E(e) = p_M(\mathbf{m}).$$

Proof. Let $\mathbf{s}$ be any L-tuple of distinct elements of S. Then, by Lemma 4.4, if $\mathbf{m}$ is any element of Y_L, there exists an encoding rule e with

$$e(\mathbf{s}) = \mathbf{m}.$$

Therefore, if we fix **s** and let **m** range over all elements of Y_L, we obtain a set of $|Y_L|$ different encoding rules. The bound follows.

Now suppose $b = |Y_L|$. Following the above argument, it is clear that fixing **s** and letting **m** range over all the elements of Y_L exhausts the set of encoding rules. Statement (i) then follows immediately.

To establish (ii) suppose **s** is any L-tuple of distinct source states and let e be the unique encoding rule which maps **s** onto **m**. Then

$$\begin{aligned} p_{S|M}(\mathbf{s}|\mathbf{m}) &= p_{E|M}(e|\mathbf{m}) \\ &= p_{M|E}(\mathbf{m}|e) \cdot p_E(e)/p_M(\mathbf{m}) \\ &= p_S(\mathbf{s}) \cdot p_E(e)/p_M(\mathbf{m}). \end{aligned}$$

But, by the definition of O(L)-secrecy,

$$p_{S|M}(\mathbf{s}|\mathbf{m}) = p_S(\mathbf{s}).$$

Hence

$$p_E(e) = p_M(\mathbf{m}).$$

Statement (ii) follows immediately. □

Using these lemmas we can now establish the following result. Note that the bound in this theorem was previously established for M(L)-secret systems by Massey [10, equation (5)].

Theorem 4.6. *If an* SC(k, v, b) *provides* O(L)*-secrecy, then*

$$b \geq v \cdot (k-1)!/(k-L)!.$$

Moreover, if

$$b = v \cdot (k-1)!/(k-L)!,$$

then:

(i) *If* $L > 1$, *for any pair of encoding rules* e_1, e_2 *either*

$$e_1(S) = e_2(S)$$

or $e_1(S)$ *and* $e_2(S)$ *are disjoint.*

(ii) *If* e_1 *and* e_2 *are encoding rules satisfying*

$$e_1(S) = e_2(S),$$

then

$$p_E(e_1) = p_E(e_2) = p_M(\mathbf{m})$$

for every **m** *in* Y_L *for which all elements in* **m** *are in* $e_1(S)$.

Proof. By Lemma 4.5, to establish the bound we need only show that

$$|Y_L| \geq v \cdot (k-1)!/(k-L)!.$$

Choose any message m; then, since $p_M(m) > 0$, there exists a source state s and an encoding rule e with

$$e(s) = m.$$

Now, it is clear that

$$|e(S)| = k,$$

and hence there are at least $(k-1)!/(k-L)!$ allowable L-tuples of distinct elements of M which have m as their first entry. Since there are precisely v choices for m this gives us

$$|Y_L| \geq v \cdot (k-1)!/(k-L)!$$

and the bound follows.

Now suppose that

$$b = v \cdot (k-1)!/(k-L)!,$$

and hence

$$(b=) \qquad |Y_L| = v \cdot (k-1)!/(k-L)!.$$

We know that each message m is included as the first element in at least $(k-1)!/(k-L)!$ allowable L-tuples; hence, since there are only $v \cdot (k-1)!/(k-L)!$ allowable L-tuples in total, each message m is contained as the first element in precisely $(k-1)!/(k-L)!$ allowable L-tuples.

Suppose also that $L > 1$. Now, if e is any encoding rule for which $m \in e(S)$, then since $|e(S)| = k$, e itself will immediately yield $(k-1)!/(k-L)!$ allowable L-tuples with first element m. Hence, if e' is any other encoding rule for which $m \in e'(S)$, then $e(S) = e'(S)$, since there are no more allowable L-tuples with m as the first element. Note that the above argument is only valid if $L > 1$. This argument applies for all messages m and (i) follows.

Statement (ii) follows immediately from Lemma 4.5(ii). □

We consider examples of O(L)-secret systems in Section 5 below. Before proceeding observe that Theorem 4.6(i) does not hold for the case $L = 1$. Counterexamples are provided by any latin rectangle scheme (see Section 5 below).

5. Examples of L-Secrecy Systems

We now consider some examples of L-secrecy systems for which the numbers of encoding rules meet the lower bounds established in Section 4 above. It is of interest to construct such systems since, for any security system, it is always desirable to minimize the number of encoding rules and hence the key size. We divide our examples into two categories; namely, those satisfying the bounds of Theorems 4.3 and 4.6, respectively.

5.1. *Systems Providing* U(*L*)*-Secrecy and* S(*L*)*-Secrecy*

If we examine the bound of Theorem 4.3, it appears reasonable first to examine the case where $v = k$, and hence

$$b = \binom{k}{L},$$

since this minimizes the number of encoding rules for a given number of source states. Indeed, if no authentication is required, then there seems no reason to choose v any larger than absolutely necessary.

In this case we may identify S with M, and each encoding rule is then no more than a permutation on M. Moreover, by Theorem 4.3(ii), each encoding rule must be equiprobable. These constraints now enable us to give a purely combinatorial necessary and sufficient condition for a set of $\binom{k}{L}$ permutations on M to form a system providing U(L)-secrecy. Before proceeding note also that in this case X_i consists of all i-subsets of M, i.e., all i-subsets of M are allowable.

Theorem 5.1. *Suppose E is a set of encoding rules (permutations) for an* $\mathrm{SC}\left(k, k, \binom{k}{L}\right)$, *where $M = S$. Then this scheme provides* U(L)*-secrecy if and only if*:

(i) $p_E(e) = 1\Big/\binom{k}{L}$ *for every encoding rule e.*

(ii) *For every pair of L-subsets M^*, S^* of M, there exists a unique encoding rule e with*

$$e(S^*) = M^*.$$

Proof. Suppose the scheme provides U(L)-secrecy. Then (i) holds by Theorem 4.3(ii). Moreover, (ii) holds by Lemma 4.2(i).

Now suppose (i) and (ii) hold and suppose S^* is an L-subset of S and M^* is an L-subset of M (and hence allowable). Then

$$\begin{aligned} p(S^*|M^*) &= p(M^*|S^*) \cdot p(S^*)/p(M^*) \\ &= p(e) \cdot p(S^*)/p(M^*) \\ &\qquad \text{(where } e \text{ is the unique encoding rule mapping } S^* \text{ to } M^*\text{)} \\ &= p(S^*)\Big/\left(\binom{k}{L} \cdot p(M^*)\right) \qquad \text{(by (i))}. \end{aligned}$$

But, by definition,

$$\begin{aligned} p(M^*) &= \sum_{(e,S'):\, e(S')=M^*} p(S') \cdot p(e) \\ &= \sum_{(e,S'):\, e(S')=M^*} p(S')\Big/\binom{k}{L} \\ &= 1\Big/\binom{k}{L} \qquad \text{(by (ii))}. \end{aligned}$$

Hence, as required,

$$p(S^*|M^*) = p(S^*)$$

and the result follows. □

Note that, for the case $L = 1$, the above theorem was first obtained by Shannon (p. 681 of [14]). In the situation where the theorem holds we also have the following result:

Theorem 5.2. *Suppose E is a set of encoding rules (permutations) for an* $\mathrm{SC}\left(k, k, \binom{k}{L}\right)$ *which provides* $\mathrm{U}(L)$*-secrecy, and where $M = S$. Then, for every $L' \leq L$, the scheme also provides* $\mathrm{U}(L')$*-secrecy if and only if, for every pair of L'-subsets M', S' of M, there exist precisely w' encoding rules e with*

$$e(S') = M',$$

where

$$w' = \binom{k}{L} \Big/ \binom{k}{L'}.$$

Proof. First, if M' and S' are any L'-subsets of M, then let $E(S', M')$ denote the set of encoding rules which map S' onto M'. By definition, the scheme provides $\mathrm{U}(L')$-secrecy

$$\text{if and only if} \qquad p(S'|M') = p(S').$$

This holds

$$\text{if and only if} \qquad p(M'|S') = p(M'),$$

$$\text{if and only if} \qquad \sum_{e \in E(S', M')} p(e) = p(M'),$$

$$\text{if and only if} \qquad |E(S', M')| \Big/ \binom{k}{L} = p(M'). \tag{$*$}$$

First suppose that $(*)$ holds. Now, if we fix M' and let S' range over all $\binom{k}{L'}$ possible L'-subsets of M, then the sets $E(S', M')$ will be pairwise disjoint and have the property that their union is E. Moreover, since the right-hand side of $(*)$ will be fixed, they must all have the same size. Hence

$$|E(S', M')| = |E| \Big/ \binom{k}{L'} = \binom{k}{L} \Big/ \binom{k}{L'} \tag{$**$}$$

as required.

Now suppose that $(**)$ holds for all M' and S'. By definition,

$$p(M') = \sum_{S'} \sum_{e \in E(S', M')} p(S') \cdot p(e)$$

$$= \sum_{S'} p(S') \Big/ \binom{k}{L'} \qquad \text{(by } **\text{)}$$

$$= 1 \Big/ \binom{k}{L'}.$$

Equation (*) follows immediately. □

Before considering actual examples we explore in a little more detail sets of permutations satisfying condition (ii) of Theorem 5.1. We make the following definition.

Definition. Suppose E is a set of permutations on the set S, where $|E| = b$ and $|S| = k$. Then E is said to be (t, w)-*homogeneous on* S if and only if, for every pair of t-subsets of S (S_1, S_2 say), there exist precisely w permutations e in E such that

$$e(S_1) = S_2.$$

By Theorem 5.1, the study of U(L)-secret systems having

$$b = \binom{k}{L}$$

is then precisely equivalent to the study of $(L, 1)$-homogeneous sets of permutations on a set of size k. Moreover, by Theorem 5.2 and Lemma 3.1, the study of S(L)-secret systems having

$$b = \binom{k}{L}$$

is precisely equivalent to the study of $(L, 1)$-homogeneous sets of permutations on a set of size k which have the property that they are also $\left(i, \binom{k}{L} \Big/ \binom{k}{i}\right)$-homogeneous for every i satisfying $1 \leq i \leq L$.

The following results hold for homogeneous sets of permutations. Note first that Lemmas 5.3 and 5.7 below have been independently derived by Kramer *et al.* [7, Theorem 1.1]. These results were also previously given by Nomura [12] for the case $w = 1$.

Lemma 5.3. *If E is (t, w)-homogeneous on S, then E is also $(k - t, w)$-homogeneous on S.*

Proof. Suppose E is (t, w)-homogeneous on S, and in addition suppose that S_1 and S_2 are $(k - t)$-subsets of S. Then it should be clear that if

$$C(S_i) = S - S_i \qquad (i = 1, 2),$$

then encoding rule e satisfies

$$e(S_1) = e(S_2)$$

if and only if

$$e(C(S_1)) = e(C(S_2)).$$

Since $|C(S_1)| = |C(S_2)| = t$ the result follows. □

Lemma 5.4. *If E is (t, w)-homogeneous on S, then*

$$b = w \cdot \binom{k}{t}.$$

Proof. Let S_1 be any fixed t-subset of S. Then for any t-subset of S (S_2 say) there exist precisely w permutations in E mapping S_1 onto S_2. Since there are $\binom{k}{t}$ such subsets S_2, and since each element of E must map S_1 onto some such t-subset, the result follows. □

Lemma 5.5 (Mowbray). *If E is (t, w)-homogeneous on S, where $1 \leq t \leq (k+1)/2$, then E is also (t', w')-homogeneous on S for every $t' \leq t$, where*

$$w' = w \cdot \binom{k}{t} \Big/ \binom{k}{t'}.$$

Proof. Suppose E is (t, w)-homogeneous on S. If X, Y are $(t-1)$-subsets of S and $0 \leq s \leq t-1$, then let $N(X, Y, s)$ denote the number of permutations e such that $e(X)$ and Y have precisely s elements in common. We now show (by induction on s) that (given $1 \leq t \leq (k+1)/2$) $N(X, Y, s)$ is independent of the choice of X and Y. This immediately yields the desired result (by setting $s = t-1$).

First suppose $s = 0$. If e is such that $e(X)$ and Y are disjoint, then there exist precisely $(k - 2(t-1))$ choices for a t-set X' where X' contains X and $e(X')$ is disjoint from Y. That is, there are exactly $(k - 2(t-1)) \cdot N(X, Y, 0)$ pairs (e, X'), where $|X'| = t$, X' contains X, and $e(X')$ and Y are disjoint. But, since E is (t, w)-homogeneous, there are also $(k-(t-1)) \cdot \binom{k-(t-1)}{t} \cdot w$ such pairs. Hence the claim is true for $s = 0$ and we have

$$N(X, Y, 0) = w \cdot \binom{k-(t-1)}{t} \cdot (k-(t-1))/(k-2(t-1)),$$

where $k - 2(t-1) > 0$, since $t \leq (k+1)/2$.

Now suppose $s > 0$ and suppose also that the inductive hypothesis is true for all s' $(0 \leq s' < s)$. First suppose e is such that $e(X)$ and Y have precisely s elements in common; then there exist precisely $(k - 2(t-1) + s)$ choices for a t-set X' where X' contains X and $e(X')$ and Y meet in precisely s elements. Second suppose e is such that $e(X)$ and Y have precisely $s-1$ elements in common; then there exist precisely $(t-s)$ choices for a t-set X' where X' contains X and $e(X')$ and Y meet in precisely s elements. That is, there are exactly $(k - 2(t-1) + s) \cdot N(X, Y, s) + (t-s) \cdot N(X, Y, s-1)$ pairs (e, X'), where $|X'| = t$, X' contains X, and $e(X')$ and Y

meet in precisely s elements of S. But, since E is (t, w)-homogeneous, there are also $(k-(t-1))\cdot\binom{k-(t-1)}{t-s}\cdot\binom{t-1}{s}\cdot w$ such pairs. The result follows. □

The last result, when taken in conjunction with Theorem 5.2 and Lemma 5.3, implies the following:

Corollary 5.6. *If an* $\mathrm{SC}\left(k, k, \binom{k}{L}\right)$ *provides* $\mathrm{U}(L)$*-secrecy and* $1 \leq L \leq (k+1)/2$, *then it also provides* $\mathrm{U}(L')$*-secrecy for every* L' *satisfying either* $1 \leq L' \leq L$ *or* $k - L \leq L' \leq k$.

The problem remains of constructing sets of permutations of cardinality $\binom{k}{L}$ with the desired property for Theorem 4.3, i.e., constructing $(L, 1)$-homogeneous sets of permutations. We first note the following result giving a necessary condition for the existence of an $(L, 1)$-homogeneous set.

Lemma 5.7. *If* E *is* $(t, 1)$*-homogeneous on the* k*-set* S $(1 \leq t \leq (k+1)/2)$, *then* $\binom{k}{t'} \Big| \binom{k}{t}$ *for every* t' $(1 \leq t' \leq t)$.

Proof. Immediate from Lemma 5.5. □

We now consider examples of $\mathrm{U}(L)$-secure systems which satisfy

$$|E| = \binom{k}{L}.$$

For the case $L = 1$, as observed by Shannon [14], the existence of such a set is precisely equivalent to the existence of a *latin square* of order k. We now describe the precise equivalence.

A latin square of order k is merely a k by k matrix all of whose entries are taken from the set $\{1, 2, \ldots, k\}$ with the property that the entries in any row are all distinct and the entries in any column are all distinct. Each row (and each column) will therefore contain a permutation of the numbers 1 to k. If row i contains the entries $r_1, r_2, \ldots, r_k$, then define the permutation p_i by

$$p_i(j) = r_j.$$

It is then clear that the k permutations $p_1, p_2, \ldots, p_k$ will form a $(1, 1)$-homogeneous set on $\{1, 2, \ldots, k\}$. Moreover, any $(1, 1)$-homogeneous set can be used to derive a latin square. It should also be clear that the one-time pad cipher (see, for example, Chapter 3 of Beker and Piper [1]) is equivalent to a latin square. It is easy to construct latin squares of any desired size (e.g., by letting the first row be any permutation and letting the subsequent rows be defined as all cyclic shifts of the first row), and hence $(1, 1)$-homogeneous sets exist for all values of k.

Finally, note that, since U(1)-secrecy, S(1)-secrecy, O(1)-secrecy, and M(1)-secrecy are all equivalent, latin squares are also in precise correspondence to key-minimal examples of these other types of perfect-secrecy schemes.

For the case $L = 2$, we assert that the existence of a (2, 1)-homogeneous set of permutations is equivalent to the existence of a *Perpendicular Array* with parameters PA(k, k). We now justify this claim.

Following Mullin *et al.* [11], a *Perpendicular Array* (*PA*) of *order* n and *depth* s (written PA(n, s)) is an s by $\binom{n}{2}$ array

$$X = (x_{ij})$$

with entries from a set M on n elements such that, for any two rows of X, the $\binom{n}{2}$ columns contain all $\binom{n}{2}$ unordered pairs of distinct elements of M. The following result, attributed by Mullin *et al.* [11] to E. Mendelsohn, is straightforward to establish:

Lemma 5.8. *In any* PA(n, s) *with* $s > 2$, *each element of* M *occurs* $(n-1)/2$ *times in each row of* X (*and hence* n *is odd*).

Now, if $s = n$, i.e., when we have a PA(n, n), then X is an n by $\binom{n}{2}$ array, and it is straightforward to see that each column of X is a permutation of the elements of M. Just as with the latin squares we thereby derive a set of $\binom{n}{2}$ permutations which forms a (2, 1)-homogeneous set on M, where $|M| = n$. Conversely, given any (2, 1)-homogeneous set of permutations on a set of size k, we may immediately derive a PA(k, k).

It is well known (see Corollary 2.5 of Mullin *et al.* [11]) that if

$$n = p^a \qquad (a \geq 1,\ p \text{ an odd prime}),$$

then there exists a PA(n, n). Hence key-minimal U(2)-secret systems can be constructed whenever k is a power of an odd prime. It appears that no PA(n, n), and hence no key-minimal U(2)-secret code, is known for any other values of n.

Finally, note that, given the above correspondence, for the case $n = s$ Mendelsohn's Lemma 5.8 above is merely a special case of Lemma 5.5 (where $w = 1$ and $t = 2$). In addition, by the same lemma, any (2, 1)-homogeneous set is also $(1, (k-1)/2)$-homogeneous, and hence, by Theorem 5.2, the existence of an S(2)-secret system with

$$b = \binom{k}{2}$$

is also equivalent to the existence of a PA(k, k).

(t, 1)-homogeneous sets of permutations have been previously studied by Nomura [12]. Recently, many (t, w)-homogeneous sets of permutations for $t \geq 3$ have been

discovered [7], [8], [19]. Before proceeding it is also interesting to note that as long ago as 1961, Rao [13] defined an *Orthogonal Array of Type* II *of strength d, s constraints, order n,* and *index h,* (N, s, n, d) : II to be an s by N array of elements of an n-set M such that, in any set of d rows, the N columns contain each of the $\binom{n}{d}$ d-subsets of M exactly h times $\left(\text{and hence } N = h \cdot \binom{n}{d}\right)$. It is then straightforward to see that a (t, w)-homogeneous set of permutations on a set of size k is precisely equivalent to a $\left(w \cdot \binom{k}{t}, k, k, t\right)$: II, i.e., an orthogonal array of type II with k constraints. Rao [13, Theorem 2] went on to show the existence of $(s(s-1)/2, s, s, 2)$: II whenever s is an odd prime power. This corresponds exactly to the known values of n for which there exists a PA(n, n) (see above).

To conclude this discussion of U(L)-secret and S(L)-secret systems, we now relax our requirement that $v = k$, and consider schemes for which

$$b = (v/k) \cdot \binom{k}{L} \quad \text{and} \quad v \geq k.$$

We first consider the (special) case $L = 1$. In this case the above equation reduces to $b = v$. Using Lemma 4.2 it is then straightforward to see that the existence of such a set of encoding rules is precisely equivalent to the existence of a k by v *latin rectangle,* where a latin rectangle is merely a k by v matrix, all of whose entries are taken from the set $\{1, 2, \ldots, v\}$ with the property that the entries in any row/column are all distinct (hence $k \leq v$). The equivalence is the same as that described above for latin squares in the case $L = 1$ and $v = k$.

If $L > 1$, then, by Theorem 4.3(i), $v = kt$ for some integer t, and the message space can be partitioned into t subsets of size k, say $M_1, M_2, \ldots, M_t$, such that, for any encoding rule e,

$$e(S) = M_i$$

for some i. Therefore let E_i denote the set of encoding rules mapping S onto M_i and then $E_1, E_2, \ldots, E_t$ will form a partition of E. Moreover, by Theorem 4.3(ii), if

$$e_1(S) = e_2(S),$$

then

$$p(e_1) = p(e_2),$$

and hence let p_i denote the probability $p(e)$ for any e in E_i. It is then straightforward to establish that each triple (S, M_i, E_i) forms an $(L, 1)$-homogeneous set of permutations. This means that the study of U(L)-secrecy schemes with

$$b = (v/k) \cdot \binom{k}{L} \quad \text{and} \quad v > k$$

is contained within the study of such schemes with $v = k$, and therefore we do not consider them further.

5.2 *Systems Providing* O(L)*-Secrecy and* M(L)*-Secrecy*

If we examine the bound of Theorem 4.6, then, as in Section 5.1, it appears reasonable first to examine the case where $v = k$, and hence $b = k!/(k - L)!$ since this minimizes the number of encoding rules for a given number of source states.

In this case we may identify S with M, and each encoding rule is then no more than a permutation on M. Moreover, by Theorem 4.6(ii), each encoding rule must be equiprobable. These constraints now enable us to give a purely combinatorial necessary and sufficient condition for a set of $\binom{k}{L}$ permutations on M to form a system providing O(L)-secrecy.

Theorem 5.9. *Suppose E is a set of encoding rules (permutations) for an* SC(k, k, $k!/(k - L)!$), *where $M = S$. Then this scheme provides* O(L)*-secrecy if and only if*:

(i) $p_E(e) = (k - L)!/k!$ *for every encoding rule e.*

(ii) *For every pair of L-tuples of distinct elements* $\mathbf{m}$, $\mathbf{s}$ *of M, there exists a unique encoding rule e with*

$$e(\mathbf{s}) = \mathbf{m}.$$

Proof. Suppose the scheme provides O(L)-secrecy. Then (i) holds by Theorem 4.6(ii). Moreover, (ii) holds by Lemma 4.5(i).

Now suppose (i) and (ii) hold and suppose $\mathbf{s}$ is an L-tuple of distinct elements of S and $\mathbf{m}$ is an allowable L-tuple of distinct elements of M. Then

$$\begin{aligned} p(\mathbf{s}|\mathbf{m}) &= p(\mathbf{m}|\mathbf{s}) \cdot p(\mathbf{s})/p(\mathbf{m}) \\ &= p(e) \cdot p(\mathbf{s})/p(\mathbf{m}) \\ &\quad \text{(where } e \text{ is the unique encoding rule mapping } \mathbf{s} \text{ to } \mathbf{m}\text{)} \\ &= p(\mathbf{s}) \cdot (k - L)!/(k! \cdot p(\mathbf{m})) \qquad \text{(by (i))}. \end{aligned}$$

But, by definition,

$$\begin{aligned} p(\mathbf{m}) &= \sum_{(e, \mathbf{s}') : e(\mathbf{s}') = \mathbf{m}} p(\mathbf{s}') \cdot p(e) \\ &= \sum_{(e, \mathbf{s}') : e(\mathbf{s}') = \mathbf{m}} p(\mathbf{s}') \cdot (k - L)!/k! \\ &= (k - L)!/k! \qquad \text{(by (ii))}. \end{aligned}$$

Hence, as required,

$$p(\mathbf{s}|\mathbf{m}) = p(\mathbf{s})$$

and the result follows. □

Note that, for the case $L = 1$, the above theorem coincides with Theorem 5.1, which, for the $L = 1$ case, was first obtained by Shannon (p. 681 of [14]). In the situation where the theorem holds we also have the following result:

Theorem 5.10. *Suppose E is a set of encoding rules (permutations) for an* $SC(k, k, k!/(k-L)!)$ *which provides* $O(L)$*-secrecy, and where* $M = S$*. Then, for every* $L' \leq L$*, there exist precisely* w' *encoding rules* e *with*

$$e(\mathbf{s}) = \mathbf{m},$$

where

$$w' = (k-L')!/(k-L)!.$$

Proof. First observe that, by Lemma 3.2, any scheme providing $O(L)$-secrecy must also provide $O(L')$-secrecy for every $L' \leq L$. Suppose $\mathbf{m}$ and $\mathbf{s}$ are any L'-tuples of distinct elements of M and let $E(\mathbf{s}, \mathbf{m})$ denote the set of encoding rules which map $\mathbf{s}$ onto $\mathbf{m}$. By definition, since the scheme provides $O(L')$-secrecy:

$$p(\mathbf{s}|\mathbf{m}) = p(\mathbf{s}).$$

Hence:

$$\begin{aligned} p(\mathbf{m}) &= p(\mathbf{m}|\mathbf{s}) \\ &= \sum_{e \in E(\mathbf{s}, \mathbf{m})} p(e) \\ &= |E(\mathbf{s}, \mathbf{m})| \cdot (k-L)!/k!. \end{aligned} \tag{$*$}$$

Now, if we fix $\mathbf{m}$ and let $\mathbf{s}$ range over all $k!/(k-L')!$ possible L'-tuples of distinct elements of M, then the sets $E(\mathbf{s}, \mathbf{m})$ will be pairwise disjoint and have the property that their union is E. Moreover, since the left-hand side of $(*)$ will be fixed, they must all have the same size. Hence

$$|E(\mathbf{s}, \mathbf{m})| = |E| \cdot (k-L')!/k! = (k-L')!/(k-L)!$$

as required. □

Before considering actual examples we explore in a little more detail sets of permutations satisfying condition (ii) of Theorem 5.9. We make the following definition.

Definition. Suppose E is a set of permutations on the set S, where $|E| = b$ and $|S| = k$. Then E is said to be (t, w)*-transitive on* S if and only if, for every pair of t-tuples of distinct elements of S ($\mathbf{s}_1$, $\mathbf{s}_2$ say), there exist precisely w permutations e in E such that

$$e(\mathbf{s}_1) = \mathbf{s}_2.$$

By Theorem 5.9, the study of $O(L)$-secret systems having $b = k!/(k-L)!$ is then precisely equivalent to the study of $(L, 1)$-transitive sets of permutations on a set of size k. Moreover, by Theorem 5.10, every $(L, 1)$-transitive set of permutations is also $(i, (k-i)!/(k-L)!)$-transitive for every i satisfying $1 \leq i \leq L$.

The problem remains of constructing sets of permutations of cardinality $k!/(k-L)!$ with the desired property for Theorem 5.9, i.e., constructing $(L, 1)$-transitive sets of permutations.

The case $L = 1$ has already been studied in Section 5.1 above.

For the case $L \geq 2$, the theory of finite groups provides a number of examples. Suppose E is a set of permutations on k elements. If E forms a subgroup of S_k, then E is a (t, w)-transitive set of permutations if and only if it is a t-transitive group. Moreover, using the language of group theory, it is a $(t, 1)$-transitive set if and only if it is a sharply t-transitive group. For a discussion of t-fold transitivity in finite permutation groups, see, for example, [20].

Two "trivial" families of group-based examples are provided by the symmetric group S_k and the alternating group A_k. As Massey [10] has noted, S_k is sharply k-transitive and hence provides an example (in fact the only example) of a key-minimal system providing $O(k)$- and $M(k)$-secrecy. In addition, A_k is sharply $(k-2)$-transitive, and hence provides an example of a key-minimal system providing $O(k-2)$- and $M(k-2)$-secrecy.

Sharply 2- and 3-transitive groups are known to exist for infinitely many values of k. However, the situation is very different for $t \geq 4$. Apart from S_k and A_k, the only t-transitive groups with $t \geq 4$ are the Mathieu groups: M_{11}, M_{12}, M_{23}, and M_{24}, where M_i acts on a set of i elements; for details of the theory of the Mathieu groups, see, for example, Chapter 20 of [9]. Groups M_{11} and M_{23} are 4-transitive and M_{12} and M_{24} are 5-transitive; M_{11} and M_{12} are sharply 4- and 5-transitive, whereas M_{23} and M_{24} are not. Hence M_{11} and M_{12} (of orders 7920 and 95040, respectively) are the only "nontrivial" examples of sharply t-transitive groups for $t \geq 4$.

To obtain further examples of $(t, 1)$-transitive sets it is therefore necessary to look for examples where the set of permutations does not form a group. The construction of such sets (often called *sharply t-transitive permutation sets*) has been the subject of research for some time (see, for example, [2]), and there are many examples known of $(t, 1)$-transitive sets which are not subgroups (or cosets of subgroups) of S_k.

To conclude this discussion of $O(L)$-secret systems, we now relax our requirement that $v = k$, and consider schemes for which

$$b = (v/k) \cdot k!/(k-L)! \quad \text{and} \quad v \geq k.$$

The case $L = 1$ coincides with the discussion in Section 5.1.

If $L > 1$, then, by Theorem 4.6(i), $v = kt$ for some integer t, and the message space can be partitioned into t subsets of size k, say $M_1, M_2, \ldots, M_t$, such that, for any encoding rule e,

$$e(S) = M_i$$

for some i. Therefore let E_i denote the set of encoding rules mapping S onto M_i and then $E_1, E_2, \ldots, E_t$ will form a partition of E. Moreover, by Theorem 4.6(ii), if

$$e_1(S) = e_2(S),$$

then

$$p(e_1) = p(e_2),$$

and hence let p_i denote the probability $p(e)$ for any e in E_i.

It is then straightforward to establish that each triple (S, M_i, E_i) forms an $(L, 1)$-transitive set of permutations. This means that the study of O(L)-secrecy schemes with

$$b = (v/k) \cdot k!/(k - L)! \quad \text{and} \quad v > k$$

is contained within the study of such schemes with $v = k$, and therefore we do not consider them further.

Acknowledgments

The authors would like to acknowledge the many valuable comments, suggestions, and corrections made by Miranda Mowbray. In particular we would like to thank her for Lemma 5.5, the example following Theorem 3.4, and pointing out that Theorems 4.3(i) and 4.6(i) only hold when $L > 1$. We would also like to thank anonymous referees for suggesting changes without which the paper would have been much poorer.

References

[1] H. J. Beker and F. C. Piper, *Cipher Systems*, Van Nostrand, Wokingham, 1982.
[2] A. Bonisoli and P. Quattrocchi, Existence and extension of sharply k-transitive permutation sets: a survey and some new results, *Ars Combinatoria*, **24A** (1987), 163–173.
[3] E. F. Brickell, A few results in message authentication, *Congressus Numerantium*, **43** (1984), 141–154.
[4] M. De Soete, Some constructions for authentication–secrecy codes, in *Advances in Cryptology: Proceedings of Eurocrypt* '88, Springer-Verlag, Berlin, 1988, pp. 57–75.
[5] M. De Soete, Bounds and constructions for authentication–secrecy codes with splitting, in *Advances in Cryptology: Proceedings of Crypto* '88, Springer-Verlag, Berlin, 1990, pp. 311–317.
[6] E. N. Gilbert, F. J. MacWilliams, and N. J. A. Sloane, Codes which detect deception, *Bell System Technical Journal*, **53** (1974), 405–424.
[7] E. S. Kramer, D. L. Kreher, R. Rees, and D. R. Stinson, On perpendicular arrays with $t \geq 3$, *Ars Combinatoria*, to appear.
[8] E. S. Kramer, S. S. Magliveras, T. van Trung, and Q. Wu, Some perpendicular arrays for arbitrarily large t, Preprint.
[9] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.
[10] J. L. Massey, Cryptography—a selective survey, in *Digital Communications* (editors: C. Biglieri and C. Prati), Elsevier (North-Holland), Amsterdam, 1986, pp. 3–21.
[11] R. C. Mullin, P. J. Schellenberg, G. H. J. van Rees, and S. A. Vanstone, On the construction of perpendicular arrays, *Utilitas Mathematica*, **18** (1980), 141–160.
[12] K. Nomura, On t-homogeneous permutation sets, *Archiv der Mathematik*, **44** (1985), 485–487.
[13] C. R. Rao, Combinatorial arrangements analogous to orthogonal arrays, *Sankhya Series A*, **23** (1961), 283–286.
[14] C. E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal*, **28** (1949), 656–715.
[15] G. Simmons, Authentication theory/coding theory, in *Advances in Cryptology: Proceedings of Crypto* '84, Springer-Verlag, Berlin, 1985, pp. 411–431.
[16] D. R. Stinson, A construction for authentication/secrecy codes from certain combinatorial designs, *Journal of Cryptology*, **1** (1988), 119–127.

[17] D. R. Stinson, Some constructions and bounds for authentication codes, *Journal of Cryptology*, **1** (1988), 37–51.
[18] D. R. Stinson, The combinatorics of authentication and secrecy codes, *Journal of Cryptology*, **2** (1990), 23–49.
[19] D. R. Stinson and L. Teirlinck, A construction for authentication/secrecy codes from 3-homogeneous permutation groups, *European Journal of Combinatorics*, to appear.
[20] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.