Designs, Codes and Cryptography, 7, 101–110 (1996)

Authentication Schemes, Perfect Local Randomizers, Perfect Secrecy and Secret Sharing Schemes

C. J. MITCHELL
Information Security Group, Royal Holloway, University of London

F. C. PIPER
Information Security Group, Royal Holloway, University of London

M. WALKER*
Information Security Group, Royal Holloway, University of London

P. WILD
Information Security Group, Royal Holloway, University of London

Abstract. In this paper we use results on authentication schemes to derive alternative proofs for results on perfect local randomness in pseudo-random sequences, on block cipher systems which afford perfect secrecy against known plaintext attacks and on secret sharing schemes.

1. Introduction

Shannon developed a theory of secrecy in his classic paper of 1949 [10]. He showed that if a cipher system provides perfect secrecy then the number of keys is greater than the number of messages, i.e. essentially only the one-time-pad provides perfect secrecy. In the 1980's, Simmons [11], [12] developed a complementary theory of authentication, relating the size of the key space to the probability of deception. This followed the early work of Gilbert et al. [3]. Massey [6] put Shannon's and Simmons' work in a combinatorial setting and drew parallels between the two theories and extended them to consider security against a known plaintext attack.

The many papers that have followed study secrecy and/or authentication either from a combinatorial point of view or using information theoretic concepts. In particular the work of Walker [16] provides information theoretic bounds relating the entropy of the key space to the probability of deception for cartesian authentication schemes. (Rosenbaum [8] extends Walker's results to non-cartesian schemes but we do not consider such schemes here.)

It is the purpose of this paper to show that these results on authentication schemes may be applied more generally to other cryptographic concepts such as perfect local randomness in pseudo-random sequences [5], perfect secrecy against known plaintext attacks on block ciphers [6], and secret sharing schemes [2].

In sections 2 and 3 we describe authentication schemes and summarise the results of [16]. In sections 4, 5 and 6 we show how each of the concepts, perfect local randomizer, block cipher system providing perfect secrecy against known plaintext attacks and secret sharing

* Vodafone Group plc, The Courtyard, 2–4 London Road, Newbury, Berks. RG13 1JL.

scheme may be viewed as a authentication scheme and how the results of [16] may be used to derive proofs of results in these topics.

2. Authentication Schemes

We consider a non-splitting cartesian authentication scheme, defined in [16] as a triple (S, M, E) of finite sets S, M and E satisfying the following conditions:

1. E is a collection of pairwise distinct functions from S into M;
2. each element of M is the image of precisely one element in S.

The elements of S are known as source states, those of M as encoded messages and those of E as encoding rules.

In the model of an authentication scheme an originator conveys source states to the recipient by transmitting across the channel the encoded messages resulting from the application of an agreed encoding rule. The sequence of source states which the originator is required to encode is modelled as a stochastic process. For each natural number n and each sequence $(s_1, \ldots, s_n) \in S^n$, $p(s_n \mid s_1, \ldots, s_{n-1})$ denotes the conditional probability that s_n is the nth source state given that $(s_1, \ldots, s_{n-1})$ is the preceding sequence produced by the process. We restrict our process to one that produces distinct messages and assume that $p(s_n \mid s_1, \ldots, s_{n-1}) > 0$ if and only if $s_1, \ldots, s_n$ are distinct. We assume that the agreed encoding rule is chosen according to a probability distribution which is independent of this process and denote the probability that $e \in E$ is the agreed encoding rule by $p_E(e)$. We assume that $p_E(e) \neq 0$ for all $e \in E$.

Thus the probability that the sequence $\mathbf{s} = (s_1, \ldots, s_n) \in S^n$ is produced by the process is

$$p(\mathbf{s}) = p(s_n \mid s_1, \ldots, s_{n-1}) \ldots p(s_2 \mid s_1) p(s_1).$$

and the conditional probability that m_n is the nth encoded message given that $(m_1, \ldots, m_{n-1})$ is the sequence of $n - 1$ preceding encoded messages is

$$p(m_n \mid m_1, \ldots, m_{n-1}) = p(S(m_n) \mid S(m_1), \ldots, S(m_{n-1})) p_E(E(m_n) \mid E(m_1, \ldots, m_{n-1}))$$

where for each $m \in M$, $S(m)$ denotes the unique element of S which it encodes and for any sequence $\mathbf{m} = (m_1, \ldots, m_l) \in M^l$, $E(\mathbf{m})$ denotes the subset of encoding rules whose image space contains $\{m_1, \ldots, m_l\}$. We also use $S(\mathbf{m})$ to denote the sequence $(S(m_1), \ldots, S(m_l))$ for any sequence $\mathbf{m} = (m_1, \ldots, m_l) \in M^l$ and $M(s \mid \mathbf{m})$ to denote the set $\{e(s) \mid e \in E(\mathbf{m})\}$ for any $s \in S$. Thus $M(s) = \{m \in M \mid S(m) = s\}$.

3. Channel Bounds

The authentication channel is modelled in terms of a third party, the spoofer, who observes the sequence $\mathbf{m} = (m_1, \ldots, m_n) \in M^n$ of encoded messages transmitted by the originator, and knows the triple (S, M, E) and the associated probability distributions. As the authentication scheme is cartesian the spoofer also knows the sequence $S(\mathbf{m}) = (S(m_1), \ldots, S(m_n))$ of source messages. The spoofer's aim is to choose $m \in M$ distinct from $m_1, \ldots, m_n$ such that m is the correct encoding of some $s \in S$ (distinct from $S(m_1), \ldots, S(m_n)$) under the encoding rule agreed by the sender and receiver. For each $\mathbf{m} \subset M^n$ with $p_E(E(\mathbf{m})) \neq 0$ and each $s \subset S$,

$$\psi(m \mid \mathbf{m}, s) = \sum_{e \in E(\mathbf{m}, m)} p_E(e \mid E(\mathbf{m})) = p_E(E(m) \mid E(\mathbf{m}))$$

is the probability that $m \in M(s)$ is the encoded message for s, given that $\mathbf{m}$ is a sequence of correctly encoded messages.

The strategy the spoofer should use is to choose m and s which maximises $\psi(m \mid \mathbf{m}, s)$ subject to the condition that $p(s \mid S(\mathbf{m})) \neq 0$. We use $P(\mathbf{m}, s)$ to denote the maximum probability of success if the spoofer chooses an encoded message in $M(s)$ and we use $P(\mathbf{m})$ to denote the probability of success if he adopts an optimal strategy. Further we denote the spoofer's expected probability of success after having observed n messages by $P(n) = \sum_{\mathbf{m} \in M^n} p(\mathbf{m})P(\mathbf{m})$.

Now

$$H(M(s) \mid \mathbf{m}) = -\sum_{m \in M(s)} \psi(m \mid \mathbf{m}, s) log_2 \psi(m \mid \mathbf{m}, s)$$

is the uncertainty faced by the spoofer as to which encoded message is the correct encoding for the source state s, given that he has observed the sequence of encoded messages $\mathbf{m}$. Walker [16] shows that $-log_2 P(\mathbf{m}) \leq H(M \mid \mathbf{m}, S)$ where $H(M \mid \mathbf{m}, S) = \sum_{s \in S} p(s \mid S(\mathbf{m}))H(M(s) \mid \mathbf{m})$ is the expected value of this uncertainty.

4. Perfect Local Randomizers

Maurer and Massey [5] define a (k, n)-sequence generator G as a function $G : \{0, 1\}^k \rightarrow \{0, 1\}^n$. For any given key $\mathbf{z} \in \{0, 1\}^k$, $G(\mathbf{z})$ is the output sequence and it could be used as the keystream in a stream cipher. A desirable property of a keystream generator is that knowledge of some of the bits should not provide information about other bits of the keystream. Maurer and Massey also describe an application of a (k, n)-sequence generator to key scheduling where this is also a desirable property.

They define a (k, n, e) perfect local randomizer (PLR) to be a (k, n)-sequence generator G such that, for any uniformly distributed $\mathbf{z} \in \{0, 1\}^k$, every subset of e bits of the output $\mathbf{s} = G(\mathbf{z})$ is a set of independent coin-tossing random variables. That is, for any e given bit positions, the 2^k output sequences of G, when restricted to those bit positions, produce each element of $\{0, 1\}^e$ equally often. Clearly knowledge of less than e bits of an output keystream of a PLR can give no information about any other bit.

Maurer and Massey [5] show that no (k, n, e) PLR exists for $e > k$, a (k, n, e) PLR with $e = k$ is an MDS (Maximum Distance Separable) code, and give constructions and examples for (k, n, e) PLRs for $e < k$. They also observe that although a (k, n, e) PLR is secure against an opponent who obtains e bits or fewer of the output, no (k, n)-sequence generator is secure against an opponent who may, for some e (possibly $e = 1$), obtain e bits of (suitable) information about the output. The reason for this is that a keystream generator may be thought of as an authentication scheme which authenticates the keystream bits of the stream cipher. From this viewpoint the shared key assures the receiver of the integrity of the keystream (which is added to some received ciphertext in order to recover the plaintext enciphered by a stream cipher). The concept of perfect local randomizer (viewed as an authentication scheme) therefore concerns the provision of security against an opponent trying to predict a subsequent encoded message (keystream bit) after observing a sequence of encoded messages (i.e. with knowledge of some output bits of the generator).

We may view a (k, n)-sequence generator G as an authentication scheme as follows. The source states are the bit positions of the output sequence $S = \{1, \ldots, n\}$. The encoding rules are the elements of the domain $\{0, 1\}^k$ of G. Thus $E = \{0, 1\}^k$. The encoded messages belong to the set $M = S \times \{0, 1\}$. If $\mathbf{z} \in E$ and $i \in S$ then the encoded message corresponding to source state i under encoding rule e is (i, s_i) where s_i is the ith bit of the output sequence $\mathbf{s} = G(\mathbf{z})$.

Now the authentication scheme provides security against an opponent who observes encoded messages (i, s_i) corresponding to source states i produced by a stochastic process. An opponent who observes a sequence $(i_1, s_{i_1}), \ldots, (i_n, s_{i_n})$ cannot predict the check bit s_i of the encoded message (i, s_i) corresponding to another source state i. That is, an opponent who has knowledge of n keystream bits $s_{i_1}, \ldots, s_{i_n}$ cannot predict another keystream bit s_i.

In this interpretation, using the notation of section 3, $M(s) = \{(s, 0), (s, 1)\}$ and $H(M(s) \mid \mathbf{m}) \leq 1$. Thus by Walker [16, Lemma 4] $P(\mathbf{m}, s) \geq 1/2$ with equality if and only if $\psi(m \mid \mathbf{m}, s)$ is uniform on $M(s)$ for all $s \not\in S(\mathbf{m})$. That $P(\mathbf{m}) = P(\mathbf{m}, s) = 1/2$ for all $s \not\in S(\mathbf{m})$ is exactly the condition that an opponent who observes $\mathbf{m}$ should have no information about any other bit and any other bit should be 0 or 1 equally likely.

Thus a (k, n, e) PLR, viewed as an authentication scheme is one for which $P(n) = 1/2$ for $n \leq e - 1$ and Walker's bound [16, Theorem 2] implies that the information conveyed about the encoding rule by an observed sequence of e encoded messages $I(E \mid M^e) = H(E) - H(E \mid M^e) \geq e$. Since $k = log_2|E| \geq H(E) \geq I(E \mid M^e)$ it follows immediately that in a (k, n, e) PLR we have $k \geq e$. Moreover, equality holds if and only if p_E is the uniform distribution, $H(E \mid M^e) = 0$ and the authentication scheme is $(e - 1)$-perfect [16]. Such an authentication scheme is associated with an orthogonal array [7], or in other words an MDS code.

5. Secrecy Against Known Plaintext

We consider block ciphers in which a message is represented as a sequence of plaintext blocks and is encrypted by transforming each block by one from a set of encryption functions. Such an encryption function is a bijection from the set of plaintext blocks to the set of ciphertext blocks, of the same size, and is determined by a key agreed upon by the sender and receiver. A message is encrypted by transforming each plaintext block according to this bijection. The resulting sequence of ciphertext blocks is transmitted.

Thus a block cipher system is a triple (P, C, T) where P is a set of plaintext blocks,

C is a set of ciphertext blocks and T is a set of bijective mappings from P onto C. We assume that a sender and receiver agree in advance upon a transformation chosen according to a probability distribution p_T on T such that $p_T(t) > 0$ for all $t \in T$. A message is a sequence $x_1, \ldots, x_n$, of arbitrary length n, of plaintext blocks and if $t \in T$ is the agreed transformation then the message is encoded by the sender as the sequence of ciphertext blocks $c_1 = t(x_1), \ldots, c_n = t(x_n)$.

We are interested in the security of the cipher system against a known plaintext attack. That is, we assume that an eavesdropper has intercepted $L - 1$ distinct plaintext/ciphertext pairs $(\mathbf{x}, \mathbf{c}) = (x_1, c_1), \ldots, (x_{L-1}, c_{L-1})$, and a further distinct ciphertext block c_L corresponding to some unknown plaintext block x_L, all encrypted under some transformation $t \in T$. We assume that the probability distribution on sequences of plaintext blocks is such that the probability, $p(x \mid \mathbf{x})$, that plaintext block x follows the sequence $\mathbf{x} = (x_1, \ldots, x_n)$ is non-zero for all $x \in P \backslash \{x_1, \ldots, x_n\}$. That is, the eavesdropper cannot rule out any plaintext block as that corresponding to c_L other than the plaintext blocks $x_1, \ldots, x_{L-1}$ whose corresponding ciphertext blocks he already knows. The cipher system has L-fold perfect secrecy against a known plaintext attack if $p(x_L = x \mid (\mathbf{x}, \mathbf{c}), c_L) = p(x_L = x \mid \mathbf{x})$ for all $x \in P \backslash \{x_1, \ldots, x_{L-1}\}$. A cipher system which has i-fold perfect secrecy against a known plaintext attack for all $i \leq L$ is said to have M(L)-secrecy [4].

Our aim is to apply the results of Walker [16], so we recast this known plaintext attack on a block cipher as an authentication scheme. Given a block cipher system (P, C, T) we consider the authentication scheme (S, M, E) where $S = C$, $M = P \times C$ and $E = \{e_t \mid t \in T\}$ is defined as follows. If $t \in T$ then $e_t : S \to M$ is defined by $e_t(c) = (t^{-1}(c), c)$ for all $c \in S$. The probability distribution p_E on E is determined by $p_E(e_t) = p_T(t)$ for all $t \in T$. We leave the probability distribution on sequences of source states (from $S = C$) unspecified.

For any sequence of plaintext/ciphertext pairs $(\mathbf{x}, \mathbf{c}) = ((x_1, c_1), \ldots, (x_n, c_n))$, we write $E(\mathbf{x}, \mathbf{c}) = \{e_t \mid t(x_i) = c_i, i = 1, \ldots, n\}$.

LEMMA 1 *Let (S, M, E) be an authentication scheme obtained from a block cipher system (P, C, T) with M(L)-secrecy. Let $(x_1, c_1), \ldots, (x_{L-1}, c_{L-1})$ be distinct plaintext/ciphertext pairs enciphered under some $t \in T$ and c_L a further distinct ciphertext. Then for $i = 0, \ldots, L - 1$ there is a constant λ_i such that for all $x \in P \backslash \{x_1, \ldots, x_i\}$, $p(E((x_1, c_1), \ldots, (x_i, c_i), (x, c_{i+1}))) = \lambda_i$.*

Proof. By M(L)-secrecy, for all $x \in P \backslash \{x_1, \ldots, x_i\}$, $E((x_1, c_1), \ldots, (x_i, c_i), (x, c_{i+1})) \neq \emptyset$ and

$$\begin{aligned} p(x_{i+1} &= x \mid (x_1, c_1), \ldots, (x_i, c_i), c_{i+1}) \\ &= \frac{p(x \mid \mathbf{x}) p(E((x_1, c_1), \ldots, (x_i, c_i), (x, c_{i+1})))}{\sum_x p(x \mid \mathbf{x}) p(E((x_1, c_1), \ldots, (x_i, c_i), (x, c_{i+1})))} \\ &= p(x_{i+1} = x \mid x_1, \ldots, x_i). \end{aligned}$$

Hence

$$p(E((x_1, c_1), \ldots, (x_i, c_i), (x, c_{i+1}))) = \sum_{x} p(x \mid \mathbf{x}) p(E((x_1, c_1), \ldots, (x_i, c_i), (x, c_{i+1})))$$

is a constant independent of x. ■

COROLLARY 2 *Let (S, M, E) be the authentication scheme determined by a block cipher system (P, C, T) with $M(L)$-secrecy and k plaintext blocks P. Let $(x_1, c_1), \ldots, (x_{L-1}, c_{L-1})$ be distinct plaintext/ciphertext pairs and c_L a further distinct ciphertext enciphered under some $t \in T$. Then*

(i) for each i, $0 \leq i \leq L-1$, $\psi((x, c) \mid (x_1, c_1), \ldots, (x_i, c_i), c) = 1/(k-i)$ for all $c \in C \backslash \{c_1, \ldots, c_i\}$ and all $(x, c) \in M(c)$ with $x \in P \backslash \{x_1, \ldots, x_i\}$.

(ii) for each i, $0 \leq i \leq L-1$, $P(i) = 1/(k-i)$.

(iii) $H(E) \geq \sum_{i=0}^{L-1} \log_2(k-i)$.

Proof. By the lemma, $\psi((x, c) \mid (x_1, c_1), \ldots, (x_i, c_i), c)$ is the same for each x. As there are $k - i$ choices for x, (i) follows. Now (ii) and (iii) follow immediately by Walker [16]. ■

This establishes the bound $|E| \geq \prod_{i=0}^{L-1}(k-i)$ on the number of transformations of a block cipher which offers perfect L-fold secrecy against a known plaintext attack. This is the same bound as that established in Godlewski and Mitchell [4] for secrecy codes offering the stronger security of ordered perfect L-fold secrecy.

6. Secret Sharing Schemes

Blakley [1] and Shamir [9] introduced the concept of threshold scheme to share a secret key among several users for the application of robust key management. Simmons [13], [14], [15] considered a more general application of shared control of information and/or actions and provided a model based on geometry for the study of secret sharing schemes.

A secret sharing scheme is a way of distributing partial information about a key to a finite set of participants so that only certain specified subsets of participants can determine the key. The partial information about a key that is assigned to a participant is called a share. When a subset of participants together use their pieces of partial information to determine a key we say they pool their shares.

The model of a secret sharing scheme that we use here is that described by Brickell and Stinson [2]. Let T be a set of s elements called shares and let P be a set of w participants. An assignment is a mapping $d : P \to T$. Let D be a collection of assignments and let P_D be a probability distribution on D. For any $\Omega \subseteq P$ and mapping $f : P \to T$ define $D(\Omega, f) = \{d \in D \mid d(Q) = f(Q)$ for all $Q \in \Omega\}$. This set identifies the assignments which assign a given collection of shares to a given subset of participants. Let X be a partition of D into q classes called keys and let Γ be a collection of subsets of P. Then (P, T, D, X) is a secret sharing scheme for Γ if for all $d \in D$ we have $D(\Omega, d) \subseteq k$ for some $k \in X$ when $\Omega \in \Gamma$ and $D(\Omega, d) \cap k \neq \emptyset$ for at least two elements $k \in X$ when $\Omega \notin \Gamma$. Thus if $d \in k$ has been used to distribute shares to the participants then a subset Ω of participants can pool their shares to determine the key k if and only if $\Omega \in \Gamma$. The set Γ is called a monotone access structure and identifies the authorised subsets of participants who can determine the key by pooling their shares.

A secret sharing scheme for w participants such that any subset of at least t participants can pool their shares to determine a key and no subset of fewer than t participants can so pool their shares is called a (t, w)-threshold scheme. In this case the access structure Γ is the collection of all subsets of P of cardinality at least t.

The probability distribution p_D on D determines a probability distribution p_X on X by $p_X(k) = \sum_{d \in k} p_D(d)$ for $k \in X$. Let $R \subseteq P$ and $f : P \to T$ be such that $D(R, f) \neq \emptyset$. Then f determines a partial assignment of shares to the participants in R which agrees with at least one assignment in D. Put $p(k \mid R, f) = \sum_{d \in k \cap D(R, f)} p_D(d)$. The conditional probability that the key is k given that the participants in R have been assigned the corresponding shares in $f(R)$ is $\psi(k \mid R, f) = \frac{p(k|R,f)}{\sum_k p(k;R,f)}$. A secret sharing scheme is perfect if $p_X(k) = \psi(k \mid R, f)$ whenever $R \notin \Gamma$. Of course, if $R \in \Gamma$ then $\psi(k \mid R, f)$ equals 1 if $D(R, f) \subseteq k$ and equals 0 otherwise. Note that if $\Omega \notin \Gamma$ then for all $d \in D$ and $k \in X$ we have $D(\Omega, d) \cap k \neq \emptyset$.

A secret sharing scheme is regular if p_D is the uniform probability distribution and $|D(R, f) \cap k|$ is independent of k for $R \notin \Gamma$. It is easily checked that a regular secret sharing scheme is perfect. The secret sharing schemes considered by Brickell and Stinson [2] are regular. We shall see that a perfect (t, w)-threshold scheme for which p_X is the uniform distribution and which meets an authentication bound, in a sense described later, is necessarily regular.

Another concept of interest in the relationship between secret sharing schemes and authentication schemes is that of an ideal secret sharing scheme. Suppose $R \notin \Gamma$ but $R \cup \{Q\} \in \Gamma$. If the secret sharing scheme is perfect then for all $d \in D$ we have $D(R, d) \cap k \neq \emptyset$ for all $k \in X$ and $D(R \cup \{Q\}, d) \subseteq k$ for some $k \in X$. It follows that for a perfect secret sharing scheme $d_1(Q) \neq d_2(Q)$ for $d_1, d_2 \in D(R, d)$ belonging to distinct classes. Thus $|T| \geq |X|$. A perfect secret sharing scheme is called ideal if $|T| = |X|$.

In an ideal secret sharing scheme, if $R \in \Gamma$ and $d' \in D(R, d)$ for some $d \in D$ then d and d' belong to the same class and $d'(Q) = d(Q)$ for all $Q \in P$. Thus we may identify d and d', i.e. $D(R, d) = \{d\}$ consists of a single element.

Let (P, T, D, X) be a secret sharing scheme. We define $|X|$ authentication schemes (S_k, M_k, E_k), $k \in X$, as follows. For $k \in X$, put $S_k = P$, $M_k = P \times T$ and $E_k = \{e_d \mid d \in k\}$ where, for each $d \in D$, $e_d : P \to P \times T$ is defined by $e_d(Q) = (Q, d(Q))$ for all $Q \in P$. Put $p_{E_k}(e_d) = p_D(d)/p_X(k)$ for all $d \in k$. Also put $(S, M, E) = (P, P \times T, \cup_{k \in X} E_k)$ with $p_E(e_d) = p_D(d)$. We leave the probability distribution on sequences of source states unspecified.

LEMMA 3 *Let (P, D, T, X) be a perfect (t, w)-threshold scheme and let the authentication schemes (S, M, E) and (S_k, M_k, E_k), $k \in X$, be determined as above. Let $R \subseteq P$ with*

$|R| \leq t-2$ and let f be a partial assignment of shares to the participants of R. Then, for all $k \in X$ and all $Q \in P \backslash R$,

(i) $M_k(Q \mid R, f) = M(Q \mid R, f)$, and

(ii) $\psi(m \mid R, f) = \psi_k(m \mid R, f) = 1/|M(Q \mid R, f)|$ for all $m \in M(Q \mid R, f)$.

Proof. Let $Q \in P \backslash R$. For any $m \in M(Q \mid R, f)$, let f_m be the partial assignment of shares to the participants of $R \cup \{Q\}$ which agrees with f on R and satisfies $m = (Q, f_m(Q))$. Then, for all $k \in X$,

$$p_X(k) = \frac{p(k \mid R \cup \{Q\}, f_m)}{\sum_{k \in X} p(k \mid R \cup \{Q\}, f_m)}$$

for all $m \in M(Q \mid R, f)$. Now (i) is immediate and (ii) follows since

$$\psi_k(m \mid R, f) = \frac{p(k \mid R \cup \{Q\}, f_m)}{\sum_{m' \in M(Q|R,f)} p(k \mid R \cup \{Q\}, f_{m'})}$$

is independent of $m \in M(Q \mid R, f)$. ■

The argument that shows that $|T| \geq |X|$ in a perfect secret sharing scheme actually shows that $|M(Q \mid R, f)| > |X|$ for any partial assignment of shares to a subset R of $t-1$ participants of a perfect (t, w)-threshold scheme. Since any partial assignment to fewer than $t-1$ participants may be extended to a partial assignment to $t-1$ participants, we have the following corollary.

COROLLARY 4 *Let (P, D, T, X), R and f be as in Lemma 3. Then, for all $k \in X$ and all $Q \in P \backslash R$, $\psi_k(m \mid R, f) \geq 1/|X|$ for all $m \in M_k(Q \mid R, f)$.*

The following corollaries follow from Walker [16] and the fact that $E = \cup_{k \in X} E_k$ is a disjoint union.

COROLLARY 5 *For each authentication scheme (S_k, M_k, E_k) the probability of deception having observed (R, f) satisfies $P(R, f) \geq 1/|X|$.*

COROLLARY 6 *For each authentication scheme (S_k, M_k, E_k), $H(E_k) \geq (t-1) log_2 |X|$.*

COROLLARY 7 *In a perfect (t, w)-threshold scheme (P, D, T, X), $|D| = |E| \geq |X|^t$.*

If equality holds in Corollary 6 for some $k \in X$, then equality holds in Corollary 4 so that (P, T, D, X) is ideal. Moreover, by Rosenbaum [8, Lemma 3.4], p_{E_k} is the uniform distribution. Further, p_X is uniform if and only if equality holds in Corollary 6 for all $k \in X$. In this case (P, D, T, X) is regular and corresponds to a $(t-1)$-perfect authentication scheme, that is, to an orthogonal array.

Finally, we remark that, in this case, $(P \cup \{X\}, (P \times T) \cup X, E')$ with $E' = \{e'_d \mid d \in D\}$ where, for all $d \in D$, $p_{E'}(e'_d) = p_D(d)$ and $e'_d : P \cup \{X\} \rightarrow (P \times T) \cup X$ satisfies

$e'_d(Q) = (Q, d(Q))$ for all $Q \in P$ and $e'_d(X) = k$ if $d \in k$, also corresponds to an orthogonal array.

7. Conclusions

We have shown how the information theoretic bounds given by Walker [16] for cartesian authentication schemes may be applied to other cryptographic concepts.

The close connection between the perfect local randomizers of Maurer and Massey [5] and MDS codes is seen to arise exactly because it is a problem in authentication. In a stream cipher an eavesdropper should not be able to predict any bit of the keystream even with knowledge of part of the keystream, just as, in an authentication scheme the spoofer should not be able to predict which encoded messages are authentic even with knowledge of some authentic encoded messages. The probability of success of the eavesdropper or the spoofer is a minimum (so that they are reduced to guessing the keystream or authentic encoded messages) when the bounds of Walker [16] are met.

In a known plaintext attack against a block cipher, corresponding plaintext/ciphertext pairs may be viewed as authentic encoded messages. Applying bounds of Walker [16] on authentication schemes we have established a bound on the number of keys required of a block cipher system providing $M(L)$-secrecy. Our result shows that $M(L)$ secrecy requires the same number of keys as the stronger condition of unordered perfect L-fold secrecy considered by Godlewski and Mitchell [4].

We have also shown that there is a relationship between secret sharing schemes and authentication schemes. We have applied the results of Walker [16] to the authentication schemes arising from a perfect threshold scheme to establish the bounds on the number of assignments in a perfect (t, w)-threshold scheme. Further, when the bound is met, we obtain the correspondence between ideal threshold schemes and orthogonal arrays.

References

1. G. R. Blakley, Safeguarding cryptographic keys, Proc AFIPS 1979 Natl. Computer Conf, New York, 48 (1979) pp. 313–317.
2. E. F. Brickell and D. R. Stinson, Some improved bounds on the information rate of perfect secret sharing schemes, *J of Cryptology*, Vol. 5 (1992) pp. 153–166.
3. E. N. Gilbert, F. J. MacWilliams, and N. J. A. Sloane, Codes which detect deception, *Bell System Technical Journal*, Vol. 53 (1974) pp. 405–424.
4. P. Godlewski and C. Mitchell, Key-minimal cryptosystems for unconditional secrecy, *J. of Cryptology*, Vol. 3 (1990) pp. 1–25.
5. U. M. Maurer and J. L. Massey, Local randomness in pseudo-random sequences, *J. of Cryptology*, Vol. 4 (1991) pp. 135–149.
6. J. L. Massey, Cryptography—a selective survey, in *Digital Communications*, C. Biglieri and C. Prati (Eds.), Elsevier (Noth-Holland) (1986) pp. 3-21.
7. C. Mitchell, M. Walker, and P. Wild, The combinatorics of perfect authentication schemes, *SIAM J. Disc. Math.*, Vol. 7 (1994) pp. 102–107.
8. U. Rosenbaum, A lower bound on authentication after having observed a sequence of messages, *J. of Cryptology*, Vol. 6 (1993) pp. 135–156.
9. A. Shamir, How to share a secret, *Comm. of the ACM*, Vol. 22 (1979) pp. 612–613.

10. C. E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal*, Vol. 28 (1949) pp. 656–715.
11. G. J. Simmons. A game theoretical model of digital message authentication, *Congressus Numerantium*, Vol. 34 (1982) pp. 413–424.
12. G. J. Simmons, Authentication theory/coding theory, Advances in Cryptology: Crypto 84, Lecture Notes in Computer Science, Springer-Verlag, Berlin, 196 (1985) pp. 411–431.
13. G. J. Simmons, Robust shared secret schemes or 'how to be sure you have the right answer even though you don't know the question', *Congressus Numerantium*, Vol. 68 (1989) pp. 215–248.
14. G. J. Simmons, How to (really) share a secret, Advances in Cryptology: Crypto 88, Lecture Notes in Computer Science, Springer-Verlag, Berlin, 403 (1990) pp. 390–448.
15. G. J. Simmons, W.-A. Jackson, and K. M. Martin, The geometry of shared secret schemes, *Bull of the ICA*, Vol. 1 (1991) pp. 71–78.
16. M. Walker, Information-theoretic bounds for authentication schemes, *J. of Cryptology* (1990) pp. 131–143.