SIAM J. DISC. MATH.
Vol. 7, No. 1, pp. 102–107, February 1994

THE COMBINATORICS OF PERFECT AUTHENTICATION SCHEMES*

CHRIS MITCHELL†, MICHAEL WALKER‡, AND PETER WILD§

Abstract. The purpose of this paper is to prove the equivalence of perfect authentication schemes and maximum distance separable codes.

Key words. authentication schemes, incidence structures, maximum distance separable codes

AMS subject classifications. 05B05, 94A60, 94B65

1. Introduction. In this paper, we consider the following communications scenario, which involves an originator of messages, a recipient of messages, and a third party called the spoofer. The originator wishes to send a sequence $s_1, \ldots, s_n$ of n distinct source messages to the recipient. To enable the recipient to verify the authenticity of these messages, the originator encodes them, prior to transmission, into a sequence of encoded messages $m_1, \ldots, m_n$, using one of a finite set of encoding rules that is agreed in advance with the recipient. The recipient verifies the authenticity of the message m_i by checking that it is a valid encoding of s_i for the agreed encoding rule e. The spoofer observes the sequence of encoded messages $m_1, \ldots, m_n$ and attempts to construct a correctly encoded message for a different source message. That is, he attempts to find a message m that is the encoding under the (to him unknown) encoding rule e of some source message that is distinct from $s_1, \ldots, s_n$.

In [6] one of the authors established an information-theoretic lower bound for the expected probability $P(n)$ that the spoofer succeeds in this task and for the arithmetic mean of $P(0), P(1), \ldots, P(N)$, where N is the maximum length of the sequence that the originator might be required to send using the same encoding rule. In addition, necessary and sufficient conditions on the encoding scheme are derived that ensure that these bounds are met, and these conditions lead to the concept of an N-perfect authentication scheme.

Associated with an authentication scheme is an incidence structure, and the conditions that ensure that the information-theoretic bounds are met are reflected in structural requirements on this incidence structure. In this paper, we characterise the incidence structures associated with N-perfect authentication schemes and thereby prove that perfect authentication schemes are equivalent to maximum distance separable codes.

The theorem proved in this paper extends a result in [3], where it is shown that an incidence structure is associated with a 1-perfect authentication scheme if and only if it is a net. It also establishes the converse of the observation made in [6], and independently by Stinson in [5], that an MDS code (or, equivalently, a transversal design) may be used to construct a perfect authentication scheme.

2. Authentication schemes, incidence structures, and codes. An *authentication scheme* is a triple $\underline{A} = \underline{A}(S, M, E)$ of finite sets S, M, and E, where each element of E is an injective function of S into M, and each element in M is the image under this set

* Received by the editors on February 26, 1990; accepted for publication (in revised form) November 13, 1992.

† Department of Computer Science, Royal Holloway, University of London, Egham, Surrey TW20 0EX, England.

‡ Vodafone Limited, The Courtyard, 2–4 London Road, Newbury, Berkshire RG13 1JL, England.

§ Department of Mathematics, Royal Holloway, University of London, Egham, Surrey TW20 0EX, England.

of functions of precisely one element in S. The elements of S are known as *source messages,* those of M are called *encoded messages*, and the functions in E are called *encoding rules*.

An authentication scheme as defined above is often referred to in the literature as a nonsplitting, Cartesian scheme (see [4]). The nonsplitting property means that, once an encoding rule has been selected, then the encoded message for each source message is unambiguously defined. For each encoding rule $e \in E$ and each source message $s \in S$, we denote by $m = e(s)$ the encoded message for s produced by e. The Cartesian property means that there is no secrecy in the scheme, in the sense that, if an encoded message is observed, then there is no ambiguity about which source message it encodes, even if the encoding rule is unknown. This is a consequence of the requirement that each encoded message is the encoding of precisely one source message. We use the notation $s = S(m)$ to denote the unique source message corresponding to the encoded message m.

With an authentication scheme $\underline{A}$, we may associate an incidence structure $\underline{I}(\underline{A}) = I(E, M, I)$. The set of points of this incidence structure is E, the set of blocks is M, and the incidence relation I is defined by the rule

$$eIm \quad \text{if and only if } m = e(S(m)).$$

That is, point e is incident with block m precisely when the encoded message m is obtained by encoding $S(m)$ under the encoding rule e. We use standard notation for incidence structures, as may be found, for instance, in [1]. Thus we denote by $(m) = \{e \in E | e(S(m)) = m\}$ the set of all points incident with the block m, and by $(e) = \{m \in M | e(S(m)) = m\}$ the set of all blocks incident with the point e. Moreover, we extend this notation by defining $(s) = \{m \in M | S(m) = s\}$ to be the set of all encoded messages that are encodings of the source s. Finally, we denote by $[x]$ the cardinality of the set (x).

The incidence structure $\underline{I} = \underline{I}(\underline{A})$ enjoys the properties that $\{(s) | s \in S\}$ is a partition of M, and, for each $s \in S$, the set $\{(m) | m \in (s)\}$ is a partition of E. That is, $\{(s) | s \in S\}$ is a parallelism of $\underline{I}$, where we recall that a parallelism of an incidence structure is a partition of its blocks into classes with the property that each point of the structure is incident with precisely one block from each of the classes. The property of having a parallelism actually characterises those incidence structures that are associated with authentication schemes as described above.

To see this, let $\underline{I} = \underline{I}(P, B, I)$ be an incidence structure, with points P and blocks B, which possesses a parallelism S. To avoid complications, assume that $\underline{I}$ does not have repeated points; that is, if $(p) = (p')$, then $p = p'$. We use each point $p \in P$ to define a function from S into B as follows: For each $s \in S$, set $p(s)$ to be the unique block in the class s that is incident with p. Then it is trivial to check that $\underline{A} = \underline{A}(S, B, P)$ is an authentication scheme and that $\underline{I}(\underline{A}) = \underline{I}$.

Having defined and characterised the incidence structure associated with an authentication scheme, we now turn to considering codes for authentication schemes. The approach we take is via the associated incidence structure. Although there are a number of other ways of associating codes and authentication schemes, this is the most convenient for our purposes.

We begin by recalling that a code $\underline{C}$ of length r over a finite alphabet A is a nonempty set of r-tuples with entries in A. The elements $c = (c_1, \ldots, c_r)$ of $\underline{C}$ are called codewords.

With any code $\underline{C}$, we can associate an incidence structure $\underline{I} = \underline{I}(\underline{C})$, which has a parallelism. The points of $\underline{I}$ are the codewords c. The blocks of $\underline{I}$ are the pairs (i, a), where $i \in \{1, \ldots, r\}$, $a \in A$, and a is the ith entry of at least one codeword. Incidence is then defined by the rule

$$cI(i, a) \quad \text{if and only if } c_i = a.$$

Now if, for each $i \in \{1, \ldots, r\}$ we define (i) to be the set of all blocks of the form (i, a), then $\{(i) \mid i \in \{1, \ldots, r\}\}$ is a parallelism of $\underline{I}$.

Conversely, to any incidence structure $\underline{I}$ with a parallelism, we can associate a code $\underline{C}$ such that $\underline{I}(\underline{C}) = \underline{I}$. To see this, let $\underline{I} = \underline{I}(P, B, I)$ be an incidence structure with parallelism S. Let $r = |S|$ and label the parallel classes $1, \ldots, r$. For each parallel class $i \in \{1, \ldots, r\}$, let φ_i be an injection from (i) into a suitably large set A and identify block $b \in (i)$ with the pair $(i, \varphi_i(b))$. For each point $p \in P$, define codeword $(p_1, \ldots, p_r)$ by $p_i = \varphi_i(b)$, where b is the unique block in the parallel class i incident with p. Then the set $\underline{C} = \{(p_i, \ldots, p_r) \mid p \in P\}$ is a code of length r over A and $\underline{I} = \underline{I}(\underline{C})$.

Combining the observations of this section, we see that, to any authentication scheme $\underline{A} = \underline{A}(S, M, E)$, we can associate a code $\underline{C} = \underline{C}(\underline{A})$. This code has length $|S|$, contains $|E|$ codewords, and is defined over an alphabet A of size equal to the maximum of the number of encodings of a source message. Conversely, given a code $\underline{C}$, we can construct an authentication scheme $\underline{A}$ with $\underline{C}(\underline{A}) = \underline{C}$.

3. MDS codes and perfect authentication schemes. Let $\underline{C}$ be a code of length r over a finite alphabet A of cardinality q. Then $\underline{C}$ is a *maximum distance separable* (MDS) code if and only if, for some t, it satisfies the following condition: Given any t distinct positions $i_1, \ldots, i_t$ and any sequence $a_1, \ldots, a_t$ of not necessarily distinct elements of A, there is exactly one codeword $c = (c_1, \ldots, c_r) \in \underline{C}$ with $c_{i_j} = a_j$ for $j = 1, \ldots, t$.

We refer to a code of this type as an MDS code with parameters (r, t, q). For further information on MDS codes, refer to [2]. It should be noted that our notation (r, t, q) is different from that used in [2].

We need the following characterisation of MDS codes in terms of their associated incidence structures as defined in the last section. The result is straightforward to prove using counting arguments and is therefore presented without proof. We use the following extension to the notation established for incidence structures in the last section. Let $\underline{b} = (b_1, \ldots, b_j)$ be a sequence of j blocks of an incidence structure. Then $(\underline{b})$ is the set of points that are incident with all the blocks $b_1, \ldots, b_j$, and $[\underline{b}]$ is the cardinality of this set.

LEMMA 3.1. *Let $\underline{I} = \underline{I}(\underline{C})$ be the incidence structure associated with an* MDS *code with parameters (r, t, q), let $0 \le j \le t$, and let $\underline{b} = (b_1, \ldots, b_j)$ be a sequence of j blocks belonging to different parallel classes. Then*

$$[\underline{b}] = q^{t-j}.$$

Conversely, if $\underline{I}$ is an incidence structure with a parallelism that satisfies this condition for some q, some t, and all $0 \le j \le t$, then $\underline{C} = \underline{C}(\underline{I})$ is MDS *with parameters (r, t, q), where r is the number of paralleled classes of $\underline{I}$.*

COROLLARY 3.2. *If an incidence structure satisfies the conditions of Lemma* 3.1, *then each parallel class contains exactly q blocks.*

We use this lemma to establish the equivalence of MDS codes and perfect authentication schemes. We begin by recalling the definition and characteristic properties of a perfect authentication as presented in [6]. To do this, we must first review the information theoretic measure of the security of an authentication scheme. For a more detailed discussion of the concepts, refer to [6].

Let $\underline{A} = \underline{A}(S, M, E)$ be an authentication scheme. To use this scheme, an originator and recipient of messages share an encoding rule e, which is selected from E according to some probability distribution $p(e)$. When the originator wishes to communicate a source message, he encodes it using e and sends the encoded message $m = e(s)$. Upon receiving m, the recipient validates it by using e to confirm that $e(S(m)) = m$. Suppose that the originator sends a sequence $m_1, \ldots, m_n$ of distinct encoded messages, all produced using the same encoding rule e, and that these messages are observed by a spoofer. The spoofer attempts to construct the correct encoding under e for some source message distinct from $S(m_1), \ldots, S(m_n)$. It is assumed that the spoofer has knowledge of $\underline{A}$ and plays the best strategy open to him. All he does not a priori know is the particular encoding rule e. We denote by $P(n)$ the expected probability that the spoofer succeeds in his task. We assume that n is not allowed to exceed some maximum value N and we let P_N be the arithmetic mean of $P(0), P(1), \ldots, P(N)$. The following lower bound for P_N is proved in [6]:

$$-\log P_N \leq H(E)/(N+1) \leq \log |E|/(N+1),$$

where $H(E)$ is the entropy of the distribution $p(e)$. These inequalities lead to the definition of an N-perfect authentication scheme.

An authentication scheme is said to be the *N-perfect* if $-\log P_N = H(E)/(N+1)$ with $p(e)$ the uniform distribution (so that, in this case, $H(E) = \log |E|$). Necessary and sufficient conditions for an authentication scheme to be N-perfect are given in [6]. These conditions form the basis for the main theorem of this paper and are summarised below in Lemma 3.3. To state these conditions and prove our theorem, it is first necessary to model the way in which source and encoded messages are generated and also to introduce more notation.

The sequence of source messages $s_1 = S(m_1), \ldots, s_n = S(m_n)$ generated by the originator and observed by the spoofer is modelled by a stochastic process $p(s_1, \ldots, s_n)$. We denote by $p(s_{n+1} | s_1, \ldots, s_n)$ the probability that the spoofer selects source message s_{n+1} with which to launch his attack, given that he has observed $s_1, \ldots, s_n$. All source messages are assumed to be distinct, so the process satisfies $p(s_j | s_1, \ldots, s_{j-1}) = 0$ whenever $s_j \in \{s_1, \ldots, s_{j-1}\}$. We also assume the converse. Thus our process satisfies

$$p(s_j | s_1, \ldots, s_{j-1}) = 0 \quad \text{if and only if } s_j \in \{s_1, \ldots, s_{j-1}\}.$$

We assume that the selection of the encoding rule is independent of the process that generates the source messages. Thus the probability that a sequence $\underline{m} = (m_1, \ldots, m_n)$ of encoded messages is produced by the originator and observed by the spoofer is given by

$$p(\underline{m}) = p(S(\underline{m}))p((\underline{m})),$$

where we use the notation

$$S(\underline{m}) = (S(m_1), \ldots, S(m_n)) \quad \text{and} \quad (\underline{m}) = \{e \in E | e(S(m_j)) = m_j, j = 1, \ldots, n\}.$$

The following additional notation will be used in the statement of Lemma 3.3 and in the proof of Theorem 3.4. Let $\underline{m} = (m_1, \ldots, m_n)$ be such that $p((\underline{m})) \neq 0$ and let $s \in S$. For each $m \in (s)$, define

$$(s | \underline{m}) = \{m \in (s) | p((m) | (\underline{m})) \neq 0\}.$$

Thus, in terms of the incidence structure $\underline{I}$ associated with $\underline{A}$, the set $(s | \underline{m})$ consists of all those blocks in the parallel class (s) that are potential valid encodings for s, given that the sequence $\underline{m}$ of encoded messages has already been produced. Observe that, if $n = 0$ so that $\underline{m}$ is the empty sequence, then $(s | \underline{m})$ consists of all those blocks of the incidence structure $\underline{I}(\underline{A})$ that belong to the parallel class (s) and are incident with at least one point $e \in E$ for which $p(e) \neq 0$.

LEMMA 3.3. *An authentication scheme $\underline{A} = \underline{A}(S, M, E)$ is N-perfect if and only if, for every $0 \leq n \leq N$, the following holds: If $\underline{m} = (m_1, \ldots, m_n)$ with $p(\underline{m}) \neq 0$, if $s \in S$ with $p(s \mid S(\underline{m})) \neq 0$, and if $m \in (s \mid \underline{m})$, then*

$$\log |E|/(N+1) = H(E)/(N+1) = -\log p((m) \mid (\underline{m})) = \log |(s \mid \underline{m})|.$$

The proof of the lemma follows immediately from [6, Thm. 2] and the definition of N-perfect. With the help of this result and Lemma 3.1, we may now prove our main theorem.

THEOREM 3.4. *Let $\underline{C} = \underline{C}(\underline{A})$ be the code associated with an N-perfect authentication scheme $\underline{A}$ with source messages S. Then $\underline{C}$ is an* MDS *code with parameters $(|S|, N+1, q)$, where $q = [s]$ for all $s \in S$. Conversely, if $\underline{C}$ is an* MDS *code with parameters $(r, N+1, q)$, then $\underline{C} = \underline{C}(\underline{A})$ for some N-perfect authentication scheme $\underline{A}$ with r source messages and q encodings for each source message.*

Proof. Let $\underline{A} = \underline{A}(S, M, E)$ be an N-perfect authentication scheme and let $\underline{I} = I(\underline{A})$ be the incidence structure associated with it. Applying Lemma 3.3 with $n = 0$ yields

$$\log [s] = \log |E|/(N+1) \quad \text{for all } s \in S.$$

Thus the number of blocks in each parallel class of $\underline{I}$ is a constant q, and $|E| = q^{N+1}$. We show that, if $0 \leq j \leq N+1$ and if $\underline{m} = (m_1, \ldots, m_j)$ is a sequence of blocks of $\underline{I}$ belonging to different parallel classes, then $[\underline{m}] = q^{N+1-j}$. The first part of the theorem then follows directly from Lemma 3.1.

To prove the above statement, we proceed by induction on j. We have already proved the result for $j = 0$, so we assume that $1 \leq j \leq N+1$, and the statement is true for $j-1$. Let $\underline{m}' = (m_1, \ldots, m_{j-1})$ and consider the terms in the identity

$$p((\underline{m})) = p((m_j) \mid (\underline{m}'))p((\underline{m}')).$$

Since $p(e)$ is uniform, and, as $|E| = q^{N+1}$, we have $p((\underline{m})) = [\underline{m}]q^{-(N+1)}$ and similarly for $p((\underline{m}'))$. Thus $[\underline{m}] = p((m_j) \mid (\underline{m}'))[\underline{m}']$. Applying the induction hypothesis to $[m']$ now gives

$$(1) \qquad [\underline{m}] = p((m_j) \mid (\underline{m}'))q^{N+1-(j-1)}.$$

Now consider the term $p((m_j) \mid (\underline{m}'))$. First, we apply Lemma 3.3 with $n = j-1$ to $\underline{m}'$ and $S(m_j)$. This gives

$$\log |(S(m_j) \mid \underline{m}')| = \log |E|/(N+1) = \log q.$$

However, we know that $[S(m_j)] = q$, so $(S(m_j) \mid \underline{m}') = (S(m_j))$. Thus $m_j \in (S(m_j) \mid \underline{m}')$, and Lemma 3.3 tells us that $-\log p((m_j) \mid (\underline{m}')) = \log q$. Thus $p((m_j) \mid (\underline{m}')) = q^{-1}$, and substitution of this in (1) proves $[\underline{m}] = q^{N+1-j}$, as required.

To prove the final part of the theorem, let $\underline{I} = \underline{I}(\underline{C})$ be the incidence structure associated with the MDS code and let $\underline{A} = \underline{A}(\underline{I})$ be the authentication scheme associated with $\underline{I}$. Let $p(e)$ be the uniform distribution on the set E of points of $\underline{I}$ and let $p(s_1, \ldots, s_n)$ be a process defined on the parallel classes S of $\underline{I}$ that satisfies $p(s_j \mid s_1, \ldots, s_{j-1}) = 0$ if and only if $s_j \in \{s_1, \ldots, s_{j-1}\}$. We prove that $\underline{A}$ is N-perfect by using Lemma 3.1 to show that the conditions of Lemma 3.3 are satisfied.

To this end, let $0 \leq n \leq N$, let $\underline{m} = (m_1, \ldots, m_n)$ be such that $p(\underline{m}) \neq 0$, let $s \in S$ with $p(s \mid S(\underline{m})) \neq 0$, and let $m \in (s \mid \underline{m})$. Since $p(\underline{m}) = p(S(\underline{m}))p(\underline{m})) \neq 0$, it follows that the parallel classes $S(m_1), \ldots, S(m_n)$ are distinct. Moreover, since

$p(s \mid S(\underline{m})) \neq 0$, the parallel class s is distinct from $S(m_1), \ldots, S(m_n)$. Thus, from Lemma 3.1, we have

$$[\underline{m}] = q^{N+1-n} \quad \text{and} \quad [\underline{m}, m] = q^{N+1-n-1}.$$

Thus

$$p((m) \mid (\underline{m})) = [\underline{m}, m]/[\underline{m}] = q^{-1}.$$

It follows that $(s \mid \underline{m}) = (s)$. However, $H(E) = \log |E|$, $|E| = q^{N+1}$ by Lemma 3.1, and $[s] = q$ by Corollary 3.2; so all the equalities in Lemma 3.3 hold.

REFERENCES

[1] P. DEMBOWSKI, *Finite Geometries*, Springer-Verlag, Berlin, Heidelberg, 1968.

[2] F. J. MAC WILLIAMS AND N. J. A. SLOANE, *The Theory of Error Correcting Codes*, North–Holland, Amsterdam, 1977.

[3] M. DE SOETE, K. VEDDER, AND M. WALKER, *Cartesian authentication schemes*, in Advances in Cryptology—Proc. of Eurocrypt 89, Lecture Notes in Computer Science, Vol. 434, Springer-Verlag, Berlin, 1990, pp. 476–490.

[4] G. J. SIMMONS, *Authentication theory/coding theory*, in Advances in Cryptology—Proc. of Crypto 84, Lecture Notes in Computer Science, Vol. 196, Springer-Verlag, Berlin, 1985, pp. 411–431.

[5] D. R. STINSON, *The combinatorics of authentication and secrecy codes*, J. Cryptology, 2 (1990), pp. 23–49.

[6] M. WALKER, *Information-theoretic bounds for authentication schemes*, J. Cryptology, 2 (1990), pp. 131–143.