MESSAGE AUTHENTICATION WITH ARBITRATION OF TRANSMITTER/RECEIVER DISPUTES*

Gustavus J. Simmons
Sandia National Laboratories
Albuquerque, NM 87185

In the most general model of message authentication, there are four essential participants: a transmitter who observes an information source†, such as a coin toss, and wishes to communicate these observations to a remotely located receiver over a publicly exposed, noiseless, communications channel; a receiver who wishes to not only learn the state of the source (as observed by the transmitter) but also to assure himself that the communications (messages) he accepts actually were sent by the transmitter and that no alterations have been made to them subsequent to the transmitter having sent them, and two other parties, the opponent and the arbiter. The opponent wishes to deceive the receiver into accepting a message that will misinform him as to the state of the source. We assume, in accordance with Kerckhoffs' criteria in cryptography, that the opponent is fully knowledgeable of the authentication system and that in addition he is able to both eavesdrop on legitimate communications in the channel and to introduce fraudulent communications of his own choice. We also assume that he has unlimited computing power, i.e., that any computation which can be done in principal can in fact be done in practice. Given this, the opponent can achieve his objective in either of two ways:

1) he can impersonate the transmitter and send a fraudulent message when in fact no message was sent by the transmitter,

or

2) he can wait to intercept a legitimate message from the transmitter and substitute in its stead some other message of his own devising.

* This work performed at Sandia National Laboratories supported by the U. S. Dept. of Energy under contract no. DE-AC04-76DP00789.

† Ideally we would call the states of the source "messages" as is the practice in communications theory. However, if we did this we would be forced to introduce terminology to designate the collection of sequences that are actually transmitted through the channel, perhaps "authenticating codewords," paralleling "error detecting and correcting codewords" from communications theory. Unfortunately, the natural contraction "codeword" already has an accepted meaning in communications theory so that we would either have to coin a new term to designate the specific sequence of symbols transmitted to convey and authenticate a message -- none of which seem very natural -- or else use the cumbersome term "authenticating codeword." The term "authenticator," which is usually used to denote an authenticating suffix appended to the information that is to be authenticated, has too restricted a connotation for the general case. We have opted instead to use the term "message" to designate the sequence of symbols actually transmitted and to tolerate the rather artificial device that the information conveyed by a message is the state of a hypothetical source.

D. Chaum and W.L. Price (Eds.): Advances in Cryptology - EUROCRYPT '87, LNCS 304, pp. 151-165, 1988.

In either case, the opponent wins if the receiver accepts the fraudulent message as being a legitimate and unmodified communication from the transmitter and ends up being misinformed as to the state of the source as a result.

In the simplest model of authentication, the transmitter and receiver are assumed to be mutually trusting and trustworthy and to act with the joint purpose of detecting attempted deceptions by the opponent. Authentication codes have been devised by Brickell [1], Simmons [2,3,4], Stinson [5,6] and others [7,8,9] that not only achieve this end, but also make perfect use of the information content of the transmitted message in the process. Unfortunately, until now this has required that the transmitter and receiver be privy to precisely the same secret (from the opponent) information about the specific authentication protocol being used and hence, that each be able to do anything the other can do, i.e., the transmitter will be able to disavow a message that he actually sent to the receiver or the receiver can fraudulently attribute a message of his own devising to the transmitter. What this means, of course, is that if the assumption of mutual trustworthiness doesn't hold, that either will be able to defraud the other in a way that cannot be verified -- or demonstrated -- to a third party. It is here that the fourth party, the arbiter, comes in. The arbiter is provided with secret (known only to him and the transmitter) information as to which messages the transmitter is supposed to use in the communications protocol and may also include information that the arbiter shares in secret with the receiver as to which messages the receiver will accept. His sole function is to certify on demand whether a particular message presented to him is one that the transmitter could have used under the established protocol. He cannot say that the transmitter did send it, only that he could have under the established protocol. In this setting, the transmitter can cheat if

3) he can cause the receiver to accept and act on a message that he (the transmitter) can later disavow. To be successful, he must not only choose a message that the receiver will accept, but also one which the arbiter will not certify, because it is not a message that would have been used by him (the transmitter) under the authentication protocol established by the arbiter.

If the transmitter succeeds in disavowing the message, the receiver will be, according to the terms of the protocol, held (unjustly) liable.

The receiver can cheat if he can successfully attribute a message of his own devising to the transmitter, i.e., a message not sent by the transmitter, but one which the arbiter will certify as being one that could have been sent by the transmitter under the established authentication protocol. There are two strategies for cheating available to the receiver, paralleling the two strategies available to the opponent:

4) He can claim to have received a message (which he fabricated) from the transmitter, when in fact no message was sent by the transmitter,

or

5) he can wait until he receives a legitimate message from the transmitter and then claim to have received some other message conveying different information than that communicated by the transmitter's message: replacing an order to buy with one to sell, for example.

In either case, if the arbiter later certifies the fraudulent message as being one that the transmitter might have sent under the established authentication protocol, the transmitter will, according to the terms of the protocol, be held (unjustly) liable.

The presence of an arbiter has no effect on the outcome of the opponent's attempted deception. If the opponent is successful in deceiving the receiver, the transmitter will, of course, appeal to the arbiter when he is later held liable (by the receiver) for a message that he (the transmitter) didn't send. The arbiter in this case, depending on whether the opponent chose a message that was not only acceptable to the receiver but which also might have been sent by the transmitter under the established authentication protocol, will assign the liability for the receiver's actions to the transmitter or otherwise to the receiver. The assignment of liability by the arbiter is unjust in either case since neither the transmitter nor the receiver cheated or failed to properly use the authentication protocol, however the arbiter can only verify whether a message is or is not consistent with the protocol in use, and not what its source might be. He can, therefore, never ascribe the liability to the opponent, even though there is always some nonzero probability that this is the source of the message.

The smallest example of an authentication code [3,4], capable of detecting attempted deceptions by an opponent, but providing no protection against deception by either the transmitter or the receiver, i.e., without arbitration, is the following: The source is a fair coin toss, by the transmitter, whose outcome denoted H or T we take to be the state of the source. There are four encoding rules, e_i, which encode states of the source into one of four possible messages, m_j, according to the scheme

(1)

	m_1	m_2	m_3	m_4
e_1	H		T	
e_2	H			T
e_3		H	T	
e_4		H		T

For the details of how authentication schemes are constructed in general see [2,3,4], but for the present discussion it suffices to note that in (1) each encoding rule uses only two out of the four possible messages and that each message appears in only two out of the four encoding rules. Consequently the probability that a randomly chosen message will be in a particular encoding rule, chosen with uniform probability, is 1/2 as is the probability of identifying the chosen encoding rule given the fact that it contains a particular message.

In the protocol for authenticating the outcome of a coin toss, the transmitter and receiver choose (in secret from the opponent) an encoding rule with the uniform probability distribution on the e_i (their optimal authentication strategy) in advance of the communication that they wish to authenticate. The opponent knows (1) and their strategy for choosing an e_i but not then choice. If he chooses to impersonate the transmitter and send an unauthentic message when no message has yet been sent by the transmitter, it should be obvious that irrespective of which message, m_j, he chooses, the probability that it will correspond to an encoding of a source state under encoding rule e_i, and hence that it will be accepted by the receiver as an authentic message, is 1/2. Similarly, if the opponent waits to observe a legitimate communication by the transmitter, his uncertainty about the encoding rule being used will drop from one out of four equally likely possibilities to one out of two. However, his probability of choosing an acceptable (to the receiver) substitute message will still be 1/2. For example, if the opponent observes m_1 he knows that the transmitter and receiver are using either encoding rule e_1 or e_2. In the first case m_3 would be an acceptable message to the receiver while m_4 would be rejected as unauthentic, while in the second case, exactly the opposite would be true. Hence, the opponent's probability of deceiving the receiver is 1/2 irrespective of whether he impersonates the transmitter or substitutes (modifies) legitimate messages.

Clearly since the transmitter and receiver must both know the chosen encoding rule -- the transmitter so that he can encode the source state into a message the receiver will accept and the receiver so that he can decode and authenticate the message -- either can do anything the other can. In particular the receiver can claim to have received a message when none was sent and the transmitter will be unable to prove to a third party that he didn't send it, or the transmitter can disavow a message that he did send and the receiver will be unable to prove that he received the message through the communications channel.

The essence of this paper is illustrated in an extension of this simple one-bit source example that in addition to one providing bit of protection against each of the two possible outsider (the opponent) deceptions, also provides one bit of protection against each of the three forms of insider (transmitter or receiver) cheating described earlier [10]. In this extended protocol, using the same source example as before, the receiver first chooses one of the 16 encoding rules defined by the Cartesian product

$$\left\{\begin{array}{cccc} H & H & - & - \\ H & - & H & - \\ - & H & - & H \\ - & - & H & H \end{array}\right\} \times \left\{\begin{array}{cccc} T & T & - & - \\ T & - & T & - \\ - & T & - & T \\ - & - & T & T \end{array}\right\}$$

with a uniform probability distribution. For example, the first row of the product would be

$$\begin{array}{c|cccccccc} & m_1 & m_2 & m_3 & m_4 & m_5 & m_6 & m_7 & m_8 \\ \hline a_1 & H & H & - & - & T & T & - & - \\ \vdots & & & & & & & & \end{array}$$

which says that a head outcome to the transmitter's coin toss could be communicated by the transmitter using either message m_1 or m_2. Similarly, messages m_5 or m_6 would communicate source state "tails", while messages m_3, m_4, m_7 and m_8 would be rejected by the receiver as unauthentic. The important point to note is that in each of the encoding rules there are exactly two acceptable (to the receiver) messages available for each state of the source. The receiver communicates his choice of an authenticating rule to the arbiter in secret (from the transmitter and the opponent(s)). What the receiver has done is to commit himself to accept as authentic any of the messages used in the authenticating rule he chose, and to reject as unauthentic any not used there. The arbiter next chooses one of the four vectors defined by the Cartesian product

$$\begin{Bmatrix} 1 & - & - & 1 \\ - & 1 & 1 & - \end{Bmatrix} \times \begin{Bmatrix} 1 & - & - & 1 \\ - & 1 & 1 & - \end{Bmatrix} ,$$

again, with a uniform probability distribution, and forms the Schur product† of the chosen vector with the authenticating rule selected by the receiver. The net result is, for the example of a_1 having been the authenticating rule chosen by the receiver, that one of the four possible encoding rules

$$\begin{array}{cccccccc} H & - & - & - & T & - & - & - \\ H & - & - & - & - & T & - & - \\ - & H & - & - & T & - & - & - \\ - & H & - & - & - & T & - & - \end{array}$$

will be selected (with a uniform probability distribution) as a result of the concatenated choices of the receiver and arbiter. The arbiter communicates, in secret (from the receiver and the opponent(s)), the resulting encoding rule to the transmitter. This rule is then the established protocol that the transmitter is supposed to use to encode the observed state of the source into the message that is to be transmitted to the receiver. The transmitter knows that only the messages used in the encoding rule given to him by the arbiter will be certified by the arbiter in the event of a later dispute. He also knows that there are other messages which the receiver will accept as authentic since they appear in the authenticating rule that he (the receiver) chose, but which the arbiter will not certify as authentic since they do not appear in the encoding rule he (the arbiter) selected. Assume, for example, that the arbiter chose the vector

$$- \; 1 \; 1 \; - \; 1 \; - \; - \; 1$$

† Given vectors $A = (a_i)$ and $B = (b_i)$ the Schur product is the vector $C = (a_i b_i)$.

so that the resulting encoding rule is

$$\begin{array}{c|cccccccc} & m_1 & m_2 & m_3 & m_4 & m_5 & m_6 & m_7 & m_8 \\ \hline e & - & H & - & - & T & - & - & - \end{array} .$$

In this example, source state "heads" is to be communicated by the transmitter sending message m_2 while "tails" is to be communicated by sending message m_5.

Using this authentication scheme we now show that the immunity provided to each of the five types of cheating described earlier is to hold the cheater to a probability of 1/2, i.e., one bit of protection, as claimed irrespective of which type of cheating is considered. The easiest of the deceptions to analyze is the case of the outsider (opponent) who only knows the "system," i.e., he knows what the procedures are but does not know the receiver's or arbiter's choices. It should be clear that if he attempts to impersonate the transmitter and send a message when none has been sent, his probability of choosing one of the four (out of eight) messages that the receiver has agreed to accept (in his choice of an encoding rule) is 1/2 since in each case there are four equally likely messages that will be accepted as authentic and four that will be rejected as unauthentic. On the other hand, if he waits to observe a message, say m_1, his uncertainty about the encoding rule chosen by the receiver drops from one out of sixteen equally likely candidates to one out of four, however these four leave him with four equally likely possibilities for the message that the transmitter is to use to communicate the other state of the source, and much more importantly, with four equally likely pairings of messages that the receiver would accept as communicating the other state of the source, with each message occurring in precisely two of the pairs. The net result is that the opponent's probability of success in substituting a message that the receiver will accept as communicating the other state of the source is still 1/2.

Consider next, the next simplest case to analyze, the transmitter disavowing a message that he actually sent. In order to succeed, the transmitter must choose a message that the receiver will accept but that is not used in the established protocol forwarded by the arbiter. In other words he must choose a message that was used in the encoding rule that the receiver chose, but not used in the final encoding rule generated by the arbiter's choice. Continuing with the example used above, the transmitter knows from the final encoding rule that was given to him by the arbiter:

$$- \ H \ - \ - \ T \ - \ - \ -$$

that the arbiter must have chosen vector

$$- \ 1 \ 1 \ - \ 1 \ - \ - \ 1$$

and hence can infer that the receiver must have chosen one of the four encoding rules.

m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8
H	H	-	-	T	T	-	-
H	H	-	-	T	-	T	-
-	H	-	H	T	T	-	-
-	H	-	H	T	-	T	-

Since messages m_3 and m_8 do not appear in any of these rules, the transmitter can be certain that they would be rejected by the receiver as unauthentic, and hence he will not send either of these. Each of the remaining four messages, m_1, m_4, m_6, and m_7, appear in two of the equally likely choices of an encoding rule, hence he cannot do better than choose one out of these four messages with equiprobability. Irrespective of which of the four he chooses, the probability that it will be accepted by the receiver is 1/2. If it is accepted, the transmitter can disavow having sent it, since he knows that the arbiter will not certify it as a message that would have been used under the established protocol.

Finally, we consider the two types of cheating available to the receiver. Of the four messages that he has agreed (with the arbiter) that he will accept as authentic, since they are used in his choice of an authenticating rule, two will be certified as being messages that could have been used under the established protocol and two will not be certified. The receiver will succeed in fraudulently attributing a message to the transmitter if he is able to choose one of the pair that the arbiter will certify and will fail otherwise. It should be clear that his probability of success is 1/2 since the arbiter's selection procedure chooses among the acceptable (to the receiver) messages with a uniform probability distribution. If he waits until he receives a message from the transmitter, say m_2, he can reduce his uncertainty about the vector that the arbiter choose from one of four equally likely cases to one of two:

$$- \ 1 \ 1 \ - \ 1 \ - \ - \ 1$$

or

$$- \ 1 \ 1 \ - \ - \ 1 \ 1 \ -$$

in the example. The result however is that either message m_5 or m_6 is equally likely to be the one that will be certified, and his probability of successfully substituting a message conveying a different state of the source than was communicated in the message sent by the transmitter, i.e., of substituting one which will both communicate a different state of the source and will subsequently be certified by the arbiter as a message the transmitter could have sent under the established authentication protocol is 1/2.

This small example illustrates all of the essential features of authentication codes that permit arbitration. In the resulting code three bits of information must be communicated to identify one of eight equally likely messages. According to the protocol, this communication provides one bit of information about the source state, one bit of protection against deception by outsiders and one bit of protection against cheating by insiders. In earlier papers on authentication codes without arbitration [3,4], codes were defined to be perfect in the natural sense that all of the information transmitted was either used to communicate the state of the source or else to confound one of the cheating parties. Consequently, it seems reasonable to also describe the code illustrated here as perfect.

Our object will be to generalize the one-bit example of the preceding section to construct an infinite class of perfect authentication codes that permit arbitration. To do this, we will carry over various properties of the small example that were essential to that construction, but without a rigorous proof that all of these conditions are necessary to construct authentication codes that permit arbitration.

We start by insisting that the extended codes also be of the form of a k-fold Cartesian product of an $m \times n$ array, A, in which each row contains r entries and each column contains $t = mr/n$ entries. k is the number of states the source can assume, i.e, the total number of distinct pieces of information that the transmitter may need to communicate to the receiver. A must satisfy several other conditions which we will derive in order for it to be suitable as a basis for constructing an authentication with arbitration code whose security is easy to calculate. The first of these is a regularity condition which can be most easily described by saying that the hypergraph defined by the rows of A is symmetric[†].

Given that the authentication code **A** is a Cartesian product, $\mathbf{A} = A^k$, each of the km messages is used in kt of the authenticating rules. The fact that A is symmetric is sufficient to insure that the optimal strategy for the receiver to use in selecting an authenticating rule is to choose with a uniform probability distribution on the rows of **A**, and hence because of the Cartesian product construction of **A**, to equivalently choose rows from the k factors A in the same manner. In this case, the opponent's probability of choosing a message which appears in the authenticating rule chosen by the receiver based only on his knowledge of the structure of **A**, i.e., of impersonating the transmitter, will be:

$$(1) \qquad P_{\mathrm{Opp}}(\text{impersonation}) = \frac{kr}{kn} = \frac{r}{n} = \frac{t}{m} \quad .$$

On the other hand, if he waits to observe a legitimate message he will have learned something about the collection of messages which the receiver will accept (conveying a particular source state) but because of the independence attributable to the Cartesian product construction of **A**, he can do no better than choose with a uniform probability distribution among the (k-1)r messages used by the other factors, hence;

[†] A hypergraph is symmetric if there exists an automorphism carrying any edge into any other edge, or equivalently any row of A can be interchanged with any other row and the resulting incidence array A' can be made identical to A by appropriate interchanges of columns and the other rows in A'.

(2) $$P_{Opp}(\text{substitution}) = \frac{(k-1)r}{(k-1)n} = \frac{r}{n} = \frac{t}{m}$$

therefore

(3) $$P_{Opp} = \frac{r}{n} = \frac{t}{m} \ .$$

We arbitrarily specialize to the case in which the arbiter is constrained to choose, with a uniform probability distribution, only one message from among the r messages that the receiver has indicated he will accept as authentic and interpret as conveying a particular state of the source. In general, the arbiter may choose some number α, $1 \leq \alpha < k$, of the acceptable messages but the analysis is only made more difficult by this generality, and with no apparent gain in security, so we have chosen to set $\alpha = 1$ for the extended authentication codes described here. The receiver knows, of course, that the transmitter will use (according to the protocol) only the k messages appearing in the encoding rule communicated to him by the arbiter. If he can find one of these, he can falsely attribute it to the transmitter and be assured that the arbiter would later certify it to be one that the transmitter could have sent under the existing protocol, i.e., the transmitter would be held liable. Clearly, the receiver's probability of successfully attributing a fraudulent message to the transmitter will be

(4) $$P_{Rx}(\text{impersonation}) = \frac{k}{kr} = P_{Rx}(\text{substitution}) = \frac{k-1}{(k-1)r} = \frac{1}{r}$$

or

(5) $$P_{Rx} = \frac{1}{r} \ .$$

The equality in (4) follows again from the independence of the factors in the Cartesian product construction for **A**.

Since our object is to make all forms of cheating equally improbable of success, we find that

(6) $$n = r^2$$

by setting $P_{Rx} = P_{Opp}$ in (3) and (5).

The analysis of the transmitter's probability of successfully being able to disavow a message which the receiver accepted as authentic is more difficult to analyze. To do this, the transmitter must choose one of the r-1 messages in one of the factors of the authenticating rule chosen by the receiver, and hence which he will accept as authentic, but which the arbiter will not certify since they do not appear in the encoding rule that he (the arbiter) constructed. Given any message M, it occurs in t rows of the corresponding factor A of **A** and hence in t^k authenticating rules. Because of the independence due to the Cartesian product construction of

A we can restrict attention to the factor A that uses the message M. Since each row of A contains r entries, there are t(r-1) occurences of other messages paired with M over all of the rows of A. It probably follows from the requirement that A represent a symmetric graph, however, instead of trying to prove this, we simply impose the constraint that any message that occurs with M in some row of A also must occur the same number of times, s, as any other message that occurs with M. The number of distinct messages that occur with M is therefore

$$(7) \qquad \frac{t(r-1)}{s} ,$$

(r-1) of which occur with M in the row of A that the receiver chose in constructing the encoding rule he communicated to the arbiter. Therefore, the probability that the transmitter chooses (at random) a message the receiver will accept as authentic but which the arbiter will not certify is;

$$(8) \qquad P_{Tx} = \frac{r-1}{\frac{t(r-1)}{s}} = \frac{s}{t} .$$

Setting $P_{Tx} = P_{Rx}$, we get

$$(9) \qquad \frac{s}{t} = \frac{1}{r} \quad \text{or} \quad s = \frac{t}{r} = \frac{m}{n} = \frac{m}{r^2}$$

Figure 1 should help make clear the canonical structure of the array A that has been forced by the conditions imposed thus far.

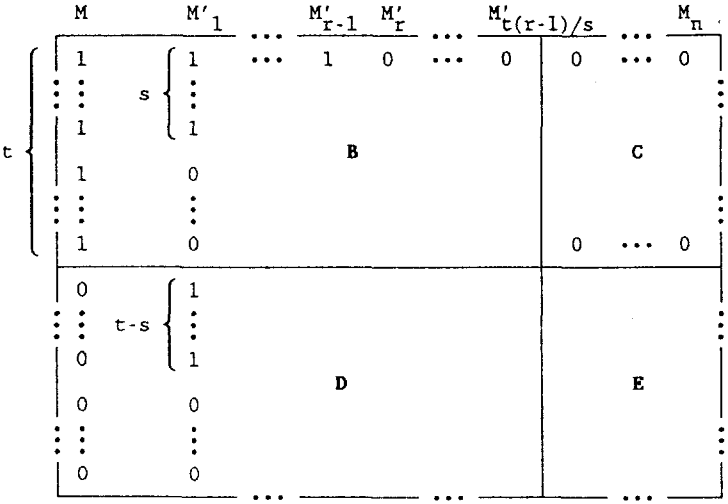

Figure 1.

The subarray C is completely filled with 0's since all of the tr 1's in the first t rows of A are accounted for in subarray B. The transmitter, knowing the structure of A and the legitimate message M cannot do better than choose one of the t(r-1)/s M' messages with a uniform probability distribution, since each occurs paired s times with M. His probability of success using this strategy would be

$$P_{Tx} = \frac{r-1}{\frac{t(r-1)}{s}} = \frac{s}{t}$$

as already noted. He would not, of course, choose any of the n-t(r-1)/s messages that do not occur paired with M since there is no chance that such a message would either be accepted by the receiver nor certified by the arbiter. In the small example we had the array A (in canonical form):

$$\begin{array}{ccc|c}
M & M_1' & M_2' & \\
\hline
1 & 1 & & \\
1 & & 1 & \\
\hline
 & 1 & & 1 \\
 & & 1 & 1 \\
\hline
\end{array}$$

where t = 2, s = 1 and r = 2. From (6) we know that n is a square, therefore the next smallest array must have r = 3 and n = 9. One such array is the following

$$\begin{array}{c|ccccccc|cc|}
 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
\hline
1 & 1 & 1 & 1 & & & & & & \\
2 & 1 & & & 1 & 1 & & & & \\
3 & 1 & & & & & 1 & 1 & & \\
\hline
4 & & 1 & & 1 & & & & & 1 \\
5 & & 1 & & & & 1 & & 1 & \\
6 & & & 1 & & 1 & & & 1 & \\
7 & & & 1 & & & & 1 & & 1 \\
8 & & & & 1 & & & 1 & 1 & \\
9 & & & & & 1 & 1 & & & 1 \\
\hline
\end{array}$$

Figure 2.

where t = 3, s = 1 and r = 3.

The reader will have probably already recognized that the two incidence arrays exhibited for r = 2 and 3 and s = 1 are examples of what Bruck [12,13] has defined to be a finite net. A finite net (i-net), **N**, is a set of n = r^2 elements (points) and ir r-subsets of points (lines) which can be grouped into i parallel classes of r lines each, such that distinct lines of the same parallel class have no points in common, while any two lines from different classes have exactly one point in common. Finite nets are closely related to finite affine planes. Under very general conditions, a finite net can be extended (but not always) to be embedded in an affine plane, however, every subset of i spreads of parallel lines from an affine plane is necessarily an i-net. It is this result that we will use to construct general authentication with arbitration codes. The parallel classes in the case $r = 3$ shown above are the sets of lines (row headings); (1,8,9)(2,5,7)(3,4,6), or in a more familiar form the sets of triples of messages (column headings)

$$\begin{array}{ll} (123)(478)(569) & \pi_1 \\ (145)(268)(379) & \pi_2 \\ (167)(249)(358) & \pi_3 \end{array}$$

The general means of constructing perfect authentication codes that permit arbitration is now obvious. We will restrict $s = 1$ which, although not necessary, makes the constructions easier. Start with any finite affine plane with $n = r^2$ points (whose existence is assured for all $r = p^\alpha$, p a prime) and form an i-net by choosing i parallel spreads of lines. Identify lines of the i-net with authenticating rules to form the factor array A. For example, there are three non-isomorphic A arrays possible when $r = 2$, corresponding to choosing one, two or all three of the parallel spreads from

$$\begin{array}{ll} (12)(34) & \pi_1 \\ (13)(24) & \pi_2 \\ (14)(23) & \pi_3 \end{array}$$

i.e., A in this case is one of the three forms

$$\left(\begin{array}{cc|cc} 1 & 1 & & \\ \hline & & 1 & 1 \end{array}\right) , \quad \left(\begin{array}{ccc|c} 1 & 1 & & \\ 1 & & 1 & \\ \hline & 1 & & 1 \\ & & 1 & 1 \end{array}\right) \quad \text{or} \quad \left(\begin{array}{cccc} 1 & 1 & & \\ 1 & & 1 & \\ 1 & & & 1 \\ \hline & 1 & 1 & \\ & 1 & & 1 \\ & & 1 & 1 \end{array}\right) .$$

All of these arrays are in the standard form of Figure 1. Clearly, by arguments given earlier

$$P_{Opp} = P_{Rx} = \frac{1}{r} . \tag{10}$$

However P_{Tx} is dependent on i. For $i = 1$, given any acceptable message the transmitter is certain of the other message the receiver will accept, i.e., once he is informed which message he is to use in the encoding rule constructed by the arbiter he knows the other acceptable message, since there is only one authenticating rule containing any given message. Similarly, he knows that one of two possible messages must be the other acceptable message when $i = 2$, however they occur uniquely in two equally likely authenticating rules, so that his probability of guessing which one the receiver will accept is only 1/2. In the general case for A an i-net, the transmitter's probability of success will be

$$P_{Tx} = \frac{(r-1)}{i(r-1)} = \frac{1}{i} \tag{11}$$

Since we wish to force

$$P_{Opp} = P_{Rx} = P_{Tx} \tag{12}$$

and by (10)

$$P_{Opp} = P_{Rx} = \frac{1}{r} \ ,$$

$i = r$. An affine plane contains $r + 1$ parallel spreads, i.e., $i \leq r + 1$, so that we can construct the desired factor A by deleting an arbitrary spread from an affine plane.

Conclusion

To summarize, we have described a construction for an infinite family of authentication codes that permit arbitration in which

$$P_{Opp} = P_{Rx} = P_{Tx} = \frac{1}{r} \tag{13}$$

whose existence is assured for r a prime power. These codes are of the form

$$\mathbf{A} = A^k$$

where k is the number of distinct pieces of information that may need to be authenticated and A is an $r^2 \times r^2$ array whose rows are identified with the lines in an r-net derived from the affine plane EG(2,r) by deleting an arbitrary parallel spread of lines.

The procedure for authentication is that the receiver will choose an authenticating rule, **a**, (row of **A**) with a uniform probability distribution and communicate this choice (in secret from the opponent and the transmitter) to the arbiter who will choose (also with a uniform probability distribution) one out of the r messages in each block of the authenticating rule to form the encoding rule, **e**, which he communicates (in secret from the opponent and the receiver) to the transmitter. The authentication protocol is that the receiver will accept as authentic only messages appearing in **a**, the transmitter is supposed to use only messages appearing in **e**, but in any event, the arbiter will certify only those messages appearing in e. All such codes satisfy (13) as was desired:

$$P_{Opp} = P_{Rx} = P_{Tx} = \frac{1}{r} = \frac{1}{p^\alpha} \tag{14}$$

p a prime, $\alpha \geq 1$. To communicate $\log_2 k$ bits of information and provide security against all five forms of deception of $\frac{1}{p^\alpha}$ requires that

$$\log_2 k + 2\log_2 r$$

bits of information be communicated through the channel, i.e., just enough information to identify which one of the kr^2 equally likely messages the transmitter is using.

References

1. E. F. Brickell, "A Few Results in Message Authentication," Proceedings of the 15th Southeastern Conference on Combinatorics, Graph Theory and Computing, Baton Rouge, LA, March 5-8, 1984, Congressus Numerantium, Vol. 43, Dec. 1984, pp. 141-154.

2. G. J. Simmons, "A Game Theory Model of Digital Message Authentication," Proceedings of the 11th Annual Conference on Numerical Mathematics and Computing, Univ. of Manitoba, Winnipeg, Canada, Oct. 1-3, 1981, Congressus Numerantium, Vol. 34, June 1982, pp. 413-424.

3. G. J. Simmons, "Message Authentication: A Game on Hypergraphs," Proceedings of the 15th Southeastern Conference on Combinatorics, Graph Theory and Computing, Baton Rouge, LA, Mar. 5-8, 1984, Congressus Numerantium, Vol. 45, December 1984, pp. 161-192.

4. G. J. Simmons, "Authentication Theory/Coding Theory," Proceedings of Crypto'84, Santa Barbara, CA, August 19-22, 1984, in Advances in Cryptology, Ed. by R. Blakley, Springer-Verlag, Berlin (1984), pp. 411-431.

5. D. R. Stinson, "Some Constructions and Bounds for Authentication Codes," presented at Crypto'86, Santa Barbara, CA, Aug. 12-15, 1986, to appear in Journal of Cryptology, 1988.

6. D. R. Stinson, "A Construction for AuthenticationSecrecy Codes from Certain Combinatorial Designs," presented at Crypto'87, Santa Barbara, CA, Aug. 16-20, 1987, to appear in Journal of Cryptology, 1988.

7. E. N. Gilbert, F. J. MacWilliams, N.J.A. Sloane, "Codes which Detect Deception," The Bell System Tech. Journal, Vol. 53, No. 3, March 1974, pp. 405-424.

8. J. L. Massey, "Cryptography -- A Selective Survey," presented at Int'l. Tirrenia Workshop on Digital Communications, Tirrenia, Italy, Sept. 2-6, 1985. Alta Frequenza, Vol. LV #1, Jan.-Feb., 1986, pp. 4-11.

9. P. Schoebi, "Perfect Authentication Systems for Data Sources with Arbitrary Statistics," presented at Eurocrypt'86, Linköping, Sweden, May 20-22, 1986.

10. G. J. Simmons, "Authentication Codes that Permit Arbitration," to appear Proceedings of the 18th Southeastern Conference on Combinatorics, Graph Theory and Computing, Boca Raton, FL, Feb. 23-27, 1987.

11. D. Raghavarao, Constructions and Combinatorial Problems in Design of Experiments, John Wiley & Sons, New York, NY (1971).

12. R. H. Brock, "Finite Nets I: Numerical Invariants," Canadian Journal of Math., Vol. 3 (1951), pp. 94-107.

13. R. H. Brock, "Finite Nets II: Uniqueness and Embedding," Pacific Journal of Math., Vol. 13 (1963), pp. 421-457.