J. Cryptology (1991) 3: 173–186

Journal of Cryptology

New Bounds and Constructions for Authentication/Secrecy Codes with Splitting[1]

Marijke De Soete
MBLE-I.S.G., Tweestationsstraat 82,
1070 Brussels, Belgium

Abstract. We investigate authentication codes with splitting, using the mathematical model introduced by Simmons. Besides an overview of the existing bounds, we obtain some new bounds for the probability of deception of the transmitter/receiver in case of an impersonation or substitution game. We also prove some new bounds for a "spoofing attack of order L." Further, we give several new constructions for authentication/secrecy codes with splitting, derived from finite incidence structures such as partial geometries and affine resolvable designs. In some of these codes the bounds are attained with equality.

Key words. Authentication codes, Splitting, Partial geometry, Combinatorial design.

1. Introduction

We deal with codes which are unconditionally secure. This means that we assume that any opponent has unlimited computational resources. We use the mathematical authentication model as introduced by Simmons [18], [19]. In this model there are three participants: a *transmitter*, a *receiver*, and an *opponent*. The transmitter wants to communicate certain information to the receiver, whereas the opponent wants to deceive the receiver, by causing him to accept a fraudulent message as original (*impersonation*) or modify a message which has been sent by the transmitter (*substitution*) that results in the receiver being misinformed with respect to what the transmitter intended to communicate to him.

More formally, we have a set of k source states S, a set of v messages M, and a set of b encoding rules E. A source state $s \in S$ is the information that the transmitter wishes to communicate to the receiver. The transmitter and receiver will have secretly chosen an encoding rule $e \in E$ beforehand. The "key" is the identification of the encoding rule they choose. An encoding rule e will be used to determine the message $e(s)$ to be sent to communicate any source state s. It is possible that more than one message can be used to communicate a particular source state; this is called *splitting*. Defining $|e(s)| = |\{m \in M: e(s) = m\}|$, splitting means $|e(s)| > 1$. However,

[1] Date received: December 1, 1988. Date revised: October 12, 1990.

in order for the receiver to be able to determine uniquely the source state from the message sent, there can be at most one source state which is encoded by any given message $m \in M$ (i.e., $e(s) \neq e(s')$ if $s \neq s'$). We denote by $AC(k, v, b)$ an authentication system with k source states, v messages, and b encoding rules.

In this paper we investigate codes with splitting. We use the following notations. Given an encoding rule e, we define $M(e) = \{e(s)\colon s \in S\}$, i.e., the set of messages permitted by encoding rule e, and let $|M(e)| = \kappa(e)$. For a set M' of distinct messages and an encoding rule e, define $f_e(M') = \{s\colon e(s) \in M'\}$, i.e., the set of source states which will be encoded under encoding rule e by a message in M'. Also, for a set M' of distinct messages, define $E(M') = \{e \in E\colon M' \subseteq M(e)\}$, i.e., the set of encoding rules under which all the messages in M' are permitted.

In [18], [19], and [23] the following scenario for authentication is investigated. After the observation of i messages $M' \subset M$, the opponent sends a fraudulent message m' to the receiver, hoping to have it accepted as authentic. Since he wants to mislead the receiver as to the state of the source, m' has to correspond to a different source state than those which are determined by a message in M'. This is called a *spoofing attack of order* i, with the special cases $i = 0$ and $i = 1$ corresponding respectively to the impersonation and substitution game. These two games have been studied extensively by several authors [3], [19], [20], [22], [23].

We are interested in the security of these codes with respect to both secrecy and authentication. Suppose an opponent observes i distinct messages being sent over the communication channel (where $i \geq 0$). He knows that the same key (encoding rule) is being used to transmit the i messages, but he does not know what that key is. If we consider the code as a secrecy system, then we make the assumption that the opponent can only observe the messages being sent. Our goal is that the opponent be unable to determine any information regarding the i source states from the i messages he has observed.

For any i, there will be a probability on the set of i source states which occur. We ignore the order in which the i source states occur, and assume that no source state occurs more than once. Also, we assume that any set of i source states has a nonzero probability of occurring. Given a set of i source states S', we define $p(S')$ to be the probability that the source states in S occur.

Given the probability distribution on the source states as described above, the receiver and transmitter will also choose a probability distribution for E, called an *encoding strategy*. Even though the choice of the encoding strategy depends on the probability distribution of the source states, after this choice is made, the two probabilities are independent in the sense that

$$p(s, e) = p(s) \cdot p(e).$$

If splitting is possible, then they must also determine a *splitting strategy* to determine $m \in M$, given $s \in S$ and $e \in E$ (this corresponds to nondeterministic encoding). Note that the receiver does not need to know the splitting strategy in order to interpret messages correctly. However, the encoding strategy is (in general) functionally dependent on the splitting strategy, so it is reasonable to say that the transmitter/receiver jointly determine the encoding and splitting strategies. The transmitter/receiver will determine these strategies to minimize the chance that an opponent can deceive them.

Once the transmitter/receiver have chosen encoding and splitting strategies, we can define for each $i \geq 0$ a probability denoted by P_{d_i}, which is the probability that the opponent can deceive the transmitter/receiver with a spoofing attack of order i.

Many of the bounds for P_{d_i} depend on the entropies of the variables used. For a probability distribution on a set X, we define the entropy of X, $H(X)$, as follows:

$$H(X) = -\sum_{x \in X} p(x) \cdot \log p(x).$$

The conditional entropy $H(X \mid Y)$ is defined by

$$H(X \mid Y) = -\sum_{y \in Y} \sum_{x \in X} p(y) \cdot p(x \mid y) \cdot \log p(x \mid y).$$

The concept of authentication codes with splitting was first introduced by Simmons [17] and studied later by Brickell [3] and Stinson [22]. It is the aim of this paper to perform some further investigations on these codes and to give some new constructions.

2. Secrecy

Considering the secrecy of a code, we desire that no information be conveyed by the observation of the messages. A code has *perfect L-fold secrecy* if, for every set M_1 of at most L messages observed in the channel, and for every set S_1 of at most $|M_1|$ source states, we have $p(S_1 \mid M_1) = p(S_1)$. This means that observing a set of at most L messages in the channel does not help the opponent to determine the L source states. At the opposite extreme, a code is said to be *Cartesian* [3], [22] if any message uniquely determines the source state, irrespective of the encoding rule.

3. Bounds on P_{d_i}

Several authors have been investigating bounds for authentication codes [3], [7], [9], [13], [18], [19], [22], [23]. In this section we give an overview of the existing bounds (both combinatorial bounds and bounds based on entropies) (see [3], [18] and [19]). Besides, we show that some of the known bounds for codes without splitting are still valid when splitting occurs [22]. Furthermore, new combinatorial bounds are given for P_{d_i}, $i > 0$, and for b, the number of encoding rules.

3.1. *Bounds on the Values of the Impersonation Game*

Theorem 3.1 [18], [19]. *In an authentication system with splitting,*

$$P_{d_0} \geq \min_{e \in E} \frac{\kappa(e)}{v}.$$

Proof. Suppose the opponent sends a message m. We denote the probability that the message m is accepted by the receiver by payoff(m). Then we have

$$\text{payoff}(m) = \sum_{e \in E(m)} p(e).$$

It follows that

$$\begin{aligned}\sum_{m\in M}\text{payoff}(m) &= \sum_{m\in M}\sum_{e\in E(m)} p(e)\\ &= \sum_{e\in E}\sum_{m\in M(e)} p(e)\\ &\geq \min_{e\in E}|M(e)|\sum_{e\in E} p(e)\\ &= \min_{e\in E}|M(e)| = \min_{e\in E}\kappa(e).\end{aligned}$$

Hence there must be some m such that

$$\text{payoff}(m) \geq \min_{e\in E}\frac{\kappa(e)}{v}. \qquad \square$$

Remark. It is clear from the above proof that

$$P_{d_0} = \min_{e\in E}\frac{\kappa(e)}{v}$$

if and only if $\kappa(e)$ is a constant, say κ', for all $e \in E$, which is equivalent to

$$\sum_{e\in E(m)} p(e) = \frac{\kappa'}{v} \qquad \text{for all} \quad m\in M.$$

Theorem 3.2 [18]. *In any authentication system,*

$$P_{d_0} \geq 2^{H(MES)-H(E)-H(M)} = 2^{H(M|ES)+H(S)-H(M)}.$$

An authentication system achieving equality in the preceding bound is called *perfect*. Brickell determined some properties for perfect authentication codes. The following holds:

Lemma 3.3 [3]. *In a perfect authentication code with splitting, the following properties are valid:*

- *For all messages m,*

$$\text{payoff}(m) = \sum_{e\in E(m)} p(e) = \frac{\kappa'}{v}.$$

- *For any message m, $p(s)\cdot p(m|e, s)$ is a constant for all s such that there is an e such that $e(s) = m$.*

3.2. *Bounds on the Values of the Substitution Game*

Next we deal with bounds on P_{d_1}. The following bound is valid for substitution with secrecy.

Theorem 3.4 [3], [18], [19].

$$P_{d_1} \geq 2^{-H(E|M)} = 2^{H(M)-H(E)-H(S)+H(M|ES)}.$$

Brickell has also given the conditions under which equality is attained for the substitution game.

Lemma 3.5 [3]. *If equality is attained, then the following properties are satisfied*:

- *For all* e, *and for all* m *such that* $m \in M(e)$,
$$p(m) \cdot P_{d_1} = p(e) \cdot p(S = f_e(m)) \cdot p(m|e, S = f_e(m))$$
holds.
- *For any* $m, m' \in M$, $m \neq m'$, *there is at most one encoding rule* e *such that* $m, m' \in M(e)$ *and* $f_e(m) \neq f_e(m')$.

Stinson [22] mentioned a generalization of this bound for codes which includes cases where the second condition does not hold. He gave a proof for codes without splitting. We prove that the same bound is valid for systems with splitting. First we introduce the following notations.

Given an encoding rule e' and given any $m, m' \in M(e')$ with $f_{e'}(m) \neq f_{e'}(m')$ define

$$\delta(e', m, m') = \frac{\sum_{\substack{e \in E(m,m') \\ f_e(m) \neq f_e(m')}} p(e) \cdot p(S = f_e(m)) \cdot p(m|e, S = f_e(m))}{p(e') \cdot p(S = f_{e'}(m)) \cdot p(m|e', S = f_{e'}(m))},$$

with $E(m, m') = \{e \in E: m, m' \in M(e)\}$. Let

$$\delta = \min\{\delta(e', m, m'): m, m' \in M(e'), m \neq m', f_{e'}(m) \neq f_{e'}(m')\}.$$

Note that $\delta \geq 1$ in general and that $\delta = 1$ if and only if the second condition in the foregoing lemma is satisfied.

Theorem 3.6. *In an authentication system with splitting,*

$$P_{d_1} \geq \delta \cdot 2^{-H(E|M)},$$

where δ *is defined as above.*

Proof. The proof is essentially the same as in [3]. Suppose the opponent substitutes message m with message m', $m \neq m'$. We denote the probability that the message m' is accepted by payoff(m, m'). We obtain

$$\text{payoff}(m, m') = \frac{\sum_{\substack{e \in E(m,m') \\ f_e(m) \neq f_e(m')}} p(e) \cdot p(S = f_e(m)) \cdot p(m|e, S = f_e(m))}{\sum_{e \in E(m)} p(e) \cdot p(S = f_e(m)) \cdot p(m|e, S = f_e(m))}$$

$$= \frac{\sum_{\substack{e \in E(m,m') \\ f_e(m) \neq f_e(m')}} p(e) \cdot p(S = f_e(m) \cdot p(m|e, S = f_e(m))}{p(m)}.$$

We define $P_{d_1}(m) = \max\{\text{payoff}(m, m'): m \neq m'\}$. Then

$$P_{d_1} = \sum_{m \in M} p(m) \cdot P_{d_1}(m)$$

holds. For any m, m', and e' such that $m \neq m'$ and $m, m' \in M(e')$, $f_{e'}(m) \neq f_{e'}(m')$, we have

$$\begin{aligned} P_{d_1}(m) &\geq \text{payoff}(m, m') \\ &= \delta(e', m, m') \cdot \frac{p(e') \cdot p(S = f_{e'}(m)) \cdot p(m \mid e', S = f_{e'}(m))}{p(m)} \\ &\geq \frac{\delta \cdot p(e') \cdot p(S = f_{e'}(m)) \cdot p(m \mid e', S = f_{e'}(m))}{p(m)}, \end{aligned}$$

and hence

$$\frac{p(e') \cdot p(S = f_{e'}(m)) \cdot p(m \mid e', S = f_{e'}(m))}{p(m)} \leq \frac{P_{d_1}(m)}{\delta}.$$

It follows, for $H(E \mid M)$, that

$$\begin{aligned} H(E \mid M) &= -\sum_{m \in M} \sum_{e \in E} p(m) \cdot p(e \mid m) \cdot \log p(e \mid m) \\ &= -\sum_{m \in M} \sum_{e \in E(m)} p(e) \cdot p(m \mid e) \cdot \log p(e \mid m) \\ &= -\sum_{m \in M} \sum_{e \in E} p(e) \cdot p(S = f_e(m)) \cdot p(m \mid e, S = f_e(m)) \\ &\quad \cdot \log \frac{p(e) \cdot p(S = f_e(m)) \cdot p(m \mid e, S = f_e(m))}{p(m)} \\ &\geq -\sum_{m \in M} \sum_{e \in E(m)} p(e) \cdot p(S = f_e(m)) \cdot p(m \mid e, S = f_e(m)) \cdot \log \frac{P_{d_1}(m)}{\delta} \\ &= -\sum_{m \in M} \log \frac{P_{d_1}(m)}{\delta} \cdot \sum_{e \in E(m)} p(e) \cdot p(S = f_e(m)) \cdot p(m \mid e, S = f_e(m)) \\ &= -\sum_{m \in M} \log \frac{P_{d_1}(m)}{\delta} \cdot p(m) \\ &\geq -\log \sum_{m \in M} \frac{P_{d_1}(m) \cdot p(m)}{\delta} \end{aligned}$$

since log is convex and $\sum_{m \in M} p(m) = 1$. Hence

$$H(E \mid M) \geq -\log \frac{P_{d_1}}{\delta}. \qquad \square$$

Remark. Recently another bound for codes with splitting based on entropies was found by Jimbo and Fuji-Hara (see [12]).

We can prove another bound for codes with splitting analogous to a known bound for codes without splitting (see [22]). Since the proof is similar to the one in the nonsplitting case we have omitted it here.

Theorem 3.7. *In an authentication system with splitting,*

$$P_{d_1} \geq \frac{\delta}{r}$$

with $r = \max_{m \in M} |E(m)|$.

Now we prove a new combinatorial bound on the value of the substitution game in an authentication code with splitting.

Theorem 3.8. *In an authentication code with splitting,*

$$P_{d_1} \geq \min_{e \in E} \frac{\kappa(e) - \max_{s \in S} |e(s)|}{v - \min_{s \in S} |e(s)|}.$$

Proof. Suppose the opponent substitutes message m with message m' $(m \neq m')$. We denote the probability that the message m' will be accepted as authentic by the receiver by payoff(m, m'). As before, we have

$$\text{payoff}(m, m') = \frac{\sum_{\substack{e \in E(m,m') \\ f_e(m) \neq f_e(m')}} p(e) \cdot p(S = f_e(m)) \cdot p(m | e, S = f_e(m))}{\sum_{e \in E(m)} p(e) \cdot p(S = f_e(m)) \cdot p(m | e, S = f_e(m))}.$$

It follows that

$$\sum_{\substack{m \neq m' \\ \exists e \in E: f_e(m) \neq f_e(m')}} \text{payoff}(m, m') \geq \min_{e \in E(m)} (\kappa(e) - \max_{s \in S} |e(s)|).$$

Hence there must be some m_0, $m_0 \neq m$ and, for at least one encoding rule e, $f_e(m_0) \neq f_e(m)$, such that

$$\max_{e \in E(m)} \left(v - \min_{s \in S} |e(s)| \right) \cdot \text{payoff}(m, m_0) \geq \min_{e \in E(m)} \left(|\kappa(e) - \max_{s \in S} |e(s)| \right)$$

holds. It follows that

$$\text{payoff}(m, m_0) \geq \min_{e \in E(m)} \frac{\kappa(e) - \max_{s \in S} |e(s)|}{v - \min_{s \in S} |e(s)|}.$$

For every m, determine such an m_0. This defines a substitution strategy in which the transmitter can be deceived with probability at least

$$\min_{e \in E} \frac{\kappa(e) - \max_{s \in S} |e(s)|}{v - \min_{s \in S} |e(s)|}.$$

When equality holds (which means P_{d_1} is a constant),

$$\frac{\kappa(e) - \max_{s \in S} |e(s)|}{v - \min_{s \in S} |e(s)|}$$

must be a constant. □

3.3. *Bounds for a "Spoofing Attack of Order L"*

The preceding result can be generalized for a spoofing attack of order L.

Theorem 3.9. *In an authentication code with splitting,*

$$P_{d_i} \geq \min_{e \in E} \frac{\kappa(e) - i \cdot \max_{s \in S} |e(s)|}{v - i \cdot \min_{s \in S} |e(s)|}.$$

As a generalization of the L-fold security for codes without splitting (see [23]), an authentication system with splitting is said to be *L-fold secure against spoofing* if

$$P_{d_i} = \min_{e \in E} \frac{\kappa(e) - i \cdot \max_{s \in S} |e(s)|}{v - i \cdot \min_{s \in S} |e(s)|} \qquad \text{for all } i, \quad 0 \leq i \leq L.$$

Next we prove a lower bound for the number of encoding rules for codes with splitting.

Theorem 3.10. *An authentication system with splitting which has perfect L-fold secrecy and* $(L - 1)$*-fold security against spoofing satisfies*

$$b \geq \frac{v \cdot \left(v - \max_{s \in S} |e(s)|\right) \cdots \left(v - (L-1) \cdot \max_{s \in S} |e(s)|\right)}{L!}.$$

Proof. Let M_1 be a set of $i \leq L - 1$ messages which are permitted under a particular encoding rule, in such a way that they define i different source states. Let x be a message which is not contained in M_1. Suppose there is no encoding rule e under which all messages in $M_1 \cup \{x\}$ are valid and for which $f_e(x) \notin f_e(M')$. However, in view of the preceding theorem this contradicts the $(L - 1)$-fold security of the code. Hence, it follows that every L-subset of messages is valid under at least one encoding rule such that they define different source states.

Now, pick any L-subset of messages of M, say M_2. In order to achieve perfect L-fold secrecy, the messages in M_2 must encode every possible L-subset of source states. Hence, M_2 is a valid set of messages under at least $\binom{k}{L}$ encoding rules. Now, if we count L-subsets of messages in such a way that they correspond to different source states, we obtain

$$b \cdot \binom{k}{L} \geq \frac{v \cdot \left(v - \max_{s \in S} |e(s)|\right) \cdots \left(v - (L-1) \cdot \max_{s \in S} |e(s)|\right)}{L!} \cdot \binom{k}{L}.$$

It follows that

$$b \geq \frac{v \cdot \left(v - \max_{s \in S} |e(s)|\right) \cdots \left(v - (L-1) \cdot \max_{s \in S} |e(s)|\right)}{L!}. \qquad \square$$

Analogously as for codes without splitting [23] we define an *optimal L-code* as a code which achieves perfect L-fold secrecy, is $(L-1)$-fold secure against spoofing, and the preceding lower bound for b is reached.

4. Constructions for Codes with Arbitrary Source Distribution

In this section we construct authentication codes which meet one or more bounds of the previous sections with equality.

4.1. *Codes Derived From Partial Geometries*

A (finite) *partial geometry* (PG) is an incidence structure $G = (P, B, I)$ in which P and B are sets of objects called points and lines, respectively, with a symmetric incidence relation I satisfying the following axioms:

1. Each point is incident with $t + 1$ lines $(t \geq 1)$ and two distinct points are incident with at most one line.
2. Each line is incident with $s + 1$ points $(s \geq 1)$ and two distinct lines are incident with at most one point.
3. If x is a point and L is a line not incident with x, then there are exactly α $(\alpha \geq 1)$ points $x_1, x_2, \ldots, x_\alpha$ and α lines $L_1, L_2, \ldots, L_\alpha$ such that $x\ I\ L_i\ I\ x_i\ I\ L$, $i = 1, 2, \ldots, \alpha$.

The numbers s, t, α are called the parameters of the partial geometry. These incidence structures were introduced by Bose in 1963 [2]. For $\alpha = 1$ they are generalized quadrangles (see [14]); "proper" partial geometries satisfy $1 < \alpha < \min(s, t)$. Therefore $|P| = (s + 1)(st + \alpha)/\alpha$ and $|B| = (t + 1)(st + \alpha)/\alpha$ hold, hence so do $\alpha | st(s + 1)$ and $\alpha | st(t + 1)$.

Further information on partial geometries can be found in [2] and [5].

We denote collinear points x and y by $x \sim y$. For $x \in P$, but $x^\perp = \{y \in P: y \sim x\}$. Note that $x \in x^\perp$. A *spread* R of a PG is a set of lines such that each point is incident with exactly one line of R. It is easy to verify that $|R| = (st + \alpha)/\alpha$.

Using partial geometries we obtain the following constructions for authentication codes with splitting.

Construction 1. Let G be a partial geometry of order (s, t), s, $t > 1$. Take an arbitrary point x. Let the source states be defined by the $t + 1$ lines which are incident with x, the messages are the points of $x^\perp \backslash \{x\}$ and the encoding rules are the points of $P \backslash x^\perp$. We define an encoding rule in the following way. Given a point $y \notin x^\perp$, we define for a source state K, $x\ I\ K$, the message $e_y(K) = \{z_1, \ldots, z_\alpha\}$, with $z_1, \ldots, z_\alpha$ the α points on K such that $y \sim z_i\ I\ L$, $1 \leq i \leq \alpha$.

Theorem 4.1. *If there exists a PG with parameters s, $t > 1$, $\alpha < s + 1$, then there exists a Cartesian authentication code $AC(t + 1, (t + 1)s, st(s + 1 - \alpha)/\alpha)$ which is 0-fold secure against spoofing.*

Proof. It is easy to verify that $k = t + 1$, $v = (t + 1)s$, and $b = (s + 1)(st + \alpha)/\alpha - (t + 1)s - 1 = st(s + 1 - \alpha)/\alpha$. We use the uniform encoding and splitting strategy.

To verify P_{d_0}, we choose an arbitrary message m. Then there exist, in view of the third axiom in Section 4.1, $t(s + 1 - \alpha)$ encoding rules containing m. Hence, payoff(m), the probability that the message m is accepted by the receiver, is given by

$$\text{payoff}(m) = \sum_{e \in E(m)} p(e) = \frac{t(s + 1 - \alpha)}{(st/\alpha)(s + 1 - \alpha)} = \frac{\alpha}{s} = \frac{\kappa'}{v},$$

with $\kappa' = \min_{e \in E} \kappa(e) = (t + 1)\alpha$. Note that we obtain the same value for the impersonation game for any source distribution. □

Remarks. (i) Using the same set of source states we can define an $AC(t + 1, (t + 1)s, st(s + 1 - \alpha)(t + 1)/\alpha)$ with $P_{d_0} = \alpha/s$, which is 0-fold secure against spoofing and which has perfect 1-fold secrecy. From each encoding rule of the preceding theorem we define $t + 1$ new encoding rules in the following way. Let $M(e_y) = M_y = \{z_{1,1}, \ldots, z_{1,\alpha}, \ldots, z_{i,j}, \ldots, z_{t+1,1}, \ldots, z_{t+1,\alpha}\}$, then we define, for each $0 \leq i \leq t$,

$$e(M_y, i) = (e_{k,j}, 1 \leq k \leq t + 1),$$

where $e_{k,j} = z_{k+i,j}$ with $k + i$ taken mod$(t + 1)$. This illustrates the influence of the secrecy of the code on the number of encoding rules b.

(ii) For $\alpha = 1$, G is a generalized quadrangle and we obtain an authentication code without splitting, which was already described in [7] and [22]. Moreover, if x is a regular point (see [14]) it was proven that the code satisfies $P_{d_0} = P_{d_1} = 1/s$ with $k = t + 1$, $v = (t + 1)s$, and $b = s^2$ (see Theorem 6.1 and the Remarks in [7]). Hence, for quadrangles of order s (this means $s = t$) with a regular point, we obtain the same codes as the one defined by Gilbert *et al.* in [9].

(iii) We refer to [4] and [5] for a description of the "known" PG which can be used to construct the preceding schemes.

Construction 2. Consider again a PG with parameters $s, t > 1$, α which contains a spread $R = \{L_1, \ldots, L_{(st+\alpha)/\alpha}\}$. Define the source states as the lines of R ($k = (st + \alpha)/\alpha$) and the messages as the points of G ($v = (s + 1)(st + \alpha)/\alpha$). Denote the points as $x_{1,1}, x_{1,2}, \ldots, x_{i,j}, \ldots, x_{(st+\alpha)/\alpha,s+1}$, with $x_{i,j}\ I\ L_i$, $1 \leq j \leq s + 1$, $1 \leq i \leq (st + \alpha)/\alpha$. Then we define an encoding rule in the following way. We associate with each point $x_{i,j}$ an encoding rule

$$e_{x_{i,j}}(L_k) = \{x_{2i+k,l'_1}, \ldots, x_{2i+k,l'_\alpha}\}$$

with $x_{2i+k,l'_1}, \ldots, x_{2i+k,l'_\alpha}$ the α points on the line L_{2i+k} which are collinear with $x_{i,j}$, if $x_{i,j}\ I\ L_{2i+k}$ or

$$e_{x_{i,j}}(L_k) = x_{i,j}$$

if $x_{i,j}\ I\ L_{2i+k}$. Note that in each case $2i + k$ is taken mod$(st + \alpha)/\alpha$.

In this way we obtain $b = (s + 1)(st + \alpha)/\alpha$ encoding rules.

Theorem 4.2. *If there exists a PG with parameters $s, t > 1, \alpha > 1$ containing a spread R, then there exists an optimal 1-code with splitting for $(st + \alpha)/\alpha$ source states and $(st + \alpha)(s + 1)/\alpha$ messages.*

Proof. We use the uniform encoding and splitting strategy. Let us first verify that $P_{d_0} = \min_{e \in E} \kappa(e)/v$.

Consider a message m. Then m occurs in $st + 1$ encoding rules (since there are st points collinear with m, not on the line of the spread through m). Hence payoff(m) is given by

$$\text{payoff}(m) = \sum_{e \in E(m)} p(e) = \frac{st + 1}{((st + \alpha)/\alpha)(s + 1)}.$$

On the other hand,

$$\min_{e \in E} \frac{\kappa(e)}{v} = \frac{(st/\alpha)\cdot\alpha + 1}{(s + 1)((st + \alpha)/\alpha)}.$$

Hence the code is 0-fold secure against spoofing.

The code has perfect 1-fold secrecy since each message occurs exactly α times in st/α columns and once in exactly one column of the $b \times k$ matrix (hence each column contains $s + 1$ entries with one message and $(s + 1)st/\alpha$ entries with α messages).

Since the number of encoding rules satisfies the lower bound given in Theorem 3.10, we indeed obtain an optimal 1-code. □

Remarks. In the case $\alpha = 1$, and hence the PG is a generalized quadrangle, a similar technique can be used to define an optimal code without splitting (see [7]).

Example. We give a short description of the PG $T_2^*(K)$ which can be used for this construction [6]. For other PGs containing a spread we refer to [5].

A *maximal arc* K [10] of degree d in a finite projective plane of order q (not necessarily desarguesian) is a (maximal) set of $qd - q + d$ points of the plane such that any line of the plane intersects K in 0 or d points. If K is a proper subset of the plane, we can easily prove that d has to divide q. Let K be a maximal arc of degree d in the projective plane $PG(2, q)$ over $GF(q)$ ($q = p^h$, p a prime). We define an incidence structure $G = (P, B, I)$ as follows. Let $PG(2, q)$ be embedded as a plane H in $PG(3, q)$. The points of G are the points of $PG(3, q)\backslash H$; the lines of G are the lines of $PG(3, q)$ which are not contained in H and meet K (necessarily in a unique point). The incidence is that of $PG(3, q)$. Then G is a partial geometry with parameters $t = qd - q + d - 1$, $s = q - 1$, $\alpha = d - 1$ and is denoted by $T_2^*(K)$. The PG $T_2^*(K)$ using an arc of degree 2^m in $PG(2, 2^h)$ has parameters $s = 2^{h-1}$, $t = (2^h + 1)(2^m - 1)$, $\alpha = 2^m - 1$. This is a GQ iff $m = 1$; i.e., K is a complete oval.

The set of lines which meet in a same point of K clearly define a spread of the PG.

Remark. In the previous codes it is precisely in the nonsplitting case (for $\alpha = 1$) that the smallest probability for the impersonation is reached. In the next example constructed from designs the splitting has no influence on the value for the impersonation probability.

4.2. *Codes Derived from Designs*

Consider an *affine resolvable* BIB design. This is a 2-(v, k, λ) design $D = (P, B, I)$ (see [1], [11], and [16]) which has a partition $\mathscr{B} = B_1 \cup B_2 \cup \cdots \cup B_r$ of the block set B

such that any point occurs exactly once in the blocks of each set B_i, $1 \leq i \leq r$ (i.e., each B_i is a parallel class of D), and any two blocks of distinct classes intersect exactly in μ, $\mu \geq 0$, points. It holds that $|B| = r \cdot n$, $|P| = k \cdot n$, $n \geq 2$, and $\lambda = r \cdot (k-1)/(n \cdot k - 1)$, $k = \mu \cdot n$.

We define the set of source states S to be one of the partition classes, say B_1, of D. Hence $|S| = n$. The messages are the points of D, so $|M| = k \cdot n$. For each block $L \notin B_1$, we define for $N_i \in B_1$, $1 \leq i \leq n$,

$$X_L(N_i) = \{x_{i,1}, \ldots, x_{i,\mu}\},$$

with $x_{i,1}, \ldots, x_{i,\mu}$ the common points of N_i and L.

From each set $X_L = \{X_L(N_i) \colon 1 \leq i \leq n\}$ we define n encoding rules in the following way:

$$e(X_L, j) = (x_{k,1}, \ldots, x_{k,\mu} \colon 1 \leq k \leq n), \qquad 0 \leq j \leq n-1,$$

with $x_{k,1} = x_{i+j(\text{mod})n,1}, \ldots, x_{k,\mu} = x_{i+j(\text{mod})n,\mu}$. In this way we defined $(r \cdot n - n) \cdot n = (r-1) \cdot n^2$ encoding rules.

Theorem 4.3. *An affine resolvable BIB design defines an* $AC(n, k \cdot n, (r-1) \cdot n^2)$ *which has perfect* 1*-fold secrecy and* 0*-fold security against spoofing.*

Proof. We use the uniform encoding and splitting strategy. Consider a message m. Then m occurs in exactly one block of each of the classes $B_2, B_3, \ldots, B_r$ and hence in $(r-1) \cdot n$ encoding rules. We obtain, for payoff(m),

$$\text{payoff}(m) = \frac{(r-1) \cdot n}{(r-1) \cdot n^2} = \frac{1}{n},$$

while on the other hand we have

$$\min_{e \in E} \frac{\kappa(e)}{v} = \frac{n \cdot \mu}{k \cdot n} = \frac{1}{n}.$$

Hence the code has 0-fold security against spoofing. It is obvious from the definition of the encoding rules that this code has perfect 1-fold secrecy. □

Remarks. (i) Considering two distinct messages m, m', we can also calculate payoff(m, m'). We may assume that m, m' belong to λ common blocks, none of which is contained in B_1 (since otherwise m, m' would define the same source state). For each such block, say L, and for each source state j, there is exactly one encoding rule $e(X_L, i)$ where $m, m' \in M(e(X_L, i))$ and $f_{e(X_L,i)}(m) = j$. This results in

$$\text{payoff}(m, m') = \frac{\lambda}{(r-1)} = \frac{r \cdot (k-1)}{(n \cdot k - 1)(r-1)} = \frac{r \cdot (k-1)}{v \cdot (r-1)}$$

while

$$\min_{e \in E} \frac{\kappa(e) - \max_{s \in S} |e(s)|}{v - \min_{s \in S} |e(s)|} = \frac{\mu \cdot n - \mu}{v - \mu} = \frac{\mu \cdot n - \mu}{\mu \cdot n^2 - \mu} = \frac{1}{n+1}.$$

It follows that the preceding code never has 1-fold security against spoofing. Indeed, for 1-fold security $r \cdot k + n \cdot k - r \cdot n - 1 = 0$ must hold. Since for affine resolvable BIB designs $b = v + r - 1$ (see [16]), this results in $r(k - 2) + 1 = 0$, which is clearly never satisfied.

(ii) Note that Gilbert, MacWilliams, and Sloane were the first to use designs, more specifically BIBD, to construct authentication codes. More recently Simmons also used affine designs to construct equitable authentication codes [21].

Acknowledgments

We would like to thank D. Stinson for the interesting suggestions and valuable discussions on the subject. We are also indebted to the Philips Research Laboratory, Brussels, for the facilities they offered during the preparation of this paper.

References

[1] T. Beth, D. Jungnickel, H. Lenz, *Design Theory*, Wissenschaftsverlag Bibliografisches Institut, Mannheim, 1985.

[2] R. C. Bose, Strongly regular graphs, partial geometries and partial balanced designs, *Pacific J. Math.* **13** (1963), 389–419.

[3] E. F. Brickell, A few results in message authentication, *Congr. Numer.* **43** (1984), 141–154.

[4] A. E. Brouwer, J. H. van Lint, Strongly regular graphs and partial geometries, in *Enumeration and Design*, eds. D. Jackson and S. Vanstone, Academic Press, New York, 1984, pp. 85–122.

[5] F. De Clerck, Strongly regular graphs and partial geometries, Preprint 37, Dipartimento di matematica e applicazioni, Università degli studi di Napoli, 1985.

[6] F. De Clerck, M. De Soete, H. Gevaert, A characterization of the partial geometry $T_2^*(K)$, *European J. Combin.* **8** (1987), 121–127.

[7] M. De Soete, Some constructions for authentication/secrecy codes, *Advances in Cryptology—Proceedings of Eurocrypt '88*, Lecture Notes in Computer Science, vol. 330, Springer-Verlag, Berlin, 1988, pp. 57–75.

[8] M. De Soete, Bounds and constructions for authentication/secrecy codes with splitting, *Advances in Cryptology—Proceedings of Crypto '88*, Lecture Notes in Computer Science, vol. 403, Springer-Verlag, Berlin, 1990, pp. 311–317.

[9] E. N. Gilbert, F. J. MacWilliams, N. J. A. Sloane, Codes which detect deception, *Bell System Tech. J.*, **53**(3) (1974), 405–424.

[10] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Clarendon Press, Oxford, 1979.

[11] D. R. Hughes, F. C. Piper, *Design Theory*, Cambridge University Press, Cambridge, 1985.

[12] M. Jimbo, R. Fuji-Hara, Optimal authentication systems and combinatorial designs, *IEEE Trans. Inform. Theory*, **36** (1990), 54–62.

[13] J. L. Massey, Cryptography—a selective survey, *Digital Communications* (Proceedings of the 1985 International Tirrenia Workshop on Digital Communications, Tirrenia, Italy, 1985), eds. E. Biglieri and G. Prati, Elsevier, Amsterdam, 1986, pp. 3–25.

[14] S. E. Payne, J. A. Thas, *Finite Generalized Quadrangles*, Research Notes in Mathematics, vol. 110, Pitman, Boston, 1984.

[15] C. E. Shannon, Communication theory of secrecy systems, *Bell System Tech. J.* **28** (1949), 656–715.

[16] S. S. Shrikhande, Affine resolvable balanced incomplete block designs: a survey, *Aequationes Math.* **14** (1976), 251–269.

[17] G. J. Simmons, A game theory model of digital message authentication, *Congr. Numer.* **34** (1982), 413–424.

[18] G. J. Simmons, Message authentication: a game on hypergraphs, *Congr. Numer.* **45** (1984), 161–192.

[19] G. J. Simmons, Authentication theory/coding theory, *Advances in Cryptology—Proceedings of Crypto '84*, Lecture Notes in Computer Science, vol. 196, Springer-Verlag, Berlin, 1985, pp. 411–432.

[20] G. J. Simmons, A natural taxonomy for digital information authentication schemes, *Advances in Cryptology—Proceedings of Crypto '87*, Lecture Notes in Computer Science, vol. 293, Springer-Verlag, Berlin, 1988, pp. 269–288.

[21] G. J. Simmons, A Cartesian product construction for unconditionally secure authentication codes, *J. Cryptology* **2** (1990), pp. 77–104.

[22] D. R. Stinson, Some constructions and bounds for authentication codes, *J. Cryptology* **1** (1988), 37–51.

[23] D. R. Stinson, A construction for authentication/secrecy codes from certain combinatorial designs, *J. Cryptology* **1** (1988), 119–127.

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