Some Constructions and Bounds for Authentication Codes

D. R. Stinson
Department of Computer Science
University of Manitoba

1. Introduction

We shall use the model of authentication theory as described by Simmons in [S1], [S2], and [S3]. In this model, there are three participants: a transmitter, a receiver, and an opponent. The *transmitter* wants to communicate some information to the *receiver*, whereas the *opponent* wants to deceive the receiver. The opponent can either impersonate the receiver, making him accept a fradulent message as authentic; or, modify a message which has been sent by the transmitter.

More formally, we have a set of source states **S**, a set of messages **M**, and a set of encoding rules **E**. A *source state* $s \in \mathbf{S}$ is the information that the transmitter wishes to communicate to the receiver. The transmitter and reciever will have secretly chosen an *encoding rule* $e \in \mathbf{E}$ beforehand. 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 message can be used to determine a particular source state (this is called *splitting*). However, in order for the receiver to be able to uniquely determine the source state from the message sent, there can be at most one source state which is encoded by any given message $m \in \mathbf{M}$.

We assume that the opponent will play either *impersonation* or *substitution*. When the opponent plays impersonation, he sends a message to the receiver, attempting to have the receiver accept the message as authentic. When the opponent plays substitution, he waits until a message m has been sent, and then replaces m with another message m' so that the receiver is misled as to the state of the source.

There will be a probability distribution on the set of source states **S**. Given the probability distribution on **S**, the reciever and transmitter will determine a probability distribution on **E**, called an *encoding strategy*. If splitting occurs, then they will also determine a *splitting strategy* to determine $m \in \mathbf{M}$, given $s \in \mathbf{S}$ and $e \in \mathbf{E}$. The transmitter / receiver will choose the encoding and splitting strategies to minimize the chance that the opponent can deceive them.

This defines two possible games, which we refer to as the impersonation game and the substitution game . Each game has a *value*, which is the possibility that the opponent can decieve the transmitter / receiver, given that they are using the optimal encoding and splitting strategies. We denote the values of these games by v_I (for impersonation) and v_S (for substitution).

Many of the bounds on the values of the games v_I and v_S depend on entropies of the various probability distributions. For a probability distribution on a set **X**, we define the *entropy* of **X**, H(**X**), as follows:

A.M. Odlyzko (Ed.): Advances in Cryptology - CRYPTO '86, LNCS 263, pp. 418-425, 1987.

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

As well, the conditional entropy $H(\mathbf{X} \mid \mathbf{Y})$ is defined to be

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

An authentication code is said to be *Cartesian* if any message uniquely determines the source state, independent of the particular encoding rule being used. In terms of entropy, this is expressed by the equation $H(\mathbf{S} \mid \mathbf{M}) = 0$. Note that in a Cartesian authentication code, there can be no secrecy.

In this paper, we primarily consider authentication systems without splitting. We shall use the following notation. Denote the number of source states by k, and let $\mathbf{S} = \{s_i: \ 1 \le i \le k\}$. Denote the number of messages by v, and let $\mathbf{M} = \{m_j: \ 1 \le j \le v\}$. Denote by b the number of encoding rules, and write any encoding rule $e \in \mathbf{E}$ as $e = (e_i: \ 1 \le i \le k)$, where e_i is the message used to communicate source state s_i, for $1 \le i \le k$. Then, the authentication system can be represented by the b x k matrix A, where row e of A consists of the entries $e_1, \ldots, e_k$. Given an encoding rule $e \in \mathbf{E}$, we define $M(e) = \{e_i: \ 1 \le i \le k\}$, where $e = (e_i: \ 1 \le i \le k)$. Also, for any encoding rule e, define $f_e(m) = s$ if and only if $e_s = m$ (if message m does not occur in encoding rule e, then $f_e(m)$ is undefined).

2. Bounds on the values of the impersonation and substitution games

Theorem (Simmons [S2, Theorem 1]) In an authentication system without splitting, $v_I \ge k / v$.

Theorem (Simmons [S2, Theorem 0]) In any authentication system, $v_I \ge 2^{H(\mathbf{MES}) - H(\mathbf{E}) - H(\mathbf{M})} = 2^{H(\mathbf{M} \mid \mathbf{ES}) + H(\mathbf{S}) - H(\mathbf{M})}$. In an authentication system without splitting, $H(\mathbf{M} \mid \mathbf{ES}) = 0$, so $v_I \ge 2^{H(\mathbf{S}) - H(\mathbf{M})}$.

Theorem (Simmons, Brickell [B1, Theorem 3]) $v_S \ge 2^{-H(\mathbf{E} \mid \mathbf{M})} = 2^{H(\mathbf{M}) - H(\mathbf{E}) - H(\mathbf{S}) + H(\mathbf{M} \mid \mathbf{ES})}$. In an authentication system without splitting, $H(\mathbf{M} \mid \mathbf{ES}) = 0$, so $v_S \ge 2^{H(\mathbf{M}) - H(\mathbf{E}) - H(\mathbf{S})}$.

Given any encoding rule e', and given any $m, m' \in M(e')$, define

$$\delta(e', m, m') = \sum_{\{e \in \mathbf{E}: \ m, m' \in M(e)\}} p(e) \cdot p(S = f_e(m)) \ / \ (p(e') \cdot p(S = f_e(m))).$$

Then, let $\delta = \min\{\delta(e', m, m'): \ m, m' \in M(e'), m \ne m'\}$.

Theorem In an authentication system without splitting, $v_S \ge \delta \cdot 2^{-H(\mathbf{E} \mid \mathbf{M})}$.

Given any message m, define $r_m = |\{e \in \mathbf{E}: m \in M(e)\}|$.

Theorem In an authentication system without splitting, $v_S \geq \delta / r$, where $r = \max\{r_m: m \in \mathbf{M}\}$.

Given any encoding rule e', and given any $m, m' \in M(e')$, define

$$\gamma(e', m, m') = \sum_{\{e \in E:\ m, m' \in M(e)\}} p(e) \cdot p(S = f_e(m)) / p(e').$$

Then, let $\gamma = \min\{\gamma(e', m, m'): m, m' \in M(e'), m \neq m'\}$.

Theorem In an authentication system without splitting, $v_S \geq \gamma \cdot 2^{H(M) - H(E)}$.

Theorem In an authentication system without splitting, $v_S \geq (k - 1) / (v - 1)$.

3. Constructions for authentication systems

Our interest is in constructing authentication systems which meet one or more of these bounds with equality. We are interested in the existence of authentication codes with a specified number of source states, and specified upper bounds on the number of encoding rules, messages, v_I, and v_S. Therefore, we define an AC(k, v, b, α, β) to be an authentication code without splitting, having k source states, at most v messages, at most b encoding rules, and where $v_I \leq \alpha$ and $v_S \leq \beta$. Then, we define

$$\varepsilon(k, \alpha, \beta) = \min\{b: \text{ there exists an AC}(k, v, b, \alpha, \beta)\},$$

and

$$\upsilon(k, \alpha, \beta) = \min\{v: \text{ there exists an AC}(k, v, b, \alpha, \beta)\}$$

That is, we are attempting to minimize the number of encoding rules (or messages) required in an authentication code for k source states, with upper bounds α and β on the impersonation and substitution games, respectively.

First, observe that we have an easy lower bound on $\upsilon(k, \alpha, \beta)$.

Theorem $\upsilon(k, \alpha, \beta) \geq \max\{k / \alpha, 1 + (k - 1) / \beta\}$.

Next, we mention a lower bound on $\varepsilon(k, \alpha, \beta)$ due to Brickell ([B1, Theorem 4]).

Theorem $\varepsilon(k, \alpha, \beta) \geq 1 / (\alpha \cdot \beta)$.

This bound can be strengthened, using the quantity δ defined earlier.

Theorem If an AC(k, v, b, α, β) exists, then $b \geq \delta / (\alpha \cdot \beta)$.

Proof: We have $\alpha \geq v_I \geq 2^{H(S) - H(M)}$ and $v_S \geq \delta \cdot 2^{-H(E|M)} = \delta \cdot 2^{H(M) - H(E) - H(S)}$. Hence, we have $\alpha \cdot \beta \geq \delta \cdot 2^{-H(E)}$. Since $H(\mathbf{E}) \leq \log b$, the result follows.

In the remainder of this paper, we shall be describing constructions for authentication codes, which will enable us to put upper bounds on ε and υ. For our first construction, we require the following definition. A *transversal design* TD(k, λ; n) is a triple (X, **G**, **A**), which satisfies the following properties:

1) X is a set of $k \cdot n$ elements called *points*
2) **G** is a partition of X into k subsets of n points, called *groups*
3) **A** is a set of $\lambda \cdot n^2$ subsets of X (called *blocks*) such that a group and a block contain at most one common point
4) every pair of points from distinct groups occurs in exactly λ blocks.

We usually denote a TD(k, 1; n) by TD(k, n). It is well-known that a TD(k, n) is equivalent to k - 2 mutually orthogonal Latin squares of order n.

Theorem (Brickell [B1, Theorems 5 and 6]) If there is a transversal design TD(k, n) then there is a Cartesian authentication system with $v_S = 2^{-H(E|M)} = 1 / n$, $v_I = 2^{H(S) - H(M)} = 1 / n$, $|\mathcal{S}| = k$, $|\mathcal{M}| = k \cdot n$, and $|\mathcal{E}| = n^2$, with no splitting. Conversely, the existence of such an authentication system implies the existence of a transversal design TD(k, n). Hence, if there exists a TD(k, n), then there is an AC(k, $k \cdot n$, n^2, 1 / n, 1 / n}, and we have the upper bounds $\varepsilon(k, 1 / n, 1 / n) \leq n^2$ and $\upsilon(k, 1 / n, 1 / n) \leq k \cdot n$.

We can prove a generalization of this result, using transversal designs with $\lambda \geq 1$.

Construction 1 If there is a transversal design TD(k, λ; n) then there is a Cartesian authentication system with $v_S = \lambda \cdot 2^{-H(E|M)} = 1 / n$, $v_I = 2^{H(S) - H(M)} = 1 / n$, $|\mathcal{S}| = k$, $|\mathcal{M}| = k \cdot n$, and $|\mathcal{E}| = \lambda \cdot n^2$, with no splitting. Conversely, the existence of such an authentication system implies the existence of a transversal design TD(k, λ; n). Hence, if there exists a TD(k, λ; n), then there is an AC(k, $k \cdot n$, $\lambda \cdot n^2$, 1 / n, 1 / n}, $\varepsilon(k, 1 / n, 1 / n) \leq \lambda \cdot n^2$, and $\upsilon(k, 1 / n, 1 / n) \leq k \cdot n$.

Suppose our desire is to construct an authentication code AC(k, k·n, b, 1 / n, 1 / n). We can construct such a code if a TD(k, λ; n) exists for $b = \lambda \cdot n^2$. (Note that this satisfies the bound $b \geq \delta / (\alpha \cdot \beta)$ with equality, where $\alpha = \beta = 1 / n$ and $\delta = \lambda$.) Thus, given k and n, we are interested in the smallest λ such that a TD(k, λ; n) exists. First, we observe that there is a simple numerical bound on k in terms of λ and n.

Theorem (Hanani [H1]). If a TD(k, λ; n) exists, then $k \leq (\lambda \cdot n^2 - 1) / (n - 1)$.

Consequently, if we use a TD(k, λ; n), then we have a lower bound on b, namely

$$b = \lambda \cdot n^2 \geq kn - k + 1.$$

We present an infinite example of transversal designs which meet this bound with equality.

Theorem For all prime powers $n \geq 2$, and for any $d \geq 1$, there is an AC(k, k·n, n^d, 1 / n, 1 / n), where $k = (n^d - 1) / (n - 1)$; hence $\varepsilon((n^d - 1) / (n - 1), 1 / n, 1 / n) \leq n^d$ and $v((n^d - 1) / (n - 1), 1 / n, 1 / n) \leq k \cdot n$.

Proof: In [H1], Hanani shows that for any prime power n, and for any $d \geq 1$, there is a TD($(n^d - 1) / (n - 1)$, n^{d-2}; n).

Corollary For any $\alpha > 0$, ε(k, α, α) is $O(k / \alpha^2)$ and v(k, α, α) is $O(k / \alpha)$.

Proof: Let $n = 2^j$, where $2^j \geq 1 / \alpha \geq 2^{j-1}$. Then n is $O(1 / \alpha)$. Now, choose d so that $n^d \geq k(n - 1) + 1 > n^{d-1}$. Since $k \leq (n^d - 1) / (n - 1)$, we have $\varepsilon(k, \alpha, \alpha) \leq n^d$. But, $n^d \leq k(n^2 - n) + n = O(k \cdot n^2)$. Since n is $O(1 / \alpha)$, therefore ε(k, α, α) is $O(k / \alpha^2)$. Also, k·n is $O(k / \alpha)$.

As another example of the use of transversal designs with $\lambda > 1$, let's consider codes with parameters AC(k, v, b, 1 / 6, 1 / 6). For k = 4, we cannot construct such a code from a TD(4, 6), since this TD does not exist (this is the famous 36 officers problem of Euler, i.e. a pair of orthogonal Latin squares of order 6). In [B1], Brickell constructs an example of an AC(4, 30, 36, 1 / 6, 1 / 6) with splitting. However, we can employ a TD(7, 2, 6), which is constructed in [H1, p. 49], to obtain an AC(7, 42, 72, 1 / 6, 1 / 6).

More generally, we have the following class of authentication codes with 7 source states.

Theorem For all $n \geq 2$, there is an AC(7, 7·n, $2n^2$, 1 / n, 1 / n); hence $\varepsilon(7, 1 / n, 1 / n) \leq 2n^2$.

Proof: For these n, there is a TD(7, 2; n) (see [H1]).

The authentication codes obtained from Construction 1 are Cartesian. Hence, the opponent, on seeing a message being sent, knows the source state. Therefore, no secrecy is possible in such an authentication system. We also want to be able to construct good authentication codes with secrecy. Ideally, we would like to have $H(\mathbf{S} \mid \mathbf{M}) = H(\mathbf{S})$; i.e. the message gives absolutely no clue as to the state of the source. If this happens, then we say that the authentication code is *perfectly* non-Cartesian.

Our main construction for perfectly non-Cartesian authentication codes uses group-divisible designs, which are a generalization of transversal designs. A *group-divisible design* GD(k, λ, n; v) is a triple (X, **G**, **A**), which satisfies the following four properties:

1) X is a set of v elements called *points*
2) **G** is a partition of X into v / n subsets of n points, called *groups*
3) **A** is a set of subsets of X (called *blocks*), each of size k, such that a group and a block contain at most one common point
4) every pair of points from distinct groups occurs in exactly λ blocks.

Note that a TD(k, λ; n) is equivalent to a GD(k, λ, n; k·n). Also, a (v, b, r, k, λ)-BIBD (balanced incomplete block design) is equivalent to a GD(k, λ, 1; v).

We have the following construction.

Construction 2 Suppose there exists a GD(k, λ, n; v). Then there is a perfectly non-Cartesian AC(k, v, λ·v·(v - n) / (k - 1), k / v, (k - 1) / (v - n)).

Proof: Let (X, **G**, **A**) be a GD(k, λ, n; v). By simple counting, each point occurs in r = λ·(v - n) / (k - 1) blocks, and the total number of blocks is λ·v·(v - n) / (k·(k - 1)). What we do is construct k encoding rules from every block of the group-divisible design: for each block A = $\{x_1, \ldots, x_k\}$ of the group-divisible design, and for each i, $0 \le i \le k - 1$, we define an encoding rule e(A, i) = $(e_j: 1 \le j \le k)$, where $e_j = x_{(j + i) \text{ modulo } k}$.

There are λ·v·(v - n) / (k - 1) encoding rules in the resulting authentication code. We shall use each encoding rule with probability (k - 1) / (λ·v·(v - n)). It is not difficult to verify that v_I = k / v and v_S = (k - 1) / (v - n).

Finally, the authentication code is perfectly non-Cartesian since p(s | m) = p(s) for every $s \in \mathbf{S}$ and every $m \in \mathbf{M}$.

It is interesting to note that this code has H(**M**) = log v, H(**E**) = log(λ·v·(v - n) / (k - 1)), and $v_S = \gamma \cdot 2^{H(\mathbf{M}) - H(\mathbf{E})}$, where γ = λ.

Corollary Suppose there exists a (v, b, r, k, λ)-BIBD. Then there is a perfectly non-Cartesian $AC(k, v, k \cdot b, k / v, (k - 1) / (v - 1))$.

Proof: This is the case where every group of the group-divisible design has size 1. Note that here we have $v_S = (k - 1) / (v - 1)$.

Corollary Suppose there is a $TD(k, \lambda; n)$. Then there is a perfectly non-Cartesian $AC(k, n \cdot k, \lambda \cdot k \cdot n^2, 1 / n, 1 / n)$.

Consequently, $\varepsilon(k, \alpha, \alpha)$ is $O(k^2 / \alpha^2)$ and $v(k, \alpha, \alpha)$ is $O(k^2 / \alpha)$, even if we restrict ourselves to perfectly non-Cartesian codes.

These two constructions for authentication codes both have two very nice properties which we have not yet emphasized. First, the encoding strategy in each case is *uniform*: each encoding rule is used with equal probability $1 / b$. Second, this encoding strategy yields the stated game values for *any* source distribution.

The final topic we consider is the construction of authentication codes for *uniform* source distributions ($p(s) = 1 / k$ for any source state s). As before we consider only codes without splitting. The best we could hope for is to attain the bounds $v_I = k / v$ and $v_S = (k - 1) / (v - 1)$. So, we shall study $AC(k, v, b, k / v, (k - 1) / (v - 1))$; such authentication codes will be called *optimal*.

We have the following characterization of authentication codes which are optimal with respect to the uniform probability distribution on the source states.

Lemma An authentication system is optimal with respect to the uniform probability distribution on the source states if and only if the following properties are satisfied:

i) for every $m \in \mathbf{M}$, $\sum_{\{e \in \mathbf{E}:\ e \in E\}} p(e) = k / v$.

ii) for every $m \neq m'$, $\sum_{\{e \in \mathbf{E}:\ m, m' \in e\}} p(e) = (k^2 - k) / (v^2 - v)$.

In many authentication codes, the optimal encoding strategy is to choose every encoding rule with probability $1 / b$. If we assume that this encoding strategy is in fact optimal, then the properties above are of a purely combinatorial nature. We have the following

Theorem An authentication system is optimal with respect to a uniform encoding strategy and a uniform probability distribution on the source states if and only the following properties are satisfied:

i) for every $m \in \mathbf{M}$, $|\{e \in \mathbf{E}: m \in e\}| = k \cdot b / v$.

ii) for every $m \neq m'$, $|\{e \in \mathbf{E}: m, m' \in e\}| = b \cdot (k^2 - k) / (v^2 - v)$.

This says that the rows of **E**, considered as unordered sets, form a balanced incomplete block design with parameters (v, b, r, k, λ), where $r = k \cdot b / v$ and $\lambda = b \cdot (k^2 - k) / (v^2 - v)$. So, we can produce optimal authentication codes from BIBDs when the source states are equiprobable.

Using known families of BIBDs, we can obtain many authentication codes for uniform source distributions. For example, using projective geometries, we have the following.

Theorem For any prime power n, and any integer $d \geq 2$, there is an optimal authentication code for the uniform source distribution on $n + 1$ source states, for $v = (n^{d+1} - 1) / (n - 1)$ and $\lambda = 1$.

References

B1. Ernest F. Brickell, A Few Results in Message Authentication, Congressus Numerantium 43 (1984), 141-154.

H1. H. Hanani, On Transversal Designs, Math. Centre Tracts 55 (1974), 42-52.

S1. Gustavus J. Simmons, A Game Theory Model of Digital Message Authentication, Congressus Numerantium 34 (1982), 413-424.

S2. Gustavus J. Simmons, Message Authentication: A Game on Hypergraphs, Congressus Numerantium 45 (1984), 161-192.

S3. Gustavus J. Simmons, Authentication Theory / Coding Theory, in "Advances in Cryptology: Proceedings of CRYPTO 84", Lecture Notes in Computer Science, vol. 196, 411-432, Springer Verlag, Berlin, 1985.