Optimal Authentication Systems

R. Safavi-Naini *
L. Tombak **

Department of Computer Science University of Wollongong
Northfields Ave., Wollongong 2522, AUSTRALIA

Abstract. In this paper we define an optimal authentication systems as a system whose minimum probability of deception is k/M, k and M being the number of source states and cryptograms respectively, and satisfies information theoretic bounds on the value of impersonation and substitution games. We will characterize order-1 perfect systems and δ-perfect systems and prove their optimality when E, the number of encoding rules, satisfies certain bounds. We will show that both types of systems, in this case, also have best game theoretic performance. This will be used to prove that optimal systems exist only if $E \geq M^2/k^2$ and for less value of E probability of deception is always greater than k/M. We will prove that doubly perfect codes are optimal systems with minimum value of E and perfect systems are not optimal. Characterization of doubly perfect systems follows from characterization theorems mentioned earlier. We give constructions for each class.

1 Introduction

In this paper we will study authentication systems (A-systems) with optimum performance and characterize two classes of such systems. In an A-system the enemy has the option of playing impersonation game (I-game), substitution game (S-game) or combined game (C-game). Values of these games are P_I, P_S and P_C. Defining optimality for an A-system is not straight forward. It is important to note that minimizing value of the games does not ensure efficient use of redundancy added during coding process. For any A-system P_C is at least equal to probability of success in randomly selecting a cryptogram from cryptogram space. We define optimality of an A-system by requiring the system to satisfy an information theoretic bound on the value of I-game, a same kind of bound on the value of S-game and having $P_C = k/M$ where k is the number of source states and M is the number of cryptograms. For impersonation game the only information theoretic bound is due to Simmons [8]. Massey [3] and Sgarro [2] gave shorter proofs of the bound and necessary and sufficient conditions for achieving the

* Support for this project was partly provided by Australian Research Council grant A49030136.

** Support for this project was provided by Australian Research Council grant A49030136.

T. Helleseth (Ed.): Advances in Cryptology - EUROCRYPT '93, LNCS 765, pp. 12-27, 1994.

bound with equality. For substitution game we have two such bound; Simmons-Brickell bound is derived in [1] and later extended by Stinson [11] where he gives necessary conditions on A-systems that satisfy the bound with equality. The second bound for substitution is by Pei [5] (we give a sketch of the proof of this bound in appendix 7.3). Pei gives necessary and sufficient conditions for systems satisfying the bound with equality. We transform Pei's conditions into equivalent ones which are similar to necessary and sufficient conditions of Simmons' bound when substitution game is played. Hence the bound can be considered as the counterpart of Simmons' bound for substitution. We define order-1 perfect systems as systems for which P_I satisfies Simmons' bound and P_S satisfies Pei's bound. Similarly δ-perfect A-systems are those for which P_I and P_S satisfy Simmons' bound and Stinson's bound respectively. We will prove that for $E \geq E_0 = M(M-1)/(k(k-1))$ order-1 perfect systems are optimal and for $M^2/k^2 \leq E \leq E_0$, δ-perfect systems are optimal. Moreover in each case the value of I-game, S-game and C-game is minimal, that is, optimal systems have best game theoretic performance too. We give a complete characterization of the two classes and list properties of them. Next we define δ-doubly perfect systems as A-systems that are δ-perfect and have minimum value of E for a given δ, that is, $E = \delta M^2/k^2$. For $\delta = 1$ we have doubly perfect system of Brickell which is in fact the optimal system with minimum possible E. This implies that for $E < M^2/k^2$ the value of the combined game is always greater than k/M. Application of our characterization theorems, mentioned earlier, gives a characterization of doubly perfect A-systems, not known before. We also examine properties of perfect A-systems, as defined by Simmons, and show that they are not optimal as the value of substitution game does not satisfy any information theoretic bound. Finally we give some construction for each class and present some concluding remarks.

2 Preliminaries

We consider an authentication system in which a transmitter wants to send the states of a source to a distant receiver over a public channel. An encoding rule is a mapping from the set S, $|S| = k$, of source states into the set $\mathcal{M}$, $|\mathcal{M}| = M$, of codewords (cryptogram). An authentication code (A-code) is a collection $\mathcal{E}$ of mappings (encoding rules), indexed by key information, such that each mapping specifies one (or a number of) cryptogram for every $s \in \mathcal{S}$. We assume the code is without splitting, that is, a source state and a key uniquely determines a cryptogram. We use $s(e,m)$ to denote the source state which is mapped into m by key e and $P_s(e,m)$ to denote its probability. We define the *incidence matrix* of an A-code to be a zero-one matrix A, the rows of which correspond to encoding rules and columns to cryptogram, and

$$a_{em} = \begin{matrix} 1 \text{ m is authentic under key } e_i \\ 0 \text{ otherwise.} \end{matrix}$$

Let $E(m)$ denotes the subset of keys that are incident with $m \in \mathcal{M}$ and $M(e)$ the subset of cryptograms incident with the key $e \in \mathcal{E}$. The communicants se-

cretly choose the encoding rule e. Enemy can use an *impersonation attack* in which he/she attempts to find an $m \in M(e)$ or a *substitution attack* in which he/she intercepts a cryptogram $m \in \mathcal{M}$ and wants to substitute it with another cryptogram $m' \in \mathcal{M}_m$ where $\mathcal{M}_m = \mathcal{M} \setminus m$. We also refer to these attacks as order zero and one attack respectively. Let $E(m, m') = \{e : e \in E(m) \bigcap E(m')\}$. Simmons showed that A-systems can be modeled using game theory [7, 9]. Enemy has the choice of playing *impersonation game* (I-game), *substitution game* (S-game) or *combined game* (C-game) whose game matrix is the concatenation of the game matrices of I-game and S-game [9]. Let P_I,P_S and P_C denote the value of the game in each case. Communicant's strategy is always a probability distribution $\pi = (\pi_1, \pi_2, ..., \pi_E)$ on the encoding rules but enemy's strategy depends on the kind of game that he/she plays. In general we have $P_C \geq max(P_I, P_S)$ but if the best strategy of the communicants' is the same for I-game and S-game (which implies the same best strategy for C-game) then $P_C = max(P_I, P_S)$ and enemy's best strategy reduces to his/her best impersonation or substitution strategy. Game matrix of I-game is the incidence matrix of the A-code. For S-game payoff of replacing m by m' is,

$$payoff(m, m') = \frac{\sum_{i=1}^{E} \pi_i a_{im} a_{im'} P_s(e_i, m)}{P(m)},$$

where $P_s(e_i, m)$ is the probability of $s(e_i, m)$ and,

$$V_S(m) = max_{m'}(payoff(m, m')).$$

An authentication system provides *perfect protection for impersonation* if enemy's best strategy is random selection from $\mathcal{M}$. Probability of success in this case is equal to k/M. An A-code provides *perfect protection for substitution* if for all $m \in \mathcal{M}$ enemy's best strategy, when m is intercepted, is random selection from $\mathcal{M}_m$. His/her probability of success is equal to $(k-1)/(M-1)$. Stinson gave the characterization of A-systems that provide perfect protection for impersonation and the ones that provide perfect protection for substitution (Theorems 2.1 and 2.4 in [13]). Perfect protection for impersonation depends only on the incidence matrix of the A-code and is independent of the source. However perfect protection for substitution depends on the incidence matrix of the code and the probability distribution of the source.

3 Bounds on Probability of Deception

3.1 Simmons-Pei bound

The first (and the only) information theoretic bound on P_I is due to Simmons [8].

Theorem 1. *For an A-code without splitting,*

$$P_I \geq 2^{-(H(E)-H(E|\mathcal{M}))}. \tag{1}$$

Equality holds if and only if,

1. *the A-code provides perfect protection for impersonation;*
2. *$P_s(e_i, m)$ is independent of e_i and $P_s(e_i, m) = P_s(m)$, that is, all the source states that map to a cryptogram m have the same probability.*

Hence to obtain equality in (1), one must use an A-code whose incidence matrix accords with theorem 2.1 of [13] with a source whose first order statistics *matches* (in the sense of condition 2) the A-code. Pei's bound for substitution is the counterpart of Simmons bound for impersonation attack. We give the sketch of the proof of this bound, first presented in Asiacrypt '91, in appendix 7.3.

Theorem 2 Pei, [5].

$$P_S \geq 2^{-(H(E|\mathcal{M})-H(E|\mathcal{M}^2))}, \tag{2}$$

and equality holds if and only if

$$\frac{P(e|m)}{P(e|m,m')}, \tag{3}$$

is independent of m,m',e, for all $m, m' \in M(e)$.

In proposition 5 we show that condition (3) can be transformed into two conditions similar to theorem 1. We need the following generalization of perfect protection for substitution. Let C_m denotes the set of the cryptograms m' that, when substituted for m, have non-zero probability of success, i.e., $C_m = \{m' \in \mathcal{M} : E(m, m') \neq \emptyset\}$ and $|C_m| = N_m$.

Definition 3. An A-code provides near-perfect protection for substitution if the enemy's best strategy, when a cryptogram m is received, is random selection from C_m.

Near-perfect protection is weaker than perfect protection as enemy's strategy is random selection from C_m for which $N_m = |C_m| \leq M - 1 = |\mathcal{M}_m|$. Although probability of success depends on the intercepted cryptogram it is easy to see that for an A-code with near-perfect protection for substitution, for all $m \in \mathcal{M}$, we have

$$V_S(m) = \frac{k-1}{N_m}.$$

Corollary 4. *An A-code provides perfect protection for substitution if and only if it provides near-perfect protection for substitution and $N_m = M - 1$.*

Near-perfect protection can be defined for higher order attacks but for impersonation it reduces to perfect protection if we assume that every cryptogram is authentic under at least one key. An A-code provides *uniform near-perfect protection* if it provides a near-perfect protection and N_m does not depend from the actual intercepted cryptogram,i.e, $N_m = N_1$

Proposition 5. *The necessary and sufficient conditions for equality in (2) are*

1. *the A-code provides uniform near-perfect protection for substitution;*
2. *$P_s(m'|e_i, m)$ is independent of e_i for all $m, m' \in \mathcal{M}$ with $E(m, m') \neq \emptyset$.*

Proof: See appendix 7.1.

Proposition 5 shows that an authentication system that satisfies bound (2) will provide near-perfect protection for substitution. Equality in (2) requires an A-code with uniform near-perfect protection for substitution together with a source whose second order statistics satisfy condition 2 of proposition 5.

Definition 6. An authentication system is called 0-perfect if it satisfies Simmons' bound and 1-perfect if it satisfies Pei's bound.

Corollary 7 is an immediate result of proposition 5 and theorem 1.

Corollary 7. *An authentication system is i-perfect ($i = 0, 1$) if and only if it provides uniform near-perfect protection for order i attack and source statistics of order $i + 1$ is 'matched' to the A-code.*

3.2 Simmons-Brickell-Stinson Bound

Simmons and Brickell derived the following bound on P_S:

Theorem 8 Simmons-Brickell, [1].

$$P_S \geq 2^{-H(E|M)}; \tag{4}$$

If equality holds then

1. $V_S(m) = \dfrac{\pi_i P_s(e_i, m)}{P(m)}$, *where $m \in \mathcal{M}$ and $e_i \in \mathcal{E}$ such that $e_i \in E(m)$;*
2. $P_S = V_S(m)$, $m \in \mathcal{M}$;
3. $|E(m, m')| \leq 1$, *and $m \in M$, $m' \in \mathcal{M}_m$.*

Stinson gave a more general form of this bound,

$$P_S \geq \delta 2^{-H(E;M)}, \tag{5}$$

where δ is equal to,

$$\delta = min_{m,m',e_i}(\delta(e_i, m, m')) = min_{m,m',e_i}(\frac{\sum \pi_i a_{im} a_{im'} P_s(e_i, m)}{\pi_i P_s(e_i, m)})$$

and proved the following.

Theorem 9 Stinson [11], Theorem 2.8. *In an A-system without splitting that satisfies bound (5) with equality we have:*

1. $|E(m)| = kE/M$,
2. $|E(m, m')| = 0$ *or* λ,
3. $\delta(e_i, m, m') = \delta = \lambda$ *for all* $e_i \in E(m, m')$,
4. $P_S = \delta M/(kE)$.

Simmons-Brickell bound is a special case of Stinson's bound when $\delta = 1$ and hence equality in Simmons-Brickell's bound implies $P_S = M/(kE)$.

4 Optimal A-Systems

As noted in previous section i-perfect A-systems satisfy the information theoretic bound and provide uniform near-perfect protection and so can be considered optimal when only one type (impersonation or substitution) of attack is considered. In this section we will consider both types of attacks. For an A-system $P_C \geq P_I \geq k/M$.

Definition 10. An A-system is optimal if it has $P_C = k/M$, satisfies Simmons' bound for P_I and an information theoretic bound (2) or (5) on P_S.

We define order-1 perfect A-systems and δ-perfect systems and show that they are optimal. We prove that they also achieve minimum value of the I-game, S-game and C-game. Our major results are complete characterization of both types of system (theorems 14, 18). Simmons' definition of perfect A-systems and Brickell's definition of doubly perfect systems are studied in this context. In particular we show that perfect A-systems are not optimal and doubly perfect systems are optimal with least possible E.

Let the communicants use their optimum strategy for combined game.

Definition 11. An authentication system is called order-1 perfect if P_I and P_S satisfy Simmons' bound and Pei's bound respectively and $|E(m, m')| \geq \lambda > 0$ for all $m, m' \in \mathcal{M}$.

Let $E_0 = \frac{M(M-1)}{k(k-1)}$.

Proposition 12. *For an order-1 perfect A-system we have,*

$$E \geq \lambda E_0.$$

Hence such systems can exist if $E \geq E_0$.

Proof: Follows from counting pairs of cryptograms and using the minimum value of $\lambda = 1$. □

Note that for order-1 perfect systems, in general, we do not have $P_I = P_S$. Enemy's best strategy for I-game and S-game are random strategies and the best C-game strategy is the same as the best I-game strategy. Proposition 13 shows that for order-1 perfect A-systems source must be uniform. It also specifies other properties of such systems.

Proposition 13. *If an A-system is order-1 perfect the followings hold,*

1. *best enemy's strategy in impersonation or substitution is random strategy and the overall best strategy is the same as the best impersonation strategy;*
2. $\sum_{j=1}^{E} \pi_j a_{jm} a_{jm'} = 1/E_0$;
3. *probability of a cryptogram m occurring in the channel is uniform ($P(m) = 1/M$));*

4. source is uniform;
5. $P_s(m'|m, e_j) = P_s(m'|m)$ *for all* $m, m' \in \mathcal{M}$ *and* $e_j \in E(m, m')$.

Proof: Let the A-system be order-1 perfect. Then property 1 follows from the definition of order-1 perfect systems and theorems 1 and 2. Enemy's overall optimal strategy is random selection from $\mathcal{M}$ (impersonation) as $P_I = k/M > (k-1)/(M-1) = P_S$ and P_I and P_S are achievable for the same communicants' strategy. Property 3 follows from Theorem 3.2 of [14] where it was proved that perfect protection for impersonation and substitution implies $P(m) = 1/M$. Also property 2 follows from the same theorem when the source is uniform. To prove property 4 we note that,

$$P(m) = \sum_{j=1}^{E} \pi_j a_{jm} P_s(e_j, m),$$

but equality in (1) implies $P_s(e_j, m) = P_s(m)$ and we have,

$$P(m) = P_s(m) \textstyle\sum_{j=1}^{E} \pi_j a_{jm} = P_s(m)(k/M), \tag{6}$$

where the last equality holds because A-system provides perfect protection for impersonation. Using $P(m) = 1/M$ with (6) we have $P_s(m) = 1/k$. Finally property (5) is true because the A-system satisfies Pei bound (2).
□

Communicants' optimal strategy can be obtained by solving a system of linear equations [6] which depends on the incidence matrix of the A-code and is independent of the source. Conditions (2) to (5) of the proposition 13 are sufficient for an A-system to be order-1 perfect. Theorem 14 characterizes such systems.

Theorem 14. *An order-1 perfect A-system satisfies conditions 1 to 5 of proposition 13. Moreover conditions 2 to 5, or equivalently, 1 (or 2), 4 and 5 are sufficient conditions.*

Proof: See appendix 7.2.

Proposition 13 and theorem 14 show that A-systems that are order-1 perfect are obtained from A-codes whose incidence matrices satisfy certain conditions together with a *'matched'* source.

Corollary 15. *An order-1 perfect A-system achieves minimum values for I-game, S-game and C-game and hence has the best game theoretic performance, that is,*

1. $P_C = k/M$;
2. $P_I = k/M$;
3. $P_S = (k-1)/(M-1)$.

Moreover we have

- *enemy's best combined strategy is the same as his/her best strategy for impersonation and is actually a random selection from $\mathcal{M}$;*
- *enemy's best substitution strategy is random selection from all the remaining cryptograms;*
- *communicants best strategy can be calculated by solving a set of linear equations whose coefficients are derived from the incidence matrix of the A-code.*

Using proposition 12 we conclude that order-1 perfect systems are optimal if $E \geq E_0$. An A-system that satisfies Simmons' bound for impersonation has $P_I = k/M$ and it is shown in [14] if $E < E_0$ then

$$P_S \geq \max[\frac{k-1}{M-1},\ \delta\frac{M}{kE}]. \tag{7}$$

δ-perfect A-systems, defined below, are optimal when $M^2/k^2 \leq E \leq E_0$.

Definition 16. An A-system is δ-perfect if it satisfies Simmons bound for P_I and
$P_S = \delta 2^{-H(E|M)}$.

Proposition 17. *A δ-perfect A-system satisfies the following,*

1. $|E(m)| = const = kE/M$;
2. $|E(m,m')| = \delta = \lambda$ *or* 0;
3. $P_s(e_j, m) = P_s(m)$;

Proof: Properties one and two follows from theorem 9 and property 3 follows from theorem 1. □

Theorem 18. *δ-perfect A-systems are optimal if $E_0 \geq E \geq M^2/k^2$. In this case communicants best strategy for combined game is uniform distribution on the key space. Moreover, this condition together with 1, 2 and 3 of proposition 17 are sufficient for an A-system to be δ-perfect.*

Proof: The system satisfies Simmons' bound and hence $P_I = k/M$. It satisfies Stinson's bound and so $P_S = \delta M/(kE)$. If $E \geq M^2/k^2$ we have $P_S \leq P_I$ and $P_C = P_I = k/M$ and the system is optimal. Communicants' best strategy for combined game will be uniform distribution on the key space.

To prove sufficiency, we note that if condition 1 of proposition 17 holds then communicants uniform strategy provides perfect protection for impersonation. Using the uniform strategy for substitution and taking into account conditions 1, 2 and 3 of proposition 17 we show that $payoff(m,m') = 0$ or $\delta M/(kE)$. This is true because,

$$payoff(m,m') = \frac{\sum_{j=1}^{E} \pi_j a_{jm} a_{jm'} P_s(e_j,m)}{\sum_{j=1}^{E} \pi_j a_{jm} P_s(e_j,m)} = \frac{\sum_j a_{jm} a_{jm'}}{\sum_j a_{jm}} = \frac{M \sum_j a_{jm} a_{jm'}}{kE}.$$

So $V_S(m) = \delta M/(kE)$ and $P_S = \delta M/(kE)$, which means that uniform strategy is the best communicants' substitution strategy. Using the same conditions it is

easy to see that $2^{-H(E|M)} = \delta M/(kE) = P_S$ and $2^{-(H(M)-H(M|E))} = k/M = P_I$, which proves the result.
□

Corollary 19. *A δ-perfect A-system achieves minimum possible value for P_S and satisfies*

1. $P_C = P_I = k/M$;
2. $P_S = \delta M/(kE)$.

Moreover enemy and communicants' best strategies are given by

- *enemy's best combined strategy is random selection from $\mathcal{M}$;*
- *enemy's best impersonation strategy is random selection from $\mathcal{M}$ and his/her best substitution strategy is random selection from keys that are incident with the received cryptogram and then randomly selecting a cryptogram which is authentic under the chosen key;*
- *communicants best strategy is uniform distribution on $\mathcal{E}$.*

Definition 20. An optimal δ-perfect A-system with minimum number of encoding rule is called δ-doubly perfect system.

Proposition 21. *For a δ-doubly perfect system $P_S = P_I = P_C$.*

Proof: We have $E = \delta M^2/k^2$ and $P_I = k/M = \delta M/(kE) = P_S$. □

4.1 Doubly Perfect A-systems

A *doubly perfect* A-system, as defined by Brickell [1], is a perfect A-system that satisfies

$$P_C = 2^{-H(E|M)}.$$

Doubly perfect A-systems are special case of δ-doubly perfect A-systems when $\delta = 1$. This is true because for perfect A-systems $P_C = P_I$ and hence we have $P_I = P_S = P_C$. Doubly perfect A-codes have all properties mentioned in corollary 19.

4.2 Perfect A-systems

Simmons defined a *perfect A-system* as an A-system that satisfies the following bound:

$$P_C = 2^{-I(M;E)}.$$

For an A-system using theorem 1, we have $P_I \geq 2^{-I(M;E)}$. So for a perfect A-system $2^{-I(M;E)} = P_C \geq P_I \geq 2^{-I(M;E)}$ and hence $P_I = 2^{-I(M;E)}$ and the A-system is 0-perfect. Moreover $P_I = P_C \geq P_S$. Hence enemy's best combined strategy is random selection from $\mathcal{M}$. However the enemy's best chance of success in substitution is not known. Communicants' optimal strategy for C-game can be obtained by solving a system of linear equations [6]. We note that for perfect A-systems we have $P_C = P_I = k/M$ and $P_S < P_I$.

Corollary 22. *Perfect A-systems are not optimal as P_S does not satisfy any bound.*

Corollary 23. *Optimal A-systems exist only if $E \geq M^2/k^2$.*

Proof: For optimal A-systems $P_C = P_I = k/M$. In this case P_S is lower bounded as in (7). If $E < M^2/k^2$ then $E < E_0$ and the best achievable value of P_S is $M/(kE)$ but in this case $M/(kE) > k/M$ and hence $P_C > k/M$. □

We summarize these results in the following corollary.

Corollary 24. *For a given E, M, k we have,*

1. *If $E < M^2/k^2$ then $P_C > k/M$.*
2. *If $E = M^2/k^2$ then doubly perfect A-systems are optimal and have $P_C = P_S = P_I = k/M = M/(kE)$.*
3. *If $M^2/k^2 < E < E_0$ then δ-perfect A-systems are optimal. We have $P_C = P_I = k/M > P_S = \lambda M/(kE)$.*
4. *If $E \geq E_0$ then order-1 perfect A-systems are optimal and we have $P_C = P_I > P_S = (k-1)/M - 1$.*

This corollary can be re-stated for A-systems for which $E(m, m') \geq \lambda$ when $E(m, m') \neq 0$.

Corollary 25. *For a given E, M, k λ we have,*

1. *If $E = \lambda M^2/k^2$ then δ-doubly perfect A-systems are optimal and $P_C = P_S = P_I = k/M = \lambda M/(kE)$.*
2. *If $\lambda M^2/k^2 < E < \lambda E_0$ then δ-perfect A-systems are optimal and have $P_C = P_I = k/M > P_S = \lambda M/(kE)$.*
3. *If $E \geq \lambda E_0$ then order-1 perfect A-systems are optimal.*

5 Construction of Optimal Codes

In this section we will give some constructions for optimal A-systems.

5.1 δ-doubly perfect A-systems and δ-perfect systems

Definition 26. $A(v, k, r, \lambda)$-PBIB is a pair (M, E),where $|M| = v$ is a set of elements called points and E is a set of blocks,where block is a k-element subset of M; such that each point occurs in exactly r-blocks, and each pair of points occurs in exactly λ blocks or does not occur at all.

Using proposition 17 we immediately get the following result.

Proposition 27. *If there exists a δ-perefct system for a uniform source then there exist a (v, k, r, λ)-PBIB. Conversely if there exist a (v, k, r, λ)-PBIB then there exist a δ-perefct A-system with k equiprobable source states, $v = M$ cryptograms and $E = rv/k$ keys.*

In order to construct a δ-doubly perfect system we need another construction called transversal design.

Definition 28. A transversal design $TD(k, \lambda, n)$ is a triple (X, G, A), which satisfies the following properties

1. X is a set of kn elements called points;
2. G is a partition of X into k subsets of n points, called groups;
3. A is a set of λn^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.

Using this combinatorial design we can construct a Cartesian δ-doubly perfect A-system.

Proposition 29 [11], theorem 3.5. *If there is a $TD(k, \lambda, n)$ then there is a δ-doubly perfect Cartesian A-system with $M = kn$ cryptograms, k-source states, $E = \lambda n^2$ keys for which $P_S = P_I = 1/n$. Conversely if there exist a δ-doubly perfect Cartesian A-system with no splitting then there exist a transversal design $TD(k, \delta, n = M/k)$.*

5.2 Order-1 perfect authentication codes

We can construct order-1 perfect authentication codes using a well known combinatorial construction called balance incomplete block design-BIBD.

Definition 30. A (v, k, r, λ)-BIBD is a collection of k-subsets, called blocks, of a v-set, called points, such that each such that each point occurs in exactly r-blocks, and each pair of points occurs in exactly λ blocks.

Proposition 31. *If there exists a (v, k, r, λ)-BIBD then there exists an order-1 perfect A-system with k-equiprobable source states, $v = M$ cryptograms and $E = vr/k$ keys.*

For a fixed parameters M, k, E, λ this order-1 perfect system has minimum possible number of keys.

6 Concluding Remarks

We have defined optimal performance of an A-system using information theory and game theory measures and have characterized them when E is within different ranges. In particular we have proved that these systems can only exist for $E \geq M^2/k^2$ and for less number of encoding rules the chance of enemy's success is always greater than k/M. We noted that perfect A-systems of Simmons are not optimal but doubly perfect systems of Brickell are optimal with least number of encoding rules. We have given some construction for each case. Further research is needed to construct larger classes of optimal systems.

7 Appendix

7.1 A

Proof of proposition 5: Necessity: We show that the above conditions could be derived from (3). To obtain first condition we have

$$\sum_{e_j \in E(m,m')} P(e_j|m,m') = 1$$

and

$$\frac{P(e_j|m)}{P(e_j|m,m')} = \frac{P(e_j|m)}{P(e_j|m,m')} \sum_{e_j \in E(m,m')} P(e_j|m,m') \tag{8}$$

$$= \frac{\sum_{e_j \in E(m,m')} P(e_j|m,m')P(e_j|m)}{P(e_j|m,m')}$$

$$= \sum_{e_j \in E(m,m')} P(e_j|m) = const \tag{9}$$

Hence $payoff(m,m')$, given in (9), is independent of m and m' and the A-code provides uniform near-perfect protection for substitution, i.e.,

$$\frac{P(e_j|m)}{P(e_j|m,m')} = \frac{k-1}{N_1}, \quad E(m,m') = 0,$$

$$= 0, \quad E(m,m') = \emptyset.$$

To get second condition we have

$$\frac{P(e_j|m)}{P(e_j|m,m')} = \frac{P(e_j,m)/P(m)}{P(e_j,m,m')/P(m,m')},$$

$$= \frac{\pi_j a_{jm} P_s(e_j,m)}{P(m)} \times \frac{P(m,m')}{\pi_j a_{jm} a_{jm'} P_s(e_j,m,m')},$$

$$= \frac{P(m,m')}{P(m)P_s(e_j,m'|m)} = const,$$

where $P_s(m'|m,e_j)$ is the conditional source probability $P_s(s(e_j,m')|s(e_j,m))$. That is, the source states that are mapped into a cryptogram m', when m is received, are equiprobable.

Sufficiency: We show that conditions 1 and 2 result in equality in (2). Using condition 1 we have

$$\frac{\sum_{j=1}^{E} \pi_j a_{jm} a_{jm'} P_s(e_j,m)}{P(m)} = const.$$

Multiplying numerator and denominator by $P_s(e_j, m'|m)$ and using condition 2 we have

$$\frac{\sum_{j=1}^{E} \pi_j a_{jm} a_{jm'} P_s(e_j, m) P_s(e_j, m'|m)}{P(m) P_s(e_j, m'|m)} =$$

$$\frac{\sum_{j=1}^{E} \pi_j a_{jm} a_{jm'} P_s(e_j, m, m')}{P(m) P_s(e_j, m'|m)} =$$

$$\frac{P(m, m')}{P(m) P_s(e_j, m'|m)} = \frac{P(m, m') P_s(e_j, m)}{P(m) P_s(e_j, m'|m) P_s(e_j, m)} =$$

$$\frac{\pi_j a_{jm} P_s(e_j, m)}{P(m)} \times \frac{P(m, m')}{\pi_j a_{jm} a_{jm'} P_s(e_j, m)} = \frac{P(e_j|m)}{P(e_j|m, m')}.$$

□

7.2 B

Proof of theorem 14:

Necessity has been already given in the proof of proposition 13.
Sufficiency: using conditions 2 and 4 we have,

$$\sum_{j=1}^{E} \pi_j a_{jm} P_s(e_j, m) = 1/M = 1/k \sum_{j=1}^{E} \pi_j a_{jm},$$

$$\sum \pi_j a_{jm} = k/M.$$

So the code provides perfect protection for impersonation and $P_I = k/M$. Moreover

$$2^{-I(E,M)} = 2^{H(S)-H(M)} = k/M,$$

and so $P_I = 2^{-I(E,M)}$ and the code is 0-perfect.

To show that the code is 1-perfect we note that,

$$\frac{P_s(e_j, m, m')}{P_s(e_j, m)} = P_s(m'|m, e_j) = P_s(m'|m),$$

where the last equality follows from condition 5. Using condition 4 we have

$$P_s(e, m, m') = P_s(m, m'),$$

which results in

$$\frac{P(e_j|m)}{P(e_j|m, m')} = \frac{P(e_j, m)/P(m)}{P(e_j, m, m')/P(m, m')}. \tag{10}$$

We make the following substitutions in (10),

$$\begin{aligned} P(e_j, m) &= (1/k)\pi_j a_{jm}, \\ P(m) &= 1/M, \\ P(e_j, m, m') &= \pi_j P_s(e_j, m, m') a_{jm} a_{jm'}, \\ P(m, m') &= \sum_{j=1}^{E} \pi_j a_{jm} a_{jm'} P_s(e_j, m, m'), \end{aligned}$$

which gives,

$$\frac{P(e_j|m)}{P(e_j|m, m')} = (k/M) \sum_j \pi_j a_{jm} a_{jm'} = (k-1)/(M-1),$$

and hence using theorem 2 the A-system is 1-perfect. □

7.3 C

Pei proved the following bound on probability of the enemy's success for spoofing attack of order r.

$$P_r \geq 2^{H(E|M^{r+1}) - H(E|M^r)}$$

The following is a proof for $r = 1$ which can be generalized for spoofing of order r. We need the following propositions.

Proposition 32. *Suppose that P and Q are probability vectors of the same dimension with non zero coordinates. So $p_i > 0$ and $q_i > 0$ $(1 < i < n)$, and*

$$\sum_{i=1}^{n} p_i = \sum_{i=1}^{n} q_i \doteq 1.$$

Then

$$\sum_{i=1}^{n} p_i \log(p_i/q_i) \geq 0$$

Moreover equality holds if and only if $p_i = q_i$

Proposition 33. *Suppose that $|E(m', m)| > 0$ then,*

$$\log(payoff(m, m')) \geq \sum_{e_j \in E(m', m)} p(e_j|m, m') \log \frac{p(e_j|m)}{p(e_j|m, m')}$$

Moreover equality holds if and only if

$$payoff(m, m') = p(e_j|m)/p(e_j|m, m')$$

for any $e_j \in E(m, m')$

Proof.
Let

$$p_j = p(e_j|m,m'),$$
$$q_j = \frac{p(e_j|m)}{\sum_{e_i \in E(m,m')} p(e_i|m)},$$

for any $e_j \in E(m,m')$ and use proposition 32. □

Proposition 34.

$$P_S \geq \sum_{m,m' \in \mathcal{M}} p(m,m') 2^{\sum_{e_i \in E(m,m')} p(e_i|m) \log \frac{p(e_i|m)}{p(e_i|m,m')}},$$

and equality holds if and only if

$$\frac{p(e_i|m)}{p(e_i|m,m')} = const = C,$$

for any $e_i \in E(m,m')$. *In the case of equality* $P_S = C$.

Proof. From proposition 33 we have

$$payoff(m,m') \geq 2^{\sum_{e_i \in E(m,m')} p(e_i|m) \log \frac{p(e_i|m)}{p(e_i|m,m')}}.$$

Averaging over all m and m' we have the desired result. □

Now we can prove the main theorem.

Theorem 35.

$$P_S \geq 2^{H(E|M^2) - H(E|M)}.$$

And equality holds if and only if the following conditions is satisfied: for any $m, m' \in \mathcal{M}$ *and* $e_J \in E(m,m')$
$p(e_j|m)/p(e_j|m,m') = const = C$. *In the case of equality* $P_S = C$

Proof.
Using proposition 34 and Jensen's inequality we have

$$\log P_S \geq \log\Big(\sum_{m,m'} p(m,m') 2^{\sum_{e_j \in E(m',m)} p(e_j|m,m') log \frac{p(e_j|m)}{p(e_j|m,m')}}$$

$$\geq \sum_{m,m'} p(m,m') \sum_{e_j \in E(m',m)} p(e_j|m,m') \log \frac{p(e_j|m)}{p(e_j|m,m')}$$

$$= \sum_{m,m'} \sum_{e_j \in E(m',m)} p(e_j,m,m') \log \frac{p(e_j|m)}{p(e_j|m,m')} = H(E|M^2) - H(E|M).$$

which completes the proof.

References

1. E. Brickell, *A Few Results in Message Authentication* , Congressus Numerantium, vol 43, 1984, pp 141-154.
2. R.Johansen, A. Sgarro *Strengthening Simmons' Bound in Impersonation* , IEEE Transactions on Information Theory, vol 37, No 4, July 1991, pp 1182-1185.
3. J.L. Massey, *Cryptography - A Selective Survey*, Proc. of 1985 Int. Tirrenia Workshop on Digital Communication, Tirrenia, 1985, Digital Communications, ed.E. Biglieri and G. Pratti, Elsevier Science Publ., 1986, North-Holland, pp 3-25
4. J.L. Massey, *Introduction to Contemporary Cryptography* , Proceedings of the IEEE, vol 76, No 5, May 1988, pp 533-549.
5. D. Pei *Information - Theoretic Bounds for Authentication Codes and PBIB* , Asiacrypt 1991, Ramp Session.
6. R. Safavi, L. Tombak, *Authentication Codes under Impersonation Attack*, Proc. of Auscrypt 1992, to appear.
7. G.J. Simmons, *Message Authentication: A Game on Hypergraphs*, Congressus Numerantium, Vol 45, 1984, pp 161-192.
8. G.J. Simmons, *Authentication Theory/Coding Theory*, Proc. of Crypto 84, Lecture Notes in Computer Science 196, Springer 1985, pp 411-432.
9. G.J. Simmons, *A Game Theory Model of Digital Message Authentication*, Congressus Numerantium, Vol. 34, 1982, pp 413-424.
10. G.J. Simmons, *A Survey of Information Authentication* , Proceedings of the IEEE vol 76, No 5, May 1988, pp 603-619.
11. D.R. Stinson, *Some Constructions and Bounds for Authentication Codes*, Journal of Cryptology, No 1, 1988, pp 37-51.
12. D.R. Stinson, *The Combinatorics of Authentication and Secrecy Codes* , Journal of Cryptology, No 2 (1990), pp 23-49.
13. D.R. Stinson, *Combinatorial Characterization of Authentication Codes* , Proceedings Crypto 91, Lecture Notes in Computer Science 576, Springer 1992, pp 62-72.
14. L. Tombak, R. Safavi, *Authentication Codes with Perfect Protection*, Proc. of Auscrypt 1992, to appear.
15. M. Walker *Information-Theoretic Bounds for Authentication Schemes*, Journal of Cryptology, No 2, 1990, pp 131-143.