Authentication schemes

Dingyi Pei
State Key Laboratory of Information Security
Graduate school of Chinese Academy of sciences
and
Guangzhou University
Email: gztcdpei@scut.edu.cn
August 2001

Abstract. These notes introduce the optimal authentication schemes, both without or with arbitration. Describe how the construction of optimal authentication schemes is reduced to the construction of certain combinatorial designs. Then based on the rational normal curves over finite fields, a new family of optimal authentication schemes with three participants is constructed.

Contents

Acknowledgments: These notes are written for tutorial lectures given at the Institute for Mathematical Sciences, National University of Singapore, when the author visits there as a senior member. The author is grateful to the institute for its hospitality.

Chapter 1

Authentication model

Secrecy and authentication are the two fundamental aspects of information security. Secrecy provides protection for sensitive messages against eavesdropping by an unauthorized person, while authentication provides protection for messages against impersonating and tampering by an active deceiver. Secrecy and authentication are two independent concepts. It is possible that only secrecy, or only authentication, or both is concerned in an information system. We mainly study one of the authentication methods- authentication schemes in this note and don't touch other authentication methods, like digital signature.

In this chapter we discuss the authentication models introduced by G.J.Simmons[8],[9].

1.1 Model with three participants

We consider the authentication model that involves three participants: a transmitter, a receiver and an opponent. The transmitter wants to communicate a sequence of source states to the receiver. In order to deceive the receiver, the opponent impersonates the transmitter to send a fraudulent message to the receiver, or to tamper the message sent to the receiver. The transmitter and the receiver must act with the common purpose to deal with the spoofing attack from the opponent. They are assumed to trust each other in this model. If the transmitter and the receiver may also cheat each other, it is necessary to introduce the fourth participant - arbiter. The model with three participants usually is called as A-code and that with arbiter is called as A^2-code in the literature. We introduce with A-code in this paragraph, and A^2-code in the next paragraph.

Let $\mathcal{S}$ denote the set of all source states which the transmitter may convey to the receiver. In order to protect against attacks from the opponent, source states are encoded using one from a set of encoding rules $\mathcal{E}$ before transmission. Let $\mathcal{M}$ denote the set of all possible encoded messages. Usually the number of encoded messages is much larger than that of source states. An encoding rule $e \in \mathcal{E}$ is an one-to-one mapping from $\mathcal{S}$ to $\mathcal{M}$. The range of the mapping $e(\mathcal{S})$ is called the set of valid messages of e, which is a subset of $\mathcal{M}$. Prior to transmission the transmitter and the receiver agree upon an encoding rule e kept secret from the opponent. The transmitter uses e to encode source states. The encoded messages are transmitted through a public insecure channel.When a message is received, the receiver checks whether it lies in the range $e(\mathcal{S})$. If it is the case, then the message is accepted as authentic, otherwise it is rejected. The receiver recovers the source states from the received messages by determining their (unique) pre-images under the agreed encoding rule e. We assume that the opponent has a complete understanding of the system including all encoding rules. The only thing he does not know is the particular encoding rule agreed upon by the transmitter and the receiver. The opponent can be success in his spoofing attack if and only if his fraudulent message is valid of the used encoding rule. The set of valid messages usually is different from rule to rule. In order to decrease the possibility of successful deception from the opponent, the used encoding rule must be alternated frequently.

The three sets $(\mathcal{S}, \mathcal{M}, \mathcal{E})$ form an authentication scheme.

We assume that the opponent has the ability to impersonate the transmitter to send messages to the receiver, or to tamper the messages sent by the transmitter. It is called a spoofing attack of order r that after observation of the first $r(r \geq 0)$ messages sent by the transmitter using the same encoding rule, the opponent places a fraudulent message into the channel attempting to make the receiver accept it as authentic. It is an impersonate attack when r is zero. Let P_r denote the expected probability of successful deception for a optimum spoofing attack of order r. We are going to find an expression for P_r.

We think of source states, encoded messages and encoding rules as random variables denoted by S, M and E respectively, i.e. there are probability distributions on the sets $\mathcal{S}, \mathcal{M}$ and $\mathcal{E}$ respectively. Let $p(S = s)$ denote the probability of the event that the variable $\mathcal{S}$ takes the value $s \in \mathcal{S}$. Similarly we have $p(E = e)$ and $p(\mathcal{M} = m)$ where $e \in \mathcal{E}$ and $m \in \mathcal{M}$. For simplicity, we abbreviate by omitting the names of random variables in a probability distribution when this causes no confusion. For instance, we write $p(s), p(e)$ and $p(m)$ for above probabilities. Similarly we write the conditional probability $p(e \mid m)$ instead of $p(E = e \mid M = m)$.

For any $m^r = (m_1, m_2, \cdots, m_r) \in \mathcal{M}^r$ and $e \in \mathcal{E}$, let $f_e(m^r) = (f_e(m_1), \cdots, f_e(m_r))$ denote the unique elements $(s_1, \cdots, s_r) \in \mathcal{S}^r$, when $m_i \in e(\mathcal{S})$ for $1 \leq i \leq r$, such that $s_i = f_e(m_i)$ is the pre-image of m_i under e.

We consider only impersonation $(r = 0)$ and plaintext substitution. The latter means that the opponent is considered to be successful only when, after observing a sequence of messages $m_1, \cdots, m_r$, he chooses a fraudulent message m' that is valid of the used encoding rule e, and $m' \neq m_i, (1 \leq i \leq r)$. In this case, the receiver is informed a source state which the transmitter does not intend to convey. If the receiver gets a particular messages twice, he cannot decide whether the message was sent twice by the transmitter or was repeated by an opponent. Hence we assume that the transmitter never sends a particular source state twice under same encoding rule. Let S^r denote the random variable of the first r source states which the transmitter intend to convey to the receiver. Accordingly we assume that

$$p(S^r = (s_1, \cdots, s_r)) > 0. \tag{1.1}$$

if and only if the components $s_1, \cdots, s_r$ are pairwise distinct. The reason of the "if" part will be explained later on.

We assume also that

$$p(e) > 0, \qquad \text{for each } e \in \mathcal{E}, \tag{1.2}$$

otherwise the encoding rule is never been used, and can be dismissed from $\mathcal{E}$.

Assume that random variables E and S^r are independent, i.e.

$$p(e, s^r) = p(e)p(s^r), \text{for all } e \in \mathcal{E},\ s^r \in \mathcal{S}^r.$$

Let $m^r = (m_1, \cdots, m_r) \in \mathcal{M}^r, m_i (1 \leq i \leq r)$ are distinct, define

$$\mathcal{E}(m^r) = \{e \in \mathcal{E} \mid m_i \in e(S), 1 \leq i \leq r\}.$$

$\mathcal{E}(m^r)$ maybe empty. We require that $\mathcal{E}(m)$ is not empty for each $m \in \mathcal{M}$, otherwise the message is never been used, it can been dismissed from $\mathcal{M}$.

Let M^r denote the random variable of the first r messages sent by the transmitter. The probability distributions on E and on S^r determine the distribution on M^r. For any $e \in \mathcal{E}$ and $m^r \in \mathcal{M}^r$, if $e \notin \mathcal{E}(m^r)$, then $p(e, m^r) = 0$; if $e \in \mathcal{E}(m^r)$, then

$$p(e, m^r) = p(e)p(f_e(m^r)). \tag{1.3}$$

Let $P(m \mid m^r)$ be the probability that the message m is valid given that m^r has been observed. Then

$$P(m \mid m^r) = \sum_{e \in \mathcal{E}(m^r * m)} p(e \mid m^r),$$

where $m^r * m$ denotes the message sequence $m_1, \cdots, m_r, m$. Given that m^r has been observed, the opponent's optimum strategy is to choose the message m' that maximizes $P(m \mid m^r)$. Thus the unconditional probability of success in an optimum spooling attack of order r is

$$P_r = \sum_{m^r \in \mathcal{M}^r} p(m^r) \max_{m \in \mathcal{M}} P(m \mid m^r). \tag{1.4}$$

1.2 Model with arbitration

In the authentication model with three participants discussed in the previous paragraph, the transmitter and the receiver are assumed trusted, they don't cheat each other. But it is not always the case: the transmitter may deny a message that he has sent, and the receiver may attribute a fraudulent message to the transmitter. A trusted third party, called arbiter is introduced.

Let $\mathcal{S}$ and $\mathcal{M}$ denote the set of source states and encoded messages respectively as before. We define encoding rules of the transmitter and decoding rules of the receiver as follows. An encoding rule is an one-to-one mapping from $\mathcal{S}$ to $\mathcal{M}$. Let $\mathcal{E}_T$ denote the set of all encoding rules. A decoding rule is a mapping from $\mathcal{M}$ onto $\mathcal{S} \cup \{\text{reject}\}$. Each message corresponds to a source state or to "reject". In the former case the message is called valid of the decoding rule, while in the latter case the message will be rejected by the receiver. The set of all decoding rules is denoted by $\mathcal{E}_R$.

Suppose $f \in \mathcal{E}_R$ is a decoding rule of the receiver and $s \in \mathcal{S}$ is a source state, let $\mathcal{M}(f,s)$ denote the set of all valid messages of f corresponding to s.The sets $\mathcal{M}(f,s) \subset \mathcal{M}$ are disjoint for different source states s.

We say that an encoding rule $e \in \mathcal{E}_T$ is valid of the decoding rule $f \in \mathcal{E}_R$ if $e(s) \in \mathcal{M}(f,s)$ for any $s \in \mathcal{S}$.

Prior transmission, the receiver selects a decoding rule $f \in \mathcal{E}_R$ and secretly gives it to the arbiter. The arbiter selects one message from $\mathcal{M}(f,s)$ for each source state $s \in \mathcal{S}$ forming an encoding rule $e \in \mathcal{E}_T$ and secretly gives it to the transmitter to be used. In this case the encoding rule e is valid of the decoding rule f. Receiving a message, the receiver checks whether it is a valid messages of f (i.e. it is in some subset $\mathcal{M}(f,s)$), if it is, then he accepts it as authentic and recovers the corresponding source state. When the transmitter and the receiver are disputing whether one message has been sent or not sent by the transmitter, the arbiter checks whether the message under dispute is valid of the encoding rule given to the transmitter. If it is valid, the arbiter thinks that the message is sent by the transmitter since only the transmitter knows the encoding rule. In the opposite case, the arbiter thinks that the message is not sent by the transmitter. Since the receiver does not know how the arbiter constructs the encoding rule e, so it is not easy for him to choose a fraudulent message which is valid of e, i.e. it is not easy for the receiver to attribute a fraudulent message to the transmitter. Similarly, since the transmitter does not know the decoding rule f selected by the receiver, it is hard for the transmitter to choose a fraudulent message which is valid of f but is not valid of e, i.e. it is hard for the transmitter to deny a message that he has sent. As for the opponent, he may success in a deception only if he can find a valid message of f.

The following three types of spoofing attacks are considered.

The spoofing attack O_r by the opponent: after observation a sequence of r distinct messages $m_1, m_2, \cdots, m_r$ using the same encoding rule, the opponent sends a message $m (m \neq m_i, 1 \leq i \leq r\ )$ to the receiver and succeeds if the receiver accepts the message as authentic and the message represents a different source state from those represented by $m_i (1 \leq i \leq r)$.

The spooling attack R_r by the receiver: after receiving a sequence of r distinct messages $m_1, m_{2,} \cdots, m_r$, the receiver claims to have received a different message m and succeeds if the message m is valid of the encoding rule used by the transmitter.

The spooling attack T by the transmitter: the transmitter sends a message to the receiver and then denies having sent it. The transmitter succeeds if this message is accepted by the receiver as authentic and it is not valid of the encoding rule used by the transmitter.

Let P_{O_r}, P_{R_r} and P_T denote the success probability for the optimal spoofing attack of the three kinds defined above respectively. We are going to find their expressions.

Assume (1.1) still hold. For a given decoding rule $f \in \mathcal{E}_{\mathcal{R},}$ define

$$\mathcal{M}(f) = \bigcup_{s \in \mathcal{S}} \mathcal{M}(f, s)$$

and

$$\mathcal{E}_T(f) = \{e \in \mathcal{E}_T | e \text{ is valid of } f\}.$$

$\mathcal{M}(f)$ is the set of all valid messages for f. $\mathcal{E}_T(f)$ is the set of all encoding rules which are valid of f.

For a given encoding rule $e \in \mathcal{E}_T$, let

$$\mathcal{M}(e) = \{e(s) \mid s \in \mathcal{S}\} \subset \mathcal{M}$$

an

$$\mathcal{E}_R(e) = \{f \in \mathcal{E}_R | e \text{ is valid of } f\}.$$

For a given $m^r = (m_1, \cdots, m_r) \in \mathcal{M}^r$, define the set

$$\mathcal{E}_R(m^r) = \{f \in \mathcal{E}_R | m_i \in \mathcal{M}(f), f(m_i) \neq f(m_j), 1 \leq i < j \leq r\}.$$

$\mathcal{E}_R(m^r)$ is the set of all decoding rules of which m^r is valid. For any given $f \in \mathcal{E}_R$ define

$$\mathcal{E}_T(f, m^r) = \{e | e \in \mathcal{E}_T(f), m_i \in \mathcal{M}(e), 1 \leq i \leq r\}.$$

This is the set of all decoding rules of which f and m^r are valid.

Similarly to the previous paragraph, let S^r and M^r denote the random variables of the first r source states and the first r encoded messages respectively, E_R and E_T denote the random variables of decoding rules and encoding rules respectively. We assume also that $p(E_R = f) > 0$ for any $f \in \mathcal{E}_R$ and $p(E_T = e \mid E_R = f) > 0$ for any $e \in \mathcal{E}_T(f)$. It follows immediately that $p(E_T = e) > 0$ for any $e \in \mathcal{E}_T$ and $p(E_R = f \mid \mathcal{E}_T = e) > 0$ for any $f \in \mathcal{E}_R(e)$.

For any message $m \in \mathcal{M}$ we assume that there exists at least one decoding rule f such that $m \in \mathcal{M}(f)$, otherwise m is never be used and can be dismissed from $\mathcal{M}$. Similarly, for any message $m \in \mathcal{M}(f)$ there exists at least one encoding rule $e \in \mathcal{E}_T(f)$ such that $m \in \mathcal{M}(e)$, otherwise m can be dismissed from $\mathcal{M}(f)$.

Let $P(m|m^r)$ denote the probability of the event that the message m is acceptable by the receiver given that the first r messages $m^r = (m_1, m_2, \cdots, m_r)$ have been observed, where $m_{1,} \cdots, m_r, m$ represent different source states. We have

$$P(m|m^r) = \sum_{f \in \mathcal{E}_R(m^r * m)} p(f|m^r).$$

Similarly to (1.4) we define

$$P_{O_r} = \sum_{m^r \in \mathcal{M}^r} p(m^r) \max_{m \in \mathcal{M}} P(m|m^r), \tag{1.5}$$

Let $P(m|f, m^r)$ denote the probability of the event that the message m could be valid of the encoding rule used by the transmitter given the decoding rule f and the first r messages $m^r = (m_1, \cdots, m_r)$. We have

$$P(m|f, m^r) = \sum_{e \in \mathcal{E}_T(f, m^r * m)} p(e|f).$$

We define

$$P_{R_r} = \max_{f \in \mathcal{E}_R} \sum_{m^r \in \mathcal{M}^r} p(m^r|f) \max_{m \in \mathcal{M}} P(m|f, m^r)), \tag{1.6}$$

For a given $f \in \mathcal{E}_R$ and $e \in \mathcal{E}_T(f)$ define

$$\mathcal{M}'(e) = \mathcal{M} \backslash \mathcal{M}(e),$$

$$\mathcal{M}'_f(e) = \mathcal{M}(f) \backslash \mathcal{M}(e) \subset \mathcal{M}^{prime}(e).$$

Let $P(m'|e)$ denote the probability of the event that the message $m' \in \mathcal{M}'(e)$ is acceptable by the receiver given the encoding rule e. We have

$$P(m'|e) = \sum_{f \in \mathcal{E}_R(e, m')} p(f|e),$$

where

$$\mathcal{E}_R(e, m') = \{f | f \in \mathcal{E}_R(e), m' \in \mathcal{M}'_f(e)\}.$$

We define

$$P_T = \max_{e \in \mathcal{E}_T} \max_{m' \in \mathcal{M}'(e)} P(m'|e). \tag{1.7}$$

Chapter 2

Authentication schemes with three participants

We study the authentication schemes with three participants in this chapter. When we say authentication schemes it always means the schemes with three participants in this chapter. The success probability P_r of optimal spooling attack of order r was introduced in section 1.1. The information-theoretic lower bound of P_r and the necessary and sufficient conditions for achieving this bound will be given in the section 2.2 of this chapter. In order to discuss the information-theoretic bound, the important concept of information theory - entropy is introduced in section 2.1, some often used properties of entropy are proven. One important aim in constructing authentication schemes is to make P_r as small as possible. When $P_r(0 \le r \le t-1)$ achieve their information-theoretic bounds and the number of encoding rules achieves also its lower bound, the authentication schemes are called optimal of order t. It is proved in the section 2.3 that each optimal authentication scheme corresponds to a strong partially balanced design (SPED will be defined in section 2.3), and vice versa, each SPED can be used to construct an optimal authentication scheme. Thus to construct optimal authentication schemes is reduced to find SPED. We will construct a new family of SPED, therefore to construct a new family of optimal authentication schemes, in the chapter 3.

2.1 Entropy

Suppose all possible values (or states) of the variable X are $x_1, \cdots, x_n$, the probability of X taking x_i is $p(x_i)$, hence

$$\sum_{i=1}^{n} p(x_i) = 1. \tag{2.1}$$

We call X as a random variable. If n=1, then $p(x_1) = 1$ and X always takes the value x_1. Therefore X is totally determined. If probabilities of X taking $x_i (1 \leq i \leq n)$ are all equal, i.e. $p(x_1) = p(x_2) = \cdots = p(x_n) = 1/n$, X is most undetermined. For a general random variables, its indeterminacy is between these two cases. We have a quantity to measure the indeterminacy, it is called entropy. The entropy of a random variable X is defined as

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log p(x_i).$$

here the base of the logarithm function is 2.

Lemma 1 *We have* $o \leq H(X) \leq \log n$. *If* X *is totally determined, then* H(X)=0; *If* $p(x_1) = \cdots = p(x_n) = 1/n$, *then* H(X) *achieves its maximum* $\log n$.

Proof It is only necessary to prove the inequality $0 \leq H(X) \leq \log n$, the latter conclusion is trivial. We write p_i for $p(x_i)$. Put

$$F = -\sum_{i=1}^{n} p_i \log p_i - \lambda \sum_{i=1}^{n} p_i,$$

If

$$\frac{\partial F}{\partial p_i} = -\log (ep_i) - \lambda = 0, \quad i = 1, 2, \cdots, n$$

(here e is the base of the natural logarithm function), then $p_1, p_2, \cdots, p_n$ are all equal with the value $1/n$. Hence $H(X)$ achieves its maximum value $\log n$ in the case. The conclusion $H(X) \geq 0$ is obvious. #

Based on the above lemma we cam think that the entropy $H(X)$ measures the indeterminacy of X. If each value of X is represented by r bits and X takes any sequence $(a_1, a_2, \cdots, a_r)$ of r bits with equal probability, then $H(X) = \log 2^r = r$. We see that bit can be taken as the unit of entropy. In the above example, the probability of X taking $(a_1, a_2, \cdots, a_r)$ is $1/2^r$, the logarithm $-\log(1/2^r) = r$ can be explained as the amount of information provided when the event takes place. When an event with probability p takes place, the amount of information it provides is $\log p^{-1}$. The entropy $H(X)$ can be explained as expected amount of information provided when X takes a value.

Let X and Y be two random variables. Let $p(x, y)$ be the union probability of $X = x$ and $Y = y$ simultaneously, and $p(y \mid x)$ be the conditional probability of $Y = y$ given $X = x$. We have

$$p(x, y) = p(x)p(y \mid x) = p(y)p(x \mid y). \tag{2.2}$$

If $p(x \mid y) = p(x)$ for any x and y, then $p(x, y) = p(x)p(y)$. We say X and Y are independent. Define the union entropy of X and Y by

$$H(X, Y) = -\sum_{x,y} p(x, y) \log p(x, y),$$

where the summation runs through all pairs (x, y) such that $p(x, y) > 0$ (in the following all summations have this restriction, we will not mention it again.) Define conditional entropy by

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

and

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

$H(X \mid Y)$ denotes the indeterminacy of X when Y is determined. If X and Y are independent, then

$$\begin{aligned} H(X \mid Y) &= -\sum_{x,y} p(x, y) \log p(x) \\ &= -\sum_{x} \log p(x) \sum_{y} p(x, y) \\ &= -\sum_{x} p(x) \log p(x) = H(X), \end{aligned}$$

similarly we have $H(Y \mid X) = H(Y)$.

Lemma 2

$$H(X, Y) = H(X) + H(Y \mid X) = H(Y) + H(X \mid Y).$$

Proof It is only necessary to prove the first equality since $H(X, Y) = H(Y, X)$. We have

$$\begin{aligned} H(X) + H(Y \mid X) &= -\sum_{x} p(x) \log p(x) - \sum_{x,y} p(x, y) \log p(y \mid x) \\ &= -\sum_{x,y} p(x, y) \log (p(x) p(y \mid x)) \\ &= -\sum_{x,y} p(x, y) \log p(x, y) = H(X, Y). \end{aligned}$$

here (2.2) is used. #

If X and Y are independent, it follows from lemma 2 that $H(X, Y) = H(X) + H(Y)$.

Lemma 3 *(Jensen inequality) Suppose* $x_i > 0, p_i > 0, (1 \leq i \leq n)$ *and* $p_1 + p_2 + \cdots + p_n = 1$. *Then*

$$\sum_{i=1}^{n} p_i \log x_i \leq \log (\sum_{i=1}^{n} p_i x_i).$$

The equality holds if and only if $x_i (1 \leq i \leq n)$ *are all equal.*

Proof It is equivalent to prove that

$$x_1^{p_1} x_2^{p_2} \cdots x_n^{p_n} \leq p_1 x_1 + p_2 x_2 + \cdots p_n x_n.$$

The left side is the geometry mean value and the right side is the arithmetic mean value. This is a well known inequality. #

Lemma 4

$$H(X \mid Y) \leq H(X).$$

Proof We have

$$\begin{aligned} H(X \mid Y) - H(X) &= -\sum_{x,y} p(x, yP \log p(x \mid y) + \sum_{x,y} p(x,y) \log p(x) \\ &= \sum_{x,y} p(x,y) \log \frac{p(x)p(y)}{p(x,y)}, \end{aligned}$$

It follows from Lemma 3 that

$$H(X \mid Y) - H(x) \leq \log (\sum_{x,y} p(x,y) \frac{p(x)p(y)}{p(x,y)}) = 0. \quad \#$$

Lemma 4 means that the indeterminacy of X could decrease and could not increase when Y is determined. One may find some information about X from determined Y. The decrease of indeterminacy $H(X) - H(X \mid Y)$ is the lost amount of information.

It was Shannon who studied the theory of secrecy based on the information theory first. This made a milestone in the development of cryptology. Simmons[8] developed an analogous theory for authentication.

2.2 Information-theoretic bound

Proposition 5 *(Pei [3]) The inequality*

$$P_r \geq 2^{H(E|M^{r+1}) - H(E|M^r)} \tag{2.3}$$

holds for any integer $r \geq 0$. The equality holds iff for any $m^r * m \in \mathcal{M}^{r+1}$ with $\mathcal{E}(m^r * m) \neq \emptyset$, the ratio

$$\frac{p(e|m^r)}{p(e|m^r * m)} \tag{2.4}$$

is independent of m^r, m and $e \in \mathcal{E}(m^r * m)$. When this equality holds, the probability P_r equals the above ratio.

Remark If $e \in \mathcal{E}(m^r * m)$, then by the assumption (1.1),(1.2) and (1.3),

$$p(m^r)p(e \mid m^r) = p(e, m^r) = p(e)p(f_e(m^r)) > 0,$$

the numerator and the denominator of the fraction (2.4) are nonzero. This is the reason of the "if" part of (1.1).

Proof Let M_{r+1} denote the random variable of the $(r+1)$-th message. For a given $m^r = (m_1, \cdots, m_r) \in \mathcal{M}^r$, let

$$\mathrm{supp}(M_{r+1}, E \mid m^r) = \{(m,e) | e \in \mathcal{E}(m^r * m), m \neq m_i (1 \leq i \leq r)\}$$

denote the support of the conditional probability distribution of the random variable pair (M_{r+1}, E) conditional on $M^r = m^r$. Then under bounding a maximum by an average gives

$$\begin{aligned}
\max_{m \in \mathcal{M}} P(m|m^r) &\geq \sum_{m \in \mathcal{M}} p(M_{r+1} = m \mid m^r) P(m|m^r) \\
&= \sum_{(m,e) \in \mathrm{supp}(M_{r+1}, E \mid m^r)} p(M_{r+1} = m \mid m^r) p(e|m^r) \\
&= \widetilde{E}\Big(\frac{p(M_{r+1} = m \mid m^r) p(e|m^r)}{p(M_{r+1} = m, e \mid m^r)}\Big) \qquad (2.5)
\end{aligned}$$

where $\widetilde{E}$ is the expectation on $\mathrm{supp}(M_{r+1}, E \mid m^r)$. By use of Jensen's inequality, we obtain

$$\begin{aligned}
&\log \max_{m \in \mathcal{M}} P(m|m^r) \geq \widetilde{E}\Big(\log \frac{p(M_{r+1} = m \mid m^r) p(e|m^r)}{p(_{r+1} = m, e \mid m^r)}\Big), \\
&= H(M_{r+1}, E | M^r = m^r) - H(M_{r+1} | M^r = m^r) - H(E | M^r = m^r), \qquad (2.6)
\end{aligned}$$

where

$$\begin{aligned}
H(M_{r+1}, E | M^r = m^r) &= - \sum_{(m,e) \in \mathrm{supp}(M_{r+1}, E | m^r)} p(M_{r+1} = m, e | m^r) \log p(M_{r+1} = m, e | m^r), \\
H(M_{r+1} | M^r = m^r) &= - \sum_{m : p(M_{r+1} = m | m^r) > 0} p(M_{r+1} = m | m^r) \log p(M_{r+1} = m | m^r), \\
H(E | M^r = m^r) &= - \sum_{e \in \mathcal{E}(m^r)} p(e|m^r) \log p(e|m^r).
\end{aligned}$$

Finally we make another use of Jensen's inequality to obtain

$$\begin{aligned}
\log P_r &= \log \sum_{m^r \in \mathcal{M}^r} p(m^r) \max_{m \in \mathcal{M}} P(m|m^r) \\
&\geq \sum_{m^r \in \mathcal{M}^r} p(m^r) \log \max_{m \in \mathcal{M}} P(m|m^r) \\
&\geq H(M_{r+1}, \mathrm{E} | M^r) - H(M_{r+1} | M^r) - H(E | M^r) \\
&= H(E | M^{r+1}) - H(M^r). \qquad (2.7)
\end{aligned}$$

Lemma 2 is used in the last equality.

¿From the above derivation, we see that equality holds in this bound if and only if the following two conditions are satisfied:

(i) $P(m|m^r)$ is independent of those m and m^r with $p(M_{r+1} = m \mid m^r) > 0$, so that its average and maximum value are coincide in (2.5).

(ii) In order to get equality in (2.6), every $m^r * m \in \mathcal{M}^{r+1}$ with $\mathcal{E}(m^r * m) \neq \emptyset$, the ratio

$$\frac{p(M_{r+1}=m|m^r)p(e|m^r)}{p(M_{r+1}=m,e \mid m^r)} = \frac{p(e|m^r)}{p(e|m^r*m)}$$

is independent of m, m^r and $e \in \mathcal{E}(m^r * m)$.

Condition (i) can be deduced from condition (ii) since, if $p(M_{r+1} = m \mid m^r) > 0$, then $\mathcal{E}(m^r * m) \neq \emptyset$ and

$$\begin{aligned} P(m|m^r) &= \sum_{e \in \mathcal{E}(m^r * m)} p(e|m^r) \\ &= \frac{p(e|m^r)}{p(e|m^r * m)} \sum_{e \in \mathcal{E}(m^r * m)} p(e|m^r * m) \\ &= \frac{p(e|m^r)}{p(e|m^r * m)} \end{aligned}$$

This completes the proof of the Proposition 5. #

The lower bound in Proposition 5 is called information-theoretic bound. Simmons proved it in the case of $r = 0$. The author gives its proof for general case and finds the necessary and sufficient condition for achieving the bound in the form stated in the Proposition 5. The result was first announced at Asiacrypt'91. (see [3],[7]).

2.3 Optimal authentication schemes

By Proposition 5 we know that

$$P_0 P_1 \cdots P_{r-1} \geq 2^{H(E|M^r) - H(E)} \geq 2^{-H(E)}, \tag{2.8}$$

Hence by lemma 1 we have

$$|\mathcal{E}| \geq 2^{H(E)} \geq (P_0 P_1 \cdots P_{r-1})^{-1}. \tag{2.9}$$

Definition 1 *An authentication scheme is called optimal of order t if its $P_r (0 \leq r \leq t-1)$ achieve their information- theoretic bounds and the number of its encoding rules also achieves its lower bound $(P_0 P_1 \cdots P_{t-1})^{-1}$.*

We study the characterization of the optimal authentication schemes and find its construction method in this paragraph.

For any positive integer r define

$$\overline{\mathcal{M}^r} = \{m^r \in \mathcal{M}^r \mid \mathcal{E}(m^r) \neq \emptyset\}.$$

We assume that $\overline{\mathcal{M}^1} = \mathcal{M}$, otherwise some messages are never used and can be dismissed. For any $m^r \in \overline{\mathcal{M}^r}$ define

$$\mathcal{M}(m^r) = \{m \in \mathcal{M} \mid \mathcal{E}(m^r * m) \neq \emptyset\}.$$

Corollary 6 *Suppose that $|\mathcal{S}| = k, |\mathcal{M}| = v$, the positive integer $t \leq k$, and*

$$P_r = 2^{H(E|M^{r+1}) - H(E|M^r)}, \quad 0 \leq r \leq t-1.$$

Then

(i) *For any $m^r \in \overline{\mathcal{M}^r}(1 \leq r \leq t)$, the probability $p(f_e(m^r))$ is independent of $e \in \mathcal{E}(m^r)$;*

(ii) *For any $m^r * m \in \overline{\mathcal{M}^r}, 1 \leq r \leq t-1$, We have*

$$P_0 = \sum_{e \in \mathcal{E}(m)} p(e), \qquad P_r = \frac{\sum_{e \in \mathcal{E}(m^r * m)} p(e)}{\sum_{e \in \mathcal{E}(m^r)} p(e)},$$

Therefore

$$\sum_{e \in \mathcal{E}(m^i)} p(e) = P_0 P_1 \cdots P_{i-1},$$

for any $m^i \in \overline{\mathcal{M}^i}, (1 \leq i \leq t)$;

(iii) *$P_0 = k/v$ and $|\mathcal{M}(m^r)| = (k-r)P_r^{-1}$ for any $m^r \in \overline{\mathcal{M}^r}$;*

(iv) *$|\overline{\mathcal{M}^i}| = C_k^i (P_0 P_1 \cdots P_{i-1})^{-1}, 2 \leq i \leq t$. (It is trivial that $|\overline{\mathcal{M}^1}| = v$.)*

Proof (i)If $e \in \mathcal{E}(m^r * m)$, we have (Proposition 5)

$$\begin{aligned} P_r &= \frac{p(e \mid m^r)}{p(e \mid m^r * m)} \\ &= \frac{p(e, m^r) p(m^r * m)}{p(e, m^r * m) p(m^r)} \\ &= \frac{p(f_e(m^r) \sum_{e' \in \mathcal{E}(m^r * m)} p(e') p(f_{e'}(m^r * m))}{p(f_e(m^r * m)) \sum_{e' \in \mathcal{E}(m^r)} p(e') p(f_{e'}(m^r))} \end{aligned} \tag{2.10}$$

Taking $r = 0$ in (2.10) we obtain

$$P_0 = \frac{\sum_{e' \in \mathcal{E}(m)} p(e') p(f_{e'}(m))}{p(f_e(m))}$$

It follows that $p(f_e(m)$ does not dependent on $e \in \mathcal{E}(m)$ and properties (i) and (ii) hold for $r = 1$. Then (i) and (ii) can be proved by induction on r.

We have

$$vP_0 = \sum_{m \in \mathcal{M}} \sum_{e \in \mathcal{E}(m)} p(e) = k \sum_{e \in \mathcal{E}} p(e) = k,$$

$$\sum_{m \in \mathcal{M}(m^r)} \sum_{e \in \mathcal{E}(m^r * m)} p(e) = (k - r) \sum_{e \in \mathcal{E}(m^r)} p(e),$$

Thus (iii) follows from (ii).

Finally, it is trivial that $\overline{\mathcal{M}^1} = v$. By (iii), when $r \geq 2$, we have

$$|\overline{\mathcal{M}^r}| = \frac{1}{r} \sum_{m^{r-1} \in \overline{\mathcal{M}^{r-1}}} |\mathcal{M}(m^{r-1})| = \frac{(k - r - 1)|\overline{\mathcal{M}^{r-1}}|}{rP_{r-1}}.$$

Thus (iv) follows by induction on r. #

We write $\mathcal{M}(e)$ instead of $e(\mathcal{S})$ for each $e \in \mathcal{E}$ in the following, it is a subset of $\mathcal{M}$ with k elements. Thus we have a family of k-subsets

$$\{\mathcal{M}(e) \subset \mathcal{M} \mid e \in \mathcal{E}\}. \tag{2.11}$$

A subset is called as a block in the combinatorial design theory also. We will see that the success probability of spoofing attack P_r is determined by the distribution of those blocks of (2.11) in $\mathcal{M}$ at great extent. For an optimal authentication scheme, this family of blocks must has some special properties. We have to introduce some concepts of combinatorial designs first.

Definition 2 *Let v, b, k, λ, t be positive integers with $t \leq k$. A partially balanced design(PBD) $t - (v, b, k; \lambda, 0)$ is a pair (M, E) where M is a set of v points and E is a family of b subsets of M, each of cardinality k (called blocks) such that any t-subset of M either occurs together in exactly λ blocks or does not occur in any block.*

Definition 3 *If a partially balanced t-design $t - (v, b, k; \lambda_t, 0)$ is also a partially balanced r-design $r - (v, b, k; \lambda_r, 0)$ for $0 \leq r < t$ as well, then it is called a strong partially balanced t-design (SPBD) and is denoted by $t - (v, b, k; \lambda_1, \lambda_2, \cdots,$ $\lambda_t, 0)$.*

If every t-subset of M always occurs in exactly λ blocks, then a $t-(v, b, k; \lambda, 0)$ design is just a t-design $t-(v, b, k, \lambda)$ which has already been extensively studied in the theory of block designs. The concept of partially balanced t-designs is a generalization of the concept of t-designs. A t-design is always strong.

Usually we assume that any element of $\mathcal{M}$ appears at least in one block $\mathcal{M}(e)$, otherwise the element can be dismissed from $\mathcal{M}$. So we only concern the SPBD which is also a 1-design.

Theorem 7 *(Pei[3]) A authentication scheme* $(\mathcal{S}, \mathcal{M}, \mathcal{E})$ *is optimal of order* t *if and only if the pair*

$$(\mathcal{M}, \{\mathcal{M}(e) \mid e \in \mathcal{E}\}) \tag{2.12}$$

is a SPBD $t-(v, b, k; \lambda_1, \lambda_2, \cdots, \lambda_t, 0)$*, the variable* E *has uniform distribution and the distributions of* $S^r (1 \leq r \leq t)$ *satisfy the condition: the probability* $p(S^r = f_e(m^r))$ *is independent of* $e \in \mathcal{E}(m^r)$ *for any* $m^r \in \overline{\mathcal{M}^r}$*. Where*

$$v = |\mathcal{M}|, \qquad b = |\mathcal{E}|, \qquad k = |\mathcal{S}|,$$
$$\lambda_r = (P_r P_{r+1} \cdots P_{t-1})^{-1} (1 \leq r \leq t-1), \qquad \lambda_t = 1.$$

Proof Assume that the authentication scheme $(\mathcal{S}, \mathcal{M}, \mathcal{E})$ is optimal of order t. Since the number of encoding rules achieves its lower bound $(P_0 P_1 \cdots, P_{t-1})^{-1}$, it follows from (2.8) and (2.9) that $|\mathcal{E}| = 2^{H(E)}$ and $H(E \mid M^t) = 0$. The former equality means that E has uniform distribution and the latter means that for any $m^t \in \mathcal{M}^t$, $|\mathcal{E}(m^t)| = 0$ or 1. Hence we know that $\lambda_t = 1$.

Since E is uniform, it follows from (ii) of Corollary 6 that

$$P_r = \frac{|\mathcal{E}(m^r * m)|}{|\mathcal{E}(m^r)|}, \qquad 1 \leq r \leq t-1. \tag{2.13}$$

for any $m^r * m \in \overline{\mathcal{M}^{r+1}}$.

For any $m^r \in \mathcal{M}^r, 1 \leq r \leq t-1$, we have or $|\mathcal{E}(m^r)| = 0$, or $m^r \in \overline{\mathcal{M}^r}$. In the latter case there exists m^t such that $m^r \subset m^t$. It follows from (2.13) that

$$|\mathcal{E}(m^r)| = (P_r P_{r+1} \cdots P_{t-1})^{-1} (= \lambda_r), \qquad 1 \leq r \leq t-1.$$

So far we have proved that the pair (2.12) is a SPBD with the given parameters. The condition satisfied by $S^r (1 \leq r \leq t)$ is nothing but the (i) of Corollary 6. Thus the conditions given in the theorem is necessary.

Now we show that the conditions are also sufficient. Assume the conditions hold. For any $m^r * m \in \overline{\mathcal{M}^{r+1}}, 0 \leq r \leq t-1$, and $e \in \mathcal{E}(m^r * m)$, we have

$$\begin{aligned}
\frac{p(e \mid m^r)}{p(e \mid m^r * m)} &= \frac{p(e, m^r) p(m^r * m)}{p(e, m^r * m) p(m^r)} \\
&= \frac{p(f_e(m^r)) \sum_{e' \in \mathcal{E}(m^r * m)} p(e') p(f_{e'}(m^r * m))}{p(f_e(m^r * m)) \sum_{e' \in \mathcal{E}(m^r)} p(e') p(f_{e'}(m^r))} \\
&= \frac{|\mathcal{E}(m^r * m)|}{|\mathcal{E}(m^r)|} = \frac{\lambda_{r+1}}{\lambda_r}.
\end{aligned}$$

(where $\lambda_0 = b$.) The above ratios are constant, hence $P_r (0 \leq r \leq t-1)$ achieve their information-theoretic bounds (Proposition 5) and

$$P_r = \frac{\lambda_{r+1}}{\lambda_r} \qquad 0 \leq r \leq t-1. \tag{2.14}$$

It is obvious that

$$b = \lambda_0 = (P_0 P_1 \cdots P_{t-1})^{-1}.$$

The theorem is proved now. #

Chapter 3

Optimal authentication schemes based on rational normal curves

We have shown in the previous chapter that to construct optimal authentication schemes is reduced to construct SPBD. We know from literature that a spacial kind of combinatorial design, called orthogonal array ([1]), is also SPBD(with t the strength of the array). Orthogonal array can be used to construct optimal Cartesian authentication schemes[11] (Cartesian authentication scheme is a special kind of authentication schemes, we do not explain it here.) Some special family of partially balanced incomplete block design (PBIB [12]) can provide SPBD with $t = 2$. In this chapter we construct a new family of SPBD by means of rational normal curves (RNC) over finite fields. Then we discuss the authentication schemes constructed from the new SPBD.

3.1 SPBD based on RNC

Let F_q be the finite field with q elements and $n \geq 2$ is a positive integer. Let $PG(n, F_q)$ be the projective space of dimension n over F_q. A point of $PG(n, F_q)$ is denoted by $(x_0, \cdots, x_n)$ where x_i $(0 \leq i \leq n)$ are elements of F_q and x_i are not all zero. If λ is a non-zero element of F_q, then $\lambda(x_0, \cdots, x_n)$ and $(x_0, \cdots, x_n)$ denote the same point of $PG(n, F_q)$. Let T be a non-singular matrix over F_q of order $n + 1$. The one to one transformation of points in $PG(n, F_q)$ defined by

$$\begin{array}{ccc} PG(n, F_q) & \longrightarrow & PG(n, F_q) \\ (x_0, \cdots, x_n) & \longmapsto & (x_0, \cdots, x_n)T \end{array}$$

is called a projective transformation of $PG(n, F_q)$. The group of all projective transformations of $PG(n, F_q)$ is denoted by $PGL_{n+1}(F_q)$. It is the factor group of the linear group $GL_{n+1}(F_q)$ of order $n+1$ over its subgroup $\{\lambda I_{n+1} \mid \lambda \neq 0\}$ where I_{n+1} is the unit matrix.

We define a curve C in $PG(n, F_q)$ to be the image of the map

$$\begin{array}{rcl} PG(1, F_q) & \longrightarrow & PG(n, F_q) \\ (x_0, x_1) & \longmapsto & (x_0^n, x_0^{n-1}x_1, \cdots, x_1^n). \end{array}$$

$PG(1, F_q)$ consists of the following $q+1$ points:

$$(1, \alpha), \qquad \alpha \in F_q; \qquad (0, 1).$$

Therefore the curve C consists of the following $q+1$ points:

$$\begin{array}{ll} (1, \alpha, \alpha^2, \cdots, \alpha^n), & \alpha \in F_q \\ (0, 0, 0, \cdots, 0, 1), & \end{array} \tag{3.1}$$

It is easy to see that the curve C is the common zero locus of the following polynomials over $X_0, \cdots, X_n$:

$$\begin{array}{c} X_i^2 - X_{i-1}X_{i+1}, (1 \leq i \leq n-1) \\ X_1 X_{n-1} - X_0 X_n. \end{array} \tag{3.2}$$

We call the image of the curve C under any projective transformation a rational normal curve(RNC). In other words, a RNC is the image of a map

$$\begin{array}{rcl} PG(1, F_q) & \longrightarrow & PG(n, F_q) \\ (x_0, x_1) & \longmapsto & (A_0(x_0, x_1), \cdots, A_n(x_0, x_1)) \end{array}$$

where $A_0(X_0, X_1), \cdots, A_n(X_0, X_1)$ is an arbitrary basis of the space of homogeneous polynomials of degree n over X_0, X_1.

There are q+1 points on each RNC of $PG(n, F_q)$.

Points $p_i = (x_{i0}, \cdots, x_{in})$ $(i = 1, \cdots, m)$ are called linearly independent (also called in general position) if the rank of the matrix (x_{ij}) $(1 \leq i \leq m,\ 0 \leq j \leq n)$ is m.

Lemma 8 *Any $n+1$ $(n \leq q)$ points on a RNC in $PG(n, F_q)$ are linearly independent.*

Proof It is only necessary to prove the lemma for the curve C. By using Vandermonde determinant

$$\begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^n \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^n \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \alpha_{n+1} & \alpha_{n+1}^2 & \cdots & \alpha_{n+1}^n \end{vmatrix} = (-1)^{n(n+1)/2} \prod_{1 \leq i \leq j \leq n+1} (\alpha_i - \alpha_j)$$

and

$$\begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^n \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^n \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \end{vmatrix} = (-1)^{n(n+1)/2} \prod_{1 \le i \le j \le n} (\alpha_i - \alpha_j),$$

the lemma can be proved easily. #

Lemma 9 *Suppose that $q \geq n+2$. Through any n+3 points in $PG(n, F_q)$, any n+1 points of which are linearly independent, passes a unique RNC.*

Proof. By taking a projective transformation, we may assume that the n+3 given points have the following form:

$$\begin{aligned} p_1 &= (1, 0, \cdots, 0), \\ p_2 &= (0, 1, \cdots, 0), \\ &\cdots \\ p_{n+1} &= (0, 0, \cdots, 1), \\ p_{n+2} &= (1, 1, \cdots, 1), \\ p_{n+3} &= (\nu_0, \nu_1, \cdots, \nu_n). \end{aligned} \tag{3.3}$$

Since any $n+1$ points among them are linearly independent, we have

$$\nu_i \quad (0 \le i \le n)$$

are distinct non-zero elements in F_q.

Define a polynomial

$$G(X_0, X_1) = \prod_{i=0}^{n} (X_0 - \nu_i^{-1} X_1).$$

in X_0, X_1. The polynomials

$$H_i(X_0, X_1) = G(X_0, X_1)/(X_0 - \nu_i^{-1} X_1) \quad (0 \le i \le n)$$

form a basis for the space of homogeneous polynomials of degree n, because if there were a linear relation

$$\sum_{i=0}^{n} a_i H_i(X_0, X_1) = 0, \quad a_i \in F_q$$

then substituting $(X_0, X_1) = (1, \nu_i)$ we could deduce that $a_i = 0 \;\; (0 \le i \le n)$. Thus the RNC defined by the map

$$\sigma : \quad (x_0, x_1) \longmapsto (H_0(x_0, x_1), \ldots, H_n(x_0, x_1)) \tag{3.4}$$

passes through the $n+3$ points $p_i \;\; (1 \le i \le n+3)$, since $\sigma(\mu_i, \nu_i) = p_i \;\; (1 \le i \le n+1)$, $\sigma(1, 0) = p_{n+2}$ and $\sigma(0, 1) = p_{n+3}$. Conversely any RNC passing through the points $p_i \;\; (1 \le i \le n+3)$ can be written in the form (3.4). This completes the proof of the lemma 9. #

Lemma 10 *Let $n \geq 2$ be an integer and $q \geq n+2$ be a prime power. The number of RNC in $PG(n, F_q)$ is*

$$q^{n(n+1)/2-1} \prod_{i=3}^{n+1} (q^i - 1).$$

Proof. We consider all sets, each of which consists of such $n+3$ points that any $n+1$ points among them are linearly independent. Let N denote the number of such sets. Suppose $\{p_1, p_2, \cdots, p_{n+3}\}$ be such a set. There are totally $(q^{n+1}-1)/(q-1)$ points in $PG(n, F_q)$. The point p_1 can be any point of $PG(n, F_q)$. So there are $(q^{n+1}-1)/(q-1)$ ways to choose p_1. After the points $p_1, \cdots, p_i \ \ (1 \leq i \leq n)$ have been chosen, the point p_{i+1} may have

$$\frac{q^{n+1}-1}{q-1} - \frac{q^i - 1}{q-1} = \frac{q^i(q^{n+1-i}-1)}{q-1}$$

choices, since there are $(q^i-1)/(q-1)$ points which are linearly dependent on $p_1, \cdots, p_i$. Now we suppose that the points $p_1, \cdots, p_{n+1}$ have been chosen. By taking a projective transformation, we can assume that the points $p_1, \cdots, p_{n+1}$ are of the form (3.3). Hence the point p_{n+2} is of the form $(a_0, \cdots, a_n)$ with $a_i \neq 0 \ \ (0 \leq i \leq n)$, it has

$$\frac{(q-1)^{n+1}}{q-1} = (q-1)^n$$

choices. Finally if the points $p_1, \cdots, p_{n+2}$ have been chosen, we can also assume that $p_1, \cdots, p_{n+1}$ are of the form in (3.3). Hence the point p_{n+3} is of the form $(b_0, \cdots, b_n)$ with $b_i \neq 0, \ \ b_i \neq b_j \ \ (0 \leq i < j \leq n)$, it has

$$(q-2)(q-3)\cdots(q-n-1)$$

choices. Therefore we have proved that

$$\begin{aligned} N &= \prod_{i=0}^{n} \frac{q^i(q^{n+1-i}-1)}{q-1} \cdot (q-1)^n \prod_{i=2}^{n+1} (q-i) \cdot ((n+3)!)^{-1} \\ &= q^{n(n+1)/2}((n+3)!)^{-1} \prod_{i=2}^{n+1} (q^i - 1)(q-i) \end{aligned}$$

By Lemma 9 and the fact that there are $q+1$ points on every RNC , it follows that the number of RNC in $PG(n, F_q)$ is

$$\frac{N}{C_{q+1}^{n+3}} = q^{n(n+1)/2-1} \prod_{i=3}^{n+1} (q^i - 1).$$

where C_{q+1}^{n+3} is the binomial coefficient. This completes the proof of Lemma 10. #

Let $\mathcal{M}$ denote the set of all points in $PG(n, F_q)$ and $\mathcal{E}$ the set of all RNC in $PG(n, F_q)$. The following theorem will prove that the pair $(\mathcal{M}, \mathcal{E})$ is a SPBD.

Theorem 11 *(Pei,[4]) Let $t \geq 5$ be an integer. For any prime power $q \geq t-1$ there exists a SPBD $t-(v,b,k;\lambda_1,\cdots,\lambda_t,0)$ where*

$$v=(q^{t-2}-1)/(q-1), \qquad k=q+1,$$
$$b=q^{(t-2)(t-3)/2-1}\prod_{i=3}^{t-2}(q^i-1),$$

and

$$\begin{aligned}
\lambda_1 &= q^{(t-2)(t-3)/2-1}\prod_{i=2}^{t-3}(q^i-1),\\
\lambda_r &= q^{(r+t-3)(t-2-r)/2}(q-1)^{r-2}\prod_{i=1}^{t-2-r}(q^i-1)\prod_{i=1}^{r-2}(q-i), \quad (2\leq r\leq t-3)\\
\lambda_{t-2} &= (q-1)^{t-4}\prod_{i=1}^{t-4}(q-i),\\
\lambda_{t-1} &= \prod_{i=2}^{t-3}(q-i).
\end{aligned}$$

(Here we use the convention that $\prod_{i=1}^{r-2}(q-i)=1$ if $r=2$.)

Proof. Take $PG(t-3,F_q)$ as the set of points and all RNC in $PG(t-3,F_q)$ as blocks. For any given t points of $PG(t-3,F_q)$, if any $t-2$ points among them are linearly independent, then there exists an unique RNC passing through them by Lemma 9, otherwise there is no RNC passing through them by Lemma 8. Thus $\lambda_t=1$.

Given any r $(1\leq r\leq t-2)$ points, if they are linearly dependent then there is no RNC passing through them, if they are linearly independent then by the proof of Lemma 10 there are λ_r RNC passing through them where

$$\begin{aligned}
\lambda_1 &= \prod_{i=1}^{t-3}\frac{q^{t-2}-q^i}{q-1}\cdot(q-1)^{t-3}\prod_{i=2}^{t-2}(q-i)\prod_{i=0}^{t-2}(q-i)^{-1}\\
&= q^{(t-2)(t-3)/2-1}\prod_{i=2}^{t-3}(q^i-1),\\
\lambda_r &= \prod_{i=r}^{t-3}\frac{q^{t-2}-q^i}{q-1}\cdot(q-1)^{t-3}\prod_{i=2}^{t-2}(q-i)\prod_{i=r-1}^{t-2}(q-i)^{-1}\\
&= q^{(r+t-3)(t-2-r)/2}(q-1)^{r-2}\prod_{i=1}^{t-2-r}(q^i-1)\prod_{i=1}^{r-2}(q-i), \quad (2\leq r\leq t-3)
\end{aligned}$$

and

$$\begin{aligned}
\lambda_{t-2} &= (q-1)^{t-3}\prod_{i=2}^{t-2}(q-i)\prod_{i=t-3}^{t-2}(q-i)^{-1} \\
&= (q-1)^{t-4}\prod_{i=1}^{t-4}(q-i).
\end{aligned}$$

Finally, for any given $t-1$ points, if there exist $t-2$ points among them which are linearly dependent, then there is no RNC passing through them, otherwise the number of RNC passing through them is λ_{t-1} where

$$\lambda_{t-1} = \prod_{i=2}^{t-2}(q-i)(q-t+2)^{-1} = \prod_{i=2}^{t-3}(q-i).$$

This completes the proof of Theorem 11. #

3.2 New family of optimal authentication schemes

Based on the SPBD constructed in the previous paragraph, we can construct a new family of optimal authentication schemes. Let the set of all points on the curve C be the set $\mathcal{S}$ of source states, and the set of all points in $PG(n, F_q)$ be the set $\mathcal{M}$ of encoded messages. The set $\mathcal{S}$ can be also understood as the union of all elements of F_q with an extra special element denoted by ∞. Let C^* be any RNC in $PG(n, F_q)$, take one fixed projective transformation T^* which carries C to C^* and define an encoding rule σ_{T^*} which acts on $\mathcal{S}$ in the following way:

$$\begin{aligned}
\sigma_{T^*}(\alpha) &= (1, \alpha, \cdots, \alpha^n)T^*, \qquad \alpha \in F_q \\
\sigma_{T^*}(\infty) &= (0, \cdots, 0, 1)T^*
\end{aligned}$$

Thus we obtain the set of encoding rules $\mathcal{E}$, the number of encoding rules is equal to the number of RNC in $PG(n, F_q)$, i.e.

$$|\mathcal{E}| = q^{n(n+1)/2-1}\prod_{i=3}^{n+1}(q^i - 1).$$

Prior to transmission the transmitter and receiver randomly choose a matrix T from $\mathcal{E}$. The receiver knows the matrix T and its inverse T^{-1}, therefore he can recover the source state s by calculating

$$\sigma_T(s)T^{-1}. \tag{3.5}$$

Only when the vector in (3.5) belongs to the set (3.1) the receiver accepts $\sigma_T(s)$ as authentic, otherwise he refuses it.

Assume that the random variables E and $S^r (1 \le r \le n+3)$ satisfy the conditions given in Theorem 7, then the probabilities P_r $(0 \le r \le n+2)$ of the authentication scheme achieve their lower bounds. Furthermore we have

$$\begin{aligned}
P_0 &= \frac{q^2-1}{q^{n+1}-1}, \\
P_1 &= \frac{q-1}{q^n-1}, \\
P_r &= \frac{(q-1)(q-r+1)}{q^{n+1}-q^r}, \quad (2 \le r \le n-1) \\
P_n &= \frac{q-n+1}{q^n}, \\
P_{n+1} &= \frac{q-n}{(q-1)^n}, \\
P_{n+2} &= \prod_{i=2}^{n}(q-i)^{-1}.
\end{aligned} \tag{3.6}$$

3.3 Encoding rules

We consider encoding rules of the authentication schemes constructed in the previous section. Let $PO_{n+1}(F_q)$ denote the subgroup of $PGL_{n+1}(F_q)$ consisting of projective transformations which carry the curve C into itself. Two projective transformations T_1 and T_2 carry the curve C into the same RNC if and only if they belong to the same coset of $PO_{n+1}(F_q)$ in $PGL_{n+1}(F_q)$. Thus we can take any representation system for cosets of $PO_{n+1}(F_q)$ in $PGL_{n+1}(F_q)$ as the set of encoding rules. To find such a representation system is not easy. We will give such a representation system for the case of $t = 5$ and q is odd later. Instead of choosing such a representation system we can also use the following way , which needs certain amount of calculation, to generate encoding rules. As mentioned above, the transmitter and receiver can determine an encoding rule by randomly choosing a non-singular matrix T of order $n+1$ over F_q. Suppose that the matrices T_1 and T_2 have been randomly chosen successively, it is necessary to check whether T_1 and T_2 belong to the same coset of $PO_{n+1}(F_q)$, i.e., to check whether $T_1T_2^{-1}$ is an element of $PO_{n+1}(F_q)$. This can be done by checking whether the point set (3.1) is carried into itself by the projective transformation $T_1T_2^{-1}$. Particularly, it is easy to see whether the point $(0, \cdots, 0, 1)T_1T_2^{-1}$ belongs to the set (3.1). If it is the case, we can try another matrix T_2 immediately. The probability of the event that $(0, \cdots, 0, 1)T_1T_2^{-1}$ belongs to the set (3.1) is small (see bellow).By this way we can successively choose several matrices T such that any two of them belong to the different cosets of $PO_{n+1}(F_q)$. This work can be done in advance of the transmission.

Since

$$|PGL_{n+1}(F_q)| = q^{n(n+1)/2}\prod_{i=2}^{n+1}(q^i-1)$$

we have, by Lemma 10, that

$$|PO_{n+1}(F_q)| = \frac{PGL_{n+1}(F_q)}{|E|} = q(q^2-1).$$

Therefore the probability of the event that two successively chosen matrices belong to the same coset of $PO_{n+1}(F_q)$ is

$$\frac{|PO_{n+1}(F_q)|-1}{|PGL_{n+1}(F_q)|-1} \sim q^{-(n-1)(n+3)}.$$

The probability of the event that the (n+1)-th row of $T_1T_2^{-1}$ is a point of the curve C is

$$\frac{(q+1)(q-1)}{q^{n+1}-1} \sim q^{-(n-1)}.$$

Let us come back to the problem: to find a representation system for cosets of $PO_{n+1}(F_q)$ in $PGL_{n+1}(F_q)$. At first we give the structure of the group $PO_{n+1}(F_q)$. For $0 \le i,\ \ k \le n$ and $t_1,\ \ t_2 \in F_q$, define

$$b_{i,k} = \begin{cases} C_k^i, & i \le k \\ 0, & i > k \end{cases}$$

and

$$c_{i,k} = \sum_{j=max(0,i-k)}^{min(i,n-k)} C_{n-k}^j C_k^{i-j} t_1^{k-(i-j)} t_2^{i-j}.$$

where C_k^i is the binomial coefficient. For any elements $a \in F_q^*$ (the set of non-zero elements of F_q) and $t \in F_q$, define two matrices:

$$\begin{aligned} T_{n+1}(a,t) &= (b_{i,k}a^i t^{k-i})_{(0\le i,k\le n)}, \\ Q_{n+1}(a,t) &= (b_{(n-i),k}a^{n-i}t^{k-n+i})_{(0\le i,k\le n)}. \end{aligned}$$

and for any elements $a \in F_q^*$ and $t_1, t_2 \in F_q$ with $t_1 \ne t_2$, define the matrix

$$R_{n+1}(a,t_1,t_2) = (c_{i,k}a^i)_{(0\le i,k\le n)}.$$

Theorem 12 *The group $PO_{n+1}(F_q)$ consists of the following $q(q^2-1)$ matrices:*

$$T_{n+1}(a,t), \qquad Q_{n+1}(a,t), \qquad R_{n+1}(a,t_1,t_2) \tag{3.7}$$

where $a \in F_q^*,\ \ t, t_1, t_2 \in F_q$ with $t_1 \ne t_2$. The number of elements for these three types is $q(q-1),\ \ q(q-1),\ \ q(q-1)^2$ respectively.

Proof. Since

$$|PO_{n+1}(F_q)| = \frac{|PGL_{n+1}(F_q)|}{|E|} = q(q^2-1),$$

it is only necessary to show that the set of points (3.1) is carried into itself by any matrix in (3.7). The last conclusion of the theorem is obvious.

We have

$$\sum_{i=0}^{n} b_{i,k} a^i t^{k-i} \alpha^i = \sum_{i=0}^{k} C_k^i (a\alpha)^i t^{k-i} = (t + a\alpha)^k,$$

hence

$$(1, \alpha, \cdots, \alpha^n) T_{n+1}(a,t) = (1, (t + a\alpha), \cdots, (t + a\alpha)^n).$$

Also we have

$$(0, \cdots, 0, 1) T_{n+1}(a,t) = (0, \cdots, 0, a^n).$$

This shows that $T_{n+1}(a,t) \in PO_{n+1}(F_q)$.

Similarly we have

$$(1, \alpha, \cdots, \alpha^n) Q_{n+1}(a,t) = \begin{cases} \alpha^n (1, t + a/\alpha, \cdots, (t + a/\alpha)^n), & \alpha \neq 0 \\ (0, \cdots, 0, a^n), & \alpha = 0 \end{cases}$$

and

$$(0, \cdots, 0, 1) Q_{n+1}(a,t) = (1, t, \cdots, t^n).$$

Therefore $Q_{n+1}(a,t) \in PO_{n+1}(F_q)$.

Finally, since

$$\begin{aligned} \sum_{i=0}^{n} c_{i,k} a^i \alpha^i &= \sum_{i=0}^{n} \sum_{j=max(0,i-k)}^{min(i,n-k)} C_{n-k}^j C_k^{i-j} t_1^{k-(i-j)} t_2^{i-j} (a\alpha)^i \\ &= \sum_{j=0}^{n-k} C_{n-k}^j (a\alpha)^j \sum_{s=0}^{k} C_k^s t_1^{k-s} (t_2 a\alpha)^s \\ &= (1 + a\alpha)^{n-k} (t_1 + t_2 a\alpha)^k, \end{aligned}$$

then

$$(1, \alpha, \cdots, \alpha^n) R_{n+1}(a, t_1, t_2)$$
$$= \begin{cases} (1 + a\alpha)^n (1, \frac{t_1 + t_2 a\alpha}{1 + a\alpha}, \cdots, \left(\frac{t_1 + t_2 a\alpha}{1 + a\alpha}\right)^n), & 1 + a\alpha \neq 0 \\ (0, \cdots, 0, (t_1 - t_2)^n), & 1 + a\alpha = 0 \end{cases}$$

Also

$$(0, \cdots, 0, 1) R_{n+1}(a, t_1, t_2) = a^n (1, t_2, \cdots, t_2^n).$$

Therefore $R_{n+1}(a, t_1, t_2) \in PO_{n+1}(F_q)$. Thus Theorem 12 is proved now. #

The elements with the form $T_{n+1}(a,t)$ form a subgroup of $PO_{n+1}(F_q)$ with the order $q(q+1)$. We denote this subgroup by T_{n+1}. A representation system for cosets of T_{n+1} in $PGL_{n+1}(F_q)$ will be given in Theorem 13.

Now we assume that $(q, n) = 1$.

Theorem 13 *All elements of $PGL_{n+1}(F_q)$ whose last two rows have the form*

$$\begin{array}{ccccccccccc} 0 & \cdots & 0 & 1 & x_{n-1,v+1} & \cdots & x_{n-1,u-1} & 0 & x_{n-1,u+1} & \cdots & x_{n-1,n} \\ 0 & \cdots & & & & & 0 & 1 & x_{n,u+1} & \cdots & x_{n,n} \end{array} \quad (v < u)$$

or

$$\begin{array}{cccccccccc} 0 & \cdots & 0 & 0 & & \cdots & 0 & 1 & x_{n-1,v+1} & \cdots & x_{n-1,n} \\ 0 & \cdots & 0 & 1 & x_{n,u+1} & \cdots & & & & & x_{n,n} \end{array} \quad (u < v)$$

form a representation system for cosets of T_{n+1} in $PGL_{n+1}(F_q)$.

Proof. Let $Y = (y_{i,j})$ be an element of $PGL_{n+1}(F_q)$. The last two rows of the product $T_{n+1}(a,t) \cdot Y$ have the form

$$\begin{array}{ccc} a^{n-1}(y_{n-1,0} + nty_{n,0}) & \cdots & a^{n-1}(y_{n-1,n} + nty_{n,n}) \\ a^n y_{n,0} & \cdots & a^n y_{n,n} \end{array}$$

Therefore any two elements, given in the theorem, corresponding to different values of u belong to different cosets. Now suppose that Y and $T_{n+1}(a,t) \cdot Y$ are two elements given in the theorem, corresponding to the same value of u, then it deduces that $a = 1, \quad t = 0$ (Notice that $(n,q) = 1$). Hence $T_{n+1}(a,t) = I$. This shows that any two elements given in the theorem belong to different cosets.

The number of the elements given in the theorem is

$$\begin{aligned} & \frac{q^{n+1}-1}{q-1} \cdot \frac{q^n - 1}{q-1} \cdot \prod_{i=2}^{n} (q^{n+1} - q^i) \\ &= q^{n(n+1)/2-1}(q+1) \prod_{i=3}^{n+1} (q^i - 1), \end{aligned}$$

which equals to

$$\frac{|PGL_{n+1}(Fq)|}{|T_{n+1}|} = \frac{q^{n(n+1)/2} \prod_{i=2}^{n+1} (q^i - 1)}{q(q-1)}.$$

This completes the proof of the theorem .

The following theorem gives a representation system for $PO_3(F_q)$ in $PGL_3(F_q)$. We omit its proof here.

Theorem 14 *The following $q^2(q^3-1)$ elements form a representation system for $PO_3(F_q)$ in $PGL_3(F_q)$:*

(i) $$\begin{pmatrix} x_{00} & x_{01} & x_{02} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad where \quad x_{00} \neq 0,$$

(ii) $$\begin{pmatrix} x_{00} & x_{01} & x_{02} \\ 1 & x_{11} & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad where \quad x_{00}x_{11} - x_{01} \neq 0,$$

(iii) $\begin{pmatrix} x_{00} & x_{01} & x_{02} \\ 0 & 0 & 1 \\ 0 & 1 & x_{22} \end{pmatrix}$ *where* $x_{00} \neq 0$,

(iv) $\begin{pmatrix} x_{00} & -x_{00}^2+k & x_{02} \\ 1 & 0 & x_{12} \\ 0 & 1 & x_{22} \end{pmatrix}$

where k *is a non-square element in* F_q^*, $x_{02} - x_{00}x_{12} + (x_{00}^2 - k)x_{22} \neq 0$, *and only one matrix is taken from the following two matrices:*

$$\begin{pmatrix} x_{00} & -x_{00}^2+k & x_{02} \\ 1 & 0 & x_{12} \\ 0 & 1 & x_{22} \end{pmatrix}, \qquad \begin{pmatrix} x_{00} & -x_{00}^2+k & x'_{02} \\ 1 & 0 & x'_{12} \\ 0 & 1 & x'_{22} \end{pmatrix}$$

with the relation

$$\begin{pmatrix} x'_{02} \\ x'_{12} \\ x'_{22} \end{pmatrix} = \begin{pmatrix} x_{00}^2/k & x_{00}(1-x_{00}^2/k) & k(1-x_{00}^2/k)^2 \\ 2x_{00}/k & 1-2x_{00}^2/k & -2x_{00}(1-x_{00}^2/k) \\ 1/k & -x_{00}/k & x_{00}^2/k \end{pmatrix} \begin{pmatrix} x_{02} \\ x_{12} \\ x_{22} \end{pmatrix}$$

(v) $\begin{pmatrix} x_{00} & x_{01} & x_{02} \\ 0 & 0 & 1 \\ 1 & x_{21} & x_{22} \end{pmatrix}$ *where* $x_{00} \neq 0$, $x_{01} - x_{00}x_{21} \neq 0$

and only one matrix is taken from the following two matrices:

$$\begin{pmatrix} x_{00} & x_{01} & x_{02} \\ 0 & 0 & 1 \\ 1 & x_{21} & x_{22} \end{pmatrix}, \qquad \begin{pmatrix} x_{00} & x_{00}x_{01} & x_{00}x_{02} \\ 0 & 0 & 1 \\ 1 & x_{01}/x_{00} & x_{02}/x_{00} \end{pmatrix}.$$

(vi) $\begin{pmatrix} x_{00} & x_{01} & x_{02} \\ 0 & 1 & x_{12} \\ 1 & x_{21} & x_{22} \end{pmatrix}$ *where* x_{00} *is a non−square element in* F_q^*,

there exist no elements r *and* $s \neq 0$ *such that* $x_{00} = r^2 - s^2$ *and* $x_{01} = x_{00}x_{21} - r$, *only* $q^3(q-1)^2/4$ *matrices among them are taken, any two of which belong to different cosets of* $PO_3(F_q)$.

The number of matrices in (i), (ii), (iii), (iv), (v) *and* (vi) *is* $q^2(q-1)$, $q^3(q-1)$, $q^3(q-1)$, $q^3(q-1)^2/4$, $q^3(q-1)^2/2$ *and* $q^3(q-1)^2/4$ *respectively.*

We have not been able to find a representation system for the $q^3(q-1)^2/4$ cosets in (vi). When we use the authentication code, to generate an encoding rule is to choose randomly a matrix among the representation system given in Theorem 14. If two successively chosen matrices belong to (vi), we must check whether they belong to the same coset of $PO_3(F_q)$.

Chapter 4

Authentication schemes with arbitration

We have discussed several properties of the authentication schemes with three participants: the information-theoretic bound for the success probability of spoofing attack, the lower bound for the number of encoding rules, the characterization of optimal schemes in Chapter 2. In this chapter we will discuss similar problems for the authentication schemes with arbitration.

4.1 Lower bounds

By the same method of Proposition 5 we can prove the information-theoretic bound for P_{O_r}, P_{R_r} and P_T respectively, and find the necessary and sufficient conditions for achieving these bounds.

Define the set

$$\mathcal{M}_R^r = \{m^r \in \mathcal{M}^r \mid \mathcal{E}_R(m^r) \neq \emptyset\}.$$

Proposition 15 *The inequality*

$$P_{O_r} \geq 2^{H(E_R|M^{r+1})-H(E_R|M^r)} \tag{4.1}$$

holds for any integer $r \geq 0$. *The equality holds iff for any* $m^r * m \in \mathcal{M}_R^{r+1}$, *the ratio*

$$\frac{p(f|m^r)}{p(f|m^r * m)}$$

is independent of m^r, m *and* $f \in \mathcal{E}_R(m^r * m)$. *When this equality holds, the probability* P_{O_r} *equals* $P(m|m^r)$, *and the above ratio also.*

Proposition 16 *The inequality*

$$P_{R_r} \geq 2^{H(E_T|E_R,M^{r+1})-H(E_T|E_R,M^r)} \tag{4.2}$$

holds for any integer $r \geq 0$. *The equality holds iff for any* $m^r * m \in \mathcal{M}_R^{r+1}$ *and* $f \in \mathcal{E}_R(m^r * m)$ *with* $\mathcal{E}_T(f, m^r * m) \neq \emptyset$ *the ratio*

$$\frac{p(e|f, m^r)}{p(e|f, m^r * m)}$$

is independent of m^r, m, $f \in \mathcal{E}_R(m^r * m)$ *and* $e \in \mathcal{E}_T(f, m^r * m)$. *When this equality holds, the probability* P_{R_r} *equals* $P(m|f, m^r)$ *and the above ratio also.*

Proposition 17 *The inequality*

$$P_T \geq 2^{H(E_R|E_T, M') - H(E_R|E_T)} \tag{4.3}$$

holds. The equality in it holds iff for any $e \in \mathcal{E}_T, m' \in \mathcal{M}'(e)$ *with* $\mathcal{E}_R(e, m') \neq \emptyset$ *the ratio*

$$\frac{p(f|e)}{p(f|e, m')}$$

is independent of e, m' *and* $f \in \mathcal{E}_R(e, m')$. *When this equality holds, the probability* P_T *equals* $P(m'|e)$ *and the above ratio also.*

The following two propositions give the lower bounds of $|\mathcal{E}_R|$ and $|\mathcal{E}_T|$ respectively.

Proposition 18 *The number of decoding rules of the receiver has the lower bound*

$$|\mathcal{E}_R| \geq (P_{O_0} P_{O_1} \cdots P_{O_{t-1}} P_T)^{-1} \tag{4.4}$$

(t is any positive integer.) Suppose that P_T *and* P_{O_r} $(0 \leq r \leq t-1)$ *achieve their lower bounds in (4.3) and (4.1), then the equality in (4.4) holds iff*

$$H(E_R|E_T, M') = 0, \quad H(E_R|M^t) = H(E_R|E_T)$$

and E_R *has a uniform probability distribution.*

Proof According to Propositions 15 and 17, we have

$$P_{O_0} P_{O_1} \cdots P_{O_{t-1}} P_T \geq 2^{H(E_R|M^t) - H(E_R) + H(E_R|E_T, M') - H(E_R|E_T)} \tag{4.5}$$

since

$$H(E_R|E_T, M') \geq 0, \tag{4.6}$$

$$H(E_R|M^t) \geq H(E_R|E_T) \tag{4.7}$$

and

$$|\mathcal{E}_R| \geq 2^{H(E_R)} \tag{4.8}$$

it follows that

$$|\mathcal{E}_R| \geq 2^{H(E_R)} \geq (P_{O_0} P_{O_1} \cdots P_{O_{t-1}} P_T)^{-1} \tag{4.9}$$

When P_{O_r} $(1 \leq r \leq t-1)$ and P_T achieve their lower bounds in (4.1) and (4.3) as assumed, the equality in (4.5) holds. Therefore the equality in (4.4) holds iff the equalities in (4.6), (4.7) and (4.8) hold. The equality of (4.8) means that E_R has a uniform probability distribution. #

Proposition 19 *The number of encoding rules of the transmitter has the lower bound*

$$|\mathcal{E}_T| \geq (P_{O_0} P_{O_1} \cdots P_{O_{t-1}} P_{R_0} \cdots P_{R_{t-1}})^{-1} \tag{4.10}$$

Suppose P_{O_r}, P_{R_r} ($0 \leq r \leq t-1$) achieve their lower bounds in (4.1) and (4.2), then $|\mathcal{E}_T|$ achieves its lower bound in (4.10) iff

$$H(E_T|E_R, M^t) = 0, \quad H(E_R|M^t) = H(E_R|E_T)$$

and E_T has a uniform distribution.

The proof of Proposition 19 is similar to that of Proposition 18.
Remark Since

$$\begin{aligned} H(E_T|E_R, M^t) &= H(E_R, E_T|M^t) - H(E_R|M^t) \\ &= H(E_T|M^T) + H(E_R|E_T) - H(E_R|M^t) \end{aligned}$$

The condition that $H(E_T|E_R, M^t)$=0 and $H(E_R|M^t) = H(E_R|E_T)$ is equivalent to that of $H(E_T|M^T) = 0$.

4.2 Combinatorial structure of optimal schemes with arbitration

Let us denote an authentication scheme with arbitration by $(\mathcal{S}, \mathcal{M}, \mathcal{E}_R, \mathcal{E}_T)$.

Definition 4 *If an authentication scheme $(\mathcal{S}, \mathcal{M}, \mathcal{E}_R, \mathcal{E}_T)$ satisfies the following conditions:*

(i) $P_{O_r} = 2^{H(E_R|M^{r+1}) - H(E_R|M^r)} \quad 0 \leq r \leq t-1$;

(ii) $P_{R_r} = 2^{H(E_T|E_R, M^{r+1}) - H(E_T|E_R, M^r)} \quad 0 \leq r \leq t-1$;

(iii) $P_T = 2^{H(E_R|E_T, M') - H(E_R|E_T)}$;

(iv) $|\mathcal{E}_R| = (P_{O_0} P_{O_1} \cdots P_{O_{t-1}} P_T)^{-1}$;

(v) $\mathcal{E}_T| = (P_{O_0} P_{O_1} \cdots P_{O_{t-1}} P_{R_0} \cdots P_{R_{t-1}})^{-1}$;

then the scheme is called optimal of order t.

We consider the combinatorial structure of the optimal schemes with arbitration. The following Corollary 20, 21 and 22 will provide a bridge between the information-theoretic lower bounds of P_{O_r}, P_{R_r} and P_T and the combinatorial structure of optimal scheme.

Corollary 20 *Suppose that E_R has a uniform probability distribution and*

$$P_{O_r} = 2^{H(E_R|M^{r+1}) - H(E_R|M^r)}, 0 \leq r \leq t-1 \tag{4.11}$$

Then for any $m^r * m \in \mathcal{M}_R^{r+1}$, we have

$$P_{O_r} = |\mathcal{E}_R(m^r * m)|/|\mathcal{E}_R(m^r)|, \qquad 0 \le r \le t-1.$$

here $\mathcal{E}_R(m^0) = \mathcal{E}_R$.

Proof If $\mathcal{R}(m^r * m) \neq \emptyset$ it follows from Proposition 15 and the assumption (1.1) that for any $f \in \mathcal{E}_R(m^r * m)$,

$$\begin{aligned}
P_{O_r} &= p(f|m^r)/p(f|m^r * m) \\
&= p(f, m^r)p(m^r * m)/p(f, m^r * m)p(m^r) \\
&= p(f) \sum_{e \in \mathcal{E}_T(f, m^r)} p(e|f)p(f(m^r)) \\
&\times \big(p(f) \sum_{e \in \mathcal{E}_T(f, m^r * m)} p(e|f)p(f(m^r))\big)^{-1} \\
&\times \sum_{f' \in \mathcal{E}_R(m^r * m)} p(f') \sum_{e' \in \mathcal{E}_T(f', m^r * m)} p(e'|f')p(f'(m^r * m)) \\
&\times \big(\sum_{f' \in \mathcal{E}_R(m^r)} p(f') \sum_{e' \in \mathcal{E}_T(f', m^r)} p(e'|f')p(f'(m^r))\big)^{-1} \qquad (4.12)
\end{aligned}$$

Now we prove by induction on r that the summation

$$\sum_{e \in \mathcal{E}_T(f, m^r * m)} p(e|f)p(f(m^r * m)), \; 0 \le r \le t-1 \qquad (4.13)$$

does not depend on $f \in \mathcal{E}_R(m^r * m)$.

When $r = 0$, we have from (4.12) that

$$\begin{aligned}
P_{O_0} &= p(f)p(m)/p(f, m) \\
&= \sum_{f' \in \mathcal{E}_R(m)} p(f') \sum_{e \in \mathcal{E}_T(f', m)} p(e|f')p(f'(m)) \Big/ \sum_{e \in \mathcal{E}_T(f, m)} p(e|f)p(f(m))
\end{aligned}$$

which does not depend on $f \in \mathcal{E}_R(m)$, therefore the summation in its denominator does not depend on f too. Now we suppose that the summation of (4.13) does not depend on $f \in \mathcal{E}_R(m^u)$ for $r = u < t-1$, then it follows also from (4.12) that

$$\begin{aligned}
P_{O_u} &= \sum_{f' \in \mathcal{E}_R(m^u * m)} p(f') \sum_{e \in \mathcal{E}_T(f', m^u * m)} p(e|f')p(f'(m^u * m)) \\
&\times \Big(\sum_{e \in \mathcal{E}_T(f, m^u * m)} p(e|f)p\big(f(m^u * m)\big) \sum_{f' \in \mathcal{E}_R(m^u)} p(f') \Big)^{-1}
\end{aligned}$$

which does not depend on $f \in \mathcal{E}_R(m^u * m)$. Hence the summation of (4.13) for $r = u + 1$ does not depend on $f \in \mathcal{E}_R(m^u * m)$.

It follows from (4.12) that

$$P_{O_r} = \sum_{f \in \mathcal{E}_R(m^r \star m)} p(f) \Big/ \sum_{f \in \mathcal{E}_R(m^r)} p(f) = \big|\mathcal{E}_R(m^r \star m)\big| \big/ \big|\mathcal{E}_R(m^r)\big|$$

where the second equality uses the assumption that E_R has a uniform distribution. #

For a given $f \in \mathcal{E}_R$, let $E_T(f)$ denote the random variable of valid encoding rules of f, it takes its values from $\mathcal{E}_T(f)$. Similarly, for a given $e \in \mathcal{E}_T$, let $E_R(e)$ denote the random variable of decoding rules of which e is valid, it takes its values from $\mathcal{E}_R(e)$.

Corollary 21 *For any given $f \in \mathcal{E}_R$, suppose that $E_T(f)$ has a uniform probability distribution and*

$$P_{R_r} = 2^{H(E_T|E_R,M^{r+1})-H(E_T|E_R,M^r)}, 0 \le r \le t-1 \tag{4.14}$$

Then for any $m^r * m \in \mathcal{M}_R^{r+1}$, $f \in \mathcal{E}_R(m^r * m)$ with $\mathcal{E}_T(f, m^r * m) \neq \emptyset$,

$$P_{R_r} = |\mathcal{E}_T(f, m^r * m)|/|\mathcal{E}_T(f, m^r)|.$$

Proof If $\mathcal{E}_T(f, m^r \star m) \neq \emptyset$, it follows from Proposition 16 and the assumption (1.1) that for any $e \in \mathcal{E}_T(f, m^r \star m)$,

$$\begin{aligned}
P_{R_r} &= p(e|f, m^r)/p(e|f, m^r * m) \\
&= p(e, f, m^r)p(f, m^r * m)/p(e, f, m^r * m)p(f, m^r) \\
&= p\big(f(m^r)\big) \sum_{e' \in \mathcal{E}_T(f, m^r * m)} p(e'|f)p\big(f(m^r * m)\big) \\
&\times \left(p\big(f(m^r * m)\big) \sum_{e' \in \mathcal{E}_T(f, m^r)} p(e'|f)p\big(f(m^r)\big)\right)^{-1} \\
&= \sum_{e' \in \mathcal{E}_T(f, m^r * m)} p(e'|f) \Big/ \sum_{e' \in \mathcal{E}_T(f, m^r)} p(e'|f) \\
&= |\mathcal{E}_T(f, m^r * m)| \,/\, |\mathcal{E}_T(f, m^r)|. \quad \#
\end{aligned}$$

Corollary 22 *For any given $e \in \mathcal{E}_T$, suppose that $E_R(e)$ has a uniform probability distribution and*

$$P_T = 2^{H(E_R|E_T,M')-H(E_R|E_T)}, \tag{4.15}$$

Then for any $e \in \mathcal{E}_T$, $m' \in \mathcal{M}'(e)$ with $\mathcal{E}_R(e, m') \neq \emptyset$,

$$P_T = |\mathcal{E}_R(e, m')|/|\mathcal{E}_R(e)|.$$

Proof It follows from Proposition 17 that for any $e \in \mathcal{E}_T$, $m' \in \mathcal{M}/\mathcal{M}(e)$ with $\mathcal{E}_R(e, m') \neq \emptyset$,

$$P_T = P(m'|e) = \sum_{f \in \mathcal{E}_R(e, m')} p(f|e) = |\mathcal{E}_R(e, m')|/|\mathcal{E}_R(e)|. \quad \#$$

The optimal schemes have a requirement for the probability distributions of $\mathcal{S}^r$.

Corollary 23 *Suppose (4.11) and (4.14) hold. Then for any $m^r \in \mathcal{M}_R^r$, the probability $p(f(m^r))$ does not depend on $f \in \mathcal{E}_R(m^r)$ $(1 \le r \le t)$.*

Proof In the proof of Corollary 20 and 21 it is shown that

$$\sum_{e\in\mathcal{E}_T(f,m^r)} p(e|f)p\big(f(m^r)\big)$$

does not depend on $f \in \mathcal{E}_R(m^r)$ and

$$\sum_{e\in\mathcal{E}_T(f,m^r)} p(e|f) = P_{R_0}P_{R_1}\cdots P_{R_{r-1}}$$

The conclusion follows immediately. #

Now we show that for an optimal scheme the number $|\mathcal{M}(f,s)|$ is a constant for any $f \in \mathcal{E}_R$ and $s \in S$.

Corollary 24 *If* $P_{R_0} = 2^{H(E_T|E_R,M)-H(E_T|E_R)}$ *then* $|\mathcal{M}(f,s)| = c$ *is a constant for any* $f \in \mathcal{E}_R$ *and* $s \in \mathcal{S}$. *Furthermore* $c = P_{R_0}^{-1}$.

Proof Given a decoding rule f, we have assumed that for any $m \in \mathcal{M}(f)$ there exists at least one encoding rule e such that $m \in \mathcal{M}(e)$. Hence $P(m|f) > 0$ for any $m \in \mathcal{M}(f)$. If P_{R_0} achieves its information–theoretic lower bound, P_{R_0} equals $P(m|f)$ for any $f \in \mathcal{E}_R$ and $m \in \mathcal{M}(f)$ by Proposition 16. Since

$$\sum_{m\in\mathcal{M}(f,s)} P(m|f) = 1$$

for any $s \in \mathcal{S}$, it follows that $|\mathcal{M}(f,s)| = P_{R_0}^{-1}$. #

Definition 5 *Let* v, b, k, c, λ, t *be positive integers. A PBD* t*-design* $(\mathcal{M}, \mathcal{E})$ *is called restricted (RPBD* t*-design) if* $|\mathcal{M}| = v, \mathcal{E} = (\mathcal{E}_1, \cdots, \mathcal{E}_b)$*, each block* $\mathcal{E}_i$ *is divided into* k *groups, each group has* c *points of* $\mathcal{M}$*. Any* t*-subset of* $\mathcal{M}$ *either occurs in exactly* λ *blocks in such a way that each point of the* t*-subset occupies one group, or does not exist such blocks at all.*

Similarly we can introduce RSPBD $t-(v, b, k, c; \lambda_1, \lambda_2, \cdots, \lambda_t, 0)$.

Our main result is the following theorem.

Theorem 25 *(Pei and Li [5], [6]) The necessary and sufficient conditions for a scheme* $(\mathcal{S}, \mathcal{M}, \mathcal{E}_R, \mathcal{E}_T)$ *being optimal are as follows.*

(i) E_T, E_R, $E_T(f)$ $(\forall f \in \mathcal{E}_R)$ *and* $E_R(e)$ $(\forall e \in \mathcal{E}_T)$ *have uniform probability distribution.*

(ii) *For any given* $m^r \in \mathcal{M}_R^r$*, the probability* $p(\mathcal{S}^r = f(m^r))$ *is constant for all* $f \in \mathcal{E}_R(m^r)$.

(iii) *For any given* $e \in \mathcal{E}_T$ *the pair*

$$(\mathcal{M}'(e), \{\mathcal{M}'_f(e)|f \in \mathcal{E}_R(e)\})$$

is a $1-(v-k, P_T^{-1}, k(c-1); 1, 0)$ *design where* $v = |M|$, $k = |\mathcal{S}|$, c *is a positive integer (in fact,* $c = |\mathcal{M}(f,s)|$ *for all* $f \in \mathcal{E}_R, s \in \mathcal{S}$*).*

(iv) *For any given* $f \in \mathcal{E}_R$*, the pair*

$$(\mathcal{M}(f), \{\mathcal{M}(e)|e \in \mathcal{E}_T(f)\})$$

is a SPBD t*-*$(kc, (P_{R_0}P_{R_1}\cdots P_{R_{t-1}})^{-1}, k; \lambda_1, \cdots, \lambda_t, 0)$ *where* $\lambda_t = 1, \lambda_r = (P_{R_r}\cdots P_{R_{t-1}})^{-1}, 1 \le r \le t-1$.

(v) *The pair*

$$(\mathcal{M}, \{\mathcal{M}(f) | f \in \mathcal{E}_R\})$$

is a RSPBD t-$(v, (P_{O_0} \cdots P_{O_{t-1}} P_T)^{-1}, k, c; \mu_1, \cdots, \mu_t, 0)$ *where*

$$\mu_t = P_T^{-1}, \mu_r = (P_{O_r} \cdots P_{O_{t-1}} P_T)^{-1}, 1 \le r \le t-1.$$

Proof Suppose the scheme ($\mathcal{S}$, $\mathcal{M}$, $\mathcal{E}_R$, $\mathcal{E}_T$) is optimal first. We prove the conditions (i)–(v) are satisfied.

According to Proposition 18 and 19, E_T and E_R has uniform probability distribution. It will be proved that $E_T(f)$ and $E_R(e)$ also have uniform probability distribution later on. The condition (ii) is nothing but Corollary 23.

For any given $e \in \mathcal{E}_T$ we have $|\mathcal{M}'(e)| = v - k$ and $|\mathcal{M}'_f(e)| = k(c-1)$ for any $f \in \mathcal{E}_R(e)$ by Corollary 24. Since

$$H(E_R | E_T, M') = -\sum p(f, e, m') \log p(f | e, m') = 0$$

by Proposition 4, it deduced that $\mathcal{E}_R(e, m') = \emptyset$ or $|\mathcal{E}_R(e.m')| = 1$ for any m'. The number of messages m' such that $|\mathcal{E}_R(e, m')| = 1$ is $k(c-1)|\mathcal{E}_R(e)|$. Thus

$$\begin{aligned} k(c-1)|\mathcal{E}_R(e)|P_T &= \sum_{m' : \mathcal{E}_R(e,m')|=1} \sum_{f \in \mathcal{E}_R(e,m')} p(f|e) \\ &= \sum_{f \in \mathcal{E}_R(e)} p(f|e) \sum_{m' \in \mathcal{M}'_f(e)} 1 = k(c-1). \end{aligned}$$

Hence $|\mathcal{E}_R(e)| = P_T^{-1}$. This proves (iii).

The above argument also shows that $p(f|e) = P_T$ for any $f \in \mathcal{E}_R(e)$, i.e. $E_R(e)$ has also a uniform probability distribution. Furthermore since

$$p(e|f) = \tfrac{p(e)p(f|e)}{p(f)}$$

$E_T(f)$ has also a uniform probability distribution. Thus the condition (i) is satisfied.

For any given $f \in \mathcal{E}_R$, we have $|\mathcal{M}(f)| = kc$ and $|\mathcal{M}(e)| = k$ for any $e \in \mathcal{E}_T(f)$. Take any r messages $m^r = (m_1, \cdots, m_r)$ from $\mathcal{M}(f)$, then $m_i \in \mathcal{M}(e)\,(1 \le i \le r)$ if and only if $e \in \mathcal{E}_T(f, m^r)$. We have $|H(E_T | E_R, M^t)| = 0$ by Proposition 19. It deduced that $|\mathcal{E}_T(f, m^t)| = 0$ or 1 as above. This means that $\lambda_t = 1$. Suppose that $|\mathcal{E}_T(f, m^t)| = 1$ for some m^t, it follows that

$$|\mathcal{E}_T(f)| = \left(P_{R_0} \cdots P_{R_{t-1}}\right)^{-1}$$

by Corollary 21 (Notice that $E_R(f)$ has a uniform probability distribution). If $\mathcal{E}_T(f, m^r) \neq \emptyset$ for some m^r $(1 \le r \le t-1)$, we can also obtain

$$\lambda_r = |\mathcal{E}_T(f, m^r)| = \left(P_{R_r} \cdots P_{R_{t-1}}\right)^{-1}$$

by Corollary 16. This proves (iv).

Take any $m^r = (m_1, \cdots, m_r)$, then $m_i \in \mathcal{M}(f)\,(1 \le i \le r)$ and each m_i occupies one different $\mathcal{M}(f, s)$ if and only if $f \in \mathcal{E}_R(m^r)$. Since E_R has a uniform probability distribution, it follows from Corollary 20 that

$$|\mathcal{E}_R(m^t)| = |\mathcal{E}_R| P_{O_0} \cdots P_{O_{t-1}} = P_T^{-1}$$

when $\mathcal{E}_R(m^t) \neq \emptyset$ for some m^t. This means $\mu_t = P_T^{-1}$. If $E_R(m^r) \neq \emptyset$ for some m^r $(1 \le r \le t-1)$ it also can be shown that

$$\mu_r = |\mathcal{E}_R(m^r)| = (P_{O_r} \cdots P_{O_{t-1}})^{-1}$$

by Corollary 6. This proves (v).

Conversely we suppose the conditions (i)–(v) hold now. We prove the scheme $(\mathcal{S}, \mathcal{M}, \mathcal{E}_R, \mathcal{E}_T)$ is optimal.

Given any $m^r * m \in \mathcal{M}_R^{r+1}$ and $f \in \mathcal{E}_R(m^r * m)\,(0 \le r \le t-1)$. Using the conditions (i), (ii) and (v) it follows from (4.12) that

$$\tfrac{p(f)}{p(f|m)} = \tfrac{|\mathcal{E}_R(m)|}{|\mathcal{E}_R|} = \tfrac{\mu_1}{|\mathcal{E}_R|}$$

and

$$\tfrac{p(f|m^r)}{p(f|m^r * m)} = \tfrac{|\mathcal{E}_R(m^r * m)|}{|\mathcal{E}_R(m^r)|} = \tfrac{\mu_{r+1}}{\mu_r},\ (1 \le r \le t-1).$$

This shows P_{O_r} $(0 \le r \le t-1)$ achieve their low bounds by Proposition 15.

Similarly we can calculate

$$\tfrac{p(e|f)}{p(e|f,m)} = \tfrac{|\mathcal{E}_T(f,m)|}{|\mathcal{E}_T(f)|} = P_{R_0},$$

$$\tfrac{p(e|f,m^r)}{p(e|f,m^r \star m)} = \tfrac{|\mathcal{E}_T(f,m^r \star m)|}{|\mathcal{E}_T(f,m^r)|} = \tfrac{\lambda_{r+1}}{\lambda_r},\ (1 \le r \le t-1).$$

for any $m^r \star m \in \mathcal{M}_R^{r+1}$, $f \in \mathcal{E}_R(m^r \star m)$ and $e \in \mathcal{E}_T(f, m^r \star m)$, and

$$\sum_{f \in \mathcal{E}_R(e,m')} p(f|e) = \tfrac{|\mathcal{E}_R(e,m')|}{|\mathcal{E}_R(e)|} = P_T$$

for any $e \in \mathcal{E}_T$, $m' \in \mathcal{M}'(e)$ and $f \in \mathcal{E}_R(e, m')$. This shows that P_{R_r} $(0 \le r \le t-1)$ and P_T achieve their low bounds by Proposition 16 and 17.

It follows from (v) that $|\mathcal{E}_R| = (P_{O_0} \cdots P_{O_{t-1}} P_T)^{-1}$ which means $|\mathcal{E}_R|$ achieves its low bound. We see that $|\mathcal{E}_T(f)| = (P_{R_0} \cdots P_{R_{t-1}})^{-1}$ for any f and $|\mathcal{E}_R(e)| = P_T^{-1}$ for any e by (iv) and (iii) respectively. Hence

$$|\mathcal{E}_T| = \tfrac{|\mathcal{E}_R||\mathcal{E}_T(f)|}{|\mathcal{E}_R(e)|} = (P_{O_0} \cdots P_{O_{t-1}} P_{R_0} \cdots P_{R_{t-1}})^{-1}.$$

This completes the proof of Theorem 25. #

Bibliography

[1] T. Beth, D. Jungnichel and H. Lenz. *Design Theory.* Bibligrahpisches Institut Mannheim, 1986.

[2] J. L. Massey. *Cryptography - a selective survey.* Alta Frequenza, LV(1)(1986), 4-11.

[3] D.Pei. *Information-theoretic bounds for authentication codes and block designs.* J. of Cryptology, 8(1995), 177-188.

[4] D. Pei. *A problem of combinatorial designs related to authentication codes.* J. of Combinatorial Designs, 417-429.

[5] D. Pei, Y. Li, Y. Wang and R. Safavi-Naini. *Characterization of authentication codes with arbitration.* Lecture Notes in Computer Science, Vol. 1587, Springer-Verlag 1999, 303-313.

[6] D. Pei and Y. Li. *Optimal authentication codes with arbitration.* preprint.

[7] R. Safavi-Naini and L. Tombak. *Optimal authentication system.* Lecture Notes in Computer Science, Vol. 765, Springer-Verlag, Berlin, 1994, 12-27.

[8] G. L. Simmons. *Authentication theory/coding theory.* Advances in Cryptology - Crypto'84, Lecture Notes in Computer Science, Vol. 196, Springer-Verlag, Berlin 1985, pp. 411-431.

[9] G. J. Simmons. *Message authentication with arbitration of transmitter/receiver disputes.* Advances in Cryptology-Eurocrypt'87, LNCS 304, Springer-Verlag, 1988, 151-165.

[10] G.J.Simmons. *A Cartesian product construction for unconditionally secure authentication codes that permit arbitration.* J.Cryptology, Vol.2(1990), 77-104.

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

[12] D. K. Ray-Chaudhuri. *Application of the geometry of quadrics for constructing PBIB design.* Annals of Mathematical Statistics, 33 (1962), 1175-1186.