ON THE CONSTRUCTION OF AUTHENTICATION CODES THAT PERMIT ARBITRATION OVER PROJECTIVE SPACES

LI RUIHU

Abstract. A family of authentication codes with arbitration are constructed over projective spaces, the parameters and the probabilities of deceptions of the codes are also computed. In a special case, a perfect authentication code with arbitration is obtained.

§ 1 Introduction

In the model of normal authentication (A-code), the transmitter and the receiver are using the same encoding rule and are thus trusting each other. However, it is not always the case that the two communicating parties want to trust each other. Inspired by this problem, Simmons has introduced an extended authentication model, here referred to as an authentication model with arbitration (A²-code). This model is taken against deception from both outsider (opponent) and insider (transmitter and receiver). The model includes four persons: the transmitter, the receiver, the opponent and the arbiter. The arbiter has access to all key information and is by definition not cheating. The arbiter does not take part in any communication activities on the channel but has to solve disputes between the transmitter and the receiver whenever such occur.

Let $\mathcal{S}$, $\mathcal{E}_T$, $\mathcal{E}_R$, and $\mathcal{M}$ be four nonempty finite sets, and $f: \mathcal{S} \times \mathcal{E}_T \to \mathcal{M}$ and $g: \mathcal{M} \times \mathcal{E}_R \to \mathcal{S} \cup \{\text{reject}\}$ be two maps; the sextuple $(\mathcal{S}, \mathcal{E}_T, \mathcal{E}_R, \mathcal{M}, f, g)$ is called an authentication code that permits arbitration if:

1. The map $f: \mathcal{S} \times \mathcal{E}_T \to \mathcal{M}$ and the map $g: \mathcal{M} \times \mathcal{E}_R \to \mathcal{S} \cup \{\text{reject}\}$ are surjective.
2. For any $M \in \mathcal{M}$ and $E_T \in \mathcal{E}_T$, if there is an $S \in \mathcal{S}$, satisfying $f(S, E_T) = M$, then such an $S$ is uniquely determined by the given $M$ and $E_T$.
3. $P(E_T, E_R) \neq 0$ and $f(S, E_T) = M$ implies $g(M, E_R) = S$, otherwise $g(M, E_R) = \{\text{reject}\}$.

Keywords: Authentication codes, arbiter, projective space.
Let \((\mathcal{S}, \mathcal{E}_F, \mathcal{E}_R, \mathcal{M}, f, g)\) be an \(A^2\)-code, \(\mathcal{S}, \mathcal{E}_F, \mathcal{E}_R\) and \(\mathcal{M}\) are called the set of source state, the set of transmitter’s encoding rule, the set of receiver’s encoding rule and the set of message, respectively.

There are five different kinds of attacks to cheat which are possible. The attacks are the following:

I (Impersonation by the opponent). The opponent sends a message to the receiver and succeeds if the message is accepted by the receiver as authentic.

S (Substitution by the opponent). The opponent observes a message that is transmitted and substitutes this message with another. The opponent succeeds if this another message is accepted by the receiver as authentic.

T (Impersonation by the transmitter). The transmitter sends a message to the receiver and denies having sent it. The transmitter succeeds if the message is accepted by the receiver as authentic and if the message is not one of the messages that the transmitter could generate due to his encoding rule.

Ro(Impersonation by the receiver). The receiver claims to have received a message from the transmitter. The receiver succeeds if this message could have been generated by the transmitter due to his encoding rule.

R₁ (Substitution by the receiver). The receiver receives a message from the transmitter but claims to have received another message. The receiver succeeds if this another message could have been generated by the transmitter due to his encoding rule.

For each way of cheating, we denote the probability of success with \(P_i, P_s, P_T, P_{Ro}\) and \(P_{R₁}\), respectively.

Definition. An \(A^2\)-code \((\mathcal{S}, \mathcal{E}_F, \mathcal{E}_R, \mathcal{M}, f, g)\) is called perfect, if

\[
\frac{1}{P_iP_sP_T} = |\mathcal{E}_R| \quad \text{and} \quad \frac{1}{P_iP_sP_{Ro}P_{R₁}} = |\mathcal{E}_F|.
\]

§ 2 Preliminaries

Let \(n\) be an integer, \(n \geq 1\) and \(F_q^{(n+1)}\) be the \((n+1)\)-dimensional row vector space over \(F_q\). Let \(PG(n,F_q)\) be the \(n\)-dimensional projective space over \(F_q\), the elements of \(PG(n,F_q)\) are called points, every point of \(PG(n,F_q)\) is a 1-dimensional subspace of \(F_q^{(n+1)}\). The \((r+1)\)-dimensional subspace of \(F_q^{(n+1)}\) now will be called \(r\)-flat in \(PG(n,F_q)\), if \(P\) is an \(r\)-flat in \(PG(n,F_q)\), then the corresponding \((r+1)\)-dimensional subspace in \(F_q^{(n+1)}\) will be denoted by \(P\). From[3] we have:

**Proposition 1.** For \(0 \leq r \leq n\), the set of \(r\)-flats in \(PG(n,F_q)\) and the set of \((r+1)\)-dimensional subspaces in \(F_q^{(n+1)}\) are in one-to-one correspondence.

**Proposition 2.** The group \(PGL_{n+1}(F_q)\) is transitive on the set of \(r\)-flats \((0 \leq r \leq n)\).

Let \(R_1\) and \(R_2\) be two flats in \(PG(n,F_q)\), the set of points contained in both \(R_1\) and \(R_2\)