On the Construction of Perfect Authentication Codes that Permit Arbitration

Thomas Johansson

Department of Information Theory, Lund University
Box 118, S-221 00 Lund, Sweden

Abstract. [1] Authentication codes that permit arbitration are codes that unconditionally protect against deceptions from the outsiders and additionally also protect against some forms of deceptions from the insiders. Simmons introduced this authentication model and he also showed a way of constructing such codes, called the Cartesian product construction. We present a general way of constructing such codes and we also derive two specific classes of such codes. One that is perfect in the sense that it meets the lower bounds on the size of the transmitter's and the receiver's keys and one that allows the number of source states to be chosen arbitrarily large.

1 Introduction

The purpose of traditional authentication codes is to protect the transmitter and the receiver from active deceptions from a third party, often called the opponent. The attacks are of two different types, impersonation and substitution. A model for this case has been developed and many different ways of constructing such codes have been proposed, [1] - [7]. However, the model is restricted in the sense that the transmitter and the receiver must both trust each other in not cheating, since they are using the same key. But it is not always the case that the two communicating parties want to trust each other. In fact, it may be that the transmitter sends a message and then later denies having sent it. Or the other way around, the receiver may claim to have received a message that was never sent by the transmitter.

Inspired by this problem Simmons has introduced an extended authentication model, referred to as the *authentication model with arbitration*, [8], [9]. Here caution is taken both against deceptions from the outsiders (opponent) and also against some forms of deceptions from the insiders (transmitter and receiver). The model includes a fourth person, called the *arbiter*. The arbiter has access to all key information and is by definition not cheating. Codes which take caution against all these kinds of deceptions are called *authentication codes that permit arbitration*, or simply A^2-codes. One proposed construction of A^2-codes is the Cartesian product construction due to Simmons, [8]. In [10] lower bounds on

---

[1] This work was supported by the TFR grant 222 92-662

D.R. Stinson (Ed.): Advances in Cryptology - CRYPTO '93, LNCS 773, pp. 343-354, 1994.
© Springer-Verlag Berlin Heidelberg 1994

the probability of success for the different kinds of deceptions were given. Also lower bounds on the number of messages and the number of encoding rules for a fixed probability of deception were given. The A^2-codes which meet these lower bounds with equality are referred to as *equitably perfect* A^2-codes.

It is easily checked that codes obtained from the Cartesian product construction are not equitably perfect. In fact, the size of the keys grows exponentially with the number of source states. In this paper we consider the problem of constructing more efficient classes of A^2-codes. In Section 2 we give a detailed description of the model of authentication with arbitration. In Section 3 we introduce a general technique to construct A^2-codes and in Section 4 we use this to give two constructions, one that is equitably perfect and one that allows the number of source states to be chosen arbitrarily large.

2 The model of authentication with arbitration

In this model there are four different participants. These are the *transmitter*, the *receiver*, the *opponent* and the *arbiter*. The transmitter wants to transmit some information, which we call a *source state*, to the receiver in such a way that the receiver can recover the transmitted source state and also verify that the transmitted message came from the legal transmitter. This is done by mapping a source state S from the set $\mathcal{S}$ of possible source states to a message M from the set $\mathcal{M}$ of possible messages. The message is then transmitted over the channel. The mapping from $\mathcal{S}$ to $\mathcal{M}$ is determined by the transmitters secret encoding rule E_T chosen from the set $\mathcal{E_T}$ of possible encoding rules. Thus we assume that the transmitter uses a mapping f such that:

$$f : S \times E_T \rightarrow M, \tag{1}$$

$$f(s, e_t) = f(s', e_t) \Rightarrow s = s'. \tag{2}$$

To be able to uniquely determine the source state from the transmitted message, we have property (2). The opponent has access to the channel in the sense that he can either impersonate a message or substitute a transmitted message for another. When the receiver receives a message that was transmitted, he must check whether this message is valid or not. For this purpose we assume that the receiver uses a mapping g from his own secret encoding rule E_R taken from the set $\mathcal{E_R}$ of possible encoding rules and from the messages $\mathcal{M}$, that determine if a message is valid and if so also the source state.

$$g : M \times E_R \rightarrow S \cup \{\text{FRAUD}\}, \tag{3}$$

$$P(e_t, e_r) \neq 0, f(s, e_t) = m \Rightarrow g(m, e_r) = s. \tag{4}$$

Since all messages generated by the transmitter are valid messages and since the receiver must be able to determine which of the source states that was transmitted, the property (4) must hold for all possible pairs (E_T, E_R). However, in general not all pairs (E_T, E_R) will be possible.

The arbiter is the supervisory person who has access to all information, including E_T and E_R. However, he does not take part in any communication activities on the channel and his only task is to solve disputes between the transmitter and the receiver whenever such occur. As said before, the arbiter is by definition not cheating. This is an assumption which can be removed if we want to consider an even more general model of authentication, where the arbiter may also cheat. See [11] and [12] for details.

There are five different kinds of attacks to cheat which are possible in this model. 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 for another. The opponent succeeds if the receiver accepts this other message as authentic.

T, Impersonation by the transmitter. The transmitter sends a message to the receiver. The transmitter succeeds if the message is accepted by the receiver as authentic and if the message is not one of those messages that the transmitter can generate due to his own encoding rule.

$\mathbf{R_0}$, Impersonation by the receiver. The receiver claims to have received a message from the transmitter. The receiver succeeds if the message could have been generated by the transmitter due to his encoding rule.

$\mathbf{R_1}$, Substitution by the receiver. The receiver receives a message from the transmitter but claims to have received another message. The receiver succeeds if this other message could have been generated by the transmitter due to his encoding rule.

In all these possible attacks to cheat it is understood that the cheating person is using an optimal strategy when choosing a message, or equivalently, that the cheating person chooses the message that maximizes his chances of success. For each way of cheating, we denote the probability of success with P_I, P_S, P_T, P_{R_0} and P_{R_1}. The *overall probability of deception* is denoted P_D and is defined to be

$$P_D = \max(P_I, P_S, P_T, P_{R_0}, P_{R_1}).$$

The setup of the encoding rules may be done in several ways. One possible way is by letting the receiver choose his own encoding rule E_R and then secretly pass this on to the arbiter. The arbiter then constructs the encoding rule E_T and pass this on to the transmitter. Another way is to do the other way around and a third way is to allow the arbiter to construct both the encoding rules.

A traditional A-code is sometimes denoted $A(\mathcal{S}, \mathcal{M}, \mathcal{E}, f)$, where f is the authentication map $f : \mathcal{S} \times \mathcal{E} \mapsto \mathcal{M}$. In similar manner we denote an A^2-code as $A^2(\mathcal{S}, \mathcal{M}, \mathcal{E}_T, \mathcal{E}_\mathcal{R}, f, g)$, where f is the transmitter's map given in (1) and g is the receiver's map given in (3). In [8] Simmons defined an authentication code to be *equitable* if the probabilities of success for all types of deceptions are the same, i.e., if $P_I = P_S = P_T = P_{R_0} = P_{R_1}$. In [10] it was shown that if an A^2-code provides $P_D = \frac{1}{q}$, then the cardinality of the sets of encoding rules must satisfy

$$|E_R| \geq q^3 \text{ and } |E_T| \geq q^4.$$

An A^2-code with $P_D = \frac{1}{q}$ is then defined to be *equitably perfect* if $|E_R| = q^3$ and $|E_T| = q^4$.

3 A general construction of A^2-codes

Let us for a moment consider the problems that occur in authentication with arbitration. Consider first the two deceptions from the receiver, R_0 and R_1, where he claims to have received a message that the transmitter never sent. We can think of a solution to this problem if we assume that the transmitter must add a "signature" to the source state S, that is to be transmitted. If the receiver now claims to have received a message from the transmitter he must also be able to produce the transmitter's signature.

This signature is actually nothing abstract but can be accomplished from a traditional A-code without secrecy. This code is a mapping from the source states and the encoding rules to the messages that has the form

$$Acode : S \times E \rightarrow M = (S, \alpha).$$

Let $\alpha = \alpha(S, E)$ be the signature. The transmitter maps the source state S into another "source state", Z, that also includes the signature α. This new source state, $Z = (S, \alpha)$, can now be transmitted in a second A-code without secrecy in order to protect against impersonation and substitution attacks from the opponent. Since this code only has to protect the original source state we can assume that the messages generated by the transmitter are of the form

$$M = (S, \alpha(S, E_T), \beta(S, E_T)) = (S, \alpha, \beta).$$

When the receiver checks a message for authenticity, he only checks whether β is correct. If the receiver claims to have received a message that the transmitter never sent, then he must be able to produce the signature α.

This concatenation of two normal A-codes gives protection against I, S, R_0 and R_1, but it realizes no protection against cheating from the transmitter. The transmitter cheats by sending a message that does not contain his own signature and succeeds if the message is accepted as authentic. In order to make this cheating difficult we introduce a modification for the receiver in the second A-code. Let this second A-code for the receiver protect both S and α. Then the received messages will have the form

$$M = (S, \alpha, \gamma) = (S, \alpha, \gamma(S, \alpha, E_R)).$$

This means that the receiver accepts all values of S and α and then checks that $\gamma = \gamma(S, \alpha, E_R)$. If properly generated messages are to be accepted and α is the transmitter's signature, we must have that

$$\forall S, \;\; \beta(S, E_T) = \gamma(S, \alpha, E_R), \text{ if } P(E_T, E_R) \neq 0. \qquad (5)$$

Also E_T and E_R must be chosen in such a way that (5) always holds when the setup of the encoding rules is done. If the transmitter now tries to cheat by changing his signature he must also determine the change in $\gamma(S, \alpha, E_R)$ which might be difficult.

We give a concrete example of these arguments.

Example 1. This example is based on the signature function $\alpha(s) = as + b$, where $a, b, s \in \mathbb{F}_2$. Assume that $S = s$, $E_T = (e_1, e_2, e_3, e_4)$ and $E_R = (f_1, f_2, f_3)$ where $s, e_i, f_i \in \mathbb{F}_2$. Let the transmitter's signature function be $\alpha(S, E_T) = e_1 + se_2$ and let $\beta(S, E_T) = e_3 + se_4$. Thus the transmitter generates messages as $M = (s, e_1 + se_2, e_3 + se_4)$. For the receiver, let $\gamma(S, \alpha, E_R) = f_1 + \alpha f_2 + sf_3$. The receiver then accepts messages of the form $M = (s, \alpha, f_1 + \alpha f_2 + sf_3)$. Also, the encoding rules must have been chosen in such a way that $\beta(S, E_T) = \gamma(S, \alpha, E_R)$, or

$$e_3 + se_4 = f_1 + (e_1 + se_2)f_2 + sf_3. \tag{6}$$

Equivalently, this can be written

$$e_3 = f_1 + e_1 f_2, \tag{7}$$

$$e_4 = f_3 + e_2 f_2. \tag{8}$$

For this A^2-code the authentication matrix for the receiver is

		Message $M = (s, \alpha, f_1 + \alpha f_2 + sf_3)$							
	S	000	001	010	011	100	101	110	111
	000	0	-	0	-	1	-	1	-
	001	0	-	0	-	-	1	-	1
	010	0	-	-	0	1	-	-	1
$E_R = (f_1, f_2, f_3)$	011	0	-	-	0	-	1	1	-
	100	-	0	-	0	-	1	-	1
	101	-	0	-	0	1	-	1	-
	110	-	0	0	-	-	1	1	-
	111	-	0	0	-	1	-	-	1

and the parameters for the code are

$$|S| = 2,\ |M| = 8,\ |E_R| = 8,\ |E_T| = 16.$$

By inspection we can check that the probabilities of the different kinds deceptions are

$$P_I = P_S = P_{R_0} = P_{R_1} = P_T = \frac{1}{2}.$$

□

4 Some specific constructions of A^2-codes

We have described an abstract way of modeling the problems in authentication with arbitration. We now deal with the problem of giving specific constructions of A^2-codes. Let us first give some preliminary definitions and results in the construction of traditional authentication codes. We consider first the case when

$|\mathcal{S}|P_D \leq 1$. Let $|\mathcal{S}| = q^n$, $|\mathcal{M}| = q^{n+m}$ and $|\mathcal{E}| = q^{2m}$, where $n \leq m$. Let $S = s$ and let the messages and the encoding rules consist of two parts,

$$M = (m_1, m_2), \tag{9}$$

$$E = (e_1, e_2). \tag{10}$$

We now assume that $s, m_1 \in \mathbb{F}_{q^n}$ and $m_2, e_1, e_2 \in \mathbb{F}_{q^m}$. Define an arbitrary injective mapping ϕ such that it maps a source state s from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^m}$,

$$\phi : \mathbb{F}_{q^n} \mapsto \mathbb{F}_{q^m}, \ \phi(s) = \hat{s},$$

where $s \in \mathbb{F}_{q^n}$ and $\hat{s} \in \mathbb{F}_{q^m}$.

From these definitions we can state the following:

Theorem 1. *Let a traditional authentication code generate messages M of the form $M = (m_1, m_2)$, where $m_1 = s$ and $m_2 = e_1 + \hat{s}e_2$. This A-code is Cartesian (no secrecy) and provide $P_I = P_S = \frac{1}{q^m}$ if $n \leq m$. Moreover, it has parameters*

$$|\mathcal{S}| = q^n, \ |\mathcal{M}| = q^{n+m}, \ |\mathcal{E}| = q^{2m}.$$

Proof. The fact that the code is Cartesian is clear and the cardinality parameters are obvious. We have to prove that $P_I = P_S = \frac{1}{q^m}$.

Impersonation: A message M can be written as the sum of two independent parts, $M = (s, \hat{s}e_2) + (0, e_1)$. Thus success in impersonation is equivalent to the problem of guessing the correct value of e_1, which is done with probability q^{-m}.

Substitution: The opponent has observed the message $M = (s, e_1 + \hat{s}e_2)$. Now he replaces this with another message M', which must correspond to another source state s'. Then $s' = s + c$, where $c \neq 0$, and since the mapping ϕ is injective we have that $\hat{s}' = \hat{s} + \hat{c}$, where $\hat{c} \neq 0$. We can write the message M' as

$$M' = (s', e_1 + \hat{s}'e_2) = (s, e_1 + \hat{s}e_2) + (c, \hat{c}e_2) = M + (c, 0) + (0, \hat{c}e_2).$$

Thus success in substitution is equivalent to the problem of guessing the value of $\hat{c}e_2$ for any $\hat{c} \neq 0$. But since $\hat{c}e_2$ runs through $\mathbb{F}_{q^m}$ for $\hat{c} \neq 0$ as e_2 runs through $\mathbb{F}_{q^m}$, the correct value is guessed with probability q^{-m}. □

We now have a simple construction of A-codes, which in fact is the best possible for this case. Our aim is to generalize this construction in such a way that we obtain A^2-codes. Assume that we want to construct an A^2-code with $|\mathcal{S}| = q^n$ and $P_D = \frac{1}{q^m}$. Assume that $n \leq m$. Let the parameters for the A^2-code be the following:

$$|\mathcal{S}| = q^n, \ |\mathcal{M}| = q^{n+2m}, \ |\mathcal{E}_T| = q^{4m}, \ |\mathcal{E}_{\mathcal{R}}| = q^{3m},$$

Consider the message and the encoding rules as consisting of several parts. Write

$$M = (m_1, m_2, m_3), \tag{11}$$

$$E_T = (e_1, e_2, e_3, e_4), \tag{12}$$

$$E_R = (f_1, f_2, f_3), \tag{13}$$

where $s, m_1 \in \mathbb{F}_{q^n}$ and $m_2, m_3, e_1, e_2, e_3, e_4, f_1, f_2, f_3 \in \mathbb{F}_{q^m}$.

Construction I: Let an A^2-code with $n \leq m$ be constructed as follows: The transmitter generates messages of the form $M = (m_1, m_2, m_3)$, where $m_1 = s$, $m_2 = e_1 + \hat{s}e_2$ and $m_3 = e_3 + \hat{s}e_4$. The receiver accepts all messages $M = (m_1, m_2, m_3)$ which has $m_3 = f_1 + \hat{m}_1 f_2 + m_2 f_3$. The encoding rules have been chosen in such a way that

$$e_3 + \hat{s}e_4 = f_1 + \hat{s}f_2 + (e_1 + \hat{s}e_2)f_3, \tag{14}$$

or equivalently,

$$e_3 = f_1 + e_1 f_3, \tag{15}$$

$$e_4 = f_2 + e_2 f_3. \tag{16}$$

From the way the encoding rules are chosen we check the following properties,

Lemma 2. *Let $\mathcal{E}_\mathcal{T} \circ \mathcal{E}_\mathcal{R}$ denote the set of all possible pairs of encoding rules (E_T, E_R). Then*

$$|\mathcal{E}_\mathcal{T} \circ \mathcal{E}_\mathcal{R}| = q^{5m}.$$

Also the transmitter has no knowledge about f_3 and the receiver has no knowledge about the pair (e_1, e_2). Expressed in terms of entropy we have $H(F_3|E_T) = m \log q$ and $H(E_1, E_2|E_R) = 2m \log q$.

Let us give the parameters of this construction.

Theorem 3. *Construction I gives a Cartesian A^2-code which has the following parameters for $n \leq m$:*

$$|\mathcal{S}| = q^n, \ |\mathcal{M}| = q^{n+2m}, \ |\mathcal{E}_\mathcal{R}| = q^{3m}, \ |\mathcal{E}_\mathcal{T}| = q^{4m}.$$

The probabilities of deceptions are

$$P_I = P_S = P_{R_0} = P_{R_1} = P_T = \tfrac{1}{q^m}.$$

Proof. The cardinality of the different sets is the number of possible values and is thus easily checked. Also, the code is Cartesian. Let us find the probabilities of success for the different kinds of deceptions.

Impersonation by the opponent, I: The opponent sends a message M and hopes for it to be authentic. The messages accepted by the receiver can be written in independent parts as

$$M = (s, \alpha, \hat{s}f_2 + \alpha f_3) + (0, 0, f_1).$$

In order to succeed the opponent must guess the value of f_1 and this is done with probability q^{-m}. Thus $P_I = q^{-m}$.

Substitution by the opponent, S: The opponent has observed a message M and substitutes this for another message M'. The substitution attack must include a change of the source state. Assume that the new source state is s', which can be written as $s' = s + c$, where $c \neq 0$. Since the map ϕ is injective we also have that $\hat{s}' = \hat{s} + \hat{c}$, where $\hat{c} \neq 0$. The observed message can be written as $M = (s, \alpha, f_1 + \hat{s}f_2 + \alpha f_3)$, where $\alpha \in \mathbb{F}_{q^m}$. The message M' is then of the form

$$M' = (s + c, \alpha + c', f_1 + (\hat{s} + \hat{c})f_2 + (\alpha + c')f_3),$$

where $c' \in \mathbb{F}_{q^m}$. This can be rewritten in independent parts as

$$M' = M + (c, c', c'f_3) + (0, 0, \hat{c}f_2).$$

Since $\hat{c} \neq 0$ and the last part is independent of the other two parts we have that success in substitution is equivalent to the problem of guessing the value of $\hat{c}f_2$ for any $\hat{c} \neq 0$. But $\hat{c}f_2$ runs through $\mathbb{F}_{q^m}$ as f_2 runs through $\mathbb{F}_{q^m}$, so the correct value is guessed with probability q^{-m}. Thus $P_S = q^{-m}$.

Impersonation by the receiver, R_0: The receiver claims to have received the message M. He succeeds if the signature α is correct. From Theorem 1 and Lemma 2 it follows that the probability of success is $P_{R_0} = q^{-m}$.

Substitution by the receiver, R_1: The receiver receives the message M but claims to have received another message M' corresponding to another source state s'. As before he succeeds if the signature α in M' is correct. From Theorem 1 and Lemma 2 it again follows that the probability of success is $P_{R_1} = q^{-m}$.

Impersonation by the transmitter, T: The transmitter sends a message M and then denies having sent it. He succeeds if the message contains a different signature from his own and is accepted by the receiver as authentic. The message received can be written as

$$M = (s, \alpha + c', f_1 + \hat{s}f_2 + \alpha f_3) + (0, 0, c'f_3),$$

where $c' \neq 0$. As before, the correct value of $c'f_3$ is guessed with probability q^{-m}, i.e., $P_T = q^{-m}$. □

Corollary 4. *Construction I is an equitably perfect A^2-code.*

Remark: A construction very similar to this was also found in [12], where the construction additionally also protected against attacks from the arbiter.

Let us give an example of how this construction works.

Example 2. Assume that we want to construct an A^2-code with the properties that $|S| = 2$ and $P_D = \frac{1}{2^2}$. Following Construction I we find that $\mathbb{F}_{q^m} = \mathbb{F}_{2^2}$ and that $\mathbb{F}_{q^n} = \mathbb{F}_2$. Let the mapping ϕ map the elements of $\mathbb{F}_2$ to the subfield $\{0, 1\}$ in $\mathbb{F}_{2^2}$, i.e., 0 maps to 0 and 1 maps to 1. The encoding rules are chosen in such a way that (14) holds. The transmitter generates messages as

$$M = (m_1, m_2, m_3) = (s, e_1 + \hat{s}e_2, e_3 + \hat{s}e_4).$$

The receiver receives messages of the form $M = (m_1, m_2, m_3)$ and checks that

$$m_3 = f_1 + \hat{m}_1 f_2 + m_2 f_3.$$

The number of messages and the number of encoding rules are

$$|\mathcal{M}| = 32, \quad |\mathcal{E}_\mathcal{R}| = 64, \quad |\mathcal{E}_T| = 256.$$

□

We have obtained a general construction for the case $n \leq m$. If we consider the same construction for the case $n > m$ we see that it is now not possible for the map ϕ to be injective. If ϕ is not injective there exist two source states s, s' that map to the same $\hat{s}$. These two source states would have the same last part in the message for all encoding rules and thus the probability of substitution becomes 1. However, with some modifications we can get a construction that can be used for the case $n > m$. In order for the construction to provide the same probability of deception we must increase the number of encoding rules. Thus the construction for the case $n > m$ will not be perfect.

As before we first give a construction of a traditional authentication code where $n \geq m$. We use the same notation as in (9)-(10), but now $s, m_1, e_2 \in \mathbb{F}_{q^n}$ and $m_2, e_1 \in \mathbb{F}_{q^m}$. Also we need a mapping ϕ, $\phi : \mathbb{F}_{q^n} \mapsto \mathbb{F}_{q^m}$ with the property that the number of $x \in \mathbb{F}_{q^n}$ such that $\phi(x) = y$ is the same for all $y \in \mathbb{F}_{q^m}$. We also assume that ϕ has the homomorphism property that $\phi(x)+\phi(x') = \phi(x+x')$. Then we state the following:

Theorem 5. *Let a traditional authentication code with* $n \geq m$ *generate messages* M *of the form* $M = (m_1, m_2)$ *where* $m_1 = s$ *and* $m_2 = e_1 + \phi(se_2)$. *This A-code is Cartesian (no secrecy) and provide* $P_I = P_S = \frac{1}{q^m}$. *Moreover, it has parameters*

$$|\mathcal{S}| = q^n, \ |\mathcal{M}| = q^{n+m}, \ |\mathcal{E}| = q^{n+m}.$$

Proof. The cardinality parameters are obvious and the A-code is Cartesian. For the different kinds of deceptions we have:

Impersonation, I: Write the message as $M = (s, \phi(se_2)) + (0, e_1)$. The value of e_1 is guessed with probability q^{-m}. Thus $P_I = q^{-m}$.

Substitution, S: The opponent has observed $M = (s, e_1 + \phi(se_2))$. Now he substitutes this message for another message, which has $s' \neq s$. The message M' is then written as

$$M' = (s', e_1 + \phi(s'e_2)) = (s, e_1 + \phi(se_2)) + (c, \phi(ce_2)) = M + (c, 0) + (0, \phi(ce_2)).$$

Since $c \neq 0$, ce_2 take any value in $\mathbb{F}_{q^n}$ with the same probability and $\phi(ce_2)$ is guessed with probability q^{-m}. Thus $P_S = q^{-m}$. □

We now give a construction of A^2-codes with $n \geq m$. We make one simplification, namely that $m = 1$. The notation is the same as in (11)-(13), but for this case we have $s, m_1, e_2, e_4, f_2 \in \mathbb{F}_{q^n}$ and $m_2, m_3, e_1, e_3, f_1, f_3 \in \mathbb{F}_q$. We also need a mapping ϕ, $\phi : \mathbb{F}_{q^n} \mapsto \mathbb{F}_q$ with the property that the number of $x \in \mathbb{F}_{q^n}$ such that $\phi(x) = y$ is the same for all $y \in \mathbb{F}_q$. We choose a specific ϕ.

Since $\mathbb{F}_{q^n}$ is an extension field of $\mathbb{F}_q$ any element $x \in \mathbb{F}_{q^n}$ can be written as $x = r_0 + r_1\alpha + \ldots + r_{n-1}\alpha^{n-1}$, where $r_i \in \mathbb{F}_q$, $i = 0, 1, \ldots, n-1$, and α is a root of an irreducible polynomial of degree n over $\mathbb{F}_q$. Define ϕ as

$$\phi : r_0 + r_1\alpha + \ldots + r_{n-1}\alpha^{n-1} \mapsto r_0.$$

From these definitions we can verify the homomorphism property. Assume that $x, x' \in \mathbb{F}_{q^n}$ and $y \in \mathbb{F}_q$. Then

$$\phi(x) + \phi(x') = \phi(x + x'), \tag{17}$$

$$\phi(x)y = \phi(xy). \tag{18}$$

We give the promised construction:

Construction II: Let an A^2-code with $n \geq m$ be constructed as follows: The transmitter generates messages of the form $M = (m_1, m_2, m_3)$, where $m_1 = s$, $m_2 = e_1 + \phi(se_2)$ and $m_3 = e_3 + \phi(se_4)$. The receiver accepts all messages $M = (m_1, m_2, m_3)$ which have $m_3 = f_1 + \phi(sf_2) + m_2 f_3$. The encoding rules have been chosen in such a way that

$$e_3 + \phi(se_4) = f_1 + \phi(sf_2) + (e_1 + \phi(se_2)) f_3, \tag{19}$$

or equivalently,

$$\begin{aligned} e_3 &= f_1 + e_1 f_3, \\ \phi(se_4) &= \phi(sf_2) + \phi(se_2) f_3. \end{aligned}$$

But from the properties (17) and (18) this is the same as

$$\begin{aligned} e_3 &= f_1 + e_1 f_3, \\ \phi(se_4) &= \phi\left(s(f_2 + e_2 f_3)\right). \end{aligned}$$

If we choose the encoding rules as

$$e_3 = f_1 + e_1 f_3, \tag{20}$$

$$e_4 = f_2 + e_2 f_3, \tag{21}$$

we know that (19) holds.

Lemma 6. *If the encoding rules are chosen as in (20) and (21) then*

$$|\mathcal{E}_\mathcal{T} \circ \mathcal{E}_\mathcal{R}| = q^{2n+3}.$$

Also, the transmitter has no knowledge about f_3 *and the receiver has no knowledge about the pair* (e_1, e_2).

Theorem 7. *Construction II gives a Cartesian* A^2*-code with the following parameters for* $n \geq m$*:*

$$|\mathcal{S}| = q^n,\ |\mathcal{M}| = q^{n+2},\ |\mathcal{E}_\mathcal{R}| = q^{n+2},\ |\mathcal{E}_\mathcal{T}| = q^{2n+2}.$$

The probabilities of deceptions are

$$P_I = P_S = P_{R_0} = P_{R_1} = P_T = \tfrac{1}{q}.$$

Proof. We determine the probabilities of success for the different kinds of deceptions.

Impersonation by the opponent, I: The message M received by the receiver can be written as

$$M = (s, \alpha, f_1 + \phi(sf_2) + \alpha f_3) = (s, \alpha, \phi(sf_2) + \alpha f_3) + (0, f_1).$$

The probability of guessing the correct value of f_1 is q^{-1} and thus $P_I = q^{-1}$.

Substitution by the opponent, S: The opponent has observed the message $M = (s, \alpha, f_1 + \phi(sf_2) + \alpha f_3)$. Now the opponent substitutes this for another message M' which correspond to a source state s', where $s' \neq s$. Write s' as $s' = s + c$, where $c \neq 0$ and $c \in \mathbb{F}_{q^n}$. The message M' is written as

$$M' = (s', \alpha + c', f_1 + \phi(s'f_2) + (\alpha + c')f_3)$$

where $c' \in \mathbb{F}_q$. But this is rewritten in independent parts as

$$M' = (s + c, \alpha + c', f_1 + \phi((s + c)f_2) + (\alpha + c')f_3) = M + (c, c', c'f_3) + (0, 0, \phi(cf_2)).$$

The probability of guessing the correct value of $\phi(cf_2)$ is q^{-1}.

Impersonation by the receiver, R_0: The receiver claims to have received the message $M = (s, \alpha, \beta)$ and succeeds if α is correct. The message generated by the transmitter is written as

$$M = (s, e_1 + \phi(se_2), m_3) = (s, \phi(se_2), m_3) + (0, e_1, 0).$$

By Lemma 6, the probability of guessing the value of e_1 is q^{-1} and $P_{R_0} = q^{-1}$.

Substitution by the receiver, R_1: The receiver receives a message M but claims to have received another message M' with another source state. If $M = (s, e_1 + \phi(se_2), m_3)$ we can write M' as

$$M' = M + (c, 0, m_3' - m_3) + (0, \phi(ce_2), 0)$$

where $c \neq 0$ and $c \in \mathbb{F}_{q^n}$. As before, the value of $\phi(ce_2)$ is guessed with probability q^{-1}, i.e. $P_{R_1} = q^{-1}$.

Impersonation by the transmitter, T: The transmitter is able to generate a message M but sends the message M' with a different signature α'. The signature is written as $\alpha' = \alpha + c'$ where $c' \neq 0$ and $c' \in \mathbb{F}_q$. Then M' can be written in independent parts as

$$M' = (s, \alpha + c', f_1 + \phi(sf_2) + (\alpha + c')f_3) = M + (0, c', c'f_3).$$

The value of $c'f_3$ is by Lemma 6 guessed with probability q^{-1} and $P_T = q^{-1}$. □

We end this section by giving a small example of how the last construction works.

Example 3. Assume that we want to construct an A^2-code with the properties that $|S| = 2^2$ and $P_D = \frac{1}{2}$. The elements of $\mathbb{F}_{2^2}$ are written as $r_0 + r_1\alpha$, where $r_0, r_1 \in \mathbb{F}_2$ and $\alpha^2 + \alpha + 1 = 0$. Assume that the encoding rules have the following values,

$$f_1 = f_3 = e_1 = 1, \ f_2 = e_2 = 1 + \alpha.$$

From (20) we have that

$$e_3 = f_1 + e_1 f_3 = 1 + 1 * 1 = 0,$$

and from (21) it follows that

$$e_4 = f_2 + e_2 f_3 = (1 + \alpha) + (1 + \alpha) * 1 = 0.$$

Assume that the transmitter wishes to communicate the source state $s = \alpha$. He then generates the message

$$M = (s, e_1 + \phi(se_2), e_3 + \phi(se_4)) = (\alpha, 1 + \phi(\alpha(1+\alpha)), 0 + \phi(\alpha * 0)) = (\alpha, 0, 0).$$

When the receiver receives this message he checks that

$$m_3 = f_1 + \phi(m_1 f_2) + m_2 f_3 = 1 + \phi(\alpha(1+\alpha)) + \phi(0 * 1) = 0.$$

Since m_3 was correct the message is accepted as authentic as it should be. □

5 Acknowledgement

Y. Desmedt is greatly acknowledged for making the author pay attention to [12].

References

1. E.N. Gilbert, F.J. MacWilliams and N.J.A. Sloane, "Codes which detect deception", *Bell Syst. Tech. J.*, Vol. 53, 1974, pp. 405–424.
2. G.J. Simmons, "Authentication theory/coding theory", in *Advances in Cryptology, Proceedings of CRYPTO 84*, G.R. Blakley and D. Chaum, Eds. Lecture notes in Computer Science, No. 196. New York, NY: Springer, 1985, pp. 411–431.
3. J.L. Massey,"Contemporary Cryptology, An Introduction", in *Contemporary Cryptology, The Science of Information Integrity*, G.J Simmons , Ed., IEEE Press, 1991, pp. 3-39.
4. G.J. Simmons, "A survey of Information Authentication", in *Contemporary Cryptology, The science of information integrity*, ed. G.J. Simmons, IEEE Press, New York, 1992.
5. D.R. Stinson, "The combinatorics of authentication and secrecy codes", Journal of Cryptology, Vol. 2, no 1, 1990, pp. 23-49.
6. D. R. Stinson, "Universal hashing and authentication codes" *Proceedings of Crypto 91*, Santa Barbara, USA, 1991, pp 74-85.
7. T. Johansson, G. Kabatianskii, B. Smeets, "On the relation between A-codes and codes correcting independent errors" *Proceedings Eurocrypt'93*, to appear.
8. G.J. Simmons,"A Cartesian Product Construction for Unconditionally Secure Authentication Codes that Permit Arbitration", in *Journal of Cryptology*, Vol. 2, no. 2, 1990, pp. 77-104.
9. G.J. Simmons, "Message authentication with arbitration of transmitter/receiver disputes", in *Proceedings of Eurocrypt '87*, D. Chaum and W.L. Price, Eds., Amsterdam, The Netherlands, April 13-15, 1987, pp. 151-165. Berlin: Springer-Verlag, 1988.
10. T. Johansson, "Lower Bounds on the Probability of Deception in Authentication with Arbitration", in *Proceedings of 1993 IEEE International Symposium on Information Theory*, San Antonio, USA, January 17-22, 1993, p. 231.
11. E.F. Brickell D.R. Stinson, "Authentication codes with multiple arbiters", in *Procceedings of Eurocrypt '88*, C.G Günter, Ed., Davos , Switzerland, May 25-27, 1988, pp. 51-55, Berlin: Springer-Verlag, 1988.
12. Y. Desmedt, M. Yung, "Asymmetric and Securely-Arbitrated Unconditional Authentication Systems", submitted to IEEE Transactions on Information Theory. A part of this paper was presented at Crypto'90.