American Journal of Computation, Communication and Control
2015; 2(2): 24-28
Published online April 30, 2015 (http://www.aascit.org/journal/ajccc)
ISSN: 2375-3943

AASCIT American Association for Science and Technology

Keywords
Authentication Code with Arbitration,
Authentication Code,
Splitting A-Code

Received: March 31, 2015
Revised: April 13, 2015
Accepted: April 14, 2015

Method to Construct A^2-Codes from A-Codes

Boubacar Abba

Dept. of Mathematics and Informatic, University of Science, Technics and Technologies, Bamako BP: E3206, Mali

Email address
abbabaoke@yahoo.fr

Citation
Boubacar Abba. Method to Construct A^2-Codes from A-Codes. *American Journal of Computation, Communication and Control.* Vol. 2, No. 2, 2015, pp. 24-28.

Abstract
Another important idea in the study of codes is the relation between authentication codes with arbitration and authentication codes without arbitration. Nowadays there is no much work about this relation, very few authors have studied it. Then in this paper we are going to study this relation and come out some important results. For this cause we established and proved two theorems, which provided a method to construct A^2-codes from A-codes. However, these codes have all the good properties of the old ones.

1. Introduction

Another problem of the research on the codes is how to construct authentication codes with arbitration from authentication codes. Only few mathematicians have worked in this erea and they found some good results.[1,2] The method to construct authentication codes has great agility, the number of source states can be arbitrarily large, and the construction is of more efficiency. The security can be designed at any level according to different requirement. The resulted codes can meet the optimal code-bound . In the model unconditionally secure authentication codes (A-codes), there are three participants, a transmitter, a receiver and an opponent. The opponent tries to cheat the receiver by impersonation attack and substitution attack. By impersonation attack we mean that the opponent sends a message through the channel to the receiver and hopes the receiver accepts it as authentic, i.e., as a message sent by the transmitter. By a substitution attack we mean that after the opponent intercepted a message sent by the transmitter to the receiver, he sends another message instead and hopes the receiver accepts it as authentic To protect against these attacks the transmitter-receiver may use an authentication code, which is open, but choose a fixed encoding rule e as secret. The set of information which the transmitter would like to transmit to the receiver should be identified with the set of source states of the code. Suppose that the transmitter wants to send some information (called a source state s) to the receiver using a public communication. At the first he has to encode s into a message m under the encoding rule e, i.e., m = f(s,e) and then he sends m to the receiver.

Once the receiver receives a message m', at first he has to judge whether m' is authentic, i.e., whether the encoding rule e is contained in m'. If $e \in m'$, then he regards m' as authentic and decode m' under e to get a source state s' so that m' = f(s', e).

If $e \notin m'$ then he regards m' as a false message.

To provide confidentially and authenticity for the source state to be transmitted to the receiver, the transmitter and the receiver need to share the same secret key. Note that there are two types of authentication codes : authentication code with secrecy and those without secrecy .In an authentication with secrecy, a source state is sent to the receiver in an encrypted form. In this case, the secret key shared by both the transmitter and the

receiver is used for both encryption and authentication purposes.

But in authentication code without secrecy, a source state is sent to the receiver in a plaintext that means the observed message uniquely determines the source state. In this case, the secret key is used only for authentication purpose.

An authentication code is said to have perfect secrecy if an observer will not gain any information about the source state from the message in the channel. It is possible that more than one message can be used to determine a source state (this is called splitting) which is very import for the present paper. An authentication code with secrecy is used as follows. Firstly encode the source state s with the encoding rule e. Then the transmitter sends the message m = e(s) to the receiver through the public communication channel. When receiving m', the receiver will first check the authenticity of the received message. If it is authentic, then the receiver will recover the source state s with the shared secret key e, otherwise the receiver will reject the message. The objective of the opponent is to choose a message and send it to the receiver so that the probability of deceiving the receiver, i.e., of causing him to accept as authentic a message not sent by the transmitter, is as large as possible. We denote by P_I and P_S, the largest probabilities that be could deceive the receiver when he plays an impersonation attack and a substitution attack and call them the probabilities of a successful impersonation and of a successful substitution attack respectively. Now let us give a mathematical description of authentication codes.

Definition: Let S, E, M be three non-empty sets and let $f: S\times E \to M$ be a map, the four tuple (S, E, M, f) is called an authentication code if

(1) The map $f: S\times E \to M$ is subjective and

(2) Given any $m\in M$ and $e\in E$ such that there is a $s\in S$ satisfying m = f(s, e), then such an s is uniquely determined by given m and e.

Suppose that (S, E, M, f) is an authentication code, then S, E, M are called the set of source states, the set of encoding rules and the set of messages, respectively and f is called the encoding map. Let $s\in S$, $e\in E$, and $m\in M$ are such that m = f (s, e), then we say that the source state s is encoded into a message m contains the encoding rule e. The cardinals |S|, |E|, and |M| are called the size of parameters of code. If the authentication code satisfies the further requirement that given any message m there is a unique source state s such that m = f (s, e) for any encoding rule contained in m, then the code is called a Cartesian authentication code.

For an authentication to be good, useful and pratical, its probabilities P_I and P_S should be as small as possible then the encoding and the decoding of such code will be easy. Many mathematicians have discussed on the combinatorial lower bound of P_I and P_S, and they prove the lower bound once more. From this proof they get some conditions when P_I and P_S achieve the bound. We can use the conditions in several times to obtain relationships between authentication code's parameters. Now consider an authentication code with parameters |S| =k, |E| = b, |M| = v. Suppose that the chosen probability of each encoding rule is the same, i.e., an encoding rule has a probability $1/|E|$ to be chosen. It is easy to see that when k = 1or b = 1 we always have $P_I = P_S$ such that k > 1, b > 1

In the model of A-code the transmitter and the receiver are both honest and believe each other because they use the same encoding rules. So this system cannot protect the deception between them. For example when the receiver receives nothing, he can say he had received some legal information (because the receiver knows the encoding rule he can easily make a false information like this). Similarly, when the receiver receives legal information, he can also say that he had received other information. In the condition of these two things, the transmitter can only think that the opponent succeeds in his attack. Moreover, when the transmitter sends a piece of information, he can also say that he had never sent any information. During this time, the receiver can only regard that the opponent succeeds in the attack of the system. Then it is natural to see some disputes will occur between the transmitter and the receiver.

However, it is not always the case that two parties want to trust each other .Inspired by this problem. Simmons introduced an extended model, called the A^2-code model in which there is a fourth person, called an arbiter. In this model, caution is taken against deception by the transmitter and the receiver as well as that by the opponent. The arbiter has access to all key information of the transmitter and the receiver, and solves disputes between them. Then there are essentially five different kinds of cheating, impersonation by the opponent, substitution by the opponent, impersonation by the transmitter, impersonation by the receiver and substitution by the receiver. So let us give first a mathematical description of authentication code with arbitration.

Definition: Suppose that S, M, E_T, E_R are four non-empty sets, let $g: S\times E_T \to M$ and $h: \mathrm{M}\times \mathrm{E}_R \to S\cup\{reject\}$ be to two maps, the six tuplet, (S, M, E_T, E_R, g ,h)is called an authentication code with arbitration or A^2-code if

(1) $g: S\times E_T \to M$ is subjective and satisfies $g(s,e_T)=g(s',e_T)\Rightarrow s=s'$ where $m\in M$ $s,s'\in S, e_T\in E_T$

(2) $h: \mathrm{M}\times \mathrm{E}_R \to S\cup\{reject\}$ satisfies: $P(e_T,e_R)\neq 0$, we have $g(s,e_T)=m\Rightarrow h(m,e_R)=s$ where $s\in S$ and $m\in M$.

S, M, E_T, E_R denote respectively the set of source states, the set of all possible messages, the set of all encoding rules of transmitter, the set of encoding rules of receiver.The two map g and h are respectively encoding and decoding functions. If $g(s,e_T) = m$ we say that m is obtained by e_T encoding s and that e_T is contained in m, and if $h(m,e_R) = s$, we say that e_R is contained in m. The cardinals |S| . |M|, $|E_T|$, $|E_R|$ are called parameters of the A^2-code. This model, the transmitter and the receiver are not mutually trust worthy, and hence disputes between them may occur, In order to solve possible disputes between the transmitter and the receiver, a fourth participant called arbiter is introduced. The arbiter has access to all key information and by definition, he doesn't cheat. He is only present to solve possible disputes

and does not take part in any communication activities. Code for this model provide protection against deceptions both from an outsider (opponent) and from the insiders (transmitter and receiver). Recall that we only consider unconditional security, i.e., against attacks performed with unlimited computing power. As in A-code the transmitter wants to send some information, called a source state, to the receiver in such a way that the receiver can both recover the transmitted source state and verify that the transmitted message originates from the legitimate transmitter. The source state s, taken from the set S of possible source states, is encoded by the transmitter into a message m from the lager set M of possible messages. The message m is subsequently transmitted over the channel. The mapping from S to M is determined by transmitter's secret encoding rule e_T, chosen from the set E_T of possible encoding rules. We may assume that the transmitter uses a mapping $g: S \times E_T \to M$. The mapping g satisfies $g(s, e_T) = g(s', e_T) \Rightarrow s = s'$.

In other words, the source state can be recovered uniquely from a transmitted message. The mapping g is deterministic, i.e., a source state cannot be mapped into several messages for a given encoding rule (splitting is not allowed). This restriction is made for simplicity and most results that will be derived are also valid for A^2-model that use splitting. As usual, the opponent has access to the channel in the sense that he can either impersonate the transmitter and send a message, or replace a transmitted message with a different one.The receiver must decide whether a received message is valid or not. For this purpose the receiver uses a mapping, determined by his own secret encoding rule e_R, taken from the set of E_R of possible encoding rules, that determines if the message is valid, and if also the source state. So we may assume a mapping $h: \mathrm{M} \times \mathrm{E}_R \to S \cup \{reject\}$, where for all possible (e_T, e_R), i.e., $P(e_T, e_R) \neq 0$, we have $g(s, e_T) = m \Rightarrow h(m, e_R) = s$. For the receiver to accept all legal messages from the transmitter and to translate them to the correct source state, property (2) must hold for all pair (e_T, e_R). However, in general not all pairs (e_T, e_R) will be possible, i.e., have a positive probability. The arbiter is the supervisory person who has access to all information, including e_T and e_R, but does not take part in any communication activities on the channel . His only task is to solve possible disputes between the transmitter and the receiver whenever such occur. This is done in the following way. If the message m, received by the receiver, could have been generated by the transmitter according to his encoding rule e_T, then the arbiter decides that the message m was sent by the transmitter, and otherwise not. The arbiter assumed to be honest.

In the authentication code with arbitration the following five type of cheating attacks are considered.

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

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

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

Attack $\mathbf{R_0}$ (Impersonation by the receiver). The receiver claims to have received a message from the transmitter. The receiver succeeds if this message could have generated by the transmitter according this encoding rule.

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

All parameters in the model except the actual choices of encoding rules are public information. In all possible attempts to cheat it is understood that the cheating person uses an optimal strategy when choosing a message, or equivalently, that the cheating person chooses the message that maximizes his chances of success. For the five types of deceptions, we denote these cheating probabilities by P_I, P_S, P_T, P_{R0}, P_{R1}. Let E_R denote the set of keys of the receiver and E_T denote the set of keys of the transmitter.

Note that for some notations and definitions we will refer to [3].Splitting A-code in an A-code, it is $|Split(e,s)| = c$ possible that more than one message can be used to communicate a particular source state, this phenomenon is called splitting.

For $e \in E$ and $s \in S$ define $\mathrm{Split}(e,s) = \{m \mid e(s) = m\}$.

An A-code is called splitting if $|Split(e,s)| \geq 1$ for some (e,s). It is called without splitting if $|\mathrm{Split(e,s)}| = 1$ for some (e,s).

Let $M(e) = \{m \mid e \text{ accepts } m\} = \bigcup_{s \in S} Split(e,s)$

Definition: An A-code is $(l,c) - splitting$ if $|M| / |S| = l$, $|Split(e,s)| = c$, for $e \in E$, and $s \in S$.

2. Construction of A^2-Codes from Splitting A-Codes

Let S denote the set of all source states, M the set of all possible messages, E_T the set of all encoding rules of transmitter, and E_R the set of encoding rules of receiver.

Set k=|S|, v=|M| and then $|M| / |S| = \frac{v}{k} = l$, let M(f,s) be the set of the messages under f which are valid and decoded into s, it is easy to see that $M(f) = \bigcup_{s \in S} M(f,s)$.

When there is any dispute between transmitter and receiver, the arbiter will solve them by admitting that M(e) is the transmitter's set where the encoding rule e act, and M(f) is the receiver's set the encoding rule f act too, $P_{R_0} \geq P_1, P_{R_1} \geq P_2$ $|M(f,s)|$ (see[4]) is always a constant c independent of f and s.

Use (S, M, E_R, E_T) to indicate an (I,c) A^2-code, we first try to construct from this code an (l,c)-splitting A-code.

Suppose P_I, P_S, P_T, P_{R_0}, P_{R_1} are the probabilities of the attacks of this A^2-code, denote by P_I' and P_S' the P_I and P_S of a splitting A-code, P_1 and P_2 denote respectively the P_I and P_S of an A-code.

Theorem 2.1 Suppose that there exists an (I,c) A^2-code (S, M, E_R, E_T).

Then there is an (l,c)-splitting A-code (S, M, E_R) such that P_I=P_I' and P_S=P_S'.

There is also exists an A-code (S, M', E') such that |M'|=c|S| and $P_{R_0} \geq P_1, P_{R_1} \geq P_2$.

Proof: We can consider an (l,c)-splitting A-code (S, E, M) from an (l,c) A^2-code (S, M, E_R, E_T) by setting E_R=E.

By definition in the A^2-code we have $P_I = \max_m P$ (m valid)= $\max_m \frac{|E_R(m)|}{|E_R|}$. Also in the A-codewe have $P_I' = \max_m P$ (m valid) = $\max_m \frac{|E(m)|}{|E|}$. Then it is obvious that $P_I = P_I'$ because they depend only on E_R=E.

Now, we are going to show that $P_S = P_S'$.

In the A^2-code, $P_S = \max_m P$ (m' valid | m) = $\max_{\substack{m,m' \\ m \neq m'}} \frac{|E_R(m) \cap E_R(m')|}{|E_R(m)|}$.

In the splitting A-code, $P_S' = \max_{\substack{m,m' \\ m \neq m'}} P$ (m' valid| m) = $\max_{\substack{m,m' \\ m \neq m'}} \frac{|E(m) \cap E(m')|}{|E(m)|}$, where $E(m) = \{e \mid e \in E, e(s) = m\}$.

Now use the fact that E_R = E, then E(m) = E_R (m), where $E_R(m) = \{f \mid f \in E_R, f(m) = valid\}$. Therefore it is easy to prove that $P_S = P_S'$.

For any $f \in E_R$ we consider an A-code (S, M(f), E_T(f)) in which the arbiter is a receiver and the receiver is an opponent.

Let P_I(f) and P_S(f) denote the P_I and the P_S of this A-code, respectively.

We know $\frac{1}{c} = P_{R_1} = P_{R_0} = \frac{|S|}{|M(f)|}$ then $|M(f)| = \sum_{s \in S} |M(f,s)| = c|s|$, and also we have $P_{R_0} = \max_{f \in E_R} P_I(f)$, $P_{R_1} = \max_{f \in E_R} P_S(f)$.

Thus for a fixed $f_0 \in E_R$ arbitrarily, the A-code $(S, M(f_0), E_T(f_0))$ satisfies the condition of this theorem.

It is natural to ask if the reciprocity of this theorem is possible. The answer of this question is of course yes, and that one can serve us to construct authentication codes with arbitration based on splitting authentication codes.

Theorem 2.2 Suppose that there exist an (l,c)-splittingA-code (S, E, M), and also suppose that there exist an A-code (S, M(f), E_T(f)) for any $f \in E_R$ and $s \in S$ such that $|M(f)| = c|S|$.

Then there exist an (I,c) A^2- code (S, M, E_R, E_T) such thatP_I = P_I', $P_S = P_S'$, $P_T = \frac{c-1}{l-1}$, $P_{R_0} = P_1, P_{R_1} = P_2$.

Proof Consider an (I,c) A^2- code (S, M, E_R, E_T)such that as follows. Let E_R = E, then we have $P_I = P_I'$ because they depend only on E_R = E.

Now let us prove that $P_S = P_S'$ we know that from [4] $P_S = \sum_{m \in M} P(m)[\max_{m'} P$ (m' valid | m] = $= \max_{m \in M} \left\{ \frac{\max_{m'} \{the\ number\ of\ e_R\ in\ m\ and\ m'\}}{the\ number\ of\ e_R\ in\ m} \right\}$

From the fact E_R = E and by similar argument in the proof of theorem 2.1, we may have $P_S = P_S'$. Suppose that the transmitter T has $e \in E_T$. T succeeds in cheating if T sends m such that $m \neq M(e)$ and R accepts m as authentic .Note $M(e) = \{m \mid m = e(s)$ for some $s \in S\}$.

Let $P_e = \max_{m \notin M(e)} \Pr$[R accepts m as authentic | $E_T = e$]. Then $P_T = \max_{e \in E_T} P_e$.

Now consider a splitting A-code $(S, E_R, \bar{M}(e))$ where $\bar{M}(e) = M \setminus M(e)$. Consider P_e asthe $P_I$of this A-code,

For $s \in S$, each $f \in E_R(e)$ accepts c-1 messages of $\bar{M}(e)$ as authentic since f accepts c messages of M as authentic. Note that each $e \in E_T$ generatesjust one message for each $s \in S$

Therefore, this is an (l'', c-1)-splitting A-code, where

$$l'' = |\bar{M}(e)|/|S| \text{ (See definition 1.1)}$$

$$= (|M| - |M(e)|)/|S| = (|M| - |S|)/|S| = l - 1$$

In a splitting A-code $(S, E_R(e), \bar{M}(e))$ we have $P_e = \frac{(c-1)|S|}{|\bar{M}(e)|}$, since $P_T = \max_{e \in E_T} P_e$, therefore $P_T = \frac{c-1}{l-1}$.

Let $f \in E_R$ and $s \in S$, consider an A-code $(S, M(f), E_T(f))$. It is easy to see that $\frac{1}{c} = P_{R_1} = P_{R_0} = \frac{|S|}{|M(f)|}$.

3. Conclusion

In this paper we start by the description of these two codes (authentication code, and authentication code with arbitration) and also some properties of them are given. By using the concept of (l,c)-splitting A-code we have studied a new method to construct authentication code with arbitration from authentication code without arbitration. For this cause we established and proved two theorems, which provided a method to construct A^2-codes from A-codes. Authentication

codes with arbitration are more complicate than authentication codes without arbitration. Since its parameters and probabilities are difficult to be computed. So my next work will be about construction of authentication with arbitration and computation of its parameters and probabilities.

References

[1] Boubacar Abba, You Hong . A construction of authentication codes with arbitration based on orthogonal spaces. J. of Harbin Institute ofTechnology, Vol.13 $N^0$2, pp 134-140, April 2006.

[2] Boubacar Abba, You Hong. Some new bounds on A^2-Model. WSEAS Trans. On Communication Vol. 5, $N^0$6, pp 1008-1014, June 2006.

[3] BoubacarAbba, You Hong . Using Pseudo-symplectic Spaces to construct authentication codes with arbitration. J. of Heilongjiang Science Nat. Vol.23, $N^0$5, pp 681-689, Oct 2006.

[4] Boubacar Abba, You Hong . Lower bounds on the sizes of keys of authentication codes with arbitration. The proceedings of the 9th Inter. Conf on applied Mathematics, Istanbul Turkey, May 27-29, 2006, 546-549.

[5] Cunsheng Ding, XiaojianTian, Three Constructions of Authentication codes with perfect secrecy, Designs, Codes and Cryptography, 33 (2004), 227-239.

[6] J. Yu, Z. Li, Construction of authentication codes with arbitration from Pseudo-symplectic geometry (in Chinese), J. of Northeast University (Natural Science Edition), 35 (1) (2005), 7-10.

[7] R. Li, Z Li, X. Li, Further Construction of authentication code with arbitration from unitary geometry. J. of Electronics and Information Technology (in Chinese), 24(3)(2002), 418-421.

[8] R. Li, L. Guo, X. Li. Construction of Cartesianauthentication codes with arbiter from error2 correcting codes (in Chinese), 29(4)(2002), 530-533.

[9] J.Z. Luo, Construction of authentication codes with arbitration, Thesis for master degree, harbinInstitute of Technology 2001, 1-55.

[10] K. Kurosowa, and S. Obana Combinatorial Bounds on authentication codes with arbitration, Designs, Codes and Cryptography, 22(2001), 265-281.

[11] K. Kurosowa, and S. Obana Combinatorial classification of optimal authentication codes with arbitration, Designs and Cryptography, 20(2000), 281-305.

[12] L. Hu, On construction of optimal A^2-model, Northeast Math, J. 17(2001), 27-33.