On A^2-codes including arbiter's attacks

Thomas Johansson, Ben Smeets

Dept. of Information Theory, University of Lund,
Box 118, S-221 00, Lund, Sweden **

Abstract. We comment on the work by R. Taylor presented at EuroCrypt'94 (see this proceedings). We first extend some known results on authentication codes with arbitration to the case when protection against arbiter's attacks is provided. We give lower bounds on the secret key size for each participant and give a construction showing that these bounds are tight. These results improve upon previously known work and show that a claim in the aforementioned paper is wrong.

1 Introduction

In conventional authentication [1] the two communicating parties share the same key and hence they must be assumed trustworthy. This assumption is in many situations unnatural and Simmons [2] therefore introduced extended authentication codes, called authentication codes with arbitration, or simply A^2-codes, where caution is taken both against deceptions from the outsider (opponent) and also against some forms of deception from the insiders (transmitter and receiver). A fourth person, called the *arbiter*, is included. The arbiter is assumed to be honest, does not take part in any communication activities and his sole task is to solve possible disputes between the transmitter and the receiver.

Several constructions showing better performance than Simmons' original Cartesian product construction [2] have since then been given, [3], [4], [5]. Bounds on the size of each participant's key for this kind of codes were given in [4]. The class of A^2-codes can be considered as a subclass of the more general concept asymmetric authentication schemes [3].

One disadvantage with the A^2-codes noted by Simmons is the fact that participants must trust the arbiter's honesty. There are of cause several situations where this is a very natural assumption, but there are nevertheless examples on the opposite. This problem has been addressed and constructions providing protection against deceptions from the arbiter have been proposed [6], [3].

This is the scenario that will be investigated in this paper. The goal of the paper is to comment on the work in [7] and to show that a claim appearing in [7] is wrong. We do this by giving a brief theoretical overview of some recent results, including lower bounds and a simple improved construction. In Section 2 we give notation and problem formulation. In Section 3 we provide lower bounds on the size of each participant's secret key. In Section 4 we give a construction showing the tightness of the bounds and in Section 5 we give the remarks on the paper [7], partly obtained from the previously derived results.

** This work was supported by the TFR grant 222 92-662

2 Notation and problem formulation

A transmitter intends to send some information, called a source state, to the receiver in such a way that the receiver can verify that the transmitted message originate from the legal transmitter. This is done by mapping a source state $s \in \mathcal{S}$ to a (channel) message $m \in \mathcal{M}$. The mapping from $\mathcal{S}$ to $\mathcal{M}$ is determined by the transmitters secret encoding rule (or key) $e_T \in \mathcal{E}_T$. The opponent can either try to simply send a message or replace a transmitted message with another. The receiver checks whether a message is valid or not. For this purpose the receiver uses a mapping from his own secret encoding rule $e_R \in \mathcal{E}_\mathcal{R}$ and from the messages $\mathcal{M}$, that determines if a received message is valid and if so also the source state. The receiver must accept all legal messages from the transmitter. Thus the encoding rules must have been chosen in such a way, i.e., there is a dependence between the two encoding rules (e_R, e_T).

The arbiter 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. Assuming an honest arbiter, there are five different attacks that are possible: Attacks **I**,**S**, Impersonation/Substitution by the opponent. Attack **T**, Impersonation by the transmitter. Attacks $\mathbf{R_0}$,$\mathbf{R_1}$, Impersonation/Substitution by the receiver.

We denote the maximum probability of success for each attack by P_I, P_S, P_T, P_{R_0} and P_{R_1} respectively. For formal definitions, see [2],[4]. When the arbiter is not to be trusted, we add two possible attacks:
Attack $\mathbf{A_0}$, Impersonation by the arbiter: The arbiter sends a message to the receiver and succeeds if the message is accepted by the receiver as authentic.
Attack $\mathbf{A_1}$, Substitution by the arbiter: The arbiter observes a message that is transmitted and replaces this message with another. The arbiter succeeds if the receiver accepts this other message as authentic.

Denote the probability of success for each attack with P_{A_0} and P_{A_1}, respectively. Even though the arbiter is not trusted, he is assumed to make honest decisions in case of a dispute. The *overall probability of deception*, denoted P_D, is defined as the maximum of the probabilities of success over all allowed attacks.

3 Bounds on A^2-codes including arbiter's attacks

To derive new bounds we examine the probabilities of success for the R_0 and R_1 attacks. From the definition of the attacks we write

$$P_{R_0} = \max_{e_R, m} P(m \text{ has success}), \tag{1}$$

$$P(m \text{ has success}) = \sum_{e_A} \chi(m, e_A) P(e_A | e_R), \tag{2}$$

where $\chi(m, e_A) = 1$ if for the encoding rule e_A the arbiter decides that m came from the transmitter and 0 otherwise. Similarly,

$$P_{R_1} = \max_{e_R, m' \neq m} P(m' \text{ has success} | m \text{ has success}), \tag{3}$$

$$P(m' \text{ has success} | m \text{ has success}) = \sum_{e_A} \chi(m', e_A) P(e_A | e_R, m). \tag{4}$$

We then derive the following bounds,

Theorem 1. *For any A^2-code we have*

$$P_{R_0} \geq 2^{-I(M;E_A)}, P_{R_1} \geq 2^{-H(E_A|M)}. \tag{5}$$

Proof. The proof is similar to proofs of lower bounds in [4].

From these bounds it follows,

Corollary 2. *For any A^2-code we have*

$$|\mathcal{E}_\mathcal{A}| \geq (P_{R_0} P_{R_1})^{-1}.$$

Using the bounds from [4] we can summarize the lower bounds for A^2-codes both with and without arbiter's attacks:

Theorem 3. *For any A^2-code we have*

$$\begin{aligned} |\mathcal{E}_\mathcal{R}| &\geq (P_I P_S P_T)^{-1}, \\ |\mathcal{E}_\mathcal{T}| &\geq (P_I P_S P_{R_0} P_{R_1})^{-1}, \\ |\mathcal{E}_\mathcal{A}| &\geq (P_{R_0} P_{R_1})^{-1} \\ |\mathcal{M}| &\geq (P_I P_{R_0})^{-1} |\mathcal{S}|. \end{aligned}$$

In particular, if $P_D = 1/q$, then $|\mathcal{E}_\mathcal{R}| \geq q^3$, $|\mathcal{E}_\mathcal{T}| \geq q^4$, $|\mathcal{E}_\mathcal{A}| \geq q^2$ and $|\mathcal{M}| \geq q^2 |\mathcal{S}|$.

Considering A^2-codes used for multiple use we can in a similar way as above derive the following:

Theorem 4. *For any A^2-code for multiple use L times with protection $P_D = 1/q$ we have*

$$|\mathcal{E}_\mathcal{R}| \geq q^{L+2}, \ |\mathcal{E}_\mathcal{T}| \geq q^{2L+2}, \ |\mathcal{E}_\mathcal{A}| \geq q^{L+1}$$

and $|\mathcal{M}| \geq q^2 |\mathcal{S}|$ at each use.

Proof. This is a simple extension of the previously derived results.

4 A construction of A^2-codes including arbiter's attacks

We consider a construction that meets the lower bounds in the previous section with equality. We construct an A^2-code with $|\mathcal{S}| = q$ and $P_D = 1/q$. Let the parameters be the following:

$$|\mathcal{S}| = q, \ |\mathcal{M}| = q^3, \ |\mathcal{E}_\mathcal{T}| = q^4, \ |\mathcal{E}_\mathcal{R}| = q^3, \ |\mathcal{E}_\mathcal{A}| = q^2,$$

Let the encoding rules be

$$e_T = (e_1, e_2, e_3, e_4), \tag{6}$$

$$e_R = (f_1, f_2, f_3), \tag{7}$$

$$e_A = (e_1, e_2). \tag{8}$$

where $e_1, e_2, e_3, e_4, f_1, f_2, f_3 \in \mathbb{F}_q$. The A^2-code is constructed as follows:
Construction I: The transmitter generates messages of the form

$$m = (s, e_1 + se_2, e_3 + se_4). \tag{9}$$

The receiver accepts all messages $m = (m_1, m_2, m_3)$ which has

$$m_3 = f_1 + m_1 f_2 + m_2 f_3.$$

In case of a dispute, the arbiter decides that the message $m = (s, m_2, m_3)$ came from the transmitter if and only if $m_2 = e_1 + se_2$. The encoding rules have in the initialization phase been chosen in such a way that

$$e_3 = f_1 + e_1 f_3, \tag{10}$$

$$e_4 = f_2 + e_2 f_3. \tag{11}$$

We must verify that the arbiter makes correct decisions, i.e., all messages generated by the transmitter must be considered by the arbiter to have been generated by the transmitter. We see that this is the case.

Theorem 5. *Construction I gives an A^2-code with parameters:*

$$|\mathcal{S}| = q,\ |\mathcal{M}| = q^3,\ |\mathcal{E}_R| = q^3,\ |\mathcal{E}_T| = q^4,\ |\mathcal{E}_A| = q^2$$

and the probabilities of success for the different deceptions are

$$P_I = P_S = P_T = P_{R_0} = P_{R_1} = P_{A_0} = P_{A_1} = 1/q.$$

Thus we have

Corollary 6. *Construction I gives an A^2-code with protection against arbiter's attacks which has optimal performance, i.e., the size of the keys are the lowest possible.*

The key initialization phase does not have the same structure as in [3]. However, the following interesting property of Construction I shows that no loss is made.

Theorem 7. *The key initialization in Construction I can be done using three interactions without changing the probabilities of success.*

The construction can be modified in order to obtain other parameters and we end this section by giving the performance of two such modifications.

Theorem 8. *Construction I can be modified in such a way that for $P_D = 1/q$ we have parameters*

$$|\mathcal{S}| = q^n,\ |\mathcal{M}| = q^{n+2},\ |\mathcal{E}_R| = q^{n+2},\ |\mathcal{E}_T| = q^{2n+2},\ |\mathcal{E}_A| = q^{n+1}.$$

Alternatively, if we consider multiple use L times with $P_D = 1/q$ at each use we can have parameters $|\mathcal{S}| = q^n$, $|\mathcal{M}| = q^{n+2}$ at each use and

$$|\mathcal{E}_R| = q^{n+L+1},\ |\mathcal{E}_T| = q^{2n+2L},\ |\mathcal{E}_A| = q^{n+L}.$$

5 Some comments on [7]

In [7] a construction of A^2-codes including arbiter's attacks is described. The author claims a good performance and gives some bounds on the size of the message (codeword) and keys. Using the previous results we want to comment on some of the statements.

Remark 1: The theorem stated in Section 5 of [7] is incorrect. It is stated that the length of the messages must be at least $\log|\mathcal{S}| + 3\log q$, but as we showed in Section 3, the lower bound on the length of the messages is $\log|\mathcal{S}| + 2\log q$ and it is tight. Note also that the construction given in Section 4 gives optimal message length and also better performance (smaller secret key) than the construction proposed in [7].

Remark 2: In Section 2 of [7] a construction of conventional authentication codes is proposed. Comparing with constructions in [8], [9] and [10] we see that the performance is not very good.

References

1. 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.
2. 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.
3. 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.
4. 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., to be published in IEEE Trans. on Information Theory.
5. T. Johansson, "On the construction of perfect authentication codes that permit arbitration", *Proceedings Crypto'93*, pp. 343-354.
6. E.F. Brickell D.R. Stinson, "Authentication codes with multiple arbiters", in *Proceedings of Eurocrypt '88*, C.G Günter, Ed., Davos , Switzerland, May 25-27, 1988, pp. 51-55, Berlin: Springer-Verlag, 1988.
7. R. Taylor, "Near Optimal Unconditionally Secure Authentication", presented at Eurocrypt'94, in *Pre-proceedings of Eurocrypt'94*, pp. 245-256.
8. T. Johansson, G. Kabatianskii, B. Smeets, "On the relation between A-codes and codes correcting independent errors" *Proceedings Eurocrypt'93*, pp. 1-11.
9. B. den Boer, "A simple and key-economical unconditionally authentication scheme", J. Computer Security, Vol. 2, 1993, pp. 65-71.
10. Bierbrauer, Johansson, Kabatianskii, Smeets, "On the construction of universal families of hash functions via geometric codes and concatenation", *Proceedings of Crypto 93*, Santa Barbara, USA, 1993, pp. 331-342.