Arbitrated Unconditionally Secure Authentication Can Be Unconditionally Protected against Arbiter's Attacks

(Extended Abstract)

Yvo Desmedt
Dept. of EE & CS
Univ. of Wisconsin –
Milwaukee
WI 53201, U.S.A.

Moti Yung
IBM
T. J. Watson Research Center
Yorktown Heights
NY 10598, U.S.A.

Abstract. *Given an arbiter whose arbitrage is trusted, an authentication scheme is presented which is unconditionally secure against impersonation and/or substitution attacks performed by the arbiter, whereas previous scheme did not protect against such attacks. Furthermore, the scheme protects unconditionally against: impersonation/substitution attacks done by an outsider, against disavowal of a message by the sender, and against the receiver forging a message which was never sent. A practical scheme based on finite geometry is presented. Adaptations of the scheme realize an asymmetric conventional authentication scheme, and the set-up of an unconditionally secure oblivious transfer system.*

1 Introduction

When Sandy sends a message to Russ, Russ wants to be certain that the message is authentic, *i.e.*, it originates from Sandy and the message has not been substituted (altered). Authentication codes protect against such attacks [16].

While authentication systems protect against attacks by outsiders, they do not necessarily protect against disputes between sender and receiver. In such disputes, Sandy could deny having sent an embarrassing message that Russ claims she did, or Russ could modify, to his own advantage, a message that he received. The first schemes protecting against disputes are signature schemes [6]. The most known one is the RSA scheme [13]. Although RSA is somewhat unsuited for certain situations [4, 2, 3], some provably secure signature systems (as secure as inverting hard functions)

A.J. Menezes and S.A. Vanstone (Eds.): Advances in Cryptology - CRYPTO '90, LNCS 537, pp. 177-188, 1991.

are around [8, 11, 14].

Signatures schemes have unfortunately to rely on some unproven assumptions [9]. In contrast, no such reliance is required by unconditionally secure authentication codes [7, 19, 16].

The first unconditionally secure authentication scheme dealing with disputes has been proposed by Simmons [15, 18]. It is based on trust in the arbiter. *Simmons' scheme, however, suffers from a major disadvantage: Arby can impersonate Sandy, and Russ will not observe it.* Simmons mentions the disadvantage of his scheme and a natural question to ask is whether it can be reduced. In [1] a system with multi arbiters was suggested by Brickell and Stinson in order to somewhat reduce the attacking power of arbitration agents, by adding assumptions and active participants. *The purpose of this paper* is to come up with a scheme which *does not suffer from this disadvantage.* To compare with Brickell and Stinson's work we only need *one* arbiter as in Simmons' original scheme.

We remark that an arbiter may be a trusted party as far as arbitration between the parties is concerned. However, even such a participant may have an interest in impersonating a party, thus influencing the course of events. An "imaginary" scenario of arbiter cheating is when a boss-of-an-agency is playing the role of an arbiter between two of his employees, an operation officer, and a field agent. The arbiter in this case may impersonate the officer to send illegal instructions for some covert operation. Because the field agent believes that the message is authentic (originates from the officer) it will be executed. In case the operation fails, it is the officer who will be blamed for it, as he was actually set up as a "fall-guy"!

We note that such cases of cheating are especially very tempting when it is known that they will go undetected. A provision of a scheme which deters the arbiter from attempting impersonation seems to be necessary in such delicate scenarios.

In Simmons' solution [15, 18] we distinguish three stages (the description of which can easily be formalized later on). Let us call S the sender, R the receiver, A the arbiter, and O the outside opponent. The three stages are:

The key initialization phase in which S, R and A interact to come up with the necessary keys.

The transmission phase in which R receives a message and wants to ascertain that the message is authentic. A does *not* interact in this stage.

The dispute phase in which A is requested to resolve a dispute between S and R, based on information gathered by A during the initialization phase.

Our scheme contains these three stages as well. This allows a fair comparison of our solution with Simmons'. We observe that the *arbiter is* not *involved in the transmission phase.* This is contrary to the classical notion of arbitered signatures [10, p. 409].

The threats that we are faced with can originate from the outside opponent O, a dishonest $\tilde{S}$, a dishonest $\tilde{R}$, and a dishonest $\tilde{A}$. We follow Simmons' description of such threats. For the first three threats see [18].

The arbiter's threat. A dishonest $\tilde{A}$ can send a message to R which R will accept as authentic. As in the case of the opponent's attack the arbiter can either choose an impersonation or a substitution attack.

The attack is successful if and only if the message originating at $\tilde{A}$ will be accepted by R.

Let us now describe an observation which is the driving force behind our solution.

It is *extremely important* to observe that the scenario we now describe is *not* considered to be a fraud! In this scenario, $\tilde{S}$ sends a message to a honest R who rejects it as being *not* authentic. However, when $\tilde{S}$ hands over this message to A, A decides that the message is authentic. If $\tilde{S}$ succeeds in sending such messages, we do *not* say that $\tilde{S}$ has performed a (successful) attack. This makes perfect sense and one should not confuse on-line authentication and contract schemes which are binding in court (practically forever). We only consider this problem and its solution in Section 5.)

In Section 2 we give an example of a scheme which achieves our goal. In Section 3 we formalize the requirements. Practical schemes are presented in Section 4. Extensions and adaptations of these schemes are discussed in Section 5. One of the adaptations allows the set-up of asymmetric conventional authentication to allow unconditionally secure authentication in network environments. In Section 5 we discuss the relation between oblivious transfer and arbitrage and we then conclude in Section 6.

2 An elementary example

To keep the example simple we will momentarily only worry about impersonation attacks. It means that S wants to send *one fixed* message at some beforehand unknown moment; so our message space $\mathcal{M} = \{h\}$. We also do not yet intend to achieve schemes for which the cheating probabilities are very small. In these schemes, as well as in all our schemes, the key initialization phase contains three parts. First, R and S agree on some common information, $X_{(S,R)}$, secret to A. Secondly, R will choose some key, $X_{(R,A)}$, and communicate it to A. This $X_{(R,A)}$ identifies some subset of codewords. Thirdly, A selects out of this a subsubset and sends the key, $X_{(S,A)}$ to S to identify the selected subsubset. The scheme relies on random decisions by the parties: when b is chosen out of the set $\mathcal{B}$ with uniform probability distribution, we denote the event $b \in_R \mathcal{B}$.

In our first example let the set of *all* codewords (valid or non-valid) be $\mathcal{C} = \{0, 1, \ldots, 7\}$. To simplify our discussion let us organize those codewords in the following matrix:

$$T = \begin{pmatrix} 0 & 2 & 4 & 6 \\ 1 & 3 & 5 & 7 \end{pmatrix}$$

The set of codewords, $\mathcal{C}$ is public. Using the key initialization phase the private sets: $\mathcal{C}_R$, $\mathcal{C}_A$, and $\mathcal{C}_S$ will be set up. $\mathcal{C}_R$ is the set of codewords that R accepts as authentic. $\mathcal{C}_A$ is the set of codewords for which A will certify that they originate from R (this certification is not necessarily correct). And finally, $\mathcal{C}_S$ is the set of codewords that S will actually use to communicate authentic messages. To build up these sets, S, R, and A are involved in the following protocol in which keys are interchanged during the key initialization phase:

Step 1 S and R agree on one bit $X_{(S,R)}$ ($X_{(S,R)} \in_R \mathcal{X}_{(S,R)} = \{0,1\}$), which identifies a row in T.

Step 2 R and A agree on the pair $X_{(R,A)} = (m,n)$, where $m \neq n$, $m,n \in \{0,1,2,3\}$. The numbers m and n indicate the codewords $2m, 2m+1, 2n, 2n+1$, which correspond to two different columns in T. In other words $X_{(R,A)} \in_R \mathcal{X}_{(R,A)} = \{(0,1),(0,2),\ldots,(2,3)\}$.

Step 3 A selects one of these columns and gives the selection to S. Hereto A sends to S: $X_{(S,A)} \in_R \{m,n\}$.

The keys $X_{(S,R)}$ and $X_{(S,A)}$ specify uniquely the set of codewords, $\mathcal{C}_S$, that S will use. When S wants to send R her message h, she will send him the codeword: $2 \cdot X_{(S,A)} + X_{(S,R)}$ (so here $\mathcal{C}_S = \{2 \cdot X_{(S,A)} + X_{(S,R)}\}$). R will accept as authentic the codewords: $\mathcal{C}_R = \{2m + X_{(S,R)}, 2n + X_{(S,R)}\}$. (So here also $X_{(S,R)}$ and $X_{(R,A)}$ determine uniquely $\mathcal{C}_R$.) A will certify as being authentic (as being a codeword which originates from S) the codewords belonging to $\mathcal{C}_A = \{2X_{(S,A)}, 2X_{(S,A)} + 1\}$. So $\mathcal{C}_A$ consists of one column of the matrix T.

Let us now discuss informally the security, against several attacks, of the above scheme. A cheating $\tilde{A}$ must guess the correct $X_{(S,R)}$, so the probability of a successful attack is $1/2$. When $\tilde{R}$ wants to cheat he could come up with $2m$, $2m+1$, $2n$, or $2n+1$. But A will only accept two of those as authentic, and because $\tilde{R}$ does not know $X_{(S,A)}$ his probability of a successful attack is $1/2$. When $\tilde{S}$ wants to perform her attack, she has to guess the other column that R has sent to A; her probability of success is $1/3$. Indeed, $\tilde{S}$ knows that 4 pairs are possible, but that the $X_{(S,A)}$'s column (which corresponds to $(2X_{(S,A)}, 2X_{(S,A)}+1)$) is impossible because A would certify it as originating from S. Thus, three columns are left over to choose from, but there is only one other column of codewords that R will accept as being authentic. Finally the outside opponent's probability of success is $1/4$, because the receiver will only accept two out of eight codewords of T as being authentic. Notice that the example above relies on the decisions made bilaterally and individually.

Observe that in this example the set $\mathcal{X}_{(S,A)} = \{0,1,2,3\}$. The probability that a particular key $X_{(S,A)}$ has been chosen depends on the actual value of $X_{(R,A)}$. Although S and A share $X_{(S,A)}$ the choice of it has only been made by A.

3 Formalizing the problem and theoretical results

Let us first formalize what our objectives are. To be general we will allow each participant (S, R and A) to make their subset of codewords using shared keys and using private information.

Definition 1 Let $\mathcal{M}$ be a non-empty message space (sometimes called the set of source states). Let $\mathcal{C}$ be the set of codewords. Let $G = (\mathcal{V}, \mathcal{E})$ be a complete graph with vertex set $\mathcal{V} = \{S, R, A\}$. Let $\mathcal{X}$ and $\mathcal{Y}$ be respectively the collection of all $\mathcal{X}_{(i,j)}$ $((i,j) \in \mathcal{E})$ and the collection of all $\mathcal{Y}_k$ $(k \in \mathcal{V})$, where $\mathcal{X}_{i,j}$ and $\mathcal{Y}_k$ are non-empty *key* sets. These sets are associated with edges and vertices, respectively. Each set of keys has a probability distribution associated with. We call the collection of these distributions $\mathcal{D}$. Let $\mathcal{F}$ be a set of functions associating a subset of codewords to keys such that $\mathcal{F} = \{f_{l,M} \mid l \in \mathcal{V} \text{ and } M \in \mathcal{M} \text{ and } f_{l,M} : \mathcal{B}_l \rightarrow \mathcal{P}(\mathcal{C})\}$ where $\mathcal{B}_S \subset \mathcal{X}_{(S,R)} \times \mathcal{X}_{(S,A)} \times \mathcal{Y}_S$, $\mathcal{B}_R \subset \mathcal{X}_{(S,R)} \times \mathcal{X}_{(R,A)} \times \mathcal{Y}_R$, and $\mathcal{B}_A \subset \mathcal{X}_{(S,A)} \times \mathcal{X}_{(R,A)} \times \mathcal{Y}_A$, and $\mathcal{P}(\mathcal{C})$ is the power set of $\mathcal{C}$. We call $\mathcal{B}$ the collection of $\mathcal{B}_l$ (where $l \in \mathcal{V}$). We say that $(G, \mathcal{M}, \mathcal{C}, \mathcal{X}, \mathcal{Y}, \mathcal{D}, \mathcal{B}, \mathcal{F})$ is a *communication scheme with sender S, receiver R, and arbiter A*, or shortly: a *communication scheme* when there is no ambiguity what S, R and A are.

In this text we will assume that there is no ambiguity when we speak about a communication scheme. In our initial example no Y_R was used. So $\mathcal{Y}_R$ contains only one element. From this viewpoint Simmons' scheme has the property that $|\mathcal{X}_{(S,R)}| = 1$.

Definition 2 In the key initialization phase each $(i,j) \in \mathcal{E}$ agrees securely on an $X_{(i,j)} \in \mathcal{X}_{(i,j)}$ and each $i \in \mathcal{V}$ chooses an $Y_i \in \mathcal{Y}_i$, which is done accordingly to distributions $\mathcal{D}_{(i,j)}$ and $\mathcal{D}_i$ respectively.

Let $\mathcal{C}_{S,M} = f_{S,M}(X_{(S,R)}, X_{(S,A)}, Y_S)$, $\mathcal{C}_{R,M} = f_{R,M}(X_{(S,R)}, X_{(R,A)}, Y_R)$, and $\mathcal{C}_{A,M} = f_{A,M}(X_{(S,A)}, X_{(R,A)}, Y_A)$. We call: $\mathcal{C}_S = \bigcup_{M \in \mathcal{M}} \mathcal{C}_{S,M}$, $\mathcal{C}_R = \bigcup_{M \in \mathcal{M}} \mathcal{C}_{R,M}$, and $\mathcal{C}_A = \bigcup_{M \in \mathcal{M}} \mathcal{C}_{A,M}$ the set of codewords that respectively S, R, and A accept.

The probability distributions $\mathcal{D}_{(R,A)}$, $\mathcal{D}_{(S,R)}$ and $\mathcal{D}_R$ can be inter dependent. Similarly the probability distributions $\mathcal{D}_{(S,A)}$ and $\mathcal{D}_A$ can be inter dependent and could be a function of $X_{(R,A)}$. Finally $\mathcal{D}_S$ can be a function of $X_{(S,R)}$ and $X_{(S,A)}$.

A communication scheme is well defined when the above probability distributions guarantee that:

$$\begin{array}{lrcl}
\forall (X_{(S,R)}, X_{(S,A)}, Y_S) \in (\mathcal{X}_{(S,R)} \times \mathcal{X}_{(S,A)} \times \mathcal{Y}_S) \setminus \mathcal{B}_S : & \Pr(X_{(S,R)}, X_{(S,A)}, Y_S) & = & 0 \\
\forall (X_{(S,R)}, X_{(R,A)}, Y_R) \in (\mathcal{X}_{(S,R)} \times \mathcal{X}_{(R,A)} \times \mathcal{Y}_R) \setminus \mathcal{B}_R : & \Pr(X_{(S,R)}, X_{(R,A)}, Y_R) & = & 0 \\
\forall (X_{(S,A)}, X_{(R,A)}, Y_A) \in (\mathcal{X}_{(S,A)} \times \mathcal{X}_{(R,A)} \times \mathcal{Y}_A) \setminus \mathcal{B}_A : & \Pr(X_{(S,A)}, X_{(R,A)}, Y_A) & = & 0.
\end{array}$$

We say that *the number of interactions* in the key initialization phase is:

$$3 - \sum_{i \in \mathcal{E}} (\text{if } \{|\mathcal{X}_i| = 1\} \text{ then } 1 \text{ else } 0).$$

All the above distributions can be public or secret. The subsets $\mathcal{B}_l$ are however *all public.*

Let us now define what a secure authentication scheme is.

Definition 3 A well defined communication scheme $(G, \mathcal{M}, \mathcal{C}, \mathcal{X}, \mathcal{Y}, \mathcal{D}, \mathcal{B}, \mathcal{F})$ with arbiter A is *uniquely decodable* when simultaneously $\forall M \in \mathcal{M} : \mathcal{C}_{S,M} \subset \mathcal{C}_{R,M}$, $\mathcal{C}_{S,M} \neq$

$\emptyset$, and also: $\mathcal{C}_S \subset \mathcal{C}_A$, and that $\{\mathcal{C}_{R,M} \mid M \in \mathcal{M}\}$ forms a partition of $\mathcal{C}_R$. This partition naturally defines the function $m_S : \mathcal{C}_S \rightarrow \mathcal{M}$ and its extension $m_R : \mathcal{C}_R \rightarrow \mathcal{M}$. We will speak about m in both cases. When $\{\mathcal{C}_{A,M} \mid M \in \mathcal{M}\}$ forms a partition of $\mathcal{C}_A$ such that $\forall M \in \mathcal{M} : \mathcal{C}_{S,M} \subset \mathcal{C}_{A,M}$ we say that there is *no privacy protection relative to A.*

Remark 1 The subsets $\mathcal{B}_S$, $\mathcal{B}_R$ and $\mathcal{B}_A$ can now be motivated. The exclusion of some undesired choices helps guarantee that a communication scheme is uniquely decodable. Our first example illustrates this. Indeed given $X_{(R,A)}$ not all choices of $X_{(S,A)}$ are possible, otherwise we could not guarantee a particular scheme to be uniquely decodable.

In the final paper [5] we formally define $P_O, P_{\tilde{S}}, P_{\tilde{R}}, P_{\tilde{A}}$ and require that they are all less than 2^{-k}, where k is the security parameter. An informal definition can be found in [18]. When $P_{O_0} = P_{O_1} = P_{\tilde{S}} = P_{\tilde{R}_0} = P_{\tilde{R}_1} = P_{\tilde{A}_0} = P_{\tilde{A}_1} < 1$, we say that the scheme is *super-equitable*, which is motivated by Simmons' definition [18].

Our definitions are quite general. No restrictions whatsoever were imposed on the sets of keys ($X_{(S,R)}$, etc.) that can be communicated between the participants S, R, and A.

In the final paper [5] we prove the following theorems.

Theorem 1 *Super-equitable schemes for which the number of iterations is* 2 *do exist.*

Theorem 2 *Let $k > 0$. For a k-secure authentication scheme (with arbiter) which uses a 2-interaction key initialization phase, holds that $k \leq 1$. So P_O or $P_{\tilde{S}}$ or $P_{\tilde{R}}$ or $P_{\tilde{A}}$ is larger or equal to 1/2.*

So, to obtain a decent security one needs 3 interactions in the key initialization phase. Practical schemes exist, in the next section we will discuss some practical schemes based on geometry.

4 Practical secure authentication schemes with arbiter

In this section we will use many sets. Hereto we first define the functions f_S, f_R, and f_A. These have the same domains and co-domains as the functions $f_{S,M}$, $f_{R,M}$, and $f_{A,M}$ respectively (see Definition 1) such that:

$$\begin{aligned}
f_S(X_{(S,R)}, X_{(S,A)}, Y_S) &= \bigcup_M f_{S,M}(X_{(S,R)}, X_{(S,A)}, Y_S) \\
f_R(X_{(S,R)}, X_{(R,A)}, Y_R) &= \bigcup_M f_{R,M}(X_{(S,R)}, X_{(R,A)}, Y_R) \\
f_A(X_{(S,A)}, X_{(R,A)}, Y_A) &= \bigcup_M f_{A,M}(X_{(S,A)}, X_{(R,A)}, Y_A)
\end{aligned}$$

and this holds for all possible inputs. So all those functions have as co-domain $\mathcal{P}(\mathcal{C})$. Using this terminology, for example, $\mathcal{C}_R = f_R(X_{(S,R)}, X_{(R,A)}, Y_R)$, which clarifies the above. The sets we define next give S some specific information about $\mathcal{C}_A$. S receives $X_{(S,A)}$ from A and this allows S to calculate the sets:

$$\mathcal{I}_A^{X(S,A)} = \bigcap_{\substack{(X_{(R,A)},Y_A) \in \mathcal{X}_{(R,A)} \times \mathcal{Y}_A \\ (X_{(S,A)},X_{(R,A)},Y_A) \in \mathcal{B}_A}} f_A(X_{(S,A)}, X_{(R,A)}, Y_A) \qquad (1)$$

$$\mathcal{U}_A^{X(S,A)} = \bigcup_{\substack{(X_{(R,A)},Y_A) \in \mathcal{X}_{(R,A)} \times \mathcal{Y}_A \\ (X_{(S,A)},X_{(R,A)},Y_A) \in \mathcal{B}_A}} f_A(X_{(S,A)}, X_{(R,A)}, Y_A) \qquad (2)$$

The notation of these sets is easy to read when the following mnemonics is used. The above sets give information about $\mathcal{C}_A$, and $\mathcal{I}_A^{X(S,A)}$ and $\mathcal{U}_A^{X(S,A)}$ can be computed starting only from $X_{(S,A)}$, that is, when $X_{(S,A)}$ is known. The symbol $\mathcal{I}$ indicates intersection and we use the symbol $\mathcal{U}$ when the union of sets is involved.

All sets defined in the sequel are denoted similarly, these are:

$$\mathcal{I}_A^{X(R,A)} = \bigcap_{\substack{(X_{(S,A)},Y_A) \in \mathcal{X}_{(S,A)} \times \mathcal{Y}_A \\ (X_{(S,A)},X_{(R,A)},Y_A) \in \mathcal{B}_A}} f_A(X_{(S,A)}, X_{(R,A)}, Y_A) \qquad (3)$$

$$\mathcal{I}_R^{X(R,A)} = \bigcap_{\substack{(X_{(S,R)},Y_R) \in \mathcal{X}_{(S,R)} \times \mathcal{Y}_R \\ (X_{(S,R)},X_{(R,A)},Y_R) \in \mathcal{B}_R}} f_R(X_{(S,R)}, X_{(R,A)}, Y_R) \qquad (4)$$

$$\mathcal{I}_R^{X(S,R)} = \bigcap_{\substack{(X_{(R,A)},Y_R) \in \mathcal{X}_{(R,A)} \times \mathcal{Y}_R \\ (X_{(S,R)},X_{(R,A)},Y_R) \in \mathcal{B}_R}} f_R(X_{(S,R)}, X_{(R,A)}, Y_R) \qquad (5)$$

and similarly we define $\mathcal{U}_A^{X(R,A)}$, $\mathcal{U}_R^{X(R,A)}$, and $\mathcal{U}_R^{X(S,R)}$ by replacing the intersection symbols by union symbols in respectively (3), (4), and (5).

In this section $|\mathcal{Y}_S| = 1$, $|\mathcal{Y}_R| = 1$ and $|\mathcal{Y}_A| = 1$. In order to facilitate reading, we will often, in this section, use the symbols $\mathcal{U}_R^{X(S,R)}$, $\mathcal{U}_R^{X(R,A)}$, etc. without proving immediately that this notation is compatible with our definitions.

Before explaining our general practical scheme (any $\mathcal{M}$) we now explain a very similar scheme for which $|\mathcal{M}| = 1$ which will facilitate the grasping of our general scheme. In this scheme p is a public prime, and $|p| \geq k$. $\mathcal{C}$ corresponds with the *three* dimensional space: $Z_p \times Z_p \times Z_p$, which co-ordinates are denoted by (x, y, z).

The key initialization phase

Step 1 R chooses $X_{(S,R)} \in_R Z_p$, $X^1_{(R,A)} \in_R Z_p$, and $X^2_{(R,A)} \in_R Z_p$. Then R sends S the number $X_{(S,R)}$ and A the pair: $X_{(R,A)} = (X^1_{(R,A)}, X^2_{(R,A)})$ to which respectively correspond the 2-dimensional planes:

$$\begin{aligned} \mathcal{U}_R^{X(S,R)} :& \qquad y &= X_{(S,R)} \\ \mathcal{U}_A^{X(R,A)} = \mathcal{U}_R^{X(R,A)} :& \qquad x + X^1_{(R,A)} \cdot z &= X^2_{(R,A)} \,. \end{aligned}$$

$\mathcal{C}_R = \mathcal{U}_R^{X(S,R)} \cap \mathcal{U}_A^{X(R,A)}$, which is always a 1-dimensional line.

Step 2 A chooses $X^1_{(S,A)} \in_R Z_p$ and calculates: $X^2_{(S,A)} = X^2_{(R,A)} - X^1_{(S,A)} \cdot X^1_{(R,A)}$ sends S the pair: $X_{(S,A)} = (X^1_{(S,A)}, X^2_{(S,A)})$. $\mathcal{C}_A$ corresponds with the 1-dimensional line:

$$\begin{cases} x = X^2_{(S,A)} \\ z = X^1_{(S,A)} . \end{cases}$$

Step 3 The set $\mathcal{C}_S = \mathcal{U}_R^{X_{(S,R)}} \cap \mathcal{C}_A = \{(X^2_{(S,A)}, X_{(S,R)}, X^1_{(S,A)})\}$.

When S wants to send her message (in the transmission phase), she sends R the following codeword: $(X^2_{(S,A)}, X_{(S,R)}, X^1_{(S,A)})$. Observe that S knows $\mathcal{C}_A$ and that $\mathcal{C}_A$ is the intersection of $\mathcal{U}_A^{X_{(R,A)}}$ with the 2-dimensional plane: $z = X^1_{(S,A)}$.

It is not too difficult to analyze that $P_{O_0} = 1/p^2$, $P_{\tilde{A}_0} = 1/p$ and that $P_{\tilde{R}_0} = 1/p$. In the final paper we will explain why $P_{\tilde{S}} = 1/p$.

Let us now explain the general scheme. In this scheme p is a public prime, and $|p| \geq k$ and $p = |\mathcal{M}|$. $\mathcal{C}$ corresponds to the *four* dimensional space: $Z_p \times Z_p \times Z_p \times Z_p$, which coordinates are denoted by (x, y, z, u). We denote this four dimensional space as: Z_p^4.

The key initialization phase

Step 1 R sends S the tuple $X_{(S,R)} = (X^1_{(S,R)}, X^2_{(S,R)}) \in_R Z_p^2$ and R sends A the tuple: $X_{(R,A)} = (X^1_{(R,A)}, X^2_{(R,A)}, X^3_{(R,A)}) \in_R Z_p^3$ to which respectively correspond the 3-dimensional planes:

$$\begin{array}{rrcll} \mathcal{U}_R^{X_{(S,R)}} : & y & = & X^1_{(S,R)} \cdot u + X^2_{(S,R)} & (6) \\ \mathcal{U}_A^{X_{(R,A)}} = \mathcal{U}_R^{X_{(R,A)}} : & x + X^1_{(R,A)} \cdot z & = & X^2_{(R,A)} \cdot u + X^3_{(R,A)}. & (7) \end{array}$$

$\mathcal{C}_R = \mathcal{U}_R^{X_{(S,R)}} \cap \mathcal{U}_A^{X_{(R,A)}}$, which is always a 2-dimensional plane.

Step 2 A chooses and/or calculates:

$$\begin{array}{rcll} X^1_{(S,A)} & \in_R & Z_p & \\ X^2_{(S,A)} & \in_R & Z_p & \\ X^3_{(S,A)} & = & X^2_{(R,A)} - X^1_{(S,A)} \cdot X^1_{(R,A)} & (8) \\ X^4_{(S,A)} & = & X^3_{(R,A)} - X^2_{(S,A)} \cdot X^1_{(R,A)} & (9) \end{array}$$

and sends S the tuple: $X_{(S,A)} = (X^1_{(S,A)}, X^2_{(S,A)}, X^3_{(S,A)}, X^4_{(S,A)})$. $\mathcal{C}_A$ corresponds with the 2-dimensional plane:

$$\begin{cases} z = X^1_{(S,A)} \cdot u + X^2_{(S,A)} \\ x = X^3_{(S,A)} \cdot u + X^4_{(S,A)} . \end{cases} \qquad (10)$$

Step 3 The set $\mathcal{C}_S = \mathcal{U}_R^{X_{(S,R)}} \cap \mathcal{C}_A$, which is always a 1-dimensional line.

When S wants to send the message $M \in \mathcal{M}$, she calculates the codeword:

$$(x_0, y_0, z_0, M) = (X^3_{(S,A)} \cdot M + X^4_{(S,A)}, X^1_{(S,R)} \cdot M + X^2_{(S,R)}, X^1_{(S,A)} \cdot M + X^2_{(S,A)}, M)$$

and she sends it to R. Observe that S knows C_A and that C_A is the intersection of $\mathcal{U}_A^{X(R,A)}$ with the 3-dimensional plane: $z = X^1_{(S,A)} \cdot u + X^2_{(S,A)}$.

Theorem 3 *When $|p| \geq k$ and $p = |\mathcal{M}|$ then the general scheme is a k-secure authentication scheme with arbiter. The length of the key is proportional to k and when $|\mathcal{M}| \leq 2^k$ the length of the key is independent of k. The length of the codewords (when $p = |\mathcal{M}|$) is $4|p|$.*

When $|\mathcal{M}| > 2^k$ the scheme can easily be adapted, however the scheme is then no more so optimal. Observe that in the Wegman-Carter (no-arbiter) scheme [19] the length of the codewords is dramatically shorter.

5 Extensions

Here we introduce the ideas, in the final paper [5] we will formalize the problem and describe in more detail the solutions.

A new fraud in arbitrated authentication is a *jamming* type fraud. Indeed when during the key initialization phase of the previous scheme $\tilde{A}$ gives S an C'_A which is *not* a subset of $U_R^{X(R,A)}$, then R will reject all S's codewords! By using a similar idea as in [17] an extensions of the geometry based scheme protects probabilisticly against such frauds. Another extension gives a family of super-equitable authentication schemes with arbiter.

We now discuss asymmetric conventional authentication. Suppose that a sender S wants to send (broadcast) the *same* message to n (*e.g.* two) individuals $R_1, R_2, \ldots, R_n$ and authenticate it with an unconditionally secure scheme. The first solution would be that S gives the *same* key to all R_i, however each R_i could impersonate S. To avoid this fraud, the obvious solution is to use n keys and to send n authenticated messages (each authenticated with a different key). This transmission procedure is slow and no real broadcast can be used. The apparent ideal solution would be a signature scheme, but as said in the introduction, this requires a one-way function and the solution is no longer unconditional secure. We now discuss a situation in which a compromise solution is quite acceptable.

Suppose that Sandy, a new president of an investment company, gives each of her n brokers a different key K_i and keeps the "master key": K. In an emergency, such as a stock exchange crash, she will use K to authenticate M giving *one* codeword C, which she will broadcast. Ideally the length of C is independent of n. By adapting our geometrical scheme, such scheme can be constructed. This is formalized and a solution is presented in [5].

A major observation is that *each family of authentication schemes with arbiter A is a 1-out-of-2 family of secure asymmetric authentication schemes.* Indeed choose

$R_1 = R$ and $R_2 = A$. However, in the key initialization phase of an asymmetric authentication scheme there is no longer a secure communication channel between R_1 and R_2, so the scheme must be adapted. To solve this let us make a very important observation (see also [18, p. 101]). The schemes of Section 4 remains functional when S chooses $X_{(S,R)}$ (i.e. the plane $\mathcal{U}_R^{X(S,R)}$) and $X_{(S,A)}$ (i.e. the set $\mathcal{C}_A$) and sends those securely to respectively R and A. Then A chooses some $X_{(R,A)}$ (i.e. a plane containing $\mathcal{C}_A$) and sends it securely to R. As before, $\mathcal{C}_R = \mathcal{U}_R^{X(S,R)} \cap \mathcal{U}_A^{X(R,A)}$. In the asymmetric authentication scheme there is no need for the communication of $X_{(R,A)}$. This remark is the driving force behind the scheme which was only introduced here; we will describe the scheme in the final paper. Another feature of the system which enhances its applicability is the fact that it may be used in such a way so that only one receiver (say, R_1) will accept the message.

Another extension allows oblivious transfer [12]. In an oblivious transfer system Bob sends a codeword to Cleo. The probability that this codeword is meaningful is 1/2. In oblivious transfer Cleo knows when she received the message, however Bob does not, thus the transfer is indeed oblivious. We now prove that this can be achieved using secure authentication systems with arbiter. Let Bob correspond to R and Cleo with S and suppose that we have an authentication system with arbiter such that: $|\mathcal{C}_R| = 2 \cdot |\mathcal{C}_S|$. Observe that the sender corresponds to R now and the potential receiver to S! In the final paper we will prove that this system is an oblivious transfer system. Our goal, of course, was not to suggest an oblivious transfer with three parties as a major discovery, but rather to draw the analogy of the requirements of the authentication scheme protected against attacks by all participants and such an oblivious transfer scheme, which actually shows the strength of the authentication scheme.

6 Conclusions

While Simmons scheme does not protect against impersonation and substitution by the arbiter, the schemes presented here do protect against such frauds. Compared with Simmons solution our schemes use one interaction more in the key initialization phase than Simmons schemes. However we have demonstrated that 3 interactions are necessary (in the key initialization phase) to come up with a decent security.

We have presented a practical scheme for which the length of the key is only proportional to $\log_2(|\mathcal{M}|)$, which is better than in Simmons scheme. And, we have shown that a scheme with an arbiter allows us to come up with an oblivious transfer system.

The paper introduces many open problems. First, can arbitrated authentication schemes be obtained which are optimal as the Wegman-Carter scheme. Do other examples exist of asymmetric conventional cryptosystems. What is the relation between sharing and authentication?

Acknowledgments

The lecture of Gus Simmons at the Monte Verita workshop (October 15–21, 1989, Ascona, Switzerland) arouse the first author's interest in the topic of arbitrage. He thanks Gus Simmons for his enlightening explanations. The second author wishes to thank the U. of Wisconsin at Milwaukee for his visit where part of this work was done.

7 References

[1] E. F. Brickell and D. R. Stinson. Authentication codes with multiple arbiters. In C. G. Günther, editor, *Advances in Cryptology, Proc. of Eurocrypt '88 (Lecture Notes in Computer Science 330)*, pp. 51–55. Springer-Verlag, May 1988. Davos, Switzerland.

[2] W. de Jonge and D. Chaum. Attacks on some RSA signatures. In *Advances in Cryptology. Proc. of Crypto'85 (Lecture Notes in Computer Science 218)*, pp. 18–27. Springer-Verlag, New York, 1986. Santa Barbara, California, U.S.A., August 18–22, 1985.

[3] W. de Jonge and D. Chaum. Some variations on RSA signatures & their security. In A. Odlyzko, editor, *Advances in Cryptology, Proc. of Crypto'86 (Lecture Notes in Computer Science 263)*, pp. 49–59. Springer-Verlag, 1987. Santa Barbara, California, U. S. A., August 11–15.

[4] D. E. R. Denning. Digital signatures with RSA and other public-key cryptosystems. *Comm. ACM 27*, pp. 388–392, 1984.

[5] Y. Desmedt and M. Yung. Arbitrated unconditionally secure authentication can be unconditionally protected against arbiter's attacks. Full paper, available from authors, 1990.

[6] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory*, IT–22(6), pp. 644–654, November 1976.

[7] E. Gilbert, F. MacWilliams, and N. Sloane. Codes which detect deception. *The BELL System Technical Journal*, 53(3), pp. 405–424, March 1974.

[8] S. Goldwasser, S. Micali, and R. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *Siam J. Comput.*, 17(2), pp. 281–308, April 1988.

[9] R. Impagliazzo and M. Luby. One-way functions are essential for complexity based cryptography. In *30th Annual Symp. on Foundations of Computer Science (FOCS)*, pp. 230–235. IEEE Computer Society Press, October 30–November 1, 1989. Research Triangle Park, NC, U.S.A.

[10] C. H. Meyer and S. M. Matyas. *Cryptography: A New Dimension in Computer Data Security.* J. Wiley, New York, 1982.

[11] M. Naor and M. Yung. Universal one-way hash functions and their cryptographic applications. In *Proceedings of the twenty first annual ACM Symp. Theory of Computing, STOC*, pp. 33–43, May 15–17, 1989.

[12] M. Rabin. How to exchange secrets by oblivious transfer. Technical Memo TR-81, Havard Center for Research in Computer Technology, 1981.

[13] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Commun. ACM*, 21, pp. 294–299, April 1978.

[14] J. Rompel. One-way functions are necessary and sufficient for secure signatures. In *Proceedings of the twenty second annual ACM Symp. Theory of Computing, STOC*, pp. 387–394, May 14–16, 1990.

[15] G. J. Simmons. Message authentication with arbitration of transmitter/receiver disputes. In D. Chaum and W. L. Price, editors, *Advances in Cryptology — Eurocrypt '87 (Lecture Notes in Computer Science 304)*, pp. 151–165. Springer-Verlag, Berlin, 1988. Amsterdam, The Netherlands, April 13–15, 1987, full paper submitted to the Journal of Cryptology.

[16] G. J. Simmons. A survey of information authentication. *Proc. IEEE*, 76(5), pp. 603–620, May 1988.

[17] G. J. Simmons. Robust shared secret schemes. *Congressus Numerantium*, 68, pp. 215–248, 1989.

[18] G. J. Simmons. A Cartesian product construction for unconditionally secure authentication codes that permit arbitration. *Journal of Cryptology*, 2(2), pp. 77–104, 1990.

[19] M. N. Wegman and J. L. Carter. New hash fuctions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22, pp. 265–279, 1981.