Secure Multiround Authentication Protocols

Christian Gehrmann

Dept. of Information Theory, Lund University,
Box 118, S-221 00, Lund, Sweden,
Tel: +46-46-104353,
Fax: +46-46-104714,
Email: chris@dit.lth.se

Abstract. Gemmell and Naor proposed a new protocol for unconditionally secure authentication of long messages. However Gehrmann showed that the proof of the security of the protocol was incorrect. Here we generalize the multiround protocol model. We prove the security of a 3-round protocol and give for this case a new easy implementable construction which has a key size close to the fundamental lower bound for even extremely long messages. Furthermore, we give a proof of a secure multiround protocol for an arbitrary number of rounds.

1 Introduction

Gemmell and Naor [1] proposed an unconditionally secure authentication scheme (or A-code) without secrecy in which, by following a protocol, codewords are passed back and forth. This scheme makes it possible, albeit at the expense of increasing data exchange, to authenticate very large messages while keeping the key size small. It was shown by Johansson, Kabatanskii and Smeets in [2] that for single round authentication the key size is bounded by the logarithm of the message size.

Denote by $\log^{(k)}(x)$ a k-times logarithm $\log(\log(...log(x)))$. Gemmell and Naor showed that their k-round protocol for a message size of n bits demands a key size

$$H(K) \approx \log^{(k)}(n) + 2\log(\frac{1}{P_s}), \tag{1}$$

where P_s is the probability of a successful substitution attack for the scheme.

However, the security analysis made by Gemmell and Naor only took into account a certain substitution attack. In [3] Gehrmann, by considering the impersonation attack, showed that protocols where the number of rounds is even are of no interest. Furthermore, he introduced a special six step substitution attack for which the probability calculation of P_s made by Gemmell and Naor did not hold. In this paper, we push the analysis further. We propose new protocols and prove their security.

In Section 2 we give a classification of possible attacks on multiround protocols. In the next section we propose a new 3-round protocol and also give a specific construction based on Reed-Solomon codes. Using the tools of Section 2 we give a proof of its security. In Section 4 we show how to make a secure protocol for an arbitrary number of rounds.

L.C. Guillou and J.-J. Quisquater (Eds.): Advances in Cryptology - EUROCRYPT '95, LNCS 921, pp. 158-167, 1995.

2 Attacks on multiround protocols

We will consider a system for message authentication in which a transmitter A wants to send a message to a receiver B by exchanging codewords. The transmission channel is supposed to be controlled by an opponent O, who can send own (new) codewords over the channel to A and B or substitute codewords sent by A or B with own new ones. A and B are assumed to share secret information, i.e., the key, unknown to the opponent. We denote by k the total number of codewords sent over the channel to authenticate the original message. Since the original message is sent by A we will denote this message by m^A. The corresponding message observed by B may have been changed by the opponent and will be denoted by m^B. The codewords used by the protocol in the authentication process we will denote by subindex. For example m_i denotes the i-th exchanged codeword. A $k = 3$ round authentication protocol is shown in the figure below.

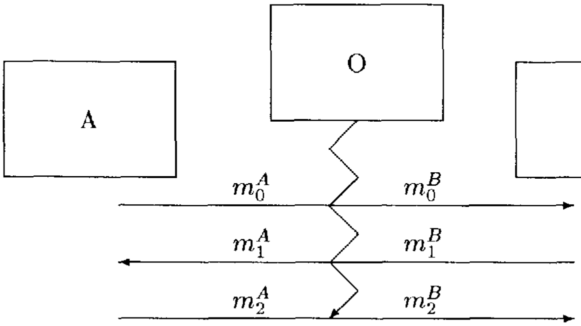

Figure 1: Multiround authentication for $k = 3$.

We will use the following notation:

$\underline{m}^A = m_0^A, (m_1^A), ..., m_{k-1}^A$: a by A sent and (received) codeword sequence.
$\underline{m}^B = (m_0^B), m_1^B, ..., (m_{k-1}^B)$: a by B sent and (received) codeword sequence.
$\underline{M}$: the set of possible codeword sequences.
K: the secret key.
P_I: probability of a successful impersonation attack.
P_S: probability of a successful substitution attack.

For the Gemmell and Naor multiround protocol it was shown [3] that the last round should be omitted if k is even. This implies that in contrast with the Gemmell and Naor model it always have to be the receiver that detects the intruder. Hence, in our generalized multiround authentication model we will in the sequel assume k to be odd.

The attack described by Gehrmann follows an asynchronous model, which was the model used by Gemmell and Naor. The attacks we describe in this paper will also be in accordance with an asynchronous protocol model. To avoid meaningless complications we make the assumption that B(A) immediately after receiving an even(odd) codeword responds with his own odd(even) codeword, i.e., we don't take into account the time delay for A and B. Depending on the secret key, not all sequences $\underline{M}$ are acceptable sequences. Denote by $\underline{M}(K)$ the subset of $\underline{M}$ that are allowable sequences under the specific key K. Depending on the odd number received codeword, his own chosen even number codeword and the key K, A will create and observe a sequence $\underline{m}^A \in \underline{M}(K)$. In a similar way B, by receiving even numbered codewords and responding odd numbered codewords, will observe a sequence $\underline{m}^B$. He accepts the sequence as a message from A if and only if $\underline{m}^B \in \underline{M}(K)$. We will deal with two attack scenarios depending on the capabilities given to the opponent.

2.1 Ordinary substitution attacks

This case corresponds to the ordinary model for single round authentication [4], [5], [6]. Here we assume that O has no capability to choose the message m^A to be authenticated. This original message m^A is for example in the Gemmell and Naor protocol equivalent with the first codeword m_0^A sent by A. All even numbered codewords observed by A and all odd numbered codewords observed by B are chosen by A and B respectively and hence the opponent O has only control over the codewords in the set

$$\mathcal{O} = \{m_0^B, m_1^A, m_2^B, ..., m_{k-2}^A, m_{k-1}^B\}.$$

O succeeds in a substitution attack if and only if he, during observation of the even codewords of $\underline{m}^A$ and odd codewords of $\underline{m}^B$, creats a sequence of codewords from the set $\mathcal{O}$, such that the corresponding sequence observed by B $\underline{m}^B \in \underline{M}(K), m^B \neq m^A$.

However as in the attack in [3], the order of the codewords substituted by the opponent could be chosen in an asynchronous way. Changing the order may increase P_s and thus all possible order of substitution must be taken into account when calculating P_s. Denote by t one particular substitution order (or type of attack) and by $\underline{m}(t), m_i(t) \in \mathcal{O}$, the corresponding sequence of codewords created by O (O-sequence). Furthermore, denote by $T_s(k)$ the set of valid differently ordered substitution sequences for a k-round protocol and by $|T_s(k)|$ the cardinality of this set.

We illustrate the notation with the following example.

Example 1. There are $|T_s(3)| = 3$ different types of attacks for the $k = 3$ round protocol. We have listed all the types in the table below together with the complete sequence of codewords observed on the channel(the codewords that O uses for a substitution attack are marked with arrows).

O-sequence	Whole sequence
$\underline{m}(1) = m_0^B, m_2^B, m_1^A$	$m_0^A, \rightarrow m_0^B, m_1^B, \rightarrow m_2^B, \leftarrow m_1^A, m_2^A$
$\underline{m}(2) = m_0^B, m_1^A, m_2^B$	$m_0^A, \rightarrow m_0^B, m_1^B, \leftarrow m_1^A, m_2^A, \rightarrow m_2^B$
$\underline{m}(3) = m_1^A, m_0^B, m_2^B$	$m_0^A, \leftarrow m_1^A, m_2^A, \rightarrow m_0^B, m_1^B, \rightarrow m_2^B$

Here $\underline{m}(3)$ is of the attack type analyzed in [3].

We have the following theorem on the number of different ordered O-sequences.

Theorem 1.

$$|T_s(k)| = \binom{k}{\frac{(k-1)}{2}}. \tag{2}$$

Proof. The subsequences $m_0^B, m_2^B, \ldots$ and $m_1^A, m_3^A, \ldots$ in $\underline{m}(t)$ have to be ordered. There are $\frac{(k-1)}{2}$ codewords in the A-subsequence, these should be chosen out of k differents positions in the O-sequence. Hence there are $\binom{k}{\frac{(k-1)}{2}}$ different O-sequences of length k.

Using the introduced definitions P_s may be written as

$$P_s = \max_{t \in T_s(k)} \max_{\underline{m}(t), m^B \neq m^A} \Pr\{\underline{m}^B \in \underline{M}(K)\}. \tag{3}$$

2.2 Chosen message substitution attacks

We will in the sequel deal with an attack model where the original message might freely be chosen by the opponent. This includes that O has the capability to choose *both* the first original message m^A *and* m^B, the one to substitute it with. When the opponent is also given the additional possibility to freely choose the original message m^A that should be authenticated, the situation looks different. The first codeword m_0^A sent by A may consists of just m^A or m^A and a second part created by A. In the chosen-message substitution scenario we assume that O may freely choose the part m^A of m_0^A and O thus has control over the set

$$\mathcal{O}' = \{m_0'^A, m_0^B, m_1^A, m_2^B, \ldots, m_{k-2}^A, m_{k-1}^B\},$$

where the $'$ marks that O maybe not might control m_0^A completely. Similar to the ordinary substitution attack case we denote by $T_c(k)$ the different ordered O-sequences of length $k+1$. We then have the following Corollary.

Corollary 2.

$$|T_c(k)| = \binom{k+1}{\frac{(k+1)}{2}}. \tag{4}$$

Proof. This case corresponds to that for Theorem 1 with a O-sequence of length $k+1$ and an A-subsequence of length $\frac{(k+1)}{2}$.

Similar to the ordinary substitution attack case we denote one particular ordered sequence by $\underline{m}(t)$. Denote by P_s' the probability of successful substitution attack for the chosen message scenario. P_s' may be written as

$$P_s' = \max_{t \in T_c(k)} \max_{\underline{m}(t), m^B \neq m^A} \Pr\{\underline{m}^B \in \underline{M}(K)\}. \tag{5}$$

Adding the chosen-message attack to the model increases the demands on the authentication protocol. A protocol that is secure in a model including the chosen-message attack is obviously also secure for the ordinary substitution attack model. We will from now on only consider protocol that are secure in the stronger chosen-message attack model sense. Change the demands on the protocols and only letting them be secure for the ordinary substitution attack might reduce the complexity.

Remark. In the single round authentication case there are different definitions of P_s in use. To ensure secure single authentication when the chosen-message attack is added to the model it is necessary to use the max max definition of P_s as for example made in [2], [7].

3 Secure k = 3 round protocols

We start with a special treatment for $k = 3$. We propose a protocol which is a modified version of that of Gemmell and Naor [1].

Let Q be a power of a prime and denote by C a code over $GF(Q)$ with length n. Let $p > \frac{1}{n}$ and the minimum distance d of the code C satisfy

$$d \geq n - np.$$

Denote by C^A an A-code for which the probability of a successful substitution attack is less or equal to p_s and the probability of a successful impersonation attack is less or equal to $p_I < p_s$. Let $C_i(m) \in GF(Q)$ be the code symbol at i-th coordinate of the codeword corresponding to message m. Denote by $a \circ b$ a concatenation between two words a and b. We suggest the following protocol for authentiation of the message m^A:

(i) A chooses a random number $j, 1 \leq j \leq l$, where l is chosen according to the desired security. A sends the codeword $m_0^A = j \circ m^A$

(ii) B receives codeword m_0^B and chooses a random number $i, 1 \leq i \leq n$. B sends codeword $m_1^B = i$.

(iii) A receives codeword m_1^A and uses the code C^A to transmit $m_2^A = C^A(m_1^A, C_{m_1^A}(m_0^A)) = C^A(m_1^A, C_{m_1^A}(j \circ m^A))$.

(iv) B receives codeword m_2^B and calculates $C^A(m_1^B, C_{m_1^B}(m_0^B))$ and accepts the codeword sequence as authentic if and only if $m_2^B = C^A(m_1^B, C_{m_1^B}(m_0^B))$.

Theorem 3. *Let* $a = \max_{m,i,c} |\{j : C_i(j \circ m) = c\}|$. *For the* $k = 3$ *round protocol above*

$$P_s' = \max(\frac{a}{l} + (1 - \frac{a}{l})p_s, p + (1-p)p_s) \tag{6}$$

the probability for a successful substitution attack when we also take into account the chosen-message attack.

Proof. Denote by $P_t = \max_{\underline{m}(t), m^B \neq m^A} \Pr\{\underline{m}^B \in \underline{M}(K)\}$. According to (4) there are $|T_c(3)| = \binom{4}{2} = 6$ possible attacks, when we also take into account the chosen-message attack, corresponding to the sequences

(1) $\rightarrow m_0^{\prime A}, \rightarrow m_0^B, m_1^B, \leftarrow m_1^A, m_2^A, \rightarrow m_2^B.$
(2) $\rightarrow m_0^{\prime A}, \leftarrow m_1^A, m_2^A, \rightarrow m_0^B, m_1^B, \rightarrow m_2^B.$
(3) $\rightarrow m_0^{\prime A}, \rightarrow m_0^B, m_1^B, \rightarrow m_2^B, \leftarrow m_1^A, m_2^A.$
(4) $\rightarrow m_0^B, m_1^B, \rightarrow m_0^{\prime A}, \rightarrow m_2^B, \leftarrow m_1^A, m_2^A.$
(5) $\rightarrow m_0^B, m_1^B, \rightarrow m_0^{\prime A}, \leftarrow m_1^A, m_2^A, \rightarrow m_2^B.$
(6) $\rightarrow m_0^B, m_1^B, \rightarrow m_2^B, \rightarrow m_0^{\prime A}, \leftarrow m_1^A, m_2^A.$

(3),(4),(6) Here O sends the last codeword m_2^B before receiving m_2^A and hence he gets no information about the secret key and the probability of a successful attack $P_3 = P_4 = P_6 = p_I < p_s$.

(1) O chooses a $m_0^B \neq m_0^{\prime A}$ and receives m_1^B. He succeeds with his attack by just letting $m_1^A = m_1^B$ and $m_2^B = m_2^A$ if $C_{m_1^B}(m_0^B) = C_{m_1^B}(m_0^{\prime A})$. Otherwise $m_1^B, C_{m_1^B}(m_0^B) \neq m_1^B, C_{m_1^B}(m_0^{\prime A})$ independent of the choice m_1^A and O has to find $C^A(m_1^B, C_{m_1^B}(m_0^B))$ given $C^A(m_1^A, C_{m_1^A}(m_0^{\prime A}))$. By the definition of the A-code the probability for this $\leq p_s$. B chooses m_1^B uniformly over $\{1, n\}$ and this together with the definition of the code C gives $\Pr\{C_{m_1^B}(m_0^B) = C_{m_1^B}(m_0^{\prime A})\} = p$ and hence the overall probability

$$P_1 = p + (1-p)p_s.$$

(2) O receives m_1^B after choosing m_1^A and hence

$$\Pr\{m_1^B, C_{m_1^B}(m_0^B) = m_1^A, C_{m_1^A}(m_0^{\prime A})\} \leq \frac{1}{n} < p.$$

If $m_1^B \neq m_1^A$ O must find $C^A(m_1^B, C_{m_1^B}(m_0^B))$ given $C^A(m_1^A, C_{m_1^1}(m_0^{\prime A}))$ and by the definition of the A-code the probability for that is less or equal to p_s and hence the overall probability satisfies

$$P_2 < p + (1-p)p_s.$$

(5) If O after receiving m_1^B finds an m^A such that $C_{m_1^B}(m_0^B) = C_{m_1^B}(m_0^{\prime A})$ he will succeed by choosing $m_1^A = m_1^B$ and $m_2^B = m_2^A$. Recall that $a = \max_{m,i,c} |\{j : C_i(j \circ m) = c\}|$ from the statement of the theorem. From

this definition and the fact that A choses j uniformly and at random over $\{1, l\}$ follows

$$\max_{m^A} \Pr\{C_{m_1^B}(m_0^B) = C_{m_1^B}(m_0'^A) | C_{m_1^B}(m_0^B)\} =$$
$$\max_{m^A} \Pr\{C_{m_1^B}(m_0^B) = C_{m_1^B}(j \circ m^A) | C_{m_1^B}(m_0^B)\} = \frac{a}{l}.$$

Otherwise $m_1^A, C_{m_1^B}(m_0^B) \neq m_1^A, C_{m_1^B}(m_0'^A)$ independent of the choice m_1^A and O has to find $C^A(m_1^B, C_{m_1^B}(m_0^B))$ given $C^A(m_1^A, C_{m_1^A}(m_0'^A))$. By the definition of the A-code the probability for this event $\leq p_s$. Hence the overall probability

$$P_5 = \frac{a}{l} + (1 - \frac{a}{l})p_s.$$

Now using (5) gives the desired result.

We will continue with giving an efficient construction by using Reed-Solomon codes (RS-codes).

Construction: For simplicity let $m = m^A$. Let $Q = 2^r, r = v2^{v-t-1}, l = 2^t$ and let C be an RS-code over $GF(Q)$ with $k = 2^s, r - s = t$. Hence

$$n = Q = 2^r$$
$$d = n - k = 2^r - 2^s.$$

Thus $p = (n - d)/n = k/n = 2^s/2^r = 2^{r-t}/2^r = 2^{-t}$. Further let $j \circ m$ be regarded as the k-tuple $(j \circ m_0, m_1, \cdots, m_{k-1})$ over $GF(Q)$, where j is the t first bits and m_0 the $r - t$ next bits of the element $j \circ m_0 \in GF(Q)$. Additionally let the code symbol of index β be obtained by evaluating the polynomial $C_\beta(j \circ m) = j \circ m_0 + m_1\beta + \cdots + m_{k-1}\beta^{k-1}$ as in the description of RS-codes [8]. Let the code C^A be the A-code obtained from a RS-code over $GF(2^v), k = 2^{v-t}$, as suggested in [2], i.e., $p_I = 2^{-v}, p_s = 2^{v-t}/2^v = 2^{-t}$. Thus we have a construction which needs t random bits at the transmission side, r random bits at the receiver side and with a key size of $2v$ bits. Furthermore, the construction allows a message size:

$$\log|M| = r(2^s - 1) + r - t = r2^{r-t} - t = v2^{v-t-1}2^{v2^{v-t-1}-t} - t. \tag{7}$$

Theorem 4. *For the construction above*

$$P_s' < 2^{1-t}. \tag{8}$$

Proof. Denote as in Theorem 3 by $a = max_{m,i,c}|\{j : C_i^1(j \circ m) = c\}|$. $\forall m, \beta, c$ the number of solutions of the following equation with respect to j

$$C_\beta(j \circ m) = j \circ m_0 + m_1\beta + \cdots + m_{k-2}\beta^{k-1} = c$$

is less or equal to 1 and hence $a = 1$. Further according to (6)

$$P_s = \max(\frac{a}{l} + (1 - \frac{a}{l})p_s, p + p_s - pp_s) =$$
$$= \max(\frac{1}{2^t} + (1 - \frac{1}{2^t})p_s, p + p_s - pp_s) =$$
$$= \max(2^{-t} + 2^{-t} - 2^{-2t}, 2^{-t} + 2^{-t} - 2^{-2t}) < 2^{1-t}.$$

The message size, key size and authenticator length for different parameters of the construction is listed in Table 1 below together with the concatenated RS-codes single authentication construction parameters of [7].

t	length of key	$\approx$ message length	
		new	[7]
20	42	22	120
20	44	2^{29}	2^{8}
20	46	2^{78}	2^{11}
20	48	2^{179}	2^{13}
40	82	82	210
40	84	2^{50}	2^{10}
40	86	2^{139}	2^{12}
40	88	2^{320}	2^{14}

Table 1. Key and message size in bits for the construction with $P_s < 2^{1-t}$.

It follows from the table above that the 3-round authentication system realizes very long message authentication by using short keys and that the key size even for extremely long messages is close to the Gilbert, MacWilliams and Sloane [9] famous square root bound for single authentication, i.e., $2\log(\frac{1}{P_s})$. The data expansion of the protocol is just $v2^{v-t}+t$ bits for a protocol with a key size of $2v$ bits and with $P_s' < 2^{1-t}$, and is hence almost negligible.

4 k $\geq$ 5 round protocol

As we have shown in the previous section, the 3-round protocol gives a secure authentication system with very short keys and few random bits for most practical situations. However to make the treatment complete we now also prove the security of a multiround protocol for an arbitrary number of rounds. Consider the following protocol:

Let p be a security parameter and C^r a code over $GF(Q_r), Q_r \geq \frac{2^{k-r}}{p}$ with length n_r and with minimum distance d satisfying

$$d \leq n_r - n_r \frac{p}{2^{k-1-r}}$$

and let C^A be a Cartesian A-code with a probability for a successful substitution and impersonation attack less than p. Furthermore, let $\forall r \leq k-2, 1 \leq i_r \leq n_r$ and $\forall r \leq k-4, 1 \leq j_r \leq \frac{2^{k-1}}{p}$, where the i's and j's chosen uniformly and random by either A or B when using the protocol. Let m_A and m_B be defined as

$$m_A = (C^{k-2}_{i^A_{k-2}}(\cdots(C^2_{i^A_2}(C^1_{i^A_1}(m^A), i^A_1), i^A_2, j^A_0)\cdots), i^A_{k-2}, j^A_{k-4}), \tag{9}$$

$$m_B = (C^{k-2}_{i^B_{k-2}}(\cdots(C^2_{i^B_2}(C^1_{i^B_1}(m^B), i^B_1), i^B_2, j^B_0)\cdots), i^B_{k-2}, j^B_{k-4}). \tag{10}$$

A $k \geq 5$ secure protocol is described below.

(i) $r = 0$, A chooses a random number j_0^A, and sends the codeword $m_0^A = (j_0^A, m^A)$.

(ii) $r = r + 1$, B receives codeword m_{r-1}^B and chooses two random numbers i_r^B, j_r^B. B sends codeword $m_r^B = (i_r^B, j_r^B)$.

(iii) If $r = k - 2$ then step v).

(iv) $r = r + 1$, A receives codeword m_{r-1}^A and chooses two random numbers i_r^A, j_r^A. A sends codeword $m_r^A = (i_r^A, j_r^A)$, back to step ii).

(v) A receives codeword m_{k-2}^A and uses the A-code to transmit codeword $m_{k-1}^A = C^A(m_A)$, where m_A is given by (9).

(vi) B receives codeword m_{k-1}^B, calculates $C^A(m_B)$, where m_B is given by (10) and accepts the codeword sequence as authentic if and only if $m_{k-1}^B = C^A(m_B)$.

Theorem 5. *For the protocol above*

$$P_s' < 2(1 - \frac{1}{2^k})p. \tag{11}$$

Proof. Among all $T_c(k)$ attacks we will consider only two types; i) either we follow the order of the protocol, i.e., the sequence

$$m_0^A, m_0^B, m_1^B, m_1^A, \ldots, m_{k-1}^A, m_{k-1}^B,$$

or ii) any of all the other types of attacks.

i) This case corresponds to that analyzed in [1] with adding the j's to the protocol. However the j's are not affecting the choice of indices and the proof still holds, giving the probability of successful attack less than

$$2(1 - \frac{1}{2^{k-1}})p.$$

ii) As in the proof of Theorem 3 if O sends the last codeword m_{k-1}^B before receiving m_{k-1}^A he succeeds with probability at most p. Thus assume m_{k-1}^B is the last codeword in the attack sequence and that after the codeword $l \geq 2, m_l^A$ (or $l \geq 3, m_l^B$) the order of the protocol is followed. An arbitrary attack sequence not equal to that of i) may then be described as

$$\cdots, m_{l-2}^A, m_{l-1}^A, m_l^A, m_l^B, m_{l+1}^B, \cdots, m_{k-1}^A, m_{k-1}^B$$

or

$$\cdots, m_{l-2}^B, m_{l-1}^B, m_l^B, m_l^A, m_{l+1}^A, \cdots, m_{k-1}^A, m_{k-1}^B,$$

where the dots $\cdots$ marks any allowable combination of the remaining part of the codewords. O succeeds by just forwarding the codewords between A and B if

$$(C_{i_l^A}^l(\cdots), i_l^A, j_{l-2}^A) = (C_{i_l^B}^l(\cdots), i_l^B, j_{l-2}^B). \tag{12}$$

O sends the codeword m_{l-2}^B (or m_{l-2}^A) before receiving m_{l-2}^A (or m_{l-2}^B) and he has thus no knowledge of j_{l-2}^A (or j_{l-2}^B) when choosing j_{l-2}^B (or j_{l-2}^A). Hence the probability of equality in (12) at most $\frac{p}{2^{k-1}}$. If $j_{l-2}^A \neq j_{l-2}^B$ it follows from i) that he succeeds with probability at most $2(1-\frac{1}{2^{k-1}})p$ and thus the overall probability of successful attack

$$\frac{p}{2^{k-1}} + (1 - \frac{p}{2^{k-1}})(2(1 - \frac{1}{2^{k-1}})p) < 2(1 - \frac{1}{2^k})p.$$

5 Conclusion

We have generalized the model of the Gemmell and Naor multiround protocol. A proof a secure 3-round protocol was given together with a very efficient construction for this protocol. The construction demands only a key size of 88 bits for a protocol which authenticate a message of size up to 2^{320} bits with probability of successful attack less than 2^{-39} and with a very small size of the data expansion. The 3-round protocol gives an unconditionally secure authentication system for most practical message sizes. Finally we have given a proof of a secure protocol for an arbitrary number of rounds.

References

1. P. Gemmell, M. Naor,"Codes for interactive authentication", *Proceedings of CRYPTO '93*, 1993, pp. 355-367.
2. T. Johansson, G. Kabatanskii, B. Smeets, "On the relation between A-codes and codes correcting independent errors", *Proceedings of Eurocrypt '93*, 1993, pp. 1-11.
3. C. Gehrmann, "Cryptanalysis of the Gemmell and Naor Multiround Authentication Protocol", *Proceedings of CRYPTO '94*, 1994, pp. 121-128.
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. J.L. Carter, M.N. Wegman, "New hash functions and their use in authentication and set equality", *J. Computer and System Sci.*, Vol 22, 1981, pp. 265-279.
6. D.R. Stinson, "Universal hashing and authentication codes", Design, Codes and Cryptography, vol. 4, no. 4, 1994. pp. 369-380.
7. J. Bierbrauer, T. Johansson, G. Kabatanskii, B. Smeets, "On Families of Hash Functions via Geometric Codes and Concatenation", *Proceedings of CRYPTO '93*, 1993, pp. 331-342.
8. I.S. Reed, G. Solomon, "Polynomial Codes over certain Finite Fields", J. Soc. Ind. Appl. Math., vol. 8, June 1960, pp. 300-304.
9. E. Gilbert, F.J. MacWilliams, N. Sloane, "Codes Which Detect Deception". Bell System Technical Journal. Vol. 53. No. 3. March 1974, pp. 405-424.