基于区组设计的具有仲裁的无条件安全认证码的构造 [1]

马文平 王新梅

(西安电子科技大学综合业务网国家重点实验室 西安 710071)

摘 要 本文借助区组设计给出一类具有仲裁的无条件安全认证码的构造方法，并给出一种安全的无条件安全认证码的构造方法，计算了有关参数.

关键词 区组设计，有仲裁的无条件安全认证码

中图号 TN918.1

1 引 言

通常的认证码 (简称 A-码) 总是假定发方和收方互相信任，共同防御对手的攻击，这类认证码得到了广泛的研究。然而，在现实生活中，发方和收方不一定互相信认，存在着互相欺骗的情况，基于这种考虑， G.J.Simmons 在文献 [1] 中提出了具有仲裁的认证码 (Authentication code that permit arbitration)，简称为 A^2-码，并给出了 A^2-码的一种构造方法。 T.Johansson 在文献 [2,3] 中分别给出了 A^2-码的有关信息论界和一些新的构造方法。 E.F.Brickell 和 D.R.Stinson 在文献 [4] 中给出了防止仲裁欺骗的多仲裁认证码。但与 A-码相比，人们对 A^2-码的研究还不够深入，特别是对 A^2-码的组合结构远没有对 A-码清楚。基于这种考虑，我们给出一种新的构造 A^2-码的方法，以及将非安全的具有仲裁的认证码改变成安全的 A^2-码的一种方法，这无疑对进一步研究 A^2-码的组合结构有一定的帮助。

一个具有仲裁的认证码具有四个参与者，即发方、收方、对手和仲裁。发方将要传寄的有关信息即源状态编码成消息后经过公开信道传给收方；收方收到消息后，不仅要从消息恢复源状态，而且要验证消息是否来自合法的发送者；为了这个目的，收方用他的秘密的编码规则来验证消息是否来自合法的发送者和由消息恢复源状态。我们用 S 表示源状态集合，用 M 表示消息集合，用 E_T 表示发方编码规则集合， E_R 表示收方编码规则集合。在构造具有仲裁的认证码时，为了防止发方和收方的互相欺骗，往往发方的一个编码规则和收方的多于一个的编码规则相关联，同时收方的一个编码规则和发方的多于一个编码规则相关联。仲裁是 A^2-码中最公正、最权威的人，发方和收方都信任仲裁，仲裁知道 A^2-码中的所有信息，包括发方和收方使用的秘密的编码规则。仲裁不参与任何通信活动，他唯一的任务是解决发方和收方发生的争端。

在 A^2-码中存在 5 种攻击，它们是： (1) 对手的模仿攻击。对手送一个消息给收方，若收方将其当作合法消息接收，就认为对手攻击成功。 (2) 对手的替换攻击。对手在信道中连续获得 L 个消息，让前 $L-1$ 个通过，然后替换第 L 个消息成对应不同源状态的另一个消息送给收方，若收方将其当作合法码字接收，则认为对手攻击成功，称这种攻击为对手的第 L 次 (L-fold) 替换攻击。 (3) 发方的模仿攻击。发方送一个消息给收方，这个消息不是由发方的编码规则产生，然后否认曾送过它，若收方将其当作合法码字接收，则认为发方模仿攻击成功。 (4) 收方的模仿攻击。在发方没有传送一个消息的清况下，收方宣称他收到了一个消息，若这个消息是由发方的编码规则产生，则认为收方模仿攻击成功。 (5) 收方的替换攻

[1] 1997-10-05 收到， 1999-01-09 定稿
国家自然科学基金 (69472083) 和国家教委博士点基金 (98070104) 资助课题

击。收方从信道中连续获得 L 个消息，将第 L 个消息替换成另一个对应于不同源状态的消息，若这个消息是发方编码规则的像，就认为收方的第 L 次 (L-fold) 替换攻击成功。

我们用 P_I, P_{S_l}, P_T, P_{R_0}, P_{R_l} 分别表示对手模仿攻击、对手的 L 次替换攻击、发方的模仿攻击、收方的模仿攻击、收方的 L 次替换攻击成功的概率。

由一般认证码 (即 A-码) 的性质我们很容易证明：在非安全 (no secrecy) 的 A^2-码中，有 $P_S \geq P_I \geq \max_{e_r}\{|e_r|\}/|M|$, $P_{R_l} \geq P_{R_{l-1}}$, $P_{S_l} \geq P_{S_{l-1}}$, $l = 1, 2, \cdots, |S| - 1$, $P_{R_0} \geq 1/\max_{e_r,s}\{|e_r(s)|\}$, $P_T \geq (\max_{e_r}\{|e_r|\} - |S|)/|M|$ 。

在这篇文章里，我们将给出一种用组合设计构造的使各种攻击成功概率 P_I, P_{S_l}, P_T, P_{R_0}, P_{R_l}, $l = 1, 2, 3, \cdots, |S| - 1$, 都达到其组合下界的不安全 (no secrecy) 的具有仲裁的认证码 (A^2-码) 的方法。 Thomas Tohanson 在文献 [2] 中采用密码技术在不安全的具有仲裁的认证码 (A^2-码) 的基础上构造了安全的具有仲裁的认证码 (A^2-码)，但怎样从组合设计角度构造安全的具有仲裁的认证码 (A^2-码)，国内外文献研究的不是很多。本文将给出一种用组合设计思想将不安全的具有仲裁的认证码 (A^2-码) 改变成安全的具有仲裁的认证码 (A^2-码) 的方法。

2　A^2-码的一种构造方法

首先我们介绍平衡不完全区组设计 (Balanced incomplete block design) 的概念。

定义　设 X 是有 v 个元素的集合，设 B 是一个 X 的 k 个元素的集合 (区组) 的集合 ($k \leq v$), 且 X 的任意两个元素都包含在 λ 个区组中，则 B 叫作平衡不完全区组设计，记作 2-(v, k, λ) 。

对于一个 2-(v, k, λ) 平衡不完全区组设计，有下列事实：区组数 $b = \lambda \begin{bmatrix} v \\ 2 \end{bmatrix} \Big/ \begin{bmatrix} k \\ 2 \end{bmatrix}$ ，集合 X 的每一个元素属于 r 个区组中，且 $bk = vr$ 。

下面给出 A^2-码的一种新的构造方法。设 $X_1, X_2, \cdots, X_n$ 分别是有 v 个元素的集合，我们用 X^n 表示这 n 个集合的笛卡儿积，即 $X^n = X_1 \times X_2 \times \cdots \times X_n$ ，我们令 $S = \{s_1, s_2, \cdots, s_n\}$ 表示源状态的集合，$e_t \in E_T$, e_t 是发方的一个编码规则，e_t : $s_i \to v_i, v_i \in X_i$ 。我们不妨假定 $X_1 = X_2 = \cdots X_n = X$, e_t: $S_i \to (s_i, v_i)$, $v_i \in X$, 发方编码规则的集合 $E_T = \{e_t\} = X^n$ ，因此，发方编码规则的数量有 v^n 个。设存在一个平衡不完全区组设计 2-$(v, k, 1)$, B 是它的区组的集合，令 $B^n = B \times B \times \cdots \times B$ 。 $e_r \in E_R$, e_r 是收方的一个编码规则， e_r: $s_i \to m_j$, $j = 1, 2, \cdots, k$, 它是一个 k 值映射，其中 $\{m_1, m_2, \cdots, m_k\}$ 构成 B 的一区组，因此收方编码规则的集合 $E_R = \{e_r\} = B^n$ ，从而我们看到收方编码规则的数量为 b^n ，这里 $b = v(v-1)/[k(k-1)]$ 。设 e_t, e_r 分别是发方和收方的一个编码规则，我们称它们是关联的当且仅当 e_t 的像包含在 e_r 的像中。显然任一个发方的编码规则与 r^n 个收方的编码规则相关联，一个收方的编码规则与 k^n 个发方的编码规则相关联。我们假定发方和收方的编码规则分布等概，源状态具有任意的概率分布。

认证通信过程的建立如下：发方在其编码规则的集合中随机的选取一个编码规则 e_t 作为自己的秘密的编码规则，然后将其通过安全信道秘密的寄给仲裁，仲裁在与发方的编码规则 e_t 相关联的收方的编码规则中随机的选取一个编码规则 e_r 秘密地寄给收方，作为收方的

验证的编码规则，这样我们就构造了一个具有仲裁的非安全认证码，即 A^2–码。我们有下列结果：

定理 1 由上面方法构造的 A^2–码，有下列事实：

(1) 发方编码规则的数量为 v^n 个，收方编码规则的数量为 b^n 个，源状态的数量为 n 个，消息的数量为 nv 个。

(2) $P_{I_0}=P_{S_l}=k/v,\ l=1,2,\cdots,n-1,\ P_{R_0}=P_{R_l}=1/k,\ l=1,2,\cdots,n-1,\ P_T=(k-1)/(v-1)$ 。

证明 (1) 由上面的构造过程很容易得出，这里省略。

(2) 依次计算五种攻击成功的概率。

(a) 对手模仿攻击成功的概率：由于收方的编码规则分布等概，对手随机的选取一个消息，不妨假定为 (S_1,v_1), 对手用它模仿攻击成功的概率为： $P_{I_0}(S_1,v_1)=rb^{n-1}/b^n=r/b=k/v$ ，因此对手模仿攻击成功的概率 $P_{I_0}=\max P_{I_0}(S_1,v_1)=k/v$ 。

(b) 对手在信道中连续获得 l 个消息 $(s_1,v_1),(s_2,v_2),\cdots,(s_l,v_l)$ 后：他会得到收方采用的编码规则的一些信息，对手通过分析可以得知，收方采用的编码规则是 r^lb^{n-l} 个中的某一个，对手让前 $l-1$ 个消息通过，并将第 l 个消息替换成消息 (S_{l+1},v_{l+1}), $S_{l+1}\neq S_i$, $i=1,2,\cdots,l$, 他成功的概率 $P_{S_l}(S_{l+1},v_{l+1})=r^lb^{n-l-1}r/(r^lb^{n-l})=r/b=k/v$, 所以对手连续获得 l 个消息后替换攻击成功的概率是： $P_{S_l}=\max P_{S_l}(S_{l+1},v_{l+1})=k/v, l=1,2,\cdots,n-1$ 。

(c) 收方模仿攻击成功的概率：由于收方拥有自己的秘密的编码规则，因此他知道发方采用的编码规则的一些信息，他知道发方采用的编码规则是与自己的秘密编码规则相关联的 K^n 个编码规则中的某一个，若收方的秘密的编码规则将源状态 s 对应于 k 个消息 $(s,v_1),(S,v_2),\cdots,(s,v_k)$, 则收方用 $(s,v_i),i=1,2,\cdots,k$, 攻击就可能成功, 用 $(s,v_{k+1}),v_{k+1}\neq v_i,i=1,2,\cdots,k$ 攻击不会成功, 收方用 $(s,v_i),i=1,2,\cdots,k$, 攻击成功的概率是 $P_{I_R}(s,v_i)=k^{n-1}/k^n=1/k$ ，所以收方模仿攻击成功的概率是 $P_{I_R}=\max P_{I_R}(s,v_i)=1/k$ 。

(d) 收方在信道中连续获得 l 个消息后替换攻击成功的概率：由于收方知道发方采用的编码规则是与自己的编码规则相关联的某个发方的编码规则，若他在信道中连续获得 l 个消息，不妨假定它们是 $(s_1,v_1),(s_2,v_2),\cdots,(s_l,v_l),\ l\leq n-1$, 则收方可通过分析得出发方采用的编码规则是 k^{n-l} 发方编码规则中的某一个，因此收方让前 $l-1$ 消息通过，用 $(s_{l+1},v_{l+1}),s_{k+1}\neq s_i,i=1,2,\cdots,l$ 替换第 l 个消息，攻击成功的概率是 $P_{R_l}(s_{l+1},v_{l+1})=k^{n-l-1}/k^{n-l}=1/k$, 故收方连续获得 l 个消息后替换攻击成功的概率是 $P_{R_l}=\max P_{R_l}(s_{l+1},v_{l+1})=1/k$ 。

(e) 发方模仿攻击成功的概率：发方从自己的秘密编码规则可得知收方采用的编码规则是与自己的秘密编码规则相关联的 r^k 个收方的编码规则中的某一个，我们假定发方的编码规则将 $s_1\to(s_1,v_1)$ ，发方用消息 (s_1,v_2) 攻击，由于我们采用平衡不完全区组设计构造 A^2–码，故 $\{v_1,v_2\}$ 包含在唯一的一个区组中，因此发方用 (s_1,v_2) 模仿攻击成功的概率是： $P_T(s_1,v_2)=r^{n-1}/r^n=1/r=(k-1)/(v-1)$ 。

至此，我们借助平衡不完全区组设计构造了使各种攻击成功的概率都达到其组合下界的认证码，这对进一步研究 A^2–码的组合结构有一定的帮助。应当看到，当我们只考虑 $l=1$ 时，使对手各种攻击成功的概率都达到最小的认证码的构造，我们的方法构造的认证码其编码规则还是比较多，不是使对手攻击成功的概率都达到最小且编码规则最少的认证码，但当

考虑 $l=1,2,\cdots,n-1$ 时，使对手各种攻击成功的概率都达到其组合下界的认证码，那么，我们上面的构造所用的编码规则却是比较少的。

3　安全的具有仲裁的认证码的构造

到目前为止，人们构造的 A^2-码大多数是非安全 (no secrecy) 的认证码，Thomas Johasson 在文献 [2] 中采用密码技术将其构造的非安全的认证码改变成安全的认证码，这个作法确实能达到将非安全的认证码改变成安全的认证码的目的，但我们认为他不能很好地体现 A^2-的组合结构。下面给出一种用组合设计的方法将不安全的 A^2-码改变成安全的 A^2-码的一般方法。首先给出一个定义：

定义　对于一个认证码，若对手从信道中获得任意一个消息 m，对于任意一个源状态 s，有 $P(s|m)=P(s)$，那么我们称这个认证码是安全的。

下面，我们给出一种将非安全的认证码改变成安全的认证码的方法。为了便于叙述，以本文构造的认证码为例说明这种思想。我们不妨假定集合 $X_0,X_1,\cdots,X_{n-1}$ 两两互不相交，用 $m_j^i,\ j=1,2,\cdots,v$ 表示集合 X_i 中的元素，$i=0,1,2,\cdots,n-1$，$S=\{s_0,s_2,\cdots,s_{n-1}\}$ 表示源状态的集合，$e_t^0\in E_T, e_t^0\colon s_i\to m_j^i$，表示前文构造中发方的任一个编码规则，$i=0,1,\cdots,n-1$。$Z/(n)$ 表示模整数 n 的环，我们对前文构造的发方的任一个编码规则进行循环置换，令：$e_t^f: s_{f+i}\to m_j^i$，这里 $f+i$ 是环 $Z/(n)$ 上的加法运算，集合 $\{e_t^f, f=0,1,2,\cdots,n-1\}$ 就构造了发方的编码规则的集合，设 e_r^0 表示前文中构造的收方的任一个编码规则，$e_r^0: s_i\to m_j^i, j=1,2,\cdots,k$，它是一个 k 值映射，其中 $\{m_1^i,m_2^i,\cdots,m_k^i\}$ 构成 B 的一个区组，我们对前面构造的收方的编码规则进行一些循环置换，我们令 e_r^f 是收方的一个编码规则，$e_r^f: s_{f+i}\to m_j^i, j=1,2,\cdots,k$，它也是一个 k 值映射，其中 $\{m_1^i,m_2^i,\cdots,m_k^i\}$ 构成 B 的一个区组，这里 $f+i$ 是环 $Z/(n)$ 上的加法运算，$f=0,1,\cdots,n-1$。集合 $\{e_r^f, f=0,1,\cdots,n-1, e_r^0\in E_R\}$ 表示收方编码规则的集合，认证通信的建立如同前文一样，这样就将前文构造的非安全认证码改变成了安全的认证码，我们有下面的定理：

定理 2　由上面步骤构造的认证码具有下面的性质：

(1) 上面的步骤将前文构造的非安全的认证码改变成安全的 A^2-码。

(2) $P_{I_0}=P_{S_l}=k/v,\ l=1,2,\cdots,n-1;\ P_{R_0}=P_{R_l}=1/k,\ l=1,2,\cdots,n-1;\ P_T=(k-1)/(v-1)$。

证明　(1) 我们假定对手在信道中获得一个消息 m，由构造过程知：对手获得消息 m 的概率 $p(m)=(rb^{n-1}/b^n)\sum_0^{n-1}P(s_i)=rb^{n-1}/b^n=r/b$，显然我们有 $P(m|s)=r/b$，所以 $P(s|m)=P(m|s)P(s)/P(m)=P(s)$。

(2) 证明与定理 1 的证明相似，我们将其省略。

参　考　文　献

[1] Simmons G J. A Cartesian product construction for unconditionally secure authentication codes that permit arbitration, J.Cryptology , 1990, 2(2): 77–104.

[2] Johansson T. Authentication codes for nontrusting parties obtained from rank metric codes,Designs Codes and Cryptography, 1995, 6(1): 205–218.

[3] Johansson T. Lower bounds on the probability of deception in authentication with arbitration, IEEE Trans. on IT, 1994, IT-40(5): 1573–1585.

[4] Brickell E F, Stinson D R. Authentication codes with multiple arbiters, Proceedings of Eurocrypt'88, Berlin: Springer-Verlag, 1988, 51–55.

[5] Stinson D R. A construction for authentication/secrecy codes from certain combinatorial designs, J. Crytology, 1988, 1(1): 119–127.

[6] Stinson D R. The combinatorics of authentication and secrecy codes, J. Crytology, 1990, 2(1): 23–49.

[7] Kurosawa K. New bound on uthentication code with arbitration, Proceedings of Crypto'94, Lecture notes in computer sicence, LNCS899, Berlin: Springer Verlag, 1989, 140–149.

A CONSTRUCTION FOR UNCONDITIONALLY SECURE AUTHENTICATION CODES WITH ARBITRATION OBTAINED FROM COMBINATORIAL DESIGNS

Ma Wenping Wang Xinmei

(*State Key Lab. on ISN, Xidian University, Xi'an* 710071)

Abstract A new method for construction of authentication codes with arbitration and secret authentication codes with arbitration is presented, some results are given.

Key words Combinatorial design, Authentication code with arbitration

马文平： 男， 1966 年生，博士，目前主要从事信息论、编码和密码研究和教学.

王新梅： 男， 1937 年生，教授，博士生导师，中国电子学会会士，长期从事信息论、编码和密码学的教学与研究.