(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104270247 B
(45)授权公告日 2018.05.01

(21)申请号 201410230418.1

(22)申请日 2014.05.23

(65)同一申请的已公布的文献号
申请公布号 CN 104270247 A

(43)申请公布日 2015.01.07

(73)专利权人 中国人民解放军信息工程大学
地址 450052 河南省郑州市高新区科学大道62号解放军信息工程大学

(72)发明人 曾光 马智 魏正超 杨阳 王洪

(74)专利代理机构 郑州大通专利商标代理有限公司 41111
代理人 陈大通

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/08(2006.01)

(56)对比文件
CN 101958790 A,2011.01.26,
CN 101242265 A,2008.08.13,
CN 1378361 A,2002.11.06,
US 2008298487 A1,2008.12.04,
崔珂等.基于FPGA的量子秘钥分发系统中身份认证的设计.《第十六届全国核电子学与核探测技术学术年会》.2012,

审查员 王亭

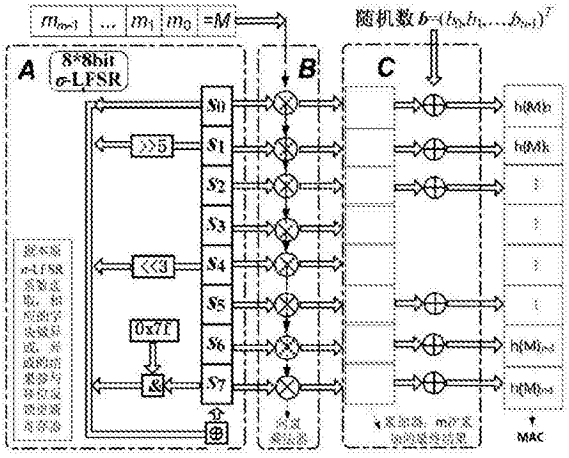
权利要求书2页 说明书6页 附图1页

(54)发明名称

适用于量子密码系统的高效泛Hash函数认证方法

(57)摘要

本发明公开了一种适用于量子密码系统的高效泛Hash函数认证方案，方案采用基于字的设计方式，方案将双方共享密钥和字线性反馈移位寄存器初始化完成后，利用字线性反馈移位寄存器的迭代和矢量乘法器，将认证消息和寄存器状态依次进行矢量乘法，并通过累加器累加，最后与随机数异或得到消息认证码，再将认证消息和消息认证码一起发送给另一方，达到身份认证的功能。本发明认证方案设计原理清晰、设计方式公开、不存在任何人为安全缺陷；所构成的认证方案可达到理想的安全属性，并具有占用资源少、可移植性好、平台适应性强的特点，可以为量子密码系统提供高效的身份认证功能。



CN 104270247 B

1.适用于量子密码系统的高效泛Hash函数认证方法，其特征在于，

组件A，一个基于字的σ-线性反馈移位寄存器，作为方法的Toeplitz矩阵生成部分，该基于字的σ-线性反馈移位寄存器共有n级，每一级含有s比特；

组件B，一个向量乘法器，作为方法的非线性变换部分，它可以完成两个s维向量到有限域元素的转换，然后进行有限域乘法，最后执行向量到有限域转换的逆变换，输出s比特向量；

组件C，累加器部分，实现所有乘法器输出的累加，并最终和随机数异或；

组件A、组件B、组件C的基本处理单元的大小都是s比特，方法首先完成初始化工作，然后进行消息迭代处理过程，在每次迭代更新组件A时，将新的消息块与基于字的σ-线性反馈移位寄存器状态进行向量乘法，然后送入累加器，最终异或随机数得到消息认证码；

认证方法采用的泛Hash函数为$h_{A,b}=A\cdot M+b$，其中A为n×m的Toeplitz矩阵，由基于字的σ-线性反馈移位寄存器构造，$M=(m_0,m_1,\cdots,m_{m-1})^T$为长度为sm bit的消息，$b=(b_0,b_1,\cdots,b_{n-1})^T$为sn bit的随机数，由量子密钥分配过程产生并存储在保密环境中，其中s为块的长度单位，认证方法具体包括如下步骤：

A)组件初始化，将双方共享的sn比特密钥值、基于字的σ-线性反馈移位寄存器的反馈逻辑、随机数和认证消息经过一系列的填充，置入到组件A的基于字的σ-线性反馈移位寄存器中；

B)泛Hash计算，组件A每迭代一步更新当前基于字的σ-线性反馈移位寄存器的状态值$(s_j,s_{j+1},\cdots s_{j+n-1})$，然后消息分块与当前基于字的σ-线性反馈移位寄存器的状态值进入组件B，即计算向量乘积

$$m_j\otimes\left(s_j,s_{j+1},\cdots,s_{j+n-1}\right)=(m_j\otimes s_j,m_j\otimes s_{j+1},\cdots,m_j\otimes s_{j+n-1}),$$

将结果反馈到累加器中进行累加，最终得到$\oplus_{j=0}^{m-1}(m_j\otimes\left(s_j,s_{j+1},\cdots s_{j+n-1}\right))$；

C)随机数异或，当所有消息处理完成后，累加器得到的结果需要和随机数做运算，计算

$$\mathrm{MAC}=[\oplus_{j=0}^{m-1}m_j\otimes\left(s_j,s_{j+1},\cdots s_{j+n-1}\right)]\oplus(b_0,b_1,\ldots,b_{n-1}),$$

此即为此时输出的n块消息认证码。

2.根据权利要求1所述的适用于量子密码系统的高效泛Hash函数认证方法，其特征在于，步骤A中所述填充方式具体过程如下：基于字的σ-线性反馈移位寄存器的初始化是将sn比特密钥$K=k_{n-1},k_{n-2},\cdots,k_0$分成n个连续的s比特块，并将其作为基于字的σ-线性反馈移位寄存器的初态，即$(s_{n-1},s_{n-2},\cdots,s_0)=K$，$k_{n-1}$是高位s比特，$k_0$是低位s比特，消息的填充方式是在消息后面首先填充一个1，然后填充若干个零，使得消息的总长度为分块的倍数，即是s的倍数；如果原始的消息恰好为s的倍数，也需要填充一个形如“1000…”的s比特填充块。

3.根据权利要求1所述的适用于量子密码系统的高效泛Hash函数认证方法，其特征在于，步骤B中基于字的σ-线性反馈移位寄存器和向量乘法器的更新方式如下：

1)基于字的σ-线性反馈移位寄存器的更新方式：组件A在初始化后按照如下的规则进行基于字的σ-线性反馈移位寄存器的状态更新：

$\mathrm{TMP\_A}=S_{n-1}A_{n-1}\oplus\ldots\oplus S_1A_1\oplus S_0A_0$；

$S_0=S_1$；

$S_1=S_2$；

…

$S_{n-2}=S_{n-1}$；

$S_{n-1}=TMP\_A$；

其中$A_0,\cdots,A_{n-1}$由基于字的σ-线性反馈移位寄存器定义，TMP_A为s比特字，$(S_{n-1},S_{n-2},\cdots,S_0)$的初始值为K；

2)向量乘法器的更新方式:组件B由有限域的一组基和有限域中的乘法构成，其更新方式为将输入两个s维向量通过有限域的基转化为两个有限域元素，然后做有限域乘法，再将其转换为一个s维向量输出。

适用于量子密码系统的高效泛Hash函数认证方法

技术领域

[0001] 本发明涉及息安全领域中的身份认证方法，特别是涉及一种适用于量子密码系统的高效泛Hash函数认证方法。

背景技术

[0002] 量子通信是近二十年发展起来的新型交叉学科，是量子论和信息论相结合的产物。它主要是利用量子纠缠效应进行信息传递，其研究主要涉及量子密码通信、量子远程传态和量子密集编码等。其中，量子密码通信实际上是一个密钥分发(QKD)的过程，其安全性主要依赖于量子力学中的海森堡不确定原理、单量子不可克隆定理和量子的不可分割性，使得窃听者的任何获取信息的操作都会因破坏量子态而被发现。以量子为载体的通信，具有以往经典通信所没有的安全优势，因而量子安全通信受到密码学界和物理学界的高度重视。

[0003] 在量子通信的经典BB84协议中，通信是由两个阶段共同完成的：第一阶段在量子通道进行密码的通信；第二阶段在经典通道进行密码的协商，检测窃听者是否存在，确定密码的内容，最终完成整个量子通信。该协议是假定收发双方都是合法的，而在实际的通信过程，不排除可能两端用户Alice或Bob有假冒的可能，因此有必要加入身份认证这一过程。

[0004] 身份认证技术是能一种能够对信息的收发方进行身份鉴别的技术，是保护信息安全的第一道大门，它的任务是识别、验证网络信息系统中用户身份的合法性、真实性以及抗抵赖性。传统的身份认证办法有很多种，如基于RSA，离散对数，椭圆曲线等身份认证方法，但是这些方法存在着面临量子计算的威胁，即它们是计算安全的。而量子通信中的认证需要达到无条件安全级别，故只能采用1979年Wegam和Carter提出的由Universal Hash族(泛Hash函数族)构造的无条件安全认证模型。使用这类函数族可以用少量共享密钥生成消息认证码，不知道密钥的窃听者只能以非常小的概率伪造有效的消息认证码，而且窃听者成功的概率不受攻击者计算能力的影响，从而保证了通信双方进行身份认证时的安全性。目前泛Hash函数有很多，如Toeplitz矩阵、UMAC、GMAC、Poly1305-AES等都是这类函数。Toeplitz矩阵和UMAC认证方法是量子密码系统常使用的方法。二者从安全性和实现效率相比来讲，后者效率较高但是需要的密钥量较多，实际中常使用密钥扩展，而这又降低了安全性；前者实现效率不高，同时安全参数与认证消息长度有关，不适合高速、大认证数据环境下使用。作为具有无条件安全属性的现代量子保密通信网络，各种机密、敏感、隐私数据的传输量将大大增加，这对无条件安全的认证技术的安全属性、速度和便捷性，提出了更高的要求。设计具有我国自主知识产权、满足现代量子保密通信网需求的认证方法，对推进我国量子保密通信技术的发展具有非常重要的理论及现实意义。

发明内容

[0005] 本发明的目的是：

[0006] 提供一种适用于量子密码系统的高效泛Hash函数认证方法。

[0007] 本发明的技术方法是：

[0008] 适用于量子密码系统的高效泛Hash函数认证方法，方法整体框架分为三个部分：组件A，一个基于字的σ-线性反馈移位寄存器(σ-LFSR)，作为方法的Toeplitz矩阵生成部分，该σ-LFSR共有n级，每一级含有s比特；

[0009] 组件B，一个向量乘法器，作为算法的非线性变换部分，它可以完成两个s维向量到有限域元素的转换，然后进行有限域乘法，最后执行向量到有限域转换的逆变换，输出s比特向量；

[0010] 组件C，累加器部分，实现所有乘法器输出的累加，并最终和随机数累加。

[0011] 方法中组件A、组件B、组件C的基本处理单元都是s比特，算法首先完成初始化工作，然后进行消息迭代处理过程，在每次迭代更新组件A时，将新的消息块与寄存器状态进行向量乘法，然后送入累加器，最终异或随机数得到消息认证码。

[0012] 认证方法采用的泛Hash函数为$h_{A,b}=A.M+b$，其中A为n×m的s-分块矩阵，$M=(m_0,m_1,\cdots,m_{m-1})^T$为长度为sm bit的消息，$b=(b_0,b_1,\cdots,b_{n-1})^T$为sn bit的随机数，其由量子密钥分配过程产生并存储在保密环境中，其中s为块的长度单位，认证方法具体包括如下步骤：

[0013] A)组件初始化，将双方共享的sn比特密钥值、字线性反馈移位寄存器的反馈逻辑、随机数和认证消息经过一系列的填充，置入到各部件的寄存器中；

[0014] B)泛Hash计算，组件A每迭代一步更新当前寄存器的状态值$(s_j,s_{j+1},\cdots s_{j+n-1})$，然后消息分块与当前寄存器的状态进入组件B，即计算向量乘积

[0015] $$m_j\otimes(s_j,s_{j+1},\cdots,s_{j+n-1})=(m_j\otimes s_j,m_j\otimes s_{j+1},\cdots,m_j\otimes s_{j+n-1}),$$

[0016] 将结果反馈到累加器中进行累加，最终得到$\oplus_{j=0}^{m-1}(m_j\otimes(s_j,s_{j+1},\cdots s_{j+n-1}))$；

[0017] C)随机数异或。当所有消息处理完成后，累加器得到的结果需要和随机数做运算，计算

[0018] $$\mathrm{MAC}=[\oplus_{j=0}^{m-1}m_j\otimes(s_j,s_{j+1},\cdots s_{j+n-1})]\oplus(b_0,b_1,\ldots,b_{n-1}),$$

[0019] 此即为此时输出的n块消息认证码。

[0020] 步骤A中所述填充方式具体过程如下：寄存器的初始化是将sn比特密钥$K=k_{n-1},k_{n-2},\cdots,k_0$分成n个连续的s比特块，并将其作为σ-LFSR的初态，即$(s_{n-1},s_{n-2},\cdots,s_0)=K$，$k_{n-1}$是高位s比特，$k_0$是低位s比特，消息的填充方式是在消息后面首先填充一个1，然后填充若干个零，使得消息的总长度为分块的倍数，即是s的倍数。如果原始的消息恰好为s的倍数，也需要填充一个形如“1000…”的s比特填充块。

[0021] 步骤B中σ-LFSR和向量乘法器的更新方式如下：

[0022] 1)σ-LFSR的更新方式：组件A在初始化后按照如下的规则进行σ-LFSR的状态更新：

[0023] $$TMP\_A=S_{n-1}A_{n-1}\oplus\ldots\oplus S_1A_1\oplus S_0A_0;$$

[0024] $S_0=S_1$；

[0025] $S_1=S_2$；

[0026] …

[0027] $S_{n-2}=S_{n-1}$；

[0028] $S_{n-1}=TMP\_A$；

[0029] 其中$A_0,\cdots,A_{n-1}$由σ-LFSR定义，TMP_A为s比特字，$(S_{n-1},S_{n-2},\cdots,S_0)$的初始值为K。

[0030] 2)向量乘法器的更新方式:组件B由有限域的一组基和有限域中的乘法构成,其更新方式为将输入两个s维向量通过有限域的基转化为两个有限域元素,然后做有限域乘法,再将其转换为一个s维向量输出。

[0031] 本发明的有益效果是:

[0032] 1)方法组件基于指令特性设计,采用自主研究的基于字的反馈移位寄存器作为认证方法的重要部件。结合Toeplitz矩阵认证方法,既保证了安全性,又降低了实现的复杂度。

[0033] 2)采用字间运算与同规模有限域运算相结合的设计框架,能够有效地增强信息扩散与混乱的程度,提高了抵典型攻击攻击的能力,方法设计方式新颖。

[0034] 3)方法适用范围广,实现可用少量基本指令完成,适合软件和硬件快速实现,而且资源消耗少,适用于低资源计算平台。

附图说明

[0035] 下面结合附图和实施例对本发明作进一步详细说明

[0036] 图1为本发明身份认证流程图;

[0037] 图2为本发明方法整体框架图。

具体实施方式

[0038] 下面将结合附图,对本发明的技术方法作进一步的描述。

[0039] 本发明是一个身份认证方法,方法采用基于字的设计方式,方法将双方共享密钥和字线性反馈移位寄存器初始化完成后,利用字线性反馈移位寄存器的迭代和向量乘法器,将认证消息和寄存器状态依次进行向量乘法,并通过累加器累加,最后与随机数异或得到消息认证码,再将认证消息和消息认证码一起发送给另一方,达到身份认证的功能。

[0040] 下面详细叙述本发明的技术方法

[0041] 1.方法整体框架

[0042] 方法整体框架分为三个部分:

[0043] 组件A:一个基于字的σ-线性反馈移位寄存器(σ-LFSR),作为方法的Toeplitz矩阵生成部分,该σ-LFSR共有n级,每一级含有s比特。σ-LFSR是设计者自主提出的一类基于字的特殊类型的反馈移位寄存器,详细研究结果参加公开文章。

[0044] 组件B:一个向量乘法器,作为算法的非线性变换部分,它可以完成两个s维向量到有限域元素的转换,然后进行有限域乘法,最后执行向量到有限域转换的逆变换,输出s比特向量。

[0045] 组件C:累加器部分,实现所有乘法器输出的累加,并最终和随机数累加。

[0046] 2.术语及符号说明

[0047] 认证方法采用的泛Hash函数为$h_{A,b}=A.M+b$,其中A为n×m的s-分块矩阵,$M=(m_0,m_1,\cdots,m_{m-1})^T$为长度为sm bit的消息,$b=(b_0,b_1,\cdots,b_{n-1})^T$为sn bit的随机数由量子密钥分配过程产生并存储在保密环境中,其中s为块的长度单位,一般为8bit的倍数。

[0048] 矩阵A为块Toeplitz矩阵,由字线性反馈移位寄存器构造。具有如下形式:

[0049] $$A=\begin{pmatrix} A_0 & A_1 & \cdots & A_{m-1} \\ A_1 & A_2 & \cdots & A_m \\ \vdots & \vdots & \ddots & \vdots \\ A_{n-1} & A_n & \cdots & A_{m+n-1} \end{pmatrix}_{n\times m}$$

[0050] 其中$\mathbb{F}_2$为二元有限域，A_i是$\mathbb{F}_2$上的s×s阶矩阵，对于角标i=0,1,…,m+n-1都成立，矩阵A的构造由认证方法的密钥和其第一列$(A_0,A_1,\cdots,A_{n-1})$完全确定，设K=$(s_{n-1},s_{n-2},\cdots,s_0)$为认证方法的sn比特密钥，视为s维二元向量空间$\mathbb{F}_2^s$上的n维向量，字线性反馈移位寄存器通过如下递归关系生成$\mathbb{F}_2^s$上的向量序列$\underline{s}=s_0,s_1,\cdots$

[0051] $$s_{n+k}=s_{n+k-1}A_{n-1}\oplus\ldots\oplus s_{k+1}A_1\oplus s_kA_0 \qquad i=0,1,2$$

[0052] 其中“⊕”为异或操作，s_k是$\mathbb{F}_2^s$中的行向量，A_i是特征2中定义的$\mathbb{F}_2$上的s×s阶矩阵。注意基本指令中的“与运算、移位运算”都可等价为$\mathbb{F}_2$上的s×s阶矩阵。

[0053] 对于任意一个s比特消息m_j和s×s阶矩阵A_i，i=0,1,…,m+n-1，j=0,1,…,m-1，则特征1中的s维向量与s×s阶矩阵的乘法由有限域$\mathbb{F}_{2^s}$中的乘法定义。即给定一组基可以将$\mathbb{F}_2^s$中的行向量m_j和s_i视为有限域$\mathbb{F}_{2^s}$中的元素，则$A_i\cdot m_j=m_j\otimes s_i$，其中“⊗”表示有限域$\mathbb{F}_{2^s}$定义的乘法。

[0054] 一步迭代：即移存器按规则运动一步并输出s比特状态。

[0055] 数据描述格式：左高右低方式。

[0056] 数据存贮格式：小数在前的格式存储，即字的低位字节放在低地址字节上。

[0057] 符号的含义：

[0058]	&	按位与运算	⊕	模2加运算
[0059]	<<n	左移n位运算	>>s	右移s位运算
[0060]	rotr(n)	循环右移n位	rotl(n)	循环左移n位
[0061]	||	数据的级联	⊗	向量乘法器
[0062]	s	字块的基本长度	m	认证消息的块数
[0063]	n	消息认证码的块数	M	认证消息
[0064]	A	块Toeplitz矩阵	b	n块长度随机数
[0065]	$A_0,\cdots,A_{n-1}$	σ-LFSR的递归矩阵		
[0066]	$(S_{n-1},S_{n-2},\cdots,S_0)$	σ-LFSR的状态寄存器		
[0067]	$\underline{s}=s_0,s_1,\cdots$	σ-LFSR生成的字序列		
[0068]	K	方法的初始密钥(sn比特)		
[0069]	MAC	方法的得到的消息认证码(sn比特)		

[0070] 3.方法流程

[0071] 认证方法的前提条件：认证双方Alice和Bob共享密钥K。

[0072] 身份认证流程参见图1：Alice和Bob共享密钥K，然后发送方Alice将认证消息M和密钥K通过认证方法计算得到消息认证码，并将消息M和消息认证码通过网络传送给接收方Bob。接收方同样利用消息M和共享密钥K计算消息认证码，比较是否与接收到的值一致，如果一致则通过Alice的身份认证。

[0073] 本发明方法包含σ-LFSR、向量乘法器、累加器三个组件，执行一次包含以下三个过

程：

[0074] 1)组件初始化。将双方共享的sn比特密钥值、字线性反馈移位寄存器的反馈逻辑、随机数和认证消息经过一系列的填充，置入到各部件的寄存器中，寄存器的初始化是将sn比特密钥$K=k_{n-1,k_{n-2}},\cdots,k_0$分成n个连续的s比特块，并将其作为σ-LFSR的初态，即$(s_{n-1},s_{n-2},\cdots,s_0)=K$，$k_{n-1}$是高位s比特，$k_0$是低位s比特。

[0075] 消息的填充方式是在消息后面首先填充一个1，然后填充若干个零，使得消息的总长度为分块的倍数，即是s的倍数。如果原始的消息恰好为s的倍数，也需要填充一个形如“1000…”的s比特填充块。

[0076] 2)泛Hash计算。组件A每迭代一步更新当前寄存器的状态值$(s_j,s_{j+1},\cdots s_{j+n-1})$，然后消息分块与当前寄存器的状态进入组件B，即计算向量乘积

[0077] $$m_j\otimes(s_j,s_{j+1},\cdots,s_{j+n-1})=(m_j\otimes s_j,m_j\otimes s_{j+1},\cdots,m_j\otimes s_{j+n-1}),$$

[0078] 将结果反馈到累加器中进行累加，最终得到$\oplus_{j=0}^{m-1}(m_j\otimes(s_j,s_{j+1},\cdots s_{j+n-1}))$。组件A在初始化后按照如下的规则进行σ-LFSR的状态更新：

[0079] $$TMP\_A=S_{n-1}A_{n-1}\oplus\ldots\oplus S_1A_1\oplus S_0A_0;$$

[0080] $S_0=S_1$；

[0081] $S_1=S_2$；

[0082] …

[0083] $S_{n-2}=S_{n-1}$；

[0084] $S_{n-1}=TMP\_A$；

[0085] 其中$A_0,\cdots,A_{n-1}$由σ-LFSR定义，TMP_A为s比特字，$(S_{n-1},S_{n-2},\cdots,S_0)$的初始值为K。

[0086] 组件B由有限域的一组基和有限域中的乘法构成，其更新方式为将输入两个s维向量通过有限域的基转化为两个有限域元素，然后做有限域乘法，再将其转换为一个s维向量输出。

[0087] 具体的设$\{\alpha_0,\alpha_1,\cdots,\alpha_{s-1}\}$为有限域$\mathbb{F}_{2^s}$在$\mathbb{F}_2$上的一组基，在这组基下$\mathbb{F}_{2^s}$可视为$\mathbb{F}_2$上的s维向量空间$\mathbb{F}_2^s$。利用这组基有$\mathbb{F}_2^s$同构于$\mathbb{F}_{2^s}$，故可以用向量表示有限域中的元素。设输入的两个字为$x=(x_0,\cdots,x_{s-1})\in\mathbb{F}_2^s$和$y=(y_0,\cdots,y_{s-1})\in\mathbb{F}_2^s$，于是可以构造$\mathbb{F}_{2^s}$中的两个元素$\alpha=x_0\alpha_0+x_1\alpha_1+\cdots x_{s-1}\alpha_{s-1}$和$\beta=y_0\alpha_0+y_1\alpha_1+\cdots y_{s-1}\alpha_{s-1}$。计算$\alpha\cdot\beta=\gamma$，再利用给出的基将γ写为$\gamma=z_0\alpha_0+z_1\alpha_1+\cdots z_{s-1}\alpha_{s-1}$。从而组件B对于输入x和y的向量乘积为$z=(z_0,\cdots,z_{s-1})\in\mathbb{F}_2^s$。

[0088] 3)随机数异或。当所有消息处理完成后，累加器得到的结果需要和随机数做运算，计算

[0089] $$MAC=[\oplus_{j=0}^{m-1}m_j\otimes(s_j,s_{j+1},\cdots s_{j+n-1})]\oplus(b_0,b_1,\ldots,b_{n-1})$$，此即为此时输出的n块消息认证码。

[0090] 三个组件A、B、C的基本处理单元都是s比特，通过基本的逻辑运算生成消息认证码。算法首先完成初始化工作，然后进行正常消息迭代处理过程，在每次迭代更新组件A时，将新的消息块与寄存器状态进行向量乘法，然后送入累加器，最终异或随机数得到MAC。

[0091] 本发明认证方法框图参见图2，图中A部分可以为任意的本原σ-LFSR，图中采用字长为8的8级本原σ-多项式

[0092] $F(x)=x^8+\&0x7f\ x^7+rotl(3)x^4+rotr(5)x+1$

[0093] 作为示例，故图1中的每个寄存器为8比特(即s=8)，最终的消息认证码为64比特。

[0094] 4.本发明的随机性测试

[0095] 测试方法:根据密钥和认证消息的特点生成5类数据,分别产生消息认证码,将所有寄存器的中间状态级联测试随机性。

[0096] 测试软件:利用NIST和DIEHARD随机性测试软件进行了测试,其标准与美国商务部国家标准技术协会(NIST)于2001年5月公布的FIPS140-2相兼容。

[0097] 测试内容:完成30种随机性测试,包含NIST软件提供的15种和DIAHARD软件提供的15种随机性测试,

[0098] 测试结果:测试结果表明方法的计算过程具有良好的伪随机性质。

[0099] 5.本发明的安全性分析

[0100] 随着认证技术的快速发展和普及应用,攻击方法呈现出日趋多样化的特点。当前,认证的主要攻击方法有长度扩展攻击、第二原像攻击、随机碰撞攻击等。本方法的设计采用了泛Hash函数族,可以在理论上保证无条件的安全性,即本发明基于σ-LFSR的字Toeplitz结构是ε-平衡的,其中$\varepsilon \leqslant 1/2^{ns-1}$。

[0101] 上述结论表明,在不知道密钥的情况下,攻击者通过任何攻击方法产生的消息认证码,与随机选取一个消息认证码作为候选没有任何区别。也就是在现有计算资源条件下,算法可以抵抗所有攻击。正由于方法拥有完美的安全属性,本发明特别适合在量子密码系统中使用。

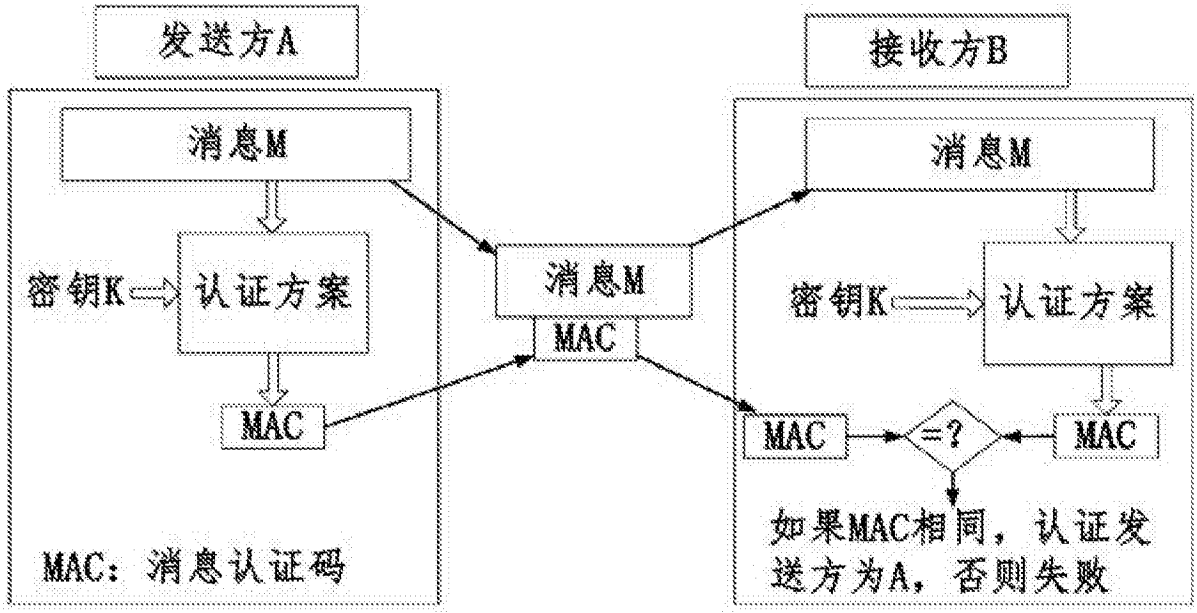

发送方A
消息M
密钥K
认证方案
MAC
MAC：消息认证码
消息M
MAC
接收方B
消息M
密钥K
认证方案
MAC
=?
MAC
如果MAC相同，认证发送方为A，否则失败

图1

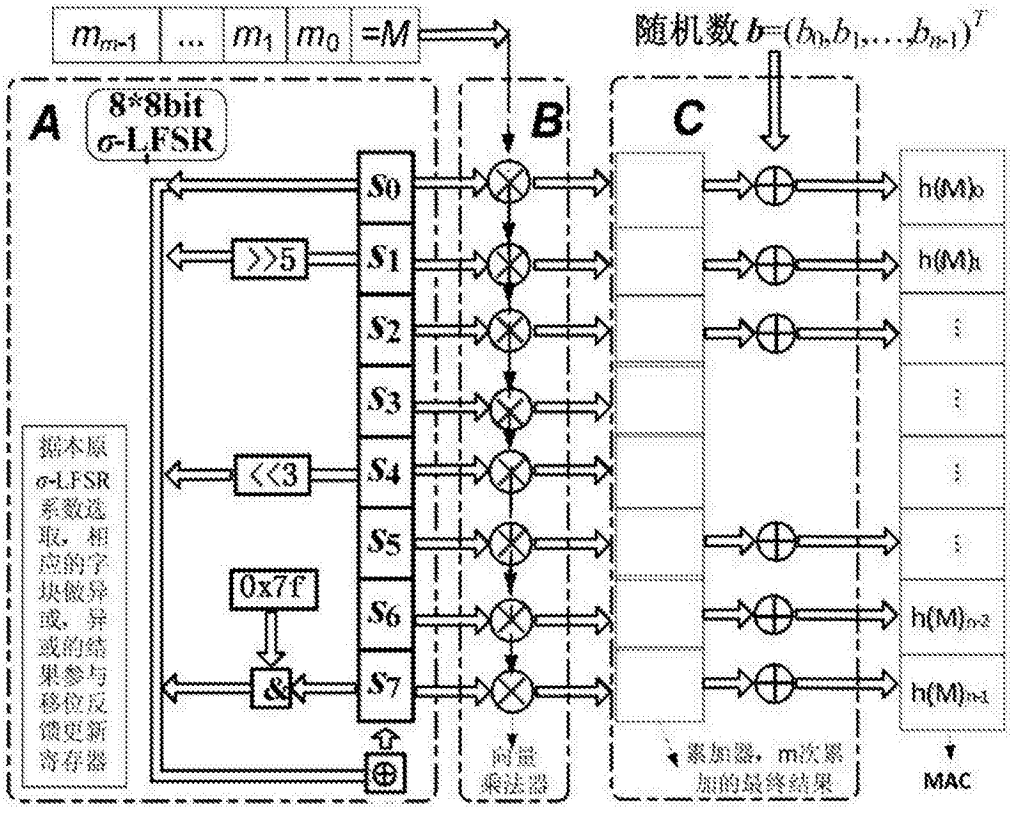

m_{n-1} ... m_1 m_0 =M
随机数 $b=(b_0,b_1,\ldots,b_{n-1})^T$
A
8*8bit σ-LFSR
B
C
S0
S1
S2
S3
S4
S5
S6
S7
>>5
<<3
0x7f
&
⊕
h(M)0
h(M)1
h(M)n-2
h(M)n-1
MAC

图2