Journal of Computer Applications
计算机应用,2015,35(10):2867 -2871
ISSN 1001-9081
CODEN JYIIDU
2015-10-10
http://www.joca.cn

文章编号:1001-9081(2015)10-2867-05
doi:10.11772/j.issn.1001-9081.2015.10.2867

基于编码的盲签名方案

王 倩[1,2*],郑 东[1,2],任 方[1,2]
(1.西安邮电大学 通信与信息工程学院,西安 710121; 2.西安邮电大学 无线网络安全技术国家工程实验室,西安 710121)
(* 通信作者电子邮箱 wangqian_1129@126.com)

摘 要: 编码密码技术由于具有抵抗量子算法攻击的优点受到了广泛的关注。针对消息的匿名保护问题,提出了一种基于编码的盲签名方案。消息拥有者通过哈希技术和盲化因子将消息进行不可逆和盲化处理后发送给签名人,签名人利用 CFS(Courtois-Finiasz-Sendrier)签名方案完成盲化签名并发回给消息拥有者,消息拥有者可通过去盲获得签名。分析表明,新的方案不仅具有一般盲签名的基本性质,而且继承了 CFS 签名方案的安全性高、签名长度短等优点,能够有效抵抗量子算法的攻击。

关键词: 编码;数字签名;盲签名;哈希;校验子译码
中图分类号: TP309 **文献标志码:** A

Code-based blind signature scheme

WANG Qian[1,2*], ZHENG Dong[1,2], REN Fang[1,2]
(1. *School of Telecommunication and Information Engineering, Xi'an University of Posts and Telecommunications, Xi'an Shaanxi* 710121, *China*;
2. *National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an Shaanxi* 710121, *China*)

Abstract: Coding cryptography is widespread concerned because it has the advantages of resisting quantum algorithm. To protect the anonymous message, a kind of blind signature scheme based on coding was proposed. By Hash technique and blind factor, message owner sent irreversible and blinding message to the signer, signer completed blind signature by using Courtois-Finiasz-Sendrier (CFS) signature scheme and sent it back to the message owner, message owner obtained signature by blind removing operation. Analysis show that the new scheme not only has the basic nature of general blind signature, but also inherit the advantages of CFS signature scheme such as high security and short signature length, in addition, it can effectively resist attacks of quantum algorithm.

Key words: coding; digital signature; blind signature; Hash; syndrome decoding

0 引言

自 20 世纪 70 年代公钥密码问世以来,密码技术已成为人们在通信及计算机领域中不可缺少的重要技术之一,如 RSA(Rivest-Shamir-Adleman)算法、数字签名算法(Digital Signature Algorithm, DSA)、椭圆曲线数字签名算法(Elliptic Curve Digital Signature Algorithm, ECDSA)及其他类似的公钥密码技术,这些密码技术的安全性是都是基于数学困难问题,如整数分解问题、离散对数问题等。量子算法的出现,对现在广泛使用的公钥密码算法构成了严重的威胁,但是对于诸如线性分组码的一般译码问题等困难问题还没有有效的量子算法[1],因此,基于线性分组码的公钥密码技术受到了广泛的关注。

1978 年 Berlekamp 等[2]证明了线性分组码理论中一般线性码的译码问题是 NPC(Non-deterministic Polynomial Complete)问题。同年 McEliece[3]利用 Goppa 码构造了第一个公钥密码体制,简称 McEliece 体制,自该体制提出至今,还没有找到有效的攻击算法;1986 年,Niederreiter[4]提出了与 McEliece 方案安全性等价的另一种公钥密码体制。2001 年,Courtois 等[5]利用线性分组码译码问题构造了安全的数字签名方案,简称 CFS 方案,这是真正严格意义上比较安全的基于编码的签名方案。

盲签名是一种特殊的数字签名,由 Chaum[6]于 1982 年首次提出,并于 1983 年提出了第一个基于 RSA 公钥密码的盲签名方案[7]。随后人们又基于离散对数问题和二次剩余提出了各种盲签名方案,目前已有多种成熟的盲签名方案应用在同时需要匿名性和认证性的应用场合中,如在电子现金[8]中实现不可跟踪的电子现金,在电子选举中实现无记名选举[9]等。虽然目前已有许多盲签名模型,并且得到了广泛的应用,但是现有的盲签名方案的安全性大多基于数学困难问题,量子算法与量子计算机的发展对它们构成了极大的威胁。基于编码技术构建的 QC(Quasi-Cyclic)盲签名[10]和基于 Niederreiter 公钥密码体制的盲签名[11]可以抵抗目前已知的量子攻击算法,但是 QC 盲签名的签名长度较长,实用性不高,而基于 Niederreiter 公钥密码体制的盲签名不满足不可伪造性。因此,本文提出了一种新的基于 CFS 方案的盲签名方案,大大缩短了签名长度,并且具有较高的安全性,是一种比较实用的盲签名方案。

收稿日期:2015-04-02;修回日期:2015-06-09。 基金项目:国家自然科学基金资助项目(61272037,61472472);陕西省自然科学基金重点项目(2013JZ020);陕西省自然科学基金资助项目(2015JQ6262);西安邮电大学青年基金资助项目(ZL2013-06)。

作者简介:王倩(1990-),女,新疆伊宁人,硕士研究生,主要研究方向:信息安全; 郑东(1964-),男,山西翼城人,教授,博士,主要研究方向:密码学、云存储安全; 任方(1981-),男,陕西西安人,讲师,博士,主要研究方向:密码学、信息安全。

1 基础知识

1.1 线性分组码的基本概念

定义1 线性分组码(Linear block codes)。

有限域$\mathbf{F}_2$上的一个(n,k)线性分组码$\mathbf{C}$是n维线性空间$\mathbf{F}_2^n$的一个k维子空间,$\mathbf{F}_2^n$中的向量称为字,$\mathbf{C}$中的向量称为码字,n称为码长,k称为码的维数。

定义2 生成矩阵(generating matrix)与校验矩阵(parity check matrix)。

(n,k)线性分组码$\mathbf{C}$的生成矩阵是一个$k\times n$阶的矩阵$\boldsymbol{G}$,其中$\boldsymbol{G}$的行向量构成了$\mathbf{C}$的一组基。校验矩阵是一个$(n-k)\times n$阶的矩阵$\boldsymbol{H}$,其中校验矩阵$\boldsymbol{H}$的任意行向量与生成矩阵$\boldsymbol{G}$的任意行向量正交,即$\boldsymbol{HG}^{\mathrm{T}}=0$。

长为n的向量$\boldsymbol{x}$是$\mathbf{C}$的一个码字的充分必要条件是$\boldsymbol{Hx}^{\mathrm{T}}=0$。对于任意的字$\boldsymbol{x}$,将$\boldsymbol{Hx}^{\mathrm{T}}$称为$\boldsymbol{x}$的校验子。

Goppa码是一种特殊的线性分组码,McEliece加密体制中使用的Goppa码具有如下形式:码的长度$n=2^m$,码的维数$k=n-mt$,t为码的纠错能力。

线性分组码理论中的NP(Non-deterministic Polynomial)问题如Goppa码的校验子译码[12]问题等是抗量子计算的,其译码问题可以归结为如定义3所示的已知校验子求错误向量的问题。

定义3 SD(Syndrome Decoding)问题。

给定有限域F_2上的$r\times n$矩阵$\boldsymbol{H}$,字$\boldsymbol{s}\in\mathbf{F}_2^r$及整数$\omega>0$,是否存在字$\boldsymbol{x}\in\mathbf{F}_2^n$满足$\boldsymbol{Hx}^{\mathrm{T}}=\boldsymbol{s}$且重量小于$\omega$。

目前,经典的基于线性分组码的McEliece公钥密码体制、Niderreiter公钥密码体制以及CFS数字签名方案均是基于Goppa码的译码困难问题,由此可见,进一步发掘基于线性分组码的NPC类问题,对于编码密码的研究具有重要的意义。

1.2 Hash函数的基本概念

定义4 Hash函数。

Hash函数[9,13]是一个公开的函数h,将任意长度的消息M压缩为定长的消息摘要$h(M)$。

Hash函数具有如下性质:

1) 输入任意长度的消息M都能产生固定长度的消息摘要$h(M)$;

2) 对任何给定的消息M,消息摘要$h(M)$容易计算,但是已知消息摘要$h(M)$,求消息M是困难的,这是Hash函数的单向性;

3) 对于任意给定的分组M,寻求不等于M的M',使得$h(M)=h(M')$在计算上是困难的,这是Hash函数的弱抗撞碰性;

4) 消息摘要$h(M)$和消息M的所有比特都相关,即改变消息M的任何一个比特,都将对摘要$h(M)$产生显著的影响。

Hash函数的用途很广,最常用的就是用于数字签名中,如使用Hash函数作用于消息M,然后对Hash函数产生的消息摘要$h(M)$进行签名,这样只需要进行一次数字签名就可以完成对整个消息M的签名。

1.3 CFS签名方案

2001年,Courtois等利用线性分组码译码困难问题构造了CFS签名方案,其安全性可以归结为一般译码问题和Goppa码与随机线性码的不可区分问题[5]169,均是NP困难问题,是真正严格意义上的比较安全的基于编码的签名方案,具体过程见算法1。

算法1 CFS签名算法。

1) 初始化阶段。

在有限域F_2上选取一个m次既约多项式$g(x)$,并由该多项式得到一个(n,k,t)既约Goppa码,其中码长$n=2^m$,码的维数$k=n-mt$,t是码的纠错能力,$\boldsymbol{H}^0$是码的$(n-k)\times n$阶校验矩阵。该Goppa码对应的译码算法为γ。

设$\boldsymbol{U}$是随机选择的$(n-k)\times(n-k)$阶非奇异矩阵,$\boldsymbol{P}$是随机选择的$n\times n$阶置换矩阵,计算$\boldsymbol{H}=\boldsymbol{UH}^0\boldsymbol{P}$。公钥$\boldsymbol{H}$公开,私钥$\boldsymbol{U}$、$\boldsymbol{H}^0$、$\boldsymbol{P}$、$\gamma$由签名人保密。$\boldsymbol{H}$可看作一般$(n,k,t)$线性分组码的校验矩阵。选择公开的Hash函数$h$。

2) 签名阶段。

① 签名人用公开的Hash函数h对消息M进行Hash运算得到$n-k$长的序列$\boldsymbol{s}$:$\boldsymbol{s}=h(M)$;

② 对于不同的i,用Hash函数h计算$n-k$长的序列$\boldsymbol{s}_i$:$\boldsymbol{s}_i=h(\boldsymbol{s}\mid i)$$(i=0,1,2,\cdots)$;

③ 签名人使用秘密的译码算法γ对$\boldsymbol{s}_i$尝试译码,将最小的使$\boldsymbol{s}_i$可译码的i记为i_0,并将译出的字记作$\boldsymbol{z}$,满足:$\boldsymbol{Hz}^{\mathrm{T}}=\boldsymbol{s}_{i_0}$,$\omega(\boldsymbol{z})=t$;

④ 计算$\boldsymbol{z}$的标号I_z:$I_z=1+\binom{i_1}{1}+\binom{i_2}{2}+\cdots+\binom{i_t}{t}$,其中$i_1i_2\cdots i_t$是$\boldsymbol{z}$中取值为1的位置标号,将$[I_z\mid i_0]$作为消息$M$的签名$\sigma$;

签名人将消息-签名对(M,σ)公开。

3) 验证阶段。

① 验证者收到消息-签名对(M,σ),并根据签名σ中的标号I_z恢复出$\boldsymbol{z}$,满足:$\omega(\boldsymbol{z})=t$。

② 将恢复出的$\boldsymbol{z}$左乘公钥$\boldsymbol{H}$计算其校验子$\boldsymbol{s}_1$:$\boldsymbol{s}_1=\boldsymbol{Hz}^{\mathrm{T}}$。

③ 根据消息M的Hash值$h(M)$和i_0计算$n-k$长的序列$\boldsymbol{s}_2$:$\boldsymbol{s}_2=h([h(M)\mid i_0])$。

④ 比较$\boldsymbol{s}_1$与$\boldsymbol{s}_2$是否相等,若相等则签名σ有效;否则签名无效。

对于一个给定的非负整数m,共有约$2^{tm}/t$个线性分组码[5]162。由于n远大于t,则可译码的校验子个数$N_d=\sum_{i=1}^{t}\binom{n}{i}\simeq\binom{n}{t}\simeq\frac{n^t}{t!}$,总的校验子个数$N_t=2^{n-k}=2^{mt}=n^t$,随机选取校验子可译码的概率$p=\frac{N_d}{N_t}\simeq\frac{1}{t!}$。

由上文分析可知,签名时的平均译码尝试次数约为$t!$次,而一个快速有界译码算法可在几分钟内完成约一百万次译码[5]162,则t的取值应不超过10($10!=3\,628\,800$)。表1中列出了t与n取不同值时的译码开销,在Canteaut-Chabaud[14]攻击下,可接受的安全强度为2^{80}次CPU运算,因此当$t=10$时,n至少取2^{15};当$t=9$时,n至少取2^{16}。

表1 译码的开销

t	n				
	2^{13}	2^{14}	2^{15}	2^{16}	2^{17}
8	$2^{61.4}$	$2^{65.3}$	$2^{67.8}$	$2^{70.7}$	$2^{73.3}$
9	$2^{69.3}$	$2^{74.0}$	$2^{78.8}$	$2^{83.7}$	$2^{88.2}$
10	$2^{72.3}$	$2^{77.4}$	$2^{87.4}$	$2^{90.9}$	$2^{94.6}$

1.4 盲签名技术

盲签名是一种特殊的数字签名,可以看作消息拥有者和

签名人之间的一种交互协议。如果协议正确执行,消息 M 的拥有者最终将获得签名人对消息 M 的数字签名 σ; 而签名人却不知道消息 M 的内容,即便以后将(M,σ) 公开,也无法追踪消息与自己执行签名过程之间的相互关系。

1.4.1　盲签名的实现过程

一个盲签名体制中存在两个参与实体: 一个是消息拥有者,另一个是签名人。盲签名示意图如图 1 所示。

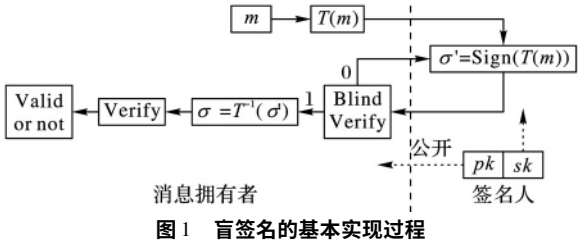

图 1　盲签名的基本实现过程

盲签名方案[10]一般有如下 6 个阶段:

1) 初始化阶段。一个概率多项式时间算法,输入安全参数,输出签名人的公私钥对(pk,sk),私钥 sk 由签名人保密,公钥 pk 公开。

2) 盲化阶段。消息拥有者引入盲化因子 T,对消息 M 进行盲化处理,得到盲化后的消息 $T(M)$,并将 $T(M)$ 发送给签名人。

3) 盲化签名阶段。一个概率多项式时间的交互协议,签名人用私钥 sk 对盲化后的消息 $T(M)$ 进行盲化签名,得到盲化后的签名 σ',并将 σ' 发送给消息拥有者。

4) 盲化验证阶段。消息拥有者用公钥 pk 和盲化后的消息 $T(M)$ 对盲化后的签名 σ' 进行盲化验证,记作 $Blind\ verify(pk,T(M),\sigma')$,输出"1"(表示签名有效)、"0"(表示签名无效)。

5) 去盲阶段。若盲化验证阶段输出"1",说明签名有效,消息拥有者用盲化因子 T、消息 M 和公钥 pk 对盲化后的签名 σ' 进行去盲,得到签名 σ。

6) 签名验证阶段。用消息 M 和公钥 pk 对签名 σ 验证,记作 $Verify(pk,M,\sigma)$,输出"1"(表示签名有效)、"0"(表示签名无效)。

1.4.2　盲签名的性质

盲签名不仅具有一般数字签名的所有性质,还有一些特有的性质[10],一个安全的盲签名体制至少需要满足下面五个性质:

1) 正确性。如果 σ 是盲签名算法正确执行后输出的对消息 M 的签名,则总有 $Verify(pk,M,\sigma)=1$。

2) 盲性。也称为匿名性,是盲签名最主要的特性。除请求签名的消息拥有者外,消息内容对任何人(包括签名人)均不可见。即使签名人对消息签名,仍然得不到消息的具体内容。

3) 不可伪造性。任何不知道签名人私钥 sk 的人都无法有效地计算出一个能够通过签名验证方程的消息-签名对(m^*,σ^*)。

4) 不可抵赖性。只要证明消息的签名是合法的,那么签名人不论如何都无法否认他签过这个消息。

5) 不可跟踪性。一旦签名消息公开,签名人不知道何时签的,即使留有当时的签名信息,也无法追踪到消息内容。

盲签名的这些良好特性使得它在诸如电子现金、电子拍卖、电子选举等诸多同时需要匿名性和认证性的应用场合中起到关键作用。正是基于这些良好的应用背景,盲签名体制自提出以来得到了广泛的研究。

2　基于 CFS 的盲签名方案

一般线性码的校验子译码问题是 NPC 问题,本章提出一个基于 CFS 方案的盲签名方案,该方案的安全性也是基于校验子译码问题。具体过程见算法 2。设 Alice 为消息拥有者,Bob 为签名人。

算法 2　基于 CFS 的盲签名。

1) 初始化阶段。

在有限域 F_2 上选取一个 m 次既约多项式 $g(x)$,并由该多项式得到一个(n,k,t) 既约 Goppa 码,其中码长 $n=2^m$,码的维数 $k=n-mt$,t 是码的纠错能力,$\boldsymbol{H}^0$ 是码的$(n-k)\times n$ 阶校验矩阵。该 Goppa 码对应的译码算法为 γ。

设 $\boldsymbol{U}$ 是随机选择的$(n-k)\times(n-k)$ 阶非奇异矩阵,$\boldsymbol{P}$ 是随机选择的 $n\times n$ 阶置换矩阵,计算 $\boldsymbol{H}=\boldsymbol{U}\boldsymbol{H}^0\boldsymbol{P}$。公钥 $\boldsymbol{H}$ 公开,私钥 $\boldsymbol{U}$、$\boldsymbol{H}^0$、$\boldsymbol{P}$、γ 由签名人保密。$\boldsymbol{H}$ 可看作一般(n,k,t) 线性分组码的校验矩阵。选择公开的 Hash 函数 h。

2) 盲化和盲化签名阶段。

①Alice 用公开的 Hash 函数 h 对消息 M 进行 Hash 运算得到 $n-k$ 长的序列 $\boldsymbol{s}$: $\boldsymbol{s}=h(M)$。

②Alice 选择非负整数 t_e,并随机选取一个 n 长序列 $\boldsymbol{e}$ 使 $\omega(\boldsymbol{e})=t_e$,左乘公钥 $\boldsymbol{H}$,将 $\boldsymbol{H}\boldsymbol{e}^{\mathrm{T}}$ 作为盲化因子。

③对于不同的 i,Alice 用 Hash 函数 h 计算 $n-k$ 长的序列 $\boldsymbol{s}_i$: $\boldsymbol{s}_i=h(\boldsymbol{s}\mid i)$ $(i=0,1,2,\cdots)$,将 $\boldsymbol{s}_i$ 加上盲化因子 $\boldsymbol{H}\boldsymbol{e}^{\mathrm{T}}$ 盲化后发送给 Bob 尝试译码,直到 Bob 成功译码并将译出的字发回给 Alice,具体过程如下:

a) Alice 取 $i=0$,并用 Hash 函数 h 计算 $n-k$ 长的序列 $\boldsymbol{s}_0$: $\boldsymbol{s}_0=h(\boldsymbol{s}\mid 0)$;

b) Alice 用盲化因子 $\boldsymbol{H}\boldsymbol{e}^{\mathrm{T}}$ 将 $\boldsymbol{s}_0$ 盲化,盲化后记为 $\boldsymbol{s}_0'$: $\boldsymbol{s}_0'=\boldsymbol{H}\boldsymbol{e}^{\mathrm{T}}+\boldsymbol{s}_0$;

c) Alice 将盲化后的消息 $\boldsymbol{s}_0'$ 发给 Bob;

d) Bob 收到 $\boldsymbol{s}_0'$ 后,用秘密的译码算法对 $\boldsymbol{s}_0'$ 译码,若不可译,请求 Alice 取其他 i 值重发,直到找到可译的 $\boldsymbol{s}_i'$,并将最小的使 $\boldsymbol{s}_i'$ 可解的 i 记为 i_0,将译出的字记为 $\boldsymbol{z}'$: $\boldsymbol{H}\boldsymbol{z}'^{\mathrm{T}}=\boldsymbol{s}_{i_0}'$,$\omega(\boldsymbol{z}')=t$; 若可译,$i_0=0$,$\boldsymbol{H}\boldsymbol{z}'^{\mathrm{T}}=\boldsymbol{s}_0'$,$\omega(\boldsymbol{z}')=t$;

e) Bob 将译出的 $\boldsymbol{z}'$ 发给 Alice。

3) 盲化验证阶段。

Alice 收到 $\boldsymbol{z}'$,左乘公钥 $\boldsymbol{H}$ 验证。若 $\boldsymbol{H}\boldsymbol{z}'^{\mathrm{T}}=\boldsymbol{s}_{i_0}'$,进行下一阶段; 否则,重新进行上一阶段。

4) 去盲阶段。

①Alice 将验证通过的 $\boldsymbol{z}'$ 与 n 长序列 $\boldsymbol{e}$ 相加进行去盲得 $\boldsymbol{z}$: $\boldsymbol{z}=\boldsymbol{z}'+\boldsymbol{e}$,其中 $\omega(\boldsymbol{z})\leqslant\omega(\boldsymbol{z}')+\omega(\boldsymbol{e})=t+t_e$;

② 计算 $\boldsymbol{z}$ 的标号 I_z: $I_z=1+\binom{i_1}{1}+\binom{i_2}{2}+\cdots+\binom{i_\omega(\boldsymbol{z})}{\omega(\boldsymbol{z})}$,其中 $i_1 i_2\cdots i_{\omega(\boldsymbol{z})}$ 是 $\boldsymbol{z}$ 中取值为 1 的位置标号,$[I_z\mid i_0]$ 作为消息 M 的签名 σ;

Alice 将消息-签名对(M,σ) 公开。

5) 签名验证阶段。

① 验证者收到消息-签名对(M,σ),并根据签名 σ 中的标号 I_z 恢复出 $\boldsymbol{z}$,满足 $\omega(\boldsymbol{z})=t+t_e$;

② 将恢复出的 z 左乘公钥 $\boldsymbol{H}$ 计算其校验子 $\boldsymbol{s}_1$:$\boldsymbol{s}_1 = \boldsymbol{H}\boldsymbol{z}^{\mathrm{T}}$;

③ 根据消息 M 的 Hash 值 $h(M)$ 和 i_0 计算 $n-k$ 长的序列 $\boldsymbol{s}_2$:$\boldsymbol{s}_2 = h(\lfloor h(M) \mid i_0 \rfloor)$;

④ 验证者比较 $\boldsymbol{s}_1$ 与 $\boldsymbol{s}_2$ 是否相等,若相等则签名 σ 有效,否则签名无效。

3 算法分析

3.1 正确性分析

如果消息拥有者 Alice 和签名人 Bob 按照上述步骤进行,则产生的签名必为消息的正确签名,且能验证签名的正确性。

1) 验证者收到消息-签名对(M,σ),并根据 σ 中的标号 I_z 恢复出 z,满足 $\omega(z) = t + t_e$;

2) 将恢复出的 z 左乘公钥 $\boldsymbol{H}$ 计算其校验子 $\boldsymbol{s}_1$:$\boldsymbol{s}_1 = \boldsymbol{H}\boldsymbol{z}^{\mathrm{T}} = \boldsymbol{H}(\boldsymbol{z}' + \boldsymbol{e})^{\mathrm{T}} = \boldsymbol{H}\boldsymbol{z}'^{\mathrm{T}} + \boldsymbol{H}\boldsymbol{e}^{\mathrm{T}}$;

3) 根据消息 M 的 Hash 值 $h(M)$ 和 i_0 计算 $n-k$ 长的序列 $\boldsymbol{s}_2$:$\boldsymbol{s}_2 = h(\lfloor h(M) \mid i_0 \rfloor) = h(\boldsymbol{s} \mid i_0) = \boldsymbol{s}_{i_0} = \boldsymbol{s}_{i_0}' - \boldsymbol{H}\boldsymbol{e}^{\mathrm{T}} = \boldsymbol{H}\boldsymbol{z}'^{\mathrm{T}} + \boldsymbol{H}\boldsymbol{e}^{\mathrm{T}}$;

4) 显然 $\boldsymbol{s}_1 = \boldsymbol{s}_2$,签名 σ 有效。

3.2 开销和长度

1) 签名的开销。

签名过程的开销为 t 的指数级,具体分析如下:

① 盲化阶段。译码的平均尝试次数为 $t!$ 次,计算可译的校验子 $\boldsymbol{s}_{i_0}'$ 需要 $t!$ 次 Hash 运算和 $t_e + t!$ 次列运算。

② 盲化签名阶段。将可译的校验子 $\boldsymbol{s}_{i_0}'$ 由秘密译码算法译出 $\boldsymbol{z}'$ 大约需要 t^2m^3 [5] 168 的操作。

③ 盲化验证阶段。需要 t 次列运算计算 $\boldsymbol{H}\boldsymbol{z}'^{\mathrm{T}}$ 进行盲化验证。

④ 去盲阶段。需要 1 次列运算得到 z 并计算其标号 I_z。

2) 验证的开销。

验证者由标号 I_z 恢复出 z,然后分别计算 $t + t_e$ 次列运算和 2 次 Hash 运算得 $\boldsymbol{s}_1$ 和 $\boldsymbol{s}_2$。

3) 签名的长度。

签名 σ 的长度取决于 z 的重量和 i_0,其中表示 i_0 的位数平均为 18.4 [5] 163,表示 I_z 的位数为 $\mathrm{lb}\binom{n}{t+t_e}$,所以签名 σ 的长度为 $\mathrm{lb}\binom{n}{t+t_e} + 18.4$。

3.3 安全性分析

由于本文方案是基于 CFS 方案设计的,故本文方案与 CFS 方案都是基于一般译码问题和 Goppa 码与随机线性码的不可区分问题构造的签名方案,安全水平为 tm 的指数级 [5] 169。目前的量子攻击算法主要是 Shor 算法和 Grover 算法,这两种算法可以攻破当前公钥密码依赖的大多数数学问题,而本文方案所依赖的两个编码问题都是 NPC 问题,这两种算法对于 NPC 问题还没有能力攻击,因此,本文签名方案能够抵抗量子算法的攻击。

当 $n = 2^{16}$,$t = 9$ 时,CFS 签名方案的安全性为 2^{80} 次 CPU 运算,相对应的工作因子为 2^{86},为指数时间,故 CFS 方案具有足够高的安全性。又由于本文方案是基于 CFS 方案构造的盲签名方案,其安全性与 CFS 方案的安全性一致,因此,本文方案的安全性也是 2^{80} 次 CPU 运算,安全性较高。

此外本文签名方案还具有以下盲签名特有的安全性。

1) 盲性。

盲因子 T 中的 $\boldsymbol{e}$ 是消息拥有者 Alice 随机选取的,并只有 Alice 拥有,其他人包括签名人 Bob 都无法获知。

① 盲化计算。

由于盲因子的私密性和随机性,盲化前的 $\boldsymbol{s}_i$ 对 Bob 是不可见的。其中 $\boldsymbol{e}$ 的可能性共有 $\binom{n}{t_e}$ 种,该值可以衡量盲化安全性。Bob 每次选择随机的 $\boldsymbol{e}$ 求盲因子 $\boldsymbol{H}\boldsymbol{e}^{\mathrm{T}}$ 需要通过 t_e 次列运算,大约需要 $(t_e+1) + \binom{n}{t_e}$ 次列运算才可以通过 $\boldsymbol{s}_i'$ 得到正确的 $\boldsymbol{s}_i$,运算次数是 n 的指数级,因此,当 n 较大时,Bob 无法根据 $\boldsymbol{s}_i'$ 得到 $\boldsymbol{s}_i$。

② 去盲计算。

由于 $\boldsymbol{e}$ 是 Alice 随机选取的,其可能性共有 $\binom{n}{t_e}$ 种,Bob 要将 z 与 z' 联系,需要 $\binom{n}{t_e}$ 次列运算,运算次数是 n 的指数级,当 n 较大时,Bob 无法将去盲后的 z 和 z' 联系起来,也就无法跟踪签名,用户也无法获知消息的签名人。

2) 不可伪造性。

由签名过程可以看出,伪造者要伪造签名 $\lfloor I_z \mid i_0 \rfloor$,需要知道标号 I_z 和 i_0。

① 伪造者无法通过伪造 I_z 或 z 伪造签名。由于 I_z 的长度为 $lb\binom{n}{t+t_e}$,z 的重量为 $t + t_e$,伪造者要直接伪造 I_z 或 z,均需要 $\binom{n}{t+t_e}$ 次伪造才可能成功,运算次数为 n 的指数级,当 n 较大时,无法直接伪造 I_z 或 z。即使伪造者伪造出 I_z 或 z,并对 z 左乘公钥 $\boldsymbol{H}$ 得 $\boldsymbol{H}\boldsymbol{z}^{\mathrm{T}} = \boldsymbol{s}_{i_0} = h(\boldsymbol{s} \mid i_0)$,由于 Hash 函数 h 的单向性,无法得到 i_0,也就无法伪造签名 $\lfloor I_z \mid i_0 \rfloor$。

② 伪造者无法通过伪造 z' 伪造签名。由于 z' 的重量为 t,伪造者要伪造 z',需要 $\binom{n}{t}$ 次伪造才可能成功,运算次数为 n 的指数级,当 n 较大时,无法伪造 z'。即使伪造者伪造出 z',由于 $\boldsymbol{e}$ 是 Alice 随机选取的,若要通过 $z = z' + \boldsymbol{e}$ 伪造 z,需要 $\binom{n}{t_e} = \frac{n!}{t_e!(n-t_e)!} = \frac{n(n-1)\cdots(n-t_e+1)}{t_e!}$ 次列运算,运算次数是 n 的指数级,当 n 较大时,无法通过 z' 伪造签名 $\lfloor I_z \mid i_0 \rfloor$,Bob 也无法伪造 Alice 去盲后的签名。

③ 伪造者无法通过伪造盲化前的消息 $\boldsymbol{s}_{i_0}$ 伪造签名。由于该 Goppa 码对应的译码算法 γ 是签名人 Bob 的私钥,只有 Bob 可以用译码算法 γ 对 $\boldsymbol{s}_{i_0}$ 译码得到 z,这是基于 Goppa 码的译码困难问题。因此,伪造者无法通过伪造 $\boldsymbol{s}_{i_0}$ 伪造签名。

④ 同理,伪造者无法通过伪造盲化后的消息 $\boldsymbol{s}_{i_0}'$ 伪造签名。伪造者没有签名人 Bob 的私钥 γ,无法将 $\boldsymbol{s}_{i_0}'$ 译码得到 z',也就无法得到 z,无法伪造签名,Alice 也无法伪造签名人 Bob 的签名。

而对于基于 Niederreiter 公钥密码体制的盲签名方案 [11],其私钥为 $\boldsymbol{S}$、$\boldsymbol{H}$、$\boldsymbol{P}$,公钥 $\boldsymbol{H}' = \boldsymbol{SHP}$,签名 c 可以通过公钥生成,

即 $c = H(m)\boldsymbol{P}^{\mathrm{T}}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{S}^{\mathrm{T}} = H(m)\boldsymbol{H}'^{\mathrm{T}}$,不满足不可伪造性。

3) 不可抵赖性。

由 $\boldsymbol{H}\boldsymbol{z}'^{\mathrm{T}} = \boldsymbol{s}_{i_0}'$ 译出 z',是基于 Goppa 码的译码困难问题,由于该 Goppa 码对应的译码算法 γ 是签名人 Bob 的私钥,只有 Bob 可以译出,所以无论何时 Bob 都不可抵赖其签名。

4) 不可跟踪性。

当签名公布后,即使留有当时的签名信息,签名者 Bob 也无法将签名 $[l_z \mid i_0]$ 得到的 z 和 z' 联系起来,也就是说 Bob 无法跟踪签名。

3.4　t_e 对盲化安全性的影响

消息的签名 $[l_z \mid i_0]$ 的长度取决于 z 的重量和 i_0,其中表示 i_0 的平均位数为 18.4,由 $\omega(z) \leqslant \omega(z') + \omega(\boldsymbol{e}) = t + t_e$ 可知: $\omega(\boldsymbol{e})$ 越小,$\omega(z)$ 越小,签名 σ 的长度越短,但是攻击者猜出 $\boldsymbol{e}$ 的概率越大; 反之,$\omega(\boldsymbol{e})$ 越大,$\omega(z)$ 越大,签名 σ 的长度越长,攻击者猜出 $\boldsymbol{e}$ 的概率越小。具体分析见表 2,取 $n = 2^{16}$, $t = 9$。

表 2　$\boldsymbol{e}$ 的重量对盲化安全性的影响

$\boldsymbol{e}$ 的重量 $\omega(\boldsymbol{e}) = t_e$	签名 σ 的长度 $\mathrm{lb}\binom{n}{t+t_e} + 18.4$/b	盲化安全性 $\boldsymbol{e}$ 的个数为 $\binom{n}{t_e}$
0	144	2^0
1	157	2^{16}
2	170	2^{31}
3	183	2^{46}
4	194	2^{60}
5	207	2^{74}
6	219	2^{87}
7	231	2^{100}
8	243	2^{113}
9	255	2^{126}
10	266	2^{139}

由表 2 可看出,不同的签名长度对应不同的盲化安全性,为达到 2^{80} 的安全级别,至少需要取 $\omega(\boldsymbol{e}) = 6$,此时盲化安全性为 2^{87},签名长度为 219 b。

当 $n = 2^{16}$, $t = 9$ 时,本文算法与 QC 盲签名的签名长度和盲化安全性[10] 的对比如表 3 所示。

表 3　2 种算法的签名长度和盲化安全性对比

算法名称	签名 σ 的长度	盲化安全性
本文算法	219 *b*	2^{87}
QC 盲签名	400 *Mb*	$>2^{80}$

由表 3 可看出,参数相同时,本文算法的签名长度较小。

当 $n = 2^{16}$, $t = 9$ 时,本文算法与基于 Niederreiter 公钥密码体制的盲签名方案[11] 的签名长度和工作因子的对比如表 4 所示。

表 4　2 种算法的签名长度和工作因子对比

算法名称	签名 σ 的长度/b	工作因子
本文算法	219	2^{86}
基于 Niederreiter 盲签名	144	2^{78}

由表 4 可看出,参数相同时,本文算法的工作因子较大,安全性较高。

4　结语

本文针对消息的匿名保护问题,提出了一种基于编码的盲签名方案。该方案是基于 CFS 方案的盲签名方案,其安全性是基于校验子译码的困难问题。分析表明,该方案不仅具有消息内容对签名者不可见、不可伪造性和不可跟踪性等一般盲签名的基本性质,而且该方案是基于编码的盲签名方案,可以抵抗量子算法的攻击,并且比目前已有的基于编码的盲签名方案性能更好。

参考文献:

[1] LIU J, JIA J, ZHANG H, *et al*. Digital signature protocol based on error-correcting codes [J]. Journal of Huazhong University of Science and Technology: Natural Science, 2014, 42(11): 97 – 101. (刘金会, 贾建卫, 张焕国, 等. 一种基于纠错码的数字签名协议[J]. 华中科技大学学报: 自然科学版, 2014, 42(11): 97 – 101.)

[2] BERLEKAMP E R, McELIECE R J, van TILBORG H C A. On the inherent intractability of certain coding problems [J]. IEEE Transactions on Information Theory, 1978, 24(3): 384 – 386.

[3] McELIECE R J. A public-key cryptosystem based on algebraic coding theory [J]. DSN Progress Report, 1978, 42(44): 114 – 116.

[4] NIEDERREITER H. Knapsack-type cryptosystems and algebraic coding theory [J]. Problems of Control and Information Theory, 1986, 15(2): 159 – 166.

[5] COURTOIS N, FINIASZ M, SENDRIER N. How to achieve a McEliece-based digital signature scheme [EB/OL]. [2015-01-03]. http://www.researchgate.net/publication/221327329_How_to_Achieve_a_McEliece-Based_Digital_Signature_Scheme.

[6] CHAUM D. Blind signature system [C]// Proceedings of Crypto 1983. Berlin: Springer, 1984: 153 – 153.

[7] CHAUM D. Blind signatures for untraceable payments [C]// Proceedings of Crypto 1982. Berlin: Springer, 1983: 199 – 203.

[8] LIU X, XIN X. Improved blind signature electronic cash scheme [J]. Computer Engineering and Applications, 2011, 47(4): 114 – 116. (刘晓亚, 辛小龙. 改进的盲签名电子现金方案[J]. 计算机工程与应用, 2011, 47(4): 114 – 116.)

[9] ZHENG D, LI X, HUANG Z. Cryptography — cryptographic algorithm and agreement [M]. Beijing: Publishing House of Electronics Industry, 2014: 104 – 106, 162 – 165. (郑东, 李祥学, 黄征. 密码学——密码算法与协议[M]. 北京: 电子工业出版社, 2014: 104 – 106, 162 – 165.)

[10] OVERBECK R. A step towards QC blind signatures [EB/OL]. [2015-01-04]. http://eprint.iacr.org/2009/102.pdf.

[11] LI Z, LI Z. Niederreiter PKC based blind signature scheme [J]. Journal of Beijing Electronic Science and Technology Institute, 2013, 21(2): 50 – 55. (李泽慧, 李子臣. 基于 Niederreiter 公钥密码体制的盲签名方案[J]. 北京电子科技学院学报, 2013, 21(2): 50 – 55.)

[12] ZHENG D, ZHAO Q, ZHANG Y. A brief overview on cryptography [J]. Journal of Xi'an University of Posts and Telecommunication, 2013, 18(6): 1 – 10. (郑东, 赵庆兰, 张应辉. 密码学综述[J]. 西安邮电大学学报, 2013, 18(6): 1 – 10.)

[13] WU S. Hash function analysis summary [R]. Beijing: Institute of Software, Chinese Academy of Science, 2010. (吴双. Hash 函数分析方法综述[R]. 北京: 中国科学院软件研究所, 2010.)

[14] CANTEAUT A. A new algorithm for finding minimum-weight words in large linear codes [C]// Proceedings of the 5th IMA Conference on Cryptography and Coding, LNCS 1025. Berlin: Springer-Verlag, 1995: 205 – 212.