文章编号:1009-3087(2016)02-0097-07 DOI:10.15961/j.jsuese.2016.02.014

基于 Niederreiter 密码的签密方案

韩益亮[1,2],李 冲[1],房鼎益[2],杨晓元[1]
(1.武警工程大学 电子技术系,陕西 西安 710086;2.西北大学 信息科学与技术学院,陕西 西安 710121)

摘 要:针对现有签密方案不能抵抗量子攻击的问题,将 Niederreiter 公钥密码和 CFS 签名方案相结合,构造了一种既能抵抗量子攻击又具有较小密钥数据量的签密方案。该方案用 Goppa 码的快速译码算法来实现对消息的认证,同时基于伴随式译码算法来实现对消息的加密。分析表明,方案在随机预言机模型下达到了 IND-CCA2 安全和 EUF-CMA 安全。在公钥量不变的情况下,新方案的签密文较"先加密后签名"减少了 44.4%。与标准签密算法相比较,签密和解签密的运算量也有着较大幅度的减少。所提出的方案可以作为抵抗量子攻击签密的参考方案。

关键词:后量子密码;公钥密码;数字签名;签密
中图分类号:TP309 **文献标志码**:A

New Signcryption Scheme Based on Niederreiter Cryptosystem

HAN Yiliang[1,2], *LI Chong*[1], *FANG Dingyi*[2], *YANG Xiaoyuan*[1]
(1. Dept. of Electronic Technol., Eng. Univ. of CAPF, Xi'an 710086, China;
2. School of Info. Sci. and Technol., Xi'an 710121, China)

Abstract: To address the issue that the existed signcryptoin schemes fail to resist the quantum attack, a new signcryption scheme that has the light key overhead was constructed, by combining the Niederreiter public cryptosystem and CFS signature scheme. The proposal employs the decode algorithm of Goppa code to authenticate the message, and keeps the secret of the message by syndrome decoding algorithms. Analysis showed that the proposed scheme has the security of IND-CCA2 and EUF-CMA in the random oracle model. The proposed scheme has high performance. Compared with "sign then encrypt" method, the ciphertext of the new scheme is reduced by 44.4% in the case that both of them have the same size of the public key. Compared with the standard signcryption scheme, the computation of the signcryption and unsigncryption is also greatly reduced. The proposal could be adapted as one of the signcryption scheme that resisting the quantum attack.

Key words: post-quantum cryptography; public key cryptosystem; digital signature; signcryption

当前所普遍使用的公钥密码算法主要基于大整数分解、离散对数等计算上困难的问题,而 Shor 等[1]于 1997 年提出的量子搜索算法有可能有效地解决该类问题,从而严重威胁到基于数论难题的公钥密码体制。为应对挑战。2006 年第一届后量子密码学国际会议(PQCrypto'2006)上提出了"后量子密码学"的概念,其中基于编码的密码是后量子密码的一种良好备选方案。基于编码的密码可以追溯到 1978 年,McEliece[2]利用最大似然译码问题和 Goppa 码的快速译码算法,首次提出基于纠错码的公钥密码体制,即 McEliece 公钥密码体制。随后,Niederreiter[3]提出另一种基于纠错码的公钥密码体制,即 Niederreiter 公钥密码体制,它隐藏了具有快速译码算法的线性分组码的校验矩阵。基于编码的密码具有安全性高、加解密复杂性低,以及对 Shor 算法免疫等特点,近几年来成为密码学界研究的热

收稿日期:2015-10-10
基金项目:国家自然科学基金资助项目(61572521;61103231;61272492);陕西省自然科学基础研究计划项目(2015JM6353);中国博士后科研基金面上项目(2014M562445);特别资助项目(2015T81047)
作者简介:韩益亮(1977—),男,副教授,博士,博士生导师. 研究方向:应用密码学. E-mail:yilianghan@hotmail.com
网络出版时间:2016-2-29 17:25:52 **网络出版地址**:http://www.cnki.net/kcms/detail/51.1596.T.20160229.1725.002.html

点[4-7]。而目前基于编码的密码体制普遍存在密钥数据量大,且所构造的应用方案功能也比较少。另一方面,公钥加密和数字签名作为公钥密码的2个重要分支,分别解决了机密性和认证性问题。如果要通过一个算法同时解决机密性和认证性问题,Zheng[8]在1997年提出一种密码原语——签密,在一个逻辑步骤内同时实现加密和签名功能,且效率远远高于传统的"先加密后签名"或"先签名后加密"方法。随后,签密的研究不断丰富和完善[9-11]。Zheng提出的SCS签密方案[8]和Malone-Lee等提出的基于RSA的"一石二鸟"签密方案[12],已经成为标准。2011年,鉴于签密在数据安全中的重要性,国际标准化组织ISO将其作为ISO/IEC NP 29150标准[13]。目前,基于编码的签密研究成果还非常少[14]。因此构造基于编码的签密方案对于探索抗量子攻击的高效密码来说是具有重要意义的。

作者将经典Niederreiter公钥密码[3]和CFS签名方案相结合[15],提出一种基于编码的签密方案。方案用Goppa码的快速译码算法来实现对消息的认证,同时基于伴随式译码算法来实现对消息的加密。安全性分析表明,该方案在随机预言模型下达到了IND-CCA2安全和EUF-CMA安全。在当前的安全参数下,方案在签密文量上较"先加密后签名"方法减少了近44.4%,在(解)签密运算量方面,比标准签密方案也有很大的提高,具有一定的实用价值。

1 预备知识

1.1 编码理论中的NPC问题

Berlekamp、MeElieee和van Tilborg在文献[16]中证明了最大似然译码问题是NPC问题,判定问题表述如下:

对于有限域$GF(2)$上的一个$n \times m$的矩阵$\boldsymbol{H}$、一个m维向量$\boldsymbol{y} = (y_1, y_2, \cdots, y_m)$以及正整数$t$,是否存在一个$GF(2)$上的向量$\boldsymbol{x} = (x_1, x_2, \cdots, x_n)$,它的汉明重量$wt(\boldsymbol{x}) \leq t$,且满足$\boldsymbol{y} = \boldsymbol{x}\boldsymbol{H}^{\mathrm{T}}$。

用(n,k,d)线性码的校验矩阵表示为$\boldsymbol{H}$,则可得如下结论:若已知(n,k,d)线性码的校验矩阵$\boldsymbol{H}$、t和伴随式$\boldsymbol{s}$,求错误向量$\boldsymbol{e}$,汉明重量$wt(\boldsymbol{e}) \leq t$,其中,$d = 2t+1$,且$\boldsymbol{e}$满足$\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}} = \boldsymbol{s}$是NPC问题。

因为纠错码的译码问题是由伴随式$\boldsymbol{s}$求错误图样$\boldsymbol{e}$,故一般线性码的译码问题是NPC问题。

1.2 Niederreiter公钥密码

1986年,Niederreiter[3]使用错误向量作为明文,并隐藏了具有快速译码算法的广义RS码的校验矩阵,构造出了基于纠错码的公钥密码。Niederreiter密码与McEliece密码体制是等价的,但在相同的参数下Niederreiter密码体制有着密钥存储量低、信率高的优点。基于Goppa码的Niederreiter公钥体制如下:

设C是有限域$GF(q)$上线性$(n,k,2t+1)$Goppa码,$\boldsymbol{H}$为码C的$(n-k) \times n$校验矩阵,$\boldsymbol{Q}$为有限域$GF(q)$上的$(n-k) \times (n-k)$非奇异矩阵,$\boldsymbol{P}$为有限域$GF(q)$上的一个$n \times n$阶置换矩阵。私钥为$\boldsymbol{H}$、$\boldsymbol{Q}$、$\boldsymbol{P}$;公钥为$\boldsymbol{H}' = \boldsymbol{Q}\boldsymbol{H}\boldsymbol{P}$,$t = (n-k)/\mathrm{lb}\, n$;明文是有限域$GF(q)$上重量为$t$的$n$维向量$\boldsymbol{e}$。

加密算法:$\boldsymbol{s} = \boldsymbol{H}'\boldsymbol{e}^{\mathrm{T}}$($\boldsymbol{s}$为一个$n-k$维向量)。

解密算法:$\boldsymbol{Q}^{-1}\boldsymbol{s} = \boldsymbol{H}\boldsymbol{P}\boldsymbol{e}^{\mathrm{T}}$,由快速译码算法得到$\boldsymbol{P}\boldsymbol{e}^{\mathrm{T}}$,因此可以求出$\boldsymbol{e}^{\mathrm{T}} = \boldsymbol{P}^{-1}\boldsymbol{P}\boldsymbol{e}^{\mathrm{T}}$。

2001年,Courtois、Finiasz和Sendrier[15]基于Niederreiter密码体制提出一种签名方案,称之为CFS签名方案,是为数不多的可证明安全的签名方案。取C是有限域$GF(q)$上线性$(n,k,2t+1)$Goppa码,哈希函数h满足$h:\{0,1\}^{*} \to F_2^n$,Decode为快速译码算法,d为待签名消息。

签名算法:

1) $i \leftarrow i+1$

2) $\boldsymbol{x}' = \mathrm{Decode}(\boldsymbol{Q}^{-1}h(h(d) \parallel i))$

3) 若$\boldsymbol{x}'$不存在,返回1)

输出$(i, \boldsymbol{x}'\boldsymbol{P})$

验证算法:

$\boldsymbol{s}' = \boldsymbol{H}\boldsymbol{x}'^{\mathrm{T}}$

$\boldsymbol{s} = h(h(d) \parallel i)$

if $\boldsymbol{s} = \boldsymbol{s}'$ then

  accepts $\boldsymbol{s}$

else reject $\boldsymbol{s}$

在签名算法中,校验子可解码成功的概率为$1/t!$,即CFS方案需要大概$t^2m^3t!$次运算可得到正确的签名,其中,签名长度为$\mathrm{lb}(r\binom{n}{t}) \approx \mathrm{lb}(n^t)$。

2 定义与安全模型

2.1 基于编码的签密定义

定义1 基于编码的签密方案包含以下4个算法:

系统建立(Setup):输入系统的安全参数cp,得到系统的公开参数。

密钥生成(KeyGen):为用户U产生公私钥对,$\{pk_U, sk_U\} \leftarrow \mathrm{Gen}\{U, cp\}$,其中,$cp$为安全参数,$sk_U$

为私钥,pk_U 为公钥。

签密(Signcryption):用户 A 要向用户 B 发送消息 $\boldsymbol{m}$,发送方输入$\{sk_A, pk_B, \boldsymbol{m}\}$,得到签密文 δ。

解签密(Unsigncryption):用户 B 接收到用户 A 发送的签密文 δ 时,输入$\{sk_A, pk_B, \boldsymbol{m}\}$,得到消息 $\boldsymbol{m}$,或拒绝该签密文。

2.2　安全性定义和模型

为同时解决消息的机密性和认证性的问题,Zheng[8] 指出签密的安全性定义应该满足机密性、不可伪造性和不可否认性。而如果签密方案的签密文是可公开验证的,则不可伪造性同时也蕴涵了不可否认性。因此,一般签密方案要求同时保证消息的机密性和不可伪造性。

1)机密性

定义 2　在如下的攻击游戏中,若任意多项式时间内的攻击者赢得挑战的优势都是可忽略的,则称该基于编码的签密方案在适应性选择密文攻击下具有不可区分性(IND-CCA2)。

机密性攻击游戏包括 5 个阶段。

第 1 阶段:挑战者运行系统参数建立算法,建立系统公共参数 cp,运行密钥建立算法,分别为挑战用户 A 和 B 建立公私钥对$\{pk_A, sk_A\}$、$\{pk_B, sk_B\}$,发送$\{pk_A, sk_A\}$给攻击者$\mathcal{A}$,输入$\{pk_A, sk_A\}$、$\{pk_B, sk_B\}$给预言机。

第 2 阶段:攻击者向挑战者进行多次的签密询问和解签密询问。

签密询问:用户提交消息 $\boldsymbol{m}$ 和收发双方的公钥对$\{pk_S, sk_R\}$给挑战者,其中,$pk_S \in \{pk_A, pk_B\}$,pk_R 可以是任意用户的公钥。挑战者以相同的输入向预言机进行签密预言询问,预言机返回计算结果,最后挑战者将此结果返回给攻击者。

解签密询问:用户提交合法的签密文 δ 和$\{pk_S, pk_R\}$给挑战者,其中,$pk_R \in \{pk_A, pk_B\}$,pk_S 可以是任意用户的公钥。挑战者以相同的输入向预言机进行解签密询问,预言机返回计算结果,最后挑战者将结果返回给攻击者。

第 3 阶段(挑战阶段):攻击者提交 2 个等长的消息 m_0、m_1,挑战收发双方的公钥对为$\{pk_S^*, pk_R^*\}$,给挑战者进行挑战询问,其中,$pk_S^*, pk_R^* \in \{pk_A, pk_B\}$。挑战者选择一个随机比特 β,并将消息 m_β 和攻击者输入的收发双方公钥作为输入向预言机进行签密询问,预言机返回签密文 δ^* 给挑战者,挑战者将此结果返回给攻击者。

第 4 阶段:攻击者继续向挑战者进行多次签密和解签密询问。但攻击者不能对挑战结果$\{\delta^*, pk_S^*, pk_R^*\}$进行解签密询问。

第 5 阶段:攻击者输出猜测的比特 β。如果 $\beta' = \beta$,则攻击者赢得挑战。定义攻击者赢得挑战的优势为:

$$Adv = |\Pr[\beta' = \beta] - 1/2|。$$

2)不可伪造性

定义 3　在下面的攻击游戏中,若任意多项式时间内的攻击者赢得挑战的优势都是可忽略的,则该基于编码的签密方案在适应性选择消息攻击下满足不可伪造性(EUF-CMA)。

不可伪造性攻击游戏包括 3 个阶段。

第 1 阶段:与机密性攻击游戏类似,但在本游戏中只存在一个挑战用户 A,没有挑战用户 B。

第 2 阶段:与机密性攻击游戏类似,但在本游戏中攻击者只进行签密询问,同时加入验证询问。

第 3 阶段:攻击者提交挑战内容,包括挑战消息 m^*,伪造的签密文 δ^*,挑战接收方的公私钥对$\{pk_R^*, sk_R^*\}$,其中挑战接收方可以是任意用户。若挑战收发双方的公钥对 $pk_R^* = pk_A$,则挑战者知道 sk_R^*,而攻击者可能不知道 sk_R^*,因此攻击者在提交挑战信息时只输出$\{m^*, \delta^*, pk_S^*, pk_R^*\}$。在此挑战中用户 A 为挑战发送方,所以挑战者运行解签密算法:Unsigncrypt$\{cp, \delta^*, sk_R^*, pk_S^*\}$。若其输出结果是 m^*,攻击者之前没有以$\{m^*, pk_S^*, pk_R^*\}$为输入进行签密询问,则用户赢得挑战。将攻击者赢得挑战的优势定义为:$Adv = \Pr[$攻击者赢得挑战$]$。

3　基于 Niederreiter 密码的签密方案

3.1　基本方案

对给定的 (n, k, d) 线性分组码,只要在 2^k 个码字集合中任意选择 k 个线性无关的码字作行,均可得到码的一个生成矩阵,因此码的可能的生成矩阵数目有$(2^k-1)(2^k-2)\cdots(2^k-2^{k-1})$个。

设 C 是有限域 $GF(q)$ 上线性 $(n, k, 2t+1)$ Goppa 码,$\boldsymbol{H}$ 为码 C 的$(n-k)\times n$ 校验矩阵,$\boldsymbol{Q}$ 为有限域 $GF(q)$ 上的$(n-k)\times(n-k)$非奇异矩阵,$\boldsymbol{P}$ 为有限域 $GF(q)$ 上的 $n\times n$ 阶置换矩阵。定义函数 $\boldsymbol{\Phi}_{n,t}: \{0,1\}^l \to W_{n,t}$,其中,$W_{n,t} = \{\boldsymbol{e} \in F_2^n \mid wt(\boldsymbol{e}) = t\}$,$l = \lfloor \mathrm{lb} | W_{n,t} | \rfloor$,$t = (n-k)/\mathrm{lb}\, n$。

发送方 S 私钥 $\boldsymbol{H}_1$、$\boldsymbol{Q}_1$、$\boldsymbol{P}_1$,公钥 $\boldsymbol{H}_1' = \boldsymbol{Q}_1\boldsymbol{H}_1\boldsymbol{P}_1$。接收方 R 私钥 $\boldsymbol{H}_2$、$\boldsymbol{Q}_2$、$\boldsymbol{P}_2$,公钥 $\boldsymbol{H}_2' = \boldsymbol{Q}_2\boldsymbol{H}_2\boldsymbol{P}_2$。$h$ 为公开哈希函数,Decode( ) 为快速译码算法,$\boldsymbol{m}$ 为待

签密消息。

1)签密(Signcrypt)

发送方S执行如下操作:

$$i \leftarrow \{1,2,\cdots,2^{n-k}\} \tag{1}$$

$\boldsymbol{x}' \leftarrow \text{Decode}(\boldsymbol{Q}_1^{-1} h(h(\boldsymbol{m}) \| i))$;

if $\boldsymbol{x}'$ 不存在,返回(1);

$\boldsymbol{e} \leftarrow \boldsymbol{x}'\boldsymbol{P}_1$;

$\boldsymbol{s} \leftarrow (\boldsymbol{\Phi}_{n,t}^{-1}(\boldsymbol{e}) \| i)$;

$\boldsymbol{x} \leftarrow \boldsymbol{\Phi}_{n,t}(\boldsymbol{m})$;

$\boldsymbol{\delta} \leftarrow \boldsymbol{H}_2'\boldsymbol{x}^{\mathrm{T}}$;

输出$(\boldsymbol{\delta},\boldsymbol{s})$。

2)解签密(Unsigncrypt)

接收方R收到签密文$(\boldsymbol{\delta},\boldsymbol{s})$后,执行如下操作:

$\boldsymbol{Q}_2^{-1}\boldsymbol{\delta} = \boldsymbol{H}_2\boldsymbol{P}_2\boldsymbol{x}^{\mathrm{T}}$;

$\text{Decode}(\boldsymbol{H}_2\boldsymbol{P}_2\boldsymbol{m}^{\mathrm{T}}) = \boldsymbol{P}_2\boldsymbol{x}^{\mathrm{T}}$;

$\boldsymbol{x}^{\mathrm{T}} = \boldsymbol{P}_2^{-1}\boldsymbol{P}_2\boldsymbol{x}^{\mathrm{T}}$;

$\boldsymbol{m} \leftarrow \boldsymbol{\Phi}_{n,t}^{-1}(\boldsymbol{x})$;

$\boldsymbol{e} \leftarrow \boldsymbol{\Phi}_{n,t}(\boldsymbol{\Phi}_{n,t}^{-1}(\boldsymbol{e}))$;

$\boldsymbol{s}_1 \leftarrow \boldsymbol{H}_1'(\boldsymbol{e}^{\mathrm{T}})$;

$\boldsymbol{s}_2 \leftarrow h(h(\boldsymbol{m}) \| i)$;

若$\boldsymbol{s}_1 = \boldsymbol{s}_2$,则返回$\boldsymbol{m}$;否则,拒绝。

3.2 可证明安全的方案

为了使方案满足更高的安全性要求,将其如下修改,使方案的安全性可以归约到解决最大似然译码问题的困难性上。

Hash为安全哈希函数,LSB_n表示字符串的左n位,r为随机比特串。Signcrypt( )表示3.1节中签密运算过程,Unsigncrypt( )表示解签密运算过程。

签密:

$\boldsymbol{z} = \text{Hash}(r \| \boldsymbol{m})$;

$\boldsymbol{y} = \boldsymbol{z} \oplus (r \| \boldsymbol{m})$;

$(\boldsymbol{\delta},\boldsymbol{s}) = \text{Signcrypt}(\boldsymbol{z})$;

$(\boldsymbol{\delta}',\boldsymbol{s}) = (\boldsymbol{\delta} \| \boldsymbol{y},\boldsymbol{s})$;

输出签密文$(\boldsymbol{\delta}',\boldsymbol{s})$;

解签密:

$\boldsymbol{\delta} = LSB_n(\boldsymbol{\delta}')$;

$\boldsymbol{z} = \text{Unsigncrypt}(\boldsymbol{\delta},\boldsymbol{s})$;

$r \| \boldsymbol{m} = \boldsymbol{z} \oplus \boldsymbol{y}$;

若$\boldsymbol{z} = \text{Hash}(r \| \boldsymbol{m})$,返回$\boldsymbol{m}$;

否则,拒绝$(\boldsymbol{\delta}',\boldsymbol{s})$。

4 安全性分析

4.1 机密性

定理1 假设在随机预言模型下,对任意的攻击者$\mathcal{A}$,若能在$t' = t + ploy(n,q_{\mathrm{H}},q_{\mathrm{G}})$时间上满足:$Adv_{\mathrm{A}}^{N} > Adv_{\mathrm{A}}^{\text{IND-CCA2}} - q_{\mathrm{H}}/2^{len(r)+1} - q_{\mathrm{D}}/C(n,t)$,则构造的方案$(Adv_{\mathrm{A}}^{\text{IND-CCA2}} q_{\mathrm{G}},q_{\mathrm{H}},q_{\mathrm{SC}},q_{\mathrm{USC}},t')$是IND-CCA2安全的,$q_{\mathrm{G}}$、$q_{\mathrm{H}}$、$q_{\mathrm{SC}}$和$q_{\mathrm{USC}}$分别是$G$预言机、$H$预言机、签密预言机和解签密预言机的最大预言次数,$t$为约束时间,$q_{\mathrm{D}}$为在解签密询问中恰好查询到正确明文的次数,$1/C(n,t)$为一次有效解密密文的概率。

证明:通过反证法构造矛盾来完成证明。基本思路是在签密过程中,如果存在一个攻击者$\mathcal{A}$能够在t内以大于Adv的不可忽略的优势猜出IND-CCA2攻击游戏中的β,即$\beta' = \beta$,那么就可以构造出一个攻击算法B,解决Goppa码的译码问题,从而推出矛盾,定理得证。

假定给攻击算法B给定一个Goppa码的译码问题的实例,其构造如下。

初始化阶段:根据新方案的系统生成算法,生成公共参数$cp = \{H,r,\boldsymbol{y},\beta\}$。其中,$r \in \{0,1\}^{|r|}$,$\boldsymbol{y},\beta \in \{0,1\}$是$B$随机选择的。$B$将公开参数发送给攻击者$\mathcal{A}$。建立表$H^{\text{list}}$:$\{\{0,1\}^{|r|},H\}$,$G^{\text{list}}$:$\{\{0,1\}^{|r|},\text{SC}^{\text{list}}$:$\{\{0,1\}^{|r|},\text{SC}\}$,$\text{USC}^{\text{list}}$:$\{\{0,1\}^{|r|},\text{USC}\}$,并初始化为空。

G询问:攻击者$\mathcal{A}$询问算法B,$\boldsymbol{z}$的值。查找G^{list}表中是否存在相应记录,若存在,返回G;否则,返回预言机的定义$G = G(\boldsymbol{z}) = (r \| \boldsymbol{m}_\beta) \oplus \boldsymbol{y}$,并将记录添加到询问表当中。

H询问:攻击者$\mathcal{A}$询问算法B,$r \| \boldsymbol{m}_\beta$的值。查找$H^{\text{list}}$表中是否存在相应记录,若存在,返回$H$;否则,返回预言机的定义$H = \text{Hash}(r \| \boldsymbol{m}_\beta) = \boldsymbol{z}$,并将此记录添加到询问表当中。

以上2个查询的定义使得对$\boldsymbol{\delta}' = \boldsymbol{\delta} \| \boldsymbol{y}$的解密为$r \| m_\beta$。对签密询问和解签密询问的模拟方法如下:

签密询问:攻击者$\mathcal{A}$询问算法B,在签密预言机中输入$\boldsymbol{m}$,查找SC^{list}表中是否存在相应记录,若存在,返回$\boldsymbol{\delta}'$;若不存在,则随机取$r \in \{0,1\}^{|r|}$,调用询问G,输入$r \| \boldsymbol{m}$,得到$\boldsymbol{z}$。运行方案中的签密算法,消息$\boldsymbol{m}$作为输入,将得到密文$\boldsymbol{\delta}'$记入签密询问表SC^{list}中。

解签密询问:攻击者$\mathcal{A}$询问算法B,在解签密预言机中输入签密文$\boldsymbol{\delta}'$,查找USC^{list}表中是否存在相应记录,若存在,返回$\boldsymbol{m}$;否则,运行方案的解签密算法,查找询问表H^{list}和G^{list},若能找到相应记录,返回消息$\boldsymbol{m}$;否则拒绝这个签密文。

挑战阶段:攻击者提交2个等长的消息$\boldsymbol{m}_0$、$\boldsymbol{m}_1$,

给算法 B。随机选择一个数 $\beta \in \{0,1\}$,并利用公钥计算 $\boldsymbol{m}$ 的签密文 $\boldsymbol{\delta}'$,将 $\boldsymbol{\delta}'$ 返回给 $\mathcal{A}$。

猜测:攻击者 $\mathcal{A}$ 输出猜测值 β'。如果 $\beta' = \beta$,则攻击者赢得挑战。

由上可知仿真算法 B 是完整的有效仿真。因为 $\mathrm{Hash}(\boldsymbol{z}) \oplus \boldsymbol{y} = \boldsymbol{z}$,所以算法 B 破解原始的 Niederreiter 签密算法的概率也就是计算 B 能得到 $\boldsymbol{z}$ 的概率。

用 E_{G} 和 E_{H} 分别表示对预言机 G、H 进行询问的事件,这 2 个事件互斥,故 $\Pr[E_{\mathrm{G}} \cap E_{\mathrm{H}}] = \Pr[E_{\mathrm{G}}] \cap \Pr[E_{\mathrm{H}}]$。当 2 个询问事件都发生时,攻击者 $\mathcal{A}$ 猜出 β 的概率很高,假设为 1。则有下式成立:$\Pr[\beta = \beta'] < \Pr[E_{\mathrm{G}} \cap E_{\mathrm{H}}] + (1 - \Pr[E_{\mathrm{G}} \cap E_{\mathrm{H}}])/2 = (\Pr[E_{\mathrm{G}} \cap E_{\mathrm{H}}] + 1)/2$。$Adv_{\mathrm{A}}^{\text{IND-CCA2}} = |\Pr[\beta = \beta'] - 1/2|$,故 $\Pr[E_{\mathrm{G}} \cap E_{\mathrm{H}}] > Adv_{\mathrm{A}}^{\text{IND-CCA2}}$。因为攻击者 $\mathcal{A}$ 若不对 E_{H} 和 E_{G} 询问,不可能知道 r、b 的值,所以在 Hash 中查询 $\boldsymbol{m}_\beta \| r$ 的概率为:$\Pr[E_{\mathrm{H}}] = 1/2^{len(r)+1}$,从而得知,$\Pr[E_{\mathrm{H}}] \le 1 - [1 - (1/2^{len(r)})]^{q_{\mathrm{H}}} \le q_{\mathrm{H}}/2^{len(r)+1}$。当事件 E_{G} 先发生时,算法 B 才能正确模拟预言机 H 和 G,进而恢复明文 $\boldsymbol{m}$。所以,先 H 询问后 G 询问恢复出明文的概率满足 $\Pr > Adv_{\mathrm{A}}^{\text{IND-CCA2}} - q_{\mathrm{H}}/2^{len(r)+1}$。定义 D 为“解签密经过 q_{D} 次询问恰好查询到正确明文”的事件,有 $\Pr[D] > 1 - [1 - (1/C(n,t))]^{q_D} \le q_{\mathrm{D}}/C(n,t)$,其中,$1/C(n,t)$ 为一次有效解密密文的概率。最后可得,

$$Adv_{\mathrm{A}}^{\mathrm{N}} > Adv_{\mathrm{A}}^{\text{IND-CCA2}} - q_{\mathrm{H}}/2^{len(r)+1} - q_{\mathrm{D}}/C(n,t),$$

与已知矛盾,故不存在优势比 $Adv_{\mathrm{A}}^{\text{IND-CCA2}}$ 大的攻击者 $\mathcal{A}$ 能成功攻破 IND-CCA2 攻击游戏,即新方案是 IND-CCA2 安全的。

再对算法的运行时间 t' 进行分析。其运行时间除解决 Goppa 码的译码问题的运行时间 t 之外,主要依赖于 H 询问、G 询问的多项式运算,因此时间复杂度为 $ploy(n, q_{\mathrm{H}}, q_{\mathrm{G}}, q_{\mathrm{SC}}, q_{\mathrm{USC}})$,所以,$t' \le t + ploy(n, q_{\mathrm{H}}, q_{\mathrm{G}}, q_{\mathrm{SC}}, q_{\mathrm{USC}})$。

证毕。

4.2　不可伪造性

定理 2　假设在随机预言模型下,本文方案对任意的攻击者 E,若能够在 $t' = t + ploy(n, q_{\mathrm{H}}, q_{\mathrm{G}}, q_{\mathrm{SC}}, q_{\mathrm{USC}})$ 时间满足 $Adv_{\mathrm{E}}^{\mathrm{N}} \ge Adv_{\mathrm{E}}^{\text{IND-CCA2}} \cdot [1 - q_{\mathrm{SC}} 2^{|r|}] \cdot [1 - q_{\mathrm{USC}}/2^{|r|}]$,则新方案是 EUF-CMA 安全的,$q_{\mathrm{G}}$、$q_{\mathrm{H}}$、$q_{\mathrm{SC}}$ 和 q_{USC} 分别为 G 预言机、H 预言机、签密预言机和解签密预言机的最大预言次数,t 为约束时间。

证明:通过反证法构造矛盾来完成证明。基本思路是在签密过程中,如果存在一个攻击算法 E 能够在 t 内以大于 Adv 的不可忽略的优势成功伪造出签密方案的有效签密文本,那么就可以构造出一个攻击者 F,能够解决 Goppa 码的译码问题,从而推出矛盾,定理得证。

对 H 和 G 模拟和定理 1 的证明相同,对签密询问和解签密询问的模拟方法如下:

签密询问:攻击者 E 询问算法 F,在签密预言机中输入 $\boldsymbol{m}$,查找 $\mathrm{SC}^{\mathrm{list}}$ 表中是否存在相应记录,若存在,返回 $\boldsymbol{s}$。若不存在,则随机取 $r \in \{0,1\}^{|r|}$,调用询问 H,输入 $r \| \boldsymbol{m}$,得到 $\boldsymbol{z}$;调用 G 询问,输入 $\boldsymbol{z}$,得到 $\boldsymbol{s}$。运行方案中的签密算法,消息 $\boldsymbol{m}$ 作为输入,将得到签密文 s 记入签密询问表 $\mathrm{SC}^{\mathrm{list}}$ 中。

解签密询问:攻击者 E 询问算法 F,在解签密预言机中输入签密文 $\boldsymbol{s}$,查找 $\mathrm{USC}^{\mathrm{list}}$ 表中是否存在相应记录,若存在,返回 $\boldsymbol{m}$;否则,运行方案中的解签密算法,查找询问表 H^{list} 和 G^{list},若能找到相应记录,返回消息 $\boldsymbol{m}$;否则拒绝这个签密文。

不可伪造性攻击游戏中前 2 个阶段与机密性攻击游戏类似,但在本游戏中攻击者只进行多次签密询问。

挑战阶段:攻击者提交挑战内容,包括消息 $\boldsymbol{m}^*$ 和伪造的签密文 $\boldsymbol{s}^*$。攻击者 E 对 $\boldsymbol{s}^*$ 进行解签密询问,如果输出结果是 $\boldsymbol{m}^*$,并且攻击者 E 之前没有以 $\boldsymbol{m}^*$ 进行签密询问,则攻击者赢得挑战。

用事件 E_F' 表示预言机模拟成功,其概率满足 $[1 - q_{\mathrm{SC}}/2^{|r|}][1 - q_{\mathrm{USC}}/2^{|r|}] \le \Pr(E_F') \le 1$。用事件 $E_{\boldsymbol{s}^* \to \boldsymbol{m}^*}$ 表示伪造的签密文可解密为 $\boldsymbol{m}^*$。其可归约到 Goppa 的译码问题,故概率为 $\Pr(E_{\boldsymbol{m}^* \leftarrow \boldsymbol{\delta}^*}) = Adv_{\mathrm{E}}^{\text{EUF-CMA}}$。所以,定义 2 成功的优势为:$Adv_{\mathrm{E}}^{\mathrm{N}} = \Pr[E_F' \cap E_{\boldsymbol{m}^* \leftarrow \boldsymbol{\delta}^*}]$,且事件 E_F' 和 $E_{\boldsymbol{s}^* \to \boldsymbol{m}^*}$ 相互独立,即 $\Pr[E_F' \cap E_{\boldsymbol{m}^* \leftarrow \boldsymbol{\delta}^*}] = \Pr[E_F'] \cdot \Pr[E_{\boldsymbol{s}^* \to \boldsymbol{m}^*}]$。最后可得出:

$$Adv_{\mathrm{E}}^{\mathrm{N}} \ge Adv_{\mathrm{E}}^{\text{EUF-CMA}} \cdot [1 - q_{\mathrm{SC}} 2^{|r|}] \cdot [1 - q_{\mathrm{USC}}/2^{|r|}]。$$

可知签密方案是 EUF-CMA 安全的。

算法的运行时间包括攻击者的时间约束 t 和 H 询问、G 询问、签密询问及解签密询问的时间,又算法 F 的时间复杂度为 $ploy(n, q_{\mathrm{H}}, q_{\mathrm{G}}, q_{\mathrm{SC}}, q_{\mathrm{USC}})$,所以可得 $t' \le t + ploy(n, q, q_{\mathrm{G}}, q_{\mathrm{SC}}, q_{\mathrm{USC}})$。

证毕。

在签密过程中,一个 EUF-CMA 攻击者伪造一个成功有效签密文的概率不会大于攻破该方案机密性的概率。综合上述,方案满足 IND-CCA2 安全和 EUF-CMA 安全,故有较强的安全性。

5 性能分析

本签密方案是在 Niederreiter 密码方案的基础上结合 CFS 签名方案构造的。在效率分析中通信代价和计算代价是2个重要因素,分别由密文量大小和(解)签密运算量决定的。就本文 Niederreiter 签密方案而言,取二元既约 Goppa 码,对系统公钥和密文数据量的大小,与 Niederreiter 密码方案及 CFS 签名方案相应变量进行了对比,结果如表1所示。

表1 签密方案数据比较

Tab.1 Comparison of the data for signature schemes

	系统公钥长度/byte	密文数据量/bit
Niederreiter 密码 $(2^{10},524,101)$	32 750	1 024
CFS 签名 $(2^{16},934,19)$	1 179 648	276
加密后签名(EtS)	32 750	2 080
本文方案	32 750	1 156

由表1可知,本文方案在公钥数据量没有增加的情况下实现了签密的功能,而较先加密后签名的组合,签密文数据量减少了44.4%。

就签密和解签密运算量,与"一石二鸟"方案和 SCS 方案进行对比,其中,e 表示模指数运算,h 代表哈希函数运算,S 表示对称加(解)密运算,m 代表矩阵乘运算,D 代表快速译码算法运算,φ 代表 $\Phi_{n,t}$ 函数运算,r 为"一石二鸟"方案选取的参数。结果如表2所示。

表2 签密方案运算量比较

Tab.2 Comparison of computational complexity for signature schemes

	签密	解签密
"一石二鸟"方案	$2e+2h\cdot 2^r$	$3e+4h$
SCS 方案	$e+2h+S$	$1.17e+2h+S$
本文方案	$3m+3h+2\varphi+D\cdot t!$	$3m+3h+2\varphi+D$

在上述方案中,哈希运算和函数运算的计算量较小,其运算量主要集中在模指数运算、对称加(解)密和矩阵乘运算上。对于计算机运算,矩阵运算明显快于模指数运算。在选取(1 024,524)的矩阵和指数为17、模为1 024 bit 的模指数情况下,在计算每信息比特的二元运算数上,矩阵乘运算量约是模指数的1/48。此外,在满足安全性的前提下,签密接收方可选取较小 t 值的二元不可约 Goppa 码,可使签密运算的计算代价进一步降低,提高了计算效率。

6 结 论

量子计算的快速发展使得抗量子攻击的密码学研究十分迫切。作为后量子密码备选方案之一的基于编码的密码有很大的发展空间。提出一个基于 Niederreiter 密码的签密方案,在随机预言机模型下的达到了 IND-CCA2 安全与 EUF-CMA 安全,同时在密文和(解)签密运算效率方面较传统方案有较大提高,具有一定的实用性。

参考文献:

[1] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Journal on Computer, 1997, 26(5): 1484 – 1509.

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

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

[4] Heyse S, Zimmermann R, Paar C. Attacking code-based cryptosystems with information set decoding using special-purpose hardware[M]//Post-quantum Cryptography. Berlin: Springer-Verlag, 2014: 126 – 141.

[5] Baldi M. QC-LDPC code-based cryptosystems[M]//QC-LDPC Code-Based Cryptography. New York: Springer International Publishing, 2014: 91 – 117.

[6] Liu Jingmei, Wang Yanli, Liang Bing, et al. McEliece public key cryptosystem attack algorithm based on enumeration error vector[J]. Journal of Communication, 2014, 35(6): 65 – 69. [刘景美, 王延丽, 梁斌, 等. 基于枚举错误向量的 McEliece 公钥密码体制攻击方法[J]. 通信学报, 2014, 35(6): 65 – 69.]

[7] Overbeck R, Sendrier N. Code-based cryptography[M]// Post-quantum Cryptography. Berlin: Springer-Verlag, 2009: 95 – 145.

[8] Zheng Yuliang. Digital signcryption or how to achieve cost (signature & encryption) ≪ cost(signature) + cost(encryption)[C]//Proceedings of the 17th Annual International

Cryptology Conference. Santa Barbara, California: Springer-Verlag, 1997: 165 – 179.

[9] Han Yiliang, Yang Xiaoyuan. New ECDSA-verifable generalized signcryption [J]. Chinese Journal of Computers, 2006, 29(11): 2003 – 2012. [韩益亮,杨晓元. 可公开验证 ECDSA 广义签密方案[J]. 计算机学报, 2006, 29(11): 2003 – 2012.]

[10] Han Yiliang, Gui Xiaolin. Adaptive secure multicast in wireless networks[J]. International Journal of Communication Systems, 2009, 22(9): 1213 – 1239.

[11] Zhang Yu, Chen Jing, Du Ruiying, et. al. An efficient signcryption scheme for secure communication of VANET [J]. Chinese Journal of Electronics, 2015, 43(3): 512 – 517. [张宇,陈晶,杜瑞颖,等. 适于车载网安全通信的高效签密方案[J]. 电子学报, 2015, 43(3): 512 – 517.]

[12] Malone-Lee J, Mao W. Two birds one stone: Signcryption using RSA[C]//Topics in Cryptology-CT-RSA 2003. Berlin: Springer-Verlag, 2003, LNCS 2612: 211 – 226.

[13] International Organization for Standard (ISO). ISO/IEC 29150 Information technology-security techniques-signcryption[S]. Geneva: International Organization for Standard (ISO), 2011.

[14] Preetha M K, Vasant S, Rangan C P. On provably secure code-based signature and signcryption scheme [R/OL]. (2013 – 06 – 29) [2015 – 04 – 15]. http://eprint.iacr.org/2012/585.

[15] Courtois N T, Finiasz M, Sendrier N. How to achieve a McEliece-based digital signature scheme [C]//Advances in Cryptology—ASIACRYPT 2001. Berlin: Springer-verlag, 2001: 157 – 174.

[16] 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.

(编辑　杨　蓓)