改进的具有轻量级结构的Veron身份认证及数字签名方案

叶君耀[1,2] 郑 东[3] 任 方[3]
(上海交通大学计算机科学与工程系 上海 200240)[1] (景德镇陶瓷大学信息工程学院 景德镇 333403)[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)[3]

摘 要 目前大部分的公钥密码方案都基于大整数分解或离散对数难题,这些困难问题在量子计算机中都可以在多项式时间内求解,而基于纠错码的密码方案可以抵抗量子计算机的攻击,所以很有必要研究基于纠错码的身份认证及数字签名方案。Veron身份认证方案总体性能不错,但公钥太大,大约有150k比特。在Veron方案的基础上,采用双循环矩阵来进一步减小Veron方案中的密钥大小,即通过双循环矩阵把私钥嵌入到公钥中。这样做的好处有3点:1)所基于的安全性是已被证明为安全的循环码;2)改进以后,公钥只有1041比特,而私钥也只有1041比特;3)每轮数据的传输量比较少。然后分析所构造方案的安全性,将其归结到GSD困难问题上。最后,采用FS方法将改进后的身份认证方案转换为数字签名方案,并对该方案进行正确性证明和安全性证明。循环结构的使用使得改进方案实现起来比较容易并且效率较高。这些特点使得所提方案在轻量级结构的场合具有广阔的应用前景,比如手持终端、云存储环境下的数字签名等场合。

关键词 后量子密码,循环码,数字签名,身份认证,纠错码
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.03.037

Improved Veron's Identification with Lightweight Structure and Digital Signature Scheme

YE Jun-yao[1,2] ZHENG Dong[3] REN Fang[3]
(Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China)[1]
(School of Information Engineering, Jingdezhen Ceramic Institute, Jingdezhen 333403, China)[2]
(National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China)[3]

Abstract At present, most of the public key cryptography schemes are based on hard problems such as large integer factorization or discrete logarithm. All these hard problems can be solved by a quantum computer in polynomial time. Cryptographic schemes based on error-correcting codes can resist the attacks by a quantum computer, so it is necessary to design identification schemes or signature schemes based on error-correcting codes. Veron's identification scheme is very nice in general, but it's public key is too long. Based on Veron's scheme, we used double circulant matrix to further reduce the size of public key in Veron's scheme. The secret key is embedded into the public key directly, which has the three following advantages. The security relies on a problem which is related to well-known and well-studied codes, namely the double circulant codes. The size of the public key is very low, only 1041 bits in a typical set-up, and the private key is also 1041bits. The transmission rate of each round is very low. Then we analyzed the security of the improved scheme. Its security can be reduced to GSD hard problem. At last, we used FS paradigm to transform the improved identification scheme into signature scheme, and then proved the correctness and security of the scheme. In the improved scheme, the use of cyclic structure makes it relatively easy to implement and have high efficiency. These characteristics make our variant highly attractive for lightweight implementations, especially in handheld terminal or cloud storage environment.

Keywords Post-quantum cryptography, Cyclic codes, Digital signature, Identification, Error correcting codes

随着网络和信息技术的发展,密码学在现代通信和网络中得到越来越广泛的应用。目前大部分公钥密码技术的研究都基于数论难题[1],很有必要研究基于其他困难问题的公钥密码技术,主要原因可以归结为以下3点。

到稿日期:2016-03-28 返修日期:2016-07-16 本文受国家自然科学基金项目(61472472,61272037),陕西省自然科学基金重点项目(2013JZ020),陕西省自然科学基金项目(2015JQ6262),江西省教育厅项目(GJJ150934,GJJ150895)资助。

叶君耀(1978—),男,博士生,CCF会员,主要研究方向为基于编码的密码学及信息安全,E-mail:sdyejunyao@sjtu.edu.cn(通信作者);郑 东(1964—),男,博士,教授,博士生导师,主要研究方向为后量子密码学、云存储安全;任 方(1981—),男,博士,副教授,主要研究方向为后量子密码学、数字水印技术、空间信息网和物联网的安全等。

(1)目前大部分公钥密码方案都基于大整数分解或离散对数难题，这些困难问题在量子计算机中都可以在多项式时间内求解[2]，导致所有的公钥方案都将面临危险；而基于纠错码的密码方案可以抵抗量子计算机的攻击，虽然现在还没有实用的量子计算机，但是应该提前做好准备。

(2)退一步说，即使这些数论难题仍然是困难的，但由于密码分析者的能力越来越强大，将迫使所设计方案选择的密钥规模越来越大。

(3)传统的算术运算速度太慢，经常含有大数的指数级运算，在一些移动式的存储设备上不适合采用这种算法，如智能卡、售货机、手持终端等，在这些场合都需要轻量级的密钥结构。

Isaac Chuang 和 Neil Gershenfeld[3]在 7 量子比特的计算机上实现了 Shor 的攻击算法。2007 年，16 量子比特的量子计算机被展示，研究人员预测在未来 10～20 年有可能出现足够强大的量子计算机使得目前使用的公钥密码体制非常容易地被攻破。未来量子计算机的问世向人们提出了现实而严峻的问题：量子计算机能够完全攻破经典密码技术，人们将用何种密码技术保护其在通信及相关领域的信息安全问题？有幸的是，除了上述传统的密码体制，还有一些重要的基于不同困难问题的密码体制。目前人们找到了 4 种能够抵御量子攻击的公钥密码体制。1)基于纠错码问题的公钥密码体制：McEliece[4]于 1978 年提出的基于 Goppa-码的公钥加密体制；2)基于 HASH 的公钥密码体制：Merkle 于 1979 年提出的基于 HASH 树的数字签名体制；3)基于多变量问题的公钥密码体制：Patarin 于 1996 年给出的“HDEv-签名方案”[5]；4)基于格问题的公钥密码体制：著名的方案是 Hoffstein-Pipher-Silverman“NTRU”公钥加密体制。

最早提出的基于纠错码的身份认证方案是 Stern 身份认证方案[6]，但由于 Stern 方案中的密钥太大，之后 Veron 提出了改进的身份认证方案[7]。Veron 方案是一个多轮交互的零知识协议，每一轮由三步在证明者和验证者之间交互的协议组成，这个交互式协议和基于大整数因子分解的简化的 Fiat-Shamir 协议[8]类似，但 Fiat-Shamir 协议中欺骗者欺骗成功的概率是 1/2，而在 Veron 方案中欺骗成功的概率是 2/3。Veron 身份认证方案的总体性能很不错，但有两个明显缺点：1)若要使得欺骗者欺骗成功的概率小于 2^{-32}，至少得交互 56 轮；2)其密钥太大，超过 150k 比特。由于第一个缺点是由纠错码本身的特性造成的，因此本文主要致力于减小 Veron 身份认证方案中的密钥。

本文考虑通过构造双循环矩阵来改进 Veron[7]身份认证方案，然后用 FS 转换规则[9]将身份认证方案转为数字签名方案，并对该签名方案进行正确性和安全性证明，使其适用于轻量级移动网络的应用环境。基于纠错码的密码学出现得较早，最著名的是 1978 年 McEliece 的公钥加密方案[4]。这种类型的方案和基于多变量[10]的公钥方案具有相同的缺点，它们基于位操作的运算速度是很快的，但是公钥都太大，不适合在移动网络中应用。在 Gaborit 的改进方案中[11]，他将 McEliece 的公钥大小由原来的 500k 减为 12k，受此启发，我们采用双循环矩阵将 Veron 的身份认证方案[7]进行改进，再采用 FS 转换规则[9]将身份认证方案转为数字签名方案，使其适用于轻量级移动网络的应用环境。

在编码密码学中，王新梅于 1990 年提出了一类基于纠错码的数字签名体制[12]，之后有很多人利用线性码来设计数字签名方案，比如文献[13-15]的方案都被证明为不安全方案。然而，研究者认为以下两个方案仍然是安全的。第一个是由 Kabatisansky-Krout-Smeets[16]于 1997 提出的基于随机码的签名方案，但是一个主动的攻击者截获到一些签名以后可以有效地找到签名私钥[17]。第二个方案是由 Courtois-Finiasz-Sendrier[18]于 2001 年提出的第一个可证明安全的基于编码的签名方案，Dallot 于 2007 年对其安全性进行了阐述[19]，并将 CFS 方案的安全性归约到 SD 问题和 Goppa 码的不可区分性。然而 Faugere 等人[20]于 2010 年指出：具有高码率的 Goppa 码和随机码是可区分的，这就导致了 Dallot 的证明是无效的。文献[21]针对这个问题证明了 CFS 签名方案对于选择消息攻击是存在性不可伪造。

目前，可以将基于纠错码的身份认证和数字签名方案应用于软件中。SIDI 等人[22]有效地在软件中实现了 Stern 方案[6]、Veron 方案[7]以及 Pierre-Louis 方案[23]。由于 Pierre-Louis 的方案是一个五步交互式的零知识身份认证方案，因此在证明者和验证者之间传输的数据量就相对较大。Rong Hu 等人[24]将五步的零知识身份认证方案改为三步的零知识身份认证方案。近年来基于纠错码的身份认证方案没有太大的进展，但文献[25-26]给出了一些构造轻量级身份认证的方法。为了让原来的 Veron 方案可以应用到轻量级的移动网络中，有必要进一步研究如何减小 Veron 方案中的密钥。

1　纠错码的基本知识

本节主要讨论基于纠错码的 SD 困难问题、GSD 困难问题和 Veron 身份认证方案，主要参考了文献[27]以及文献[7]。

1.1　基本概念

定义 1(线性码)　F_q 上的(n,k)码 C 是线性空间 F_q^n 上的子空间。F_q^n 中的元素称为字，C 中的元素称为码字，n 称为 C 的码长，k 称为 C 的维数。

定义 2(汉明距离，重量)　两个字 x 和 y 的汉明距离 $d(x,y)$是指 x 和 y 在相同位置的值不同的个数，也即 $d(x,y)=|\{i:x_i\neq y_i\}|$，设 $x=(x_1,\cdots,x_n)$，$y=(y_1,\cdots,y_n)$。用 $|S|$表示集合 S 中元素的个数。特别地，$d(x,0)$表示 x 的汉明重量，0 代表由 n 个 0 组成的零向量。线性码 C 的最小距离指任意两个码字之间的最小汉明距离。

定义 3(生成矩阵)　(n,k)线性码 C 的生成矩阵是 $k\times n$ 的矩阵 G，矩阵 G 的行是线性子空间 C 的一组基。对于一个线性码 C，如果它的生成矩阵 $G=(I_{k\times k}|A_{k\times(n-k)})$，$I_{k\times k}$是 $k\times k$ 的单位阵，A 是 $k\times(n-k)$ 矩阵，则此线性码 C 称为系统码。

定义 4(校验矩阵)　(n,k)线性码 C 的校验矩阵是$(n-k)\times n$ 的矩阵 H，矩阵 H 的行是线性子空间 C 的正交补空间的一组基，满足 $C=\{c\in F_q^n:Hc^{\mathrm{T}}=0\}$。

1.2　SD 困难问题

任何一个公钥密码系统都要基于某一个困难问题，Stern 方案[6]所基于的困难问题是 SD 问题。

SD(Syndrome Decoding)问题的描述如下。

输入:有限域 F_q 上的$(n-k)\times n$校验矩阵 H,长度为$(n-k)$的向量 $i\in F_q^{n-k}$ 以及一个正整数$\omega>0$。

问题:是否存在一个向量 $s\in F_q^n$ 并且 $wt(s)\leqslant\omega$,使得 $Hs^{\mathrm{T}}=i^{\mathrm{T}}$。

这个问题在 1978 年被证明为 NPC 问题[28]。

1.3 GSD 困难问题

文献[28]提到,如果以生成矩阵的形式来描述 SD 问题,这也将是一个 NPC 问题,因为可以在多项式时间内将校验矩阵转化为生成矩阵,此时的 SD 问题将转化为 GSD 问题。Veron[7]中所基于的困难问题是 GSD 问题。

GSD(Generator Syndrome Decoding)问题的描述如下。

输入:有限域 F_q 上的 $k\times n$ 生成矩阵 G,长度为 n 的向量 $x\in F_q^n$ 以及一个正整数$\omega>0$。

问题:是否存在一个向量 $e\in F_q^n$ 且 $wt(e)\leqslant\omega$,使得$x+e$为一个码字。

该 GSD 问题也就是寻找(m,e),使得 $x=mG+e$,并且满足 $wt(e)\leqslant\omega$。

1.4 Veron 身份认证方案

本文主要讨论对 Veron 身份认证方案[7]进行改进,下面先简单介绍 Veron 身份认证方案。

设哈希函数为 h,生成矩阵 G 为 $k\times n$ 的二元矩阵,h 和 G 为公共数据,证明者和验证者在计算中都要使用 h 和 G。Veron 方案的私钥为向量 $e\in F_2^n$ 和向量 $m\in F_2^k$,并且$wt(e)=\omega>0$,公钥为 $x\in F_2^n$ 和整数 ω,满足 $x=mG+e$。Veron 身份认证协议的交互过程如下:

1)证明者 P 随机选择一个长度为 k 的向量 u,选择一个随机置换 π,然后将承诺值 C_1,C_2,C_3 发送给验证者 V:

$C_1=h(\pi),C_2=h((u+m)G\pi),C_3=h((uG+x)\pi)$

其中,$arg.\pi$ 表示对 arg 进行 π 置换运算的结果。

2)验证者 V 发送给证明者 P 一个随机挑战位 $b\in\{0,1,2\}$。

3)证明者 P 根据接收到的 b 值,进行以下操作:

如果 $b=0$,P 将出示 $u+m$ 和 π;

如果 $b=1$,P 将出示$(u+m)G\pi$ 和 $e\pi$;

如果 $b=2$,P 将出示 π 和 u。

4)验证者 V 根据所发送的 b 的值进行如下验证:

如果 $b=0$,V 将验证 C_1 和 C_2;

如果 $b=1$,V 将验证 $wt(e\pi)$的重量是否为 ω,如果相等,再验证 C_2 和 C_3;如果不等,则验证不通过。C_2 可以直接计算,C_3 可以这样计算:$h((u+m)G\pi+e\pi)=h((uG+mG+e)\pi)=h((uG+x)\pi)=C_3$。

如果 $b=2$,V 将验证 C_1 和 C_3。

5)重复上面的步骤 1)—步骤 4),直到达到指定的安全性为止。

这个协议已经在文献[7]中被证明为交互式零知识协议,欺骗者在不知道私钥的情况下能够以 2/3 的概率成功欺骗验证者。这个协议应用到身份认证方案中有两个缺点:1)公钥是非常大的,超过 150k 比特;2)每一轮中,欺骗者都能够以 2/3 的概率欺骗成功,为了达到指定的安全性,必须运行协议多轮。根据 ISO/IEC-9785-5 标准,要达到最弱和最强的安全性能 2^{-16} 和 2^{-32},协议需要分别运行 28 轮和 56 轮。

2 改进的 Veron 认证方案及其安全性分析

本节将介绍如何改进 Veron 身份认证方案并对改进的方案进行安全性分析。

2.1 如何获得短密钥

下面介绍如何才能获得比较短的密钥,主要是采用循环码将私钥 e 嵌入到公共矩阵 G 中。

为了把私钥 e 嵌入到公共矩阵 G 中,设法构造一个 $n\times 2n$ 的双循环矩阵 G。随机选择向量 $a=(a_1,\cdots,a_n)$,$b=(b_1,\cdots,b_n)$,构造 $e=(a,b)$,e 必须满足 Veron 算法所选私钥重量的条件,即 $e=(a,b)$的重量为 ω。

设向量 $a=(a_1,\cdots,a_n)$,$b=(b_1,\cdots,b_n)$,然后构造 Veron 方案所对应的生成矩阵 $G=(A|B)$,A 和 B 都为循环矩阵。

$$A=\begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_2 & a_3 & a_4 & \cdots & a_1 \end{pmatrix}$$

$$B=\begin{pmatrix} b_1 & b_2 & b_3 & \cdots & b_n \\ b_n & b_1 & b_2 & \cdots & b_{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ b_2 & b_3 & b_4 & \cdots & b_1 \end{pmatrix}$$

不失一般性,假定矩阵 A 是可逆的,如果不可逆,可以重新选择向量 a,使得 A 为可逆矩阵。此时能够构造矩阵:

$G'=A^{-1}G=(I|A^{-1}B)=(I|D)$

因为 A 和 B 都为循环矩阵,所以矩阵 $D=A^{-1}B$ 也为循环矩阵。由生成矩阵 G 可构造出系统码生成矩阵 G',此时的系统码生成矩阵 G'就是改进方案中的公共矩阵。

由原有的 Veron 方案可知,生成矩阵 G'和哈希函数 h 为公共数据,公钥为向量 x 和整数 ω,私钥为向量 m 和向量 e。证明者需要存储的数据包括私钥和公共数据,称之为私有数据;验证者需要存储的数据包括公钥和公共数据,称之为公有数据。在所改进的方案中,私钥 m 的长度为 n,私钥 $e=(a,b)$,长度为 $2n$,生成矩阵 G'可以只存储矩阵 D 的第一行向量 d,行向量 d 可以通过向量 a 和向量 b 进行简单运算得到,这种方法在相关编码文献中都可找到,可以参考文献[29]。得到新方案中的私有数据为:$n+2n=3n$。另外,公钥为向量 x,长度为 $2n$;再加上生成矩阵 G'的第一行向量,长度为 n,所以公有数据为:$2n+n=3n$。

2.2 改进方案的身份认证过程

设哈希函数为 h,生成矩阵为上文所生成的 G',它是 $k\times n$ 的二元矩阵,h 和 G'为公共数据,证明者和验证者在计算中都会用到 h 和 G'。Veron 方案的私钥为向量 $e\in F_2^n$ 和向量 $m\in F_2^k$,并且 $wt(e)=\omega>0$,公钥为 $x\in F_2^n$ 和整数 ω,满足 $x=mG+e$。Veron 身份认证协议的交互过程如下:

1)证明者 P 随机选择一个长为 k 的向量 u,选择一个随机置换 π,然后将承诺值 C_1,C_2,C_3 发送给验证者 V:

$C_1=h(\pi),C_2=h((u+m)G\pi),C_3=h((uG+x)\pi)$

其中,$arg.\pi$ 表示对 arg 进行 π 置换运算的结果。

2）验证者 V 发送给证明者 P 一个随机挑战位 $b\in\{0,1,2\}$。

3）证明者 P 根据接收到的 b 值，进行以下操作：

如果 $b=0$，P 将出示 $u+m$ 和 π；

如果 $b=1$，P 将出示 $(u+m)G\pi$ 和 $e\pi$；

如果 $b=2$，P 将出示 π 和 u。

4）验证者 V 根据所发送的 b 值进行如下验证：

如果 $b=0$，V 将验证 C_1 和 C_2；

如果 $b=1$，V 将验证 $wt(e\pi)$ 的重量是否为 ω，如果相等，再验证 C_2 和 C_3；否则，验证不通过。C_2 可以直接计算，C_3 可以这样计算：$h((u+m)G\pi+e\pi)=h((uG+mG+e)\pi)=h((uG+x)\pi)=C_3$。

如果 $b=2$，V 将验证 C_1 和 C_3。

5）重复上面的步骤 1）—步骤 4），直到达到指定的安全性为止。

2.3 改进方案的安全性分析

2.3.1 Veron 方案的安全性

文献[27]中提到 GV 界限：如果 $[n,k,d]$ 线性码满足 GV 界限，则参数 n,k,d 满足 $\sum_{i=0}^{d-1}\binom{n}{i}\approx 2^{n-k}$。这个 GV 界限保证了线性码具有一个很好的最小重量，很难进行译码攻击。Veron 方案的安全性主要依赖于线性码的 3 个特性，后面讨论所改进的方案的安全性也是基于以下 3 个特性。

1）随机线性码满足 GV 界限的要求[27]；

2）n 足够大的线性码都依赖于 GV 界限[22]；

3）解决随机线性码的 GSD 问题已被证明为 NPC 问题[28]。

特性 1）和 2）可以从实践的角度来评估信息集攻击对 Veron 方案的攻击强度，特性 3）从理论上保证了 Veron 方案的安全性。

2.3.2 随机双循环码的安全性

在 Veron 方案中主要使用随机二元线性码，而在改进的新方案中使用了随机双循环码来替代随机线性码。如果在码的长度上做一个小限制，即设原方案中码长 n 为维数 k 的两倍，那么随机双循环码 $[2n,n,d]$ 就会满足前面讨论的两点性质。如果 n 为素数，并且 2 是 Z/nZ 中的本原元，那么所有的随机双循环码 $[2n,n]$ 码都依赖于 GV 界限。这是因为对于给定的 n，$x^n-1=(x+1)(1+x+x^2+\cdots+x^{n-1})$，这时由任意一个重量为奇数的随机向量产生的循环矩阵都是可逆的，这点保证了与随机线性码具有一样的安全属性，因此具有足够长度的随机双循环码存在比较好的最小重量，同时也满足上面提到的前两点安全性质，这些也都得到了 Gaborit 等人[30]的证明。

那么关于保证安全性质的第 3 点会怎么样呢？先把 GSD 问题转化为在双循环码条件下的情况。

问题：双循环线性码条件下的 GSD 问题

输入：有限域 F_q 上的 $n\times 2n$ 生成矩阵 G，长度为 $2n$ 的向量 $x\in F_q^{2n}$ 以及一个正整数 $\omega>0$；

问题：是否存在一个向量 $e\in F_q^{2n}$ 且 $wt(e)\leqslant\omega$，使得 $x+e$ 为一个码字？

到目前为止，无法证明这个问题是否是 NPC 问题，但下面的分析可以说明这是一个相当难的问题。假如这个问题不是 NPC 问题，那么就存在一个多项式时间算法可以找到满足 GV 界限要求的二元码。但到目前为止，满足这种性质的二元码没有被找到，如果在编码理论中能找到，这将会是一个重大的突破。另外，也没有特别的算法能够破译达到 GV 界限的拟循环码。从以上讨论可知，虽然双循环线性码条件下的 GSD 问题还没有被证明为 NPC 问题，但在实际应用中是非常难解的问题，因此可以认为其是安全的。

3 参数选择及与原方案的比较

3.1 安全参数的选择

在改进的新方案中，先选择一个具有重量 ω 的向量 $e=(a,b)$，ω 的值比 GV 界限值略小。由前面的讨论可知，n 足够大的随机双循环码都依赖于 GV 界限。如果从重量略比 GV 界限小的码字开始，就可以认为该重量是码字的最小重量，通过模拟可知，这个 n 值为 120。

通过向量 e 的拟循环性来提高信息集攻击的方法有以下两种。

1）由于循环性，一个码字的移位仍然是一个码字，这说明译码攻击的复杂性与 n 相关，并且这一点也没有很大程度地改变译码的复杂度。

2）将攻击 NTRU 方案的参数进行适当调整就可以用来攻击新的方案，n 的选择比矩阵参数 A 略大，$n\approx 350$，此时可以达到的安全强度大约为 2^{80}。因此，在这种情况下，建议改进方案的安全参数：$n=347$，$\omega=76$，此时公有数据的长度为 1041 比特，私有数据的长度也为 1041 比特。另外，此时译码攻击的安全强度为 2^{83}。

3.2 与 Veron 身份认证方案的比较

表 1 列出了改进的方案和 Veron 方案的比较，它们都共同使用了相同大小的 $n\times 2n$ 公共矩阵。在这两种方案中，为了达到某一个级别的安全强度，协议所需要执行的轮数都是一样的，如要使欺骗者欺骗成功的概率小于 2^{-32}，协议需要运行 56 轮。文中主要比较每一轮协议运行的计算复杂度和每一轮传输的数据量。

表 1　与 Veron 身份认证方案的比较

	Veron	改进的方案
公共数据	$2n^2+2n$	$3n$
私有数据	$2n^2+3n$	$3n$
每轮传输数据量	cs	cv
每轮计算量	$n\omega_\beta$	$n(n+1)/2$

在 Veron 方案中，$\omega_\beta=(\omega_\beta(\gamma_1)+\omega_\beta(\gamma_2))-2$，$\omega_\beta(\gamma_1)$ 和 $\omega_\beta(\gamma_2)$ 分别表示 γ_1 和 γ_2 的汉明重量，具体可参考文献[7]。符号 h 表示哈希函数的输出长度，l_s 表示产生置换的伪随机数生成器种子的长度。表 1 中的 cs 和 cv 表示计算复杂性，$cs=3h+\frac{2}{3}(4n+l_s)$，$cv=3h+\frac{2}{3}(3n+l_s)$。在 $n>256$ 的情况下，建议 $\omega_\beta(\gamma_1)=\omega_\beta(\gamma_2)=80$。

为了达到指定的安全强度 2^{-32}，取 $n=347$，$\omega=76$；设哈希函数输出长度 $h=160$，产生随机置换的种子长度 $l_s=160$，将这些数值代入表 1 中的公式进行计算，可以得到表 2 中的结果。

表 2 与 Veron 身份认证方案具体数值的比较/bits

	Veron	改进的方案
公共数据	241512	1041
私有数据	241859	1041
每轮传输数据量	84672	71717
每轮计算量	2^{22}	2^{21}

从表 2 中具体数值的比较可以看出，所改进的新方案不论是在公有数据还是私有数据上，都比原方案小很多，并且每轮传输的数据量比原方案小 1 万多个比特位，在多轮交互的过程中其优势明显；另外，改进的方案中每轮的计算量也比原方案小。因此，改进的新方案适用于轻量级移动网络的应用环境。

4 改进的方案转换为数字签名方案

4.1 将身份认证方案转为数字签名方案

采用文献[9]中的方法将改进的具有轻量级的 Veron 身份认证方案转换为数字签名方案，具体过程描述如下。

1)密钥产生

公共数据：生成矩阵 G，G 是 $k\times n$ 的矩阵；公共哈希函数 h；待签名的消息 M，伪随机函数 f。

私钥：长度为 k 的二元向量 m，长度为 n 的二元错误向量 e。

公钥：长度为 n 的二元向量 x，满足 $x=mG+e$，e 的重量 $wt(e)=\omega$。

2)签名算法

签名者随机选择长度为 k 的二元向量 $u_1,\cdots,u_t$，再选择集合$\{1,\cdots,n\}$上的随机置换 $\pi_1,\cdots,\pi_t$，计算 $C_{i1}=h(\pi_i)$，$C_{i2}=h((u_i+m)G\pi_i)$，$C_{i3}=h((u_iG+x)\pi_i)$，$b=f(M,u_1,\cdots,u_t,\pi_1,\cdots,\pi_t)$，$b$ 是长度为 t 的一维数组，$b[i]\in\{0,1,2\}$，$i=1,\cdots,t$。

则签名 $\sigma=(M,b,\sigma_1,\cdots,\sigma_t)$。

签名 σ 中的每个 σ_i 是由 $b[i]$的值决定的：

若 $b[i]=0$，则 $\sigma_i=(u_i+m,\pi_i)$；

若 $b[i]=1$，则 $\sigma_i=((u_i+m)G\pi_i,e\pi_i)$；

若 $b[i]=2$，则 $\sigma_i=(\pi_i,u_i)$。

3)验证算法

接收者收到签名 $\sigma=(M,b,\sigma_1,\cdots,\sigma_t)$时，按如下的方式进行验证。

若 $b[i]=0$，则由相对应的 σ_i 计算 $C'_{i1}=h(\pi_i)$，$C'_{i2}=h((u_i+m)G\pi_i)$，验证 C'_{i1}是否和 C_{i1}相等以及C'_{i2}是否和 C_{i2}相等。如果不等，则签名无效。

若 $b[i]=1$，则由相对应的 σ_i 先检查 $wt(e\pi_i)$是否等于 ω，若不等，则签名无效；若相等，则计算 $C'_{i2}=h((u_i+m)G\pi_i)$，$C'_{i3}=h((u_i+m)G\pi_i+e\pi_i)$，验证 C'_{i2}是否和 C_{i2}相等以及 C'_{i3}是否和 C_{i3}相等。如有不等，则签名无效。

若 $b[i]=2$，则由相对应的 σ_i 计算 $C'_{i1}=h(\pi_i)$，$C'_{i3}=h((u_iG+x)\pi_i)$，验证 C'_{i1}是否和 C_{i1}相等以及 C'_{i3}是否和 C_{i3}相等。如有不等，则签名无效。

要经过 t 次比较之后才能确定一个签名$\sigma=(M,b,\sigma_1,\cdots,\sigma_t)$是否为有效的签名；如果在某一次验证中没有通过，则认为此签名为无效签名，就没有必要再继续验证。

4.2 数字签名算法的正确性

引理 1 如果签名者和验证者按照以上协议进行，则验证者就会接受签名是有效的。

证明：按照签名算法的过程：

如果 $b[i]=0$，则由相对应的 σ_i 计算 $C'_{i1}=h(\pi_i)=C_{i1}$，$C'_{i2}=h((u_i+m)G\pi_i)=C_{i2}$；

如果 $b[i]=1$，则由相对应的 σ_i 先检查 $wt(e\pi_i)$是否等于 ω，若不等，则签名无效；若相等，则计算 $C'_{i2}=h((u_i+m)G\pi_i)=C_{i2}$，$C'_{i3}=h((u_i+m)G\pi_i+e\pi_i)=h((u_iG+mG+e)\pi_i)=h((u_iG+x)\pi_i)=C_{i3}$；

如果 $b[i]=2$，则由相对应的 σ_i 计算 $C'_{i1}=h(\pi_i)=C_{i1}$，$C'_{i3}=h((u_iG+x)\pi_i)=C_{i3}$。

因此由以上 3 种情况可知，该签名方案是正确的。

4.3 数字签名算法的不可伪造性

引理 2 如果敌手能够伪造一个有效的签名 $\sigma=(M,b,\sigma_1,\cdots,\sigma_t)$的概率大于或等于$(\frac{2}{3})^t+\varepsilon$，那么就存在一个概率多项式时间的算法 χ 以绝对优势的概率计算出有效的私钥对(m,e)或者找到哈希函数的碰撞。

证明：为了证明的需要，引入文献[7]中的执行树，用 T 表示敌手和验证者之间交互的执行树[7]，敌手拥有概率分布空间 RA。除非哈希的碰撞能够被找到，否则从具有 3 个孩子结点的树中可以计算出私钥对(m,e)。用 V 代表树结构中具有 3 个孩子结点的某个顶点，这就等同于签名中的 3 个承诺 C_{i1},C_{i2},C_{i3}。当 $b=0$ 时，查询所对应的应答为 $u'+m'$和 π'；当 $b=1$ 时，查询所对应的应答为 y''和 e''；当 $b=2$ 时，查询所对应的应答为 u'''和 π'''，此时有下列等式：

$h(\pi')=C_{i1}=h(\pi''')$

$wt(e'')=\omega$

$h((u'+m')G\pi')=C_{i2}=h(y'')$

$h(y''+e'')=C_{i3}=h((u'''G+x)\pi''')$

于是，或者能找到一个哈希函数的碰撞，或者满足：

$x=(u'+m'+u''')G+e''\pi'^{-1}$

其中，$e''\pi'^{-1}$是一个长度为 n、重量为 ω 的字。因此，$(u'+m'+u''',e''\pi'^{-1})$是敌手的一个有效的私钥对，可以用来冒充真正的签名者。

假设树 T 中某个顶点具有 3 个孩子结点的概率至少为 ε。假设 RA 为含有 μ 个元素的集合，敌手可以从中随机选择元素，Q 表示集合$\{0,1,2\}$。假设这两个集合都是均匀概率分布的。

$(c,b)\in(RA,Q)^t$ 表示在签名和验证的过程中敌手和验证者之间交互的信息。如果敌手的签名能够得到验证者的验证，就称(c,b)是一个有效对。

用 V 表示所有有效对的集合，它是$(RA,Q)^t$ 的一个子集合。

引理 2 所隐含的含义为：

$$\frac{|V|}{|(RA,Q)^t|}\geqslant(\frac{2}{3})^t+\varepsilon$$

设 Q_t 为 RA^t 的一个子集，且满足：

如果 $c\in Q_t$，则 $2^t+1\leqslant|\{b,(c,b)\text{为有效对}\}|\leqslant 3^t$；

如果 $c\in RA^t\backslash Q_t$，则 $0\leqslant|\{b,(c,b)\text{为有效对}\}|\leqslant 2^t$；

所以，$V=|valid(c,b),c\in Q_t\}\cup\{valid(c,b),c\in RA^t\backslash Q_t\}$，因此$|V|\leqslant|Q_t|\cdot 3^t+(\mu^t-|Q_t|)\cdot 2^t$。

于是：$\frac{|V|}{|(RA,Q)^t|}\leqslant(\frac{|Q|}{|RA^t|}+2^t\cdot(3^{-t}-\frac{|Q|}{|(RA,Q)^t|}))\leqslant\frac{|Q_t|}{|RA^t|}+(\frac{2}{3})^t$。

这意味着$\frac{|Q_t|}{|RA^t|}\geqslant\varepsilon$，即表明一个假冒者通过随机选择参数至少可以以 ε 的概率回答验证者的 2^t+1 个提问，如果假冒者的查询超过了 2^t+1 次，那么执行树就至少有 2^t+1 个叶子结点，而执行树至少存在一个结点拥有 3 个孩子结点。

因此，若敌手能够伪造签名，则概率算法 χ 执行$\frac{1}{\varepsilon}$次就一定能够找到某一棵具有 3 个孩子结点的执行树，这样就可以找到哈希函数的碰撞，但实际上这是不可能的，所以所提签名方案是安全的。

结束语　本文通过双循环矩阵改进了 Veron 身份认证方案，并且将所构造方案的安全性归结到 GSD 困难问题上。Veron 方案因为公用矩阵太大，所以不实用，对其改进以后，可以应用到移动网络环境下。另外，公共矩阵的循环结构使得其计算非常简单，因为不必产生整个矩阵，整个方案只需要很小的存储空间。在改进的新方案中，公有数据的大小只有 1041 比特，私有数据的大小也为 1041 比特，用信息集攻击方法攻破的强度为 2^{83}。最后采用 FS 方法将改进后的身份认证方案转换为数字签名方案，并对转换后的方案进行了正确性证明和安全性证明，使得改进的方案就可以应用到云计算环境需要轻量级的数字签名中。

总体来说，所改进的方案是非常实用的，对当前大部分基于数论困难问题的身份认证方案来说是另一种非常好的选择，而且其非常适用于轻量级的移动网络环境。

参 考 文 献

[1] ZHAO S R. New Discrete Logarithm Problems over Finite Fields[D]. Jinan: Shandong University, 2014: 14-20, 35-50. (in Chinese)
赵书让. 有限域上新的离散对数问题[D]. 济南：山东大学，2014：14-20，35-50.

[2] SHOR P. Polynomial-Time Algorithms For Prime Factorization and Discrete Logarithms on A Quantum Computer[J]. Siam Review, 1997, 41(5): 1484-1509.

[3] GERSHENFELD N, CHUANG I. Quantum Computing with Molecules[J]. Scientific American, 1998, 282(6): 86-93.

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

[5] PATARIN J. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms[M]// Advances in Cryptology — EUROCRYPT '96. Springer Berlin Heidelberg, 1996: 33-48.

[6] STERN J. A New Identification Scheme Based On Syndrome Decoding[C]// Crypto'93. 1993: 13-21.

[7] VERON P. Improved Identification Schemes Based On Error-Correcting Codes[J]. Applicable Algebra in Engineering, Communication and Computing, 1997, 8(1): 57-69.

[8] 杨波. 现代密码学[M]. 北京：清华大学出版社，2015：198-199

[9] FIAT A, SHAMIR A. How to Prove Yourself: Practical Solutions to Identification and Signature Problems[C]// Odlyzko AM(ed) Advances in Cryptology-CRYPTO'86. LNCS, Springer, Berlin, 1987: 186-194.

[10] YI H, LI W. Fast Three-Input Multipliers over Small Composite Fields for Multivariate Public Key Cryptography[J]. International Journal of Security & Its Applications, 2015, 9(9): 165-178.

[11] GABORIT P. Shorter Seys For The McEliece Cryptosystem[J]. Proceedings of WCC, 2005, 30(6): 124-133.

[12] WANG X M. Digital Signature scheme based on error-correcting codes[J]. Electronics Letters, 1990, 26(13): 898-899.

[13] ALABBADI M, WICKER S B. Security of Xinmei Digital Signature Scheme[J]. Electronics, 1992, 28(9): 890-891.

[14] ALABBADI M, WICKER S B. Digital Signature Scheme Based on Error-Correcting Codes[C]// IEEE International Symposium on Information Theory. IEEE, 1993: 9-19.

[15] HARN L, WANG D C. Cryptoanalysis and Modification of Digital Signature Scheme Based on Error-Correcting Codes[J]. Electronics Letters, 1992, 28(2): 157-159.

[16] KABATIANSKII V, KROUK E, SMEETS B J M. A Digital Signature Scheme Based on Random Error-Correcting Codes[M]// Crylography and Coding. Springer Berlin Heidelberg, 1997: 161-167.

[17] CAYREL P L, OTMANI A, VERGNAUD D. On Kabatianskii-Krouk-Smeets Signatures[M]// Carlet S C, Sunar B, eds. Arithmetic of Finite Fields. Springer, Heidelberg, 2007: 237-251.

[18] COURTOIS N, FINIASZ M, SENDRIER N. How to achieve a McEliece-based digital signature schem[M]// Advances in cryptology-ASIACRYPT 2001. LNCS, vol 2248, Springer, Berlin, 2001: 157-174.

[19] DALLOT L. Towards a Concrete Security Proof of Courtois, Finiasz and Sendrier Signature Scheme[M]// Research in Cryptology. LNCS 4945, Springer, 2007: 65-77.

[20] FAUGÉRE J C, GAUTHIER V, OTMANI A, et al. A distinguisher for high rate mceliece cryptosystems: Report 2010/331 [R/OL]. http://eprint.iacr.org.

[21] PREETHA M P, VASANT S, RANGAN C P. On Provably Secure Code based Signature and Signcryption Scheme: Report 2012/585[R]. 2012.

[22] SIDI M, PIERRE-LOUIS C, RACHID E. Code-Based Identification and Signature Schemes in Software[M]// Security Engineering and Intelligence Informatics. Germany, LNCS 8128. 2014: 122-136.

[23] PIERRE-LOUIS C, VERON P, ALAOUI S. A Zero-Knowledge Identification Scheme Based on The Q-ary Syndrome Decoding Problem[C]// 2013 Eighth Asia Joint Conference on Selected Areas in Cryptography 2011. Berlin: Springer, 2013: 171-186.

[24] RONG H, MOROZOV K, TAKAGI T. On Zero-Knowledge Identification Based on Q-ary Syndrome Decoding[C]// 2013 Eighth Asia Joint Conference on Information Security (Asia JCIS). IEEE, 2013: 12-18.

[25] GABORIT P. Method of authentication using a decoding of an error correcting code on the basis of a public matrix: US, US8817972 [P]. 2014.

[26] GADAT B, VAN N, RIES L. Method Of Decoding A Correcting Code, For Example A Turbo-code, By Analysis Of The Extended Spectrum Of The Words Of The Code: US, US20140351667 [P]. 2014.

[27] El YOUSFI A. Code-based Identification and Signature Schemes [D]. Technische Universitat Darmastadt. 2013.

[28] BERLEKAMP E R, MCELIECE R J, TILBORG H C A V. On The Inherent Intractability Of Certain Coding Problems [J]. IEEE Transactions on Information Theory, 1978, 24(3): 384-386.

[29] 岳殿武. 信息论与编码简明教程[M]. 清华大学出版社, 2015: 166-178.

[30] GABORIT P, ZEMOR G. Asymptotic improvement of the Gilbert Varshamov bound for linear codes[J]. IEEE Transactions on Information Theory, 208, 54(9): 3865-3872.

(上接第 152 页)

的身份和安全等级授予其相应的数据操作权限，有效保障数据的安全性和机密性。

应用安全审计机制记录和分析所有用户对数据的所有相关操作，加强数据溯源能力，数据文件一旦被非法访问，通过日志文件就能快速定位到出现问题的访问端，并可以查看和还原出数据文件被泄漏的原因、时间和访问人，避免否认抵赖等恶意行为。

(2)法律方面

确立数据安全的核心内容，如基本原则、监管模式、等级保护等，在此基础上完善数据保护的相关法律。

(3)管理机制方面

对重要的数据文件进行定期备份，保证数据的可用性。

完善数据管理制度，严格管理存储介质和移动外设的使用，避免信息泄漏。

4.3 服务层防护措施

服务层根据从数据层中获取的信息，通过分析处理为业务系统提供服务，是电网融合泛在网信息平台做出决策的核心部分。以下是针对服务层安全威胁的一些防护措施。

(1)技术方面

使用标准化方式在信任边界的各种认证、授权系统之间共享身份和策略信息。使用联合身份管理，在各目标应用服务之间建立可信关系，并共享身份和策略，确保已通过认证的身份能够被任何一个应用服务识别，从而使该身份相关联的用户能够在不同应用服务之间进行跨域访问，同时避免身份伪造和命令伪造。

加强不同安全环境下和安全域中的服务间的有效安全协作，从而确保整个体系的安全。

对服务进行管控，保证服务的受限受控调用，对服务的调用过程进行认证授权，以防止服务被攻击者或用户非法使用以及服务器的拒绝访问等问题出现。

使用漏洞挖掘技术检测代码漏洞并进行修补，防止攻击者利用代码漏洞对平台进行攻击。

(2)法律方面

对利用电网融合泛在网信息平台威胁用户或者系统安全的行为立法，准确把握和适当增补、完善相关法律条款。

(3)管理机制方面

加强人事安全管理，依据行政上的管理体系建立起自上而下的安全管理机构，并为每一级设立相应的安全策略，明确各级权限职责和操作规范，加强账号安全管理。

结束语 本文分析了 SOA 的参考体系架构，即数据层、基本层、组合层、流程层和前端层，给出了基于 SOA 的电网融合泛在网信息平台架构，其主要包括基础设施层、数据层、服务层、数据总线和企业服务总线。针对给出的信息平台体系架构，详细分析了各层中可能存在的安全威胁，并提出了相应的防护措施。电网融合泛在网信息平台能够解决现阶段电力系统信息化建设中异构网络资源共用和信息共享的难题，但同时又会带来许多信息安全方面的新问题。因此，需要对其进行深入研究和探讨，消除安全隐患和威胁，促进电力系统信息化建设的安全发展。

参 考 文 献

[1] XU W B, SUN Z, CHEN J J. Research on Power System Integration Based on SOA[J]. China Instrumentation, 2007(6): 46-49. (in Chinese)
许卫兵，孙佐，陈继军. 面向服务架构(SOA)的电力系统信息集成研究[J]. 中国仪器仪表，2007(6)：46-49.

[2] BI R H, YANG Z C, WANG Y Z. Studies on Information Integration of MAS-based SOA Model in Power System[J]. Power System Protection and Control, 2010, 38(7): 63-67. (in Chinese)
毕睿华，杨志超，王玉忠. 基于多智能体 SOA 模型的电力系统信息集成的应用研究[J]. 电力系统保护与控制，2010，38(7)：63-67.

[3] LIU G M, SONG Y, TENG X L, et al. Development of Electric Power Information Integration Platform Based on SOA Framework[J]. Electric Power, 2012, 45(6): 96-99. (in Chinese)
刘国民，宋雨，滕晓雷，等. 基于 SOA 架构的电力信息一体化平台开发研究[J]. 中国电力，2012，45(6)：96-99.

[4] XU W B. Research on Information Integration Platform of Power System Based on SOA [D]. Nanjing: Southeast University, 2008. (in Chinese)
许卫兵. 基于 SOA 的电力系统信息集成平台的研究[D]. 南京：东南大学，2008.

[5] HIRSCHHEIM R, WELKE R, SCHWARZ A. Service-Oriented Architecture: Myths, Realities and a Maturity Model[J]. MIS Quarterly, 2010, 9(1): 37-48.

[6] ZHEN F, LIU M, DONG M Y. SOA Message-oriented Middleware Based System Integration Method for Business Process [J]. Computer Integrated Manufacturing Systems, 2009, 15(5): 968-989. (in Chinese)
甄甫，刘民，董明宇. 基于面向服务架构消息中间件的业务流程系统集成方法研究[J]. 计算机集成制造系统，2009，15(5)：968-989.

[7] LI Z, PENG Y, XIE F, et al. Security Threats and Measures for the Cyber-physical System[J]. Journal of Tsinghua University (Science and Technology), 2012, 52(10): 1482-1487. (in Chinese)
李钊，彭勇，谢丰，等. 信息物理系统安全威胁与措施[J]. 清华大学学报(自然科学版)，2012，52(10)：1482-1487.