doi:10.16180/j.cnki.issn1007-7820.2018.07.006

在区块链中基于混合算法的数字签名技术

田道坤,彭亚雄

(贵州大学 大数据与信息工程学院,贵州 贵阳 550025)

摘 要 随着加密数字货币的崛起,新兴的区块链技术成为了研究热点,由于区块链技术的去中心化和信任机制的提出,数字签名显得尤为重要。为提高数字签名的安全性,文中在交易过程中提出了一种基于高级加密标准(AES)和椭圆曲线密码算法(ECC)的混合加密算法,双方经过 Diffie-Hellman(DH)算法管理密钥的方法实现签名,使其各自检验对方的身份。既实现了对称加密技术运行速度快的特点,又实现了非对称加密密钥的安全性,同时也使签名更具真实性和可靠性。

关键词 区块链;去中心化;高级加密标准;椭圆曲线密码算法;DH 算法

中图分类号 TN918.91 **文献标识码** A **文章编号** 1007-7820(2018)07-019-05

Digital Signature Technology Based on Hybrid Algorithm in Blockchain

TIAN Daokun, PENG Yaxiong

(School of Big Data and Information Engineering, Guizhou University, Guiyang 550025, China)

Abstract With the rise of encrypted digital money, the emerging blockchain technology has become a research hotspot, because the block chain technology to the centralization and trust mechanism proposed, digital signature is particularly important. In order to improve the security of digital signature, a hybrid encryption algorithm based on Advanced Data Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) is proposed in the process. The two sides pass the Diffie-Hellman (DH) algorithm to manage the key The way to achieve the signature, so that each of their own identity. Not only achieved the characteristics of symmetric encryption technology running fast, but also to achieve the security of the asymmetric encryption key, but also make the signature more authenticity and reliability.

Keywords blockchain; de-centering; advanced data encryption standard; elliptic curve cryptography; DH algorithm

区块链产生于比特币,但不同于比特币。比特币之后区块链技术创新发展,并且不断探索新的应用领域。区块链的诞生为互联网带来了新的曙光,其技术的应用打破了互联网无序、混沌、不安全的状态,且试图构造一个更加有序、安全、稳定的新世界。《块数据 3.0》[1]指出,区块链就是一个块数据组织,或者说是一个在公正算法控制下的数据化组织。

区块链技术具有去中心化、去信任、集体维护、可靠、开源、匿名等特征,对解决传统中心化系统的成本高、效率低、储存数据不安全等问题提出了更好的解决方法。区块链技术利用了密码学中的数字时间戳、哈希函数、非对称加密、数字签名等手段来解决交易中存在的虚假交易和双重支付等问题。区块链中的数字签名技术使用非对称加密原理,在使用过程中需要同时拥有公钥和私钥,公钥和私钥一一对应。比如:*A*、*B* 双方进行交易,*A* 生成一对密钥,把其中的一份密钥作为公钥发送给 *B*,同时用自己的私钥信息进行加密后发送给 *B*,*B* 使用接收到的公钥对加密数据进行解密,如果成功解密即证实信息确实由 *A* 所发送,这样就形成了签名。数字签名技术最开始应用于用户的登录验证,即验证用户名和密码是否相匹配。其中 EIGamal 签名[2]是一种经常使用的数字签名。在 1991 年,文献[3]提出了多重数字签名[3]概念,文献[4~5]提出了不同类型的多重数字签名[4-5]。本文基于区块链技术下,运用 AES(Advanced Data Encryption Standard)和 ECC(Elliptic Curve Cryptography)算法混合,然后双方

收稿日期:2017-07-18

基金项目:贵州省科技厅项目(2015BAK28B00)

作者简介:田道坤(1992-),男,硕士研究生。研究方向:通信与信息工程。彭亚雄(1963-),男,副教授。研究方向:信号处理。

利用DH算法对密钥进行计算分配，实现数字签名的方案。该方案运用3种混合加密算法，使系统具有很强的抗攻击能力，能更好的完成身份认证，并提高了数字签名的安全性和真实性。

1 高级加密标准算法

高级加密标准（AES），在密码学中又称Rijndael加密法。2001年由美国国家标准技术研究所发布，旨在取代数据加密算法（DES）成为广泛使用的标准。AES是一种对称分组加密算法。其加密的数据块分组长度必须为128 Byte，密钥长度可以是128 Byte，192 Byte和256 Byte，形式分别为AES－128，AES－192和AES－256。如果以上二者长度不够时，该算法会自动补齐[6]。AES加解密流程图如图1所示。

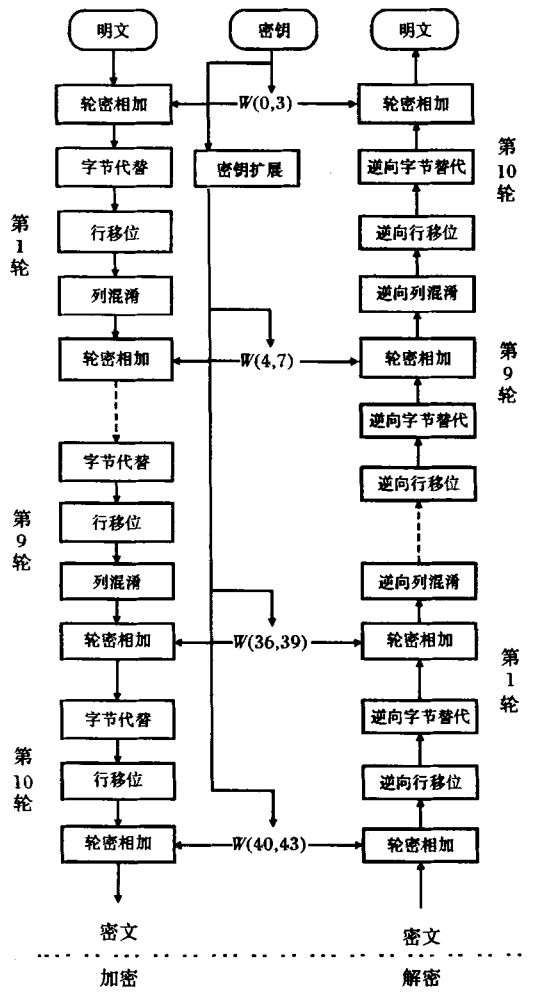

图1 AES加解密流程图

从图1可知AES加密过程共分4个步骤[7]：字节代替、行移位、列混淆以及轮密相加。解密过程是加密过程对应的逆过程，所以按照加密过程相反的顺序进行解密即可得到明文。

1.1 字节代替

字节代替主要是通过S盒完成一个字节到另一个字节的映射，S盒是AES定义的矩阵，把State（数据块要经过多次数据转换操作，每次转换操作产生一个中间结果，中间结果即State）中每个字节的高4位作为行值，低4位作为列值，然后取S盒对应行列元素作为输出。这种方法提高了AES加密的非线性变换能力。

1.2 行移位

行移位分为两种：正向行移位和逆向行移位。行移位的功能是实现一个4×4矩阵字节之间转换，即State第1行字节维持不变，第2行向左循环移1 Byte，第3行向左循环移2 Byte，第4行向左循环移3 Byte，如式（1）所示。

$$\begin{bmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{bmatrix} \rightarrow \begin{bmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,1} & S_{1,2} & S_{1,2} & S_{1,0} \\ S_{2,2} & S_{2,3} & S_{2,0} & S_{2,1} \\ S_{3,3} & S_{3,0} & S_{3,1} & S_{3,2} \end{bmatrix} \tag{1}$$

其中，$S_{i,j}$代表每个字节，i、j分别代表行、列，$0 \leqslant i \leqslant 3$，$0 \leqslant j \leqslant 3$。

以上是正向行移的转移方程，其逆向行移位是正向行移位的逆操作。

1.3 列混淆

列混淆[8]分为正向列混淆和逆向列混淆。原理是每列的4 Byte通过线下变换后相互结合，对每列进行独立操作。其中在每列中被当做系数的4个元素，合并以后即为有限域中的一个多项式，然后将该多项式和固定的矩阵多项式相乘，相似于有限域下的矩阵乘法。

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{bmatrix} = \begin{bmatrix} S'_{0,0} & S'_{0,1} & S'_{0,2} & S'_{0,3} \\ S'_{1,1} & S'_{1,2} & S'_{1,2} & S'_{1,0} \\ S'_{2,2} & S'_{2,3} & S'_{2,0} & S'_{2,1} \\ S'_{3,3} & S'_{3,0} & S'_{3,1} & S'_{3,2} \end{bmatrix} \tag{2}$$

式（2）即正向列混淆。依照矩阵的乘法法则可知，列混淆中的每个对应的值仅和列的4个值有关系。

逆向列混淆的原理：把式（2）得出的结果左乘$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}$就可以得出原来的矩阵方程。即

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} S'_{0,0} & S'_{0,1} & S'_{0,2} & S'_{0,3} \\ S'_{1,1} & S'_{1,2} & S'_{1,2} & S'_{1,0} \\ S'_{2,2} & S'_{2,3} & S'_{2,0} & S'_{2,1} \\ S'_{3,3} & S'_{3,0} & S'_{3,1} & S'_{3,2} \end{bmatrix} = \begin{bmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{bmatrix} \tag{3}$$

又因为

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} = \begin{bmatrix} 01 & 00 & 00 & 00 \\ 00 & 01 & 00 & 00 \\ 00 & 00 & 01 & 00 \\ 00 & 00 & 00 & 01 \end{bmatrix} \tag{4}$$

从式(4)可以看出,等号左边的两个矩阵互逆。由式(2)~式(4)可以看出,经过一次逆向列混淆即可恢复出明文。

1.4 轮密钥加

在每轮的循环加密中,都会由主密钥扩展产生一组轮密钥,轮密钥的大小和原来的矩阵大小一样。在加密过程中,每轮的输入与轮密钥异或一次;解密时再次异或该轮的密钥就可以得出该轮的输入。密钥扩展的复杂性,确保了该算法的安全性[9]。

AES 综合运用了置换、代替、矩阵的乘法等多种方法,加密速度快,适合加密较长明文。但是,由于 AES 采用的是单一的密码系统,在密钥管理方面,算法需要在密钥秘密分配之前继续保密通信。所以密钥替换比较困难。

2 椭圆曲线加密算法

椭圆曲线加密算法(ECC)作为一种公钥加密算法,不仅在功能上和 RSA 加密算法相同,而且具有加密强度高、密钥短等诸多技术优点,因此应用非常广泛。椭圆曲线提供了"元素"和"组合规则"来组成群的构造方式,用这些群来构造密码算法具有完全相似的特性。但它们并没有减少密码的分析量。换句话说,椭圆曲线密码体制是基于有限域上椭圆曲线的有限群,而不是离散对数中的有限循环群得到的一种新型密码体制[10],其目的是在椭圆曲线系统上实现各种密码编码方案。

2.1 椭圆曲线的定义[11]

椭圆曲线是由椭圆周长计算以及椭圆积分得到

$$\int \frac{\mathrm{d}x}{\sqrt{E(x)}} \tag{5}$$

式(5)中 $E(x)$ 为 x 的 3 次或 4 次多项式,由于这样的积分形式不能用初等函数来表达,所以引入椭圆曲线函数的概念。椭圆曲线是由一个三次方程

$$y^2 + axy + by = x^3 + cx^2 + dx + e \tag{6}$$

所确立的平面曲线。

设 F 是一个域,如果 F 中(x,y)满足方程式(6),然后加上一个无穷远点 O,就组成了椭圆曲线。

2.2 椭圆曲线的数字签名

椭圆曲线的数字签名的定义实际上是一种基于椭圆曲线上乘法群离散对数的数字签名的模拟。算法过程有:参数选取、密码生成、签名和认证。参数组 $D=(q,FR,S,A,B,P,n,h)$,其中[12],q 表示有限域的阶;FR 表示有限域;S 为椭圆曲线生成时的种子,即计算椭圆曲线方程中参数所需的种子;a、b 为椭圆曲线方程中的俩个系数,且 $a,b\in F_q$;P 为椭圆曲线上的基点(生成元);n 表示基点的阶;h 表示余因子。

数字签名过程[13]:

(1) 在区间$[1,n-1]$内选取一个随机数 k,并计算$(x_1,y_1)=kP$;

(2) 计算 $r=h(m)+x_1 \bmod n$;

(3) 若 $r+d=0(\bmod n)$,则返回步骤(1),否则计算 $(r+d)^{-1} \bmod n$;

(4) 计算 $s=(r+d)^{-1}(k-dr) \bmod n$,若 $s=0$,则返回步骤(1);

(5) 将带有附加消息(r,s)的 m 发送给接受者。

接收方验证签名:

(1) 验证 r 和 s 是否是区间$[1,n-1]$中的整数;其中任何一个检验失败,则拒绝签名。否则进行以下操作;

(2) 计算散列函数 $h(m)$的值;

(3) 计算 $w=s^{-1} \bmod n, \varphi_1=ew \bmod n\ \varphi_2=rw \bmod n$;

(4) 计算 $X=\varphi_1 P+\varphi_2 Q$;

(5) 若 $X=0$ 或∞ 时,则拒绝签名,否则在直角坐标系上把 X 在 x 轴的投影转换成整数 x'_1;

(6) 计算 $v=x'_1 \bmod n$;

(7) 若 $v=r$ 时,则接受签名。否则,拒绝签名。

3 DH 算法

Diffie-Hellman(DH)算法是第一个公开密钥算法,DH 算法能够用于密钥分配,即发、收双方可以用

DH 算法产生秘密密钥,发、收双方共同拥有这个密钥。首先,发送方 A 和接收方 B 协商一个大的素数 n 和 g,g 是模 n 的本原元。n 和 g 可以选择是公开的,所以 A 和 B 不必要秘密的协商它们。具体协议如下[14]:

(1) A 取一个随机整数 x,并发送到 B:

$$X = g^x \bmod n;$$

(2) B 取一个随机整数 y,并发送到 A:

$$Y = g^y \bmod n;$$

(3) A 计算 $k = Y^x \bmod n$;

(4) B 计算 $k' = X^y \bmod n$;

k 和 k'都等于 $g^{xy} \bmod n$。即使在发送过程中被窃听了,窃听者也无法计算出这个值。因此 k 就是 A 和 B 独立计算的共享私密密钥。

4 改进的数字签名技术

由于区块链技术的"去中心化"的提出,为了防止在交易过程中数据被非法篡改和非法使用。本文通过分析 AES 算法和 ECC 算法的性能,综合 AES 算法和 ECC 算法的优点,提出二者混合的方案[15],且在密钥管理方面,提出用 DH 算法对密钥进行计算分配。3 种算法的相互结合,提高了数字签名的安全性。

4.1 数字签名生成过程

(1) 发送方 A 和接收方 B 在通信之前构建自己的密钥对,即 $(d_A, Q_A)(d_B, Q_B)$ d_A、d_B 为私钥,Q_A、Q_B 为公钥;

(2) 发、收双方互相交换公钥,A 有 B 的公钥 Q_B,B 有 A 的公钥 Q_A,然后 A 用自己的私钥 d_A 和接收到的公钥 Q_B 用 DH 算法计算出一个密钥 d_a,同理 B 也可以得到一个密钥 d_b,由 DH 算法的分析可知,$d_a = d_b = d$,即生成的密钥是双方私有且共享的,如图 2 所示;

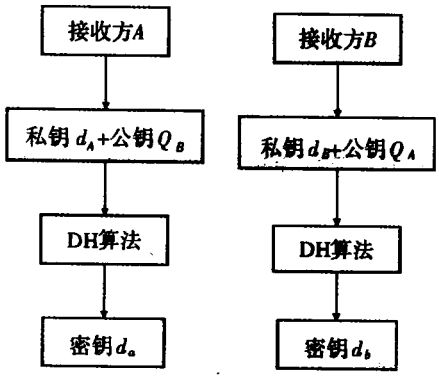

图 2 双方由 DH 算法产生密钥

(3) 发送方 A 将发送的明文 m 用哈希函数生成消息摘要 M;

(4) 将明文 m 用 AES 算法进行加密,得到密文 C_m;

(5) A 使用自己私钥对生成的消息摘 M 要进行加密,得到摘要的签名 C_M;

(6) A 将 AES 的密钥和双方产生的私有共享密钥 d 用接收到公钥 Q_B 进行加密形成密文 C_e;

(7) 最后把 C_m、C_M、C_e 一起发送给接收者。如图 3 所示。

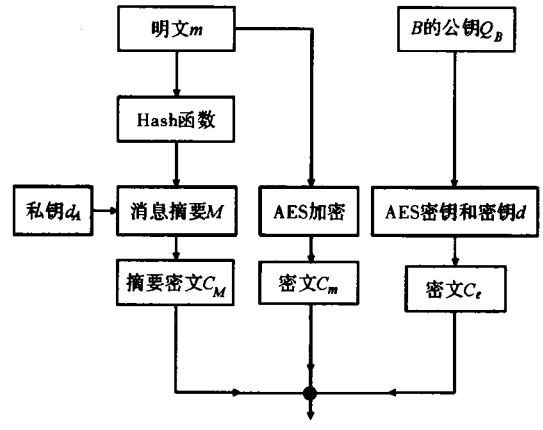

图 3 生成数字签名

4.2 验证数字签名

(1) B 接收到 A 发送的所有密文,首先 B 用自己的私钥 d_B 把接收到的密文中的 C_e 部分进行解密,得到 AES 的密钥和共享密钥 d';

(2) B 验证自己共享密钥 d 和解密后得到的 d'是否相等,若 $d = d'$则进行下一步,否则,拒绝签名;

(3) 将获得的 AES 密钥对密文中的 C_m 进行解密,得到解密明文 m';

(4) 用接收到的 Q_A 对摘要密文 C_M 进行解密得到 M。

(5) 将解密后的密文 m'进行 Hash( ) 运算得到 M';

(6) 若 $M = M'$则签名成功;否则,拒绝签名。如图 4 所示。

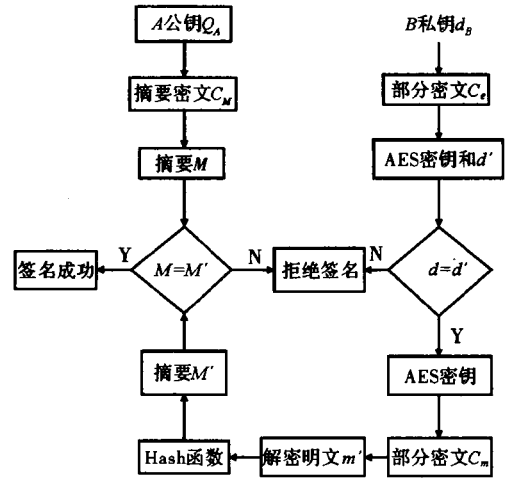

图 4 验证数字签名

5 结束语

本文提出的对称加密算法 AES 和公钥加密算法 ECC 相结合,交易双方由 DH 算法产生共享密钥的混合加密方案,既能对数据进行快速加密,也可以较好的解决密钥分配的问题,使双方在交易过程中可以进行双向私有的认证和识别[16],防止攻击者的篡改,有效的保证了数据的完整性,也保障了数字签名的时效性。如果可以进行深入的研究,在双方签名的过程中加上时间戳记,然后再由时间戳服务商予以签章记录,作为时间的证明。这样的数字签名更加具有时效性、安全性,为双方交易提供更可靠的保障。

参考文献

[1] 大数据战略重点实验室. 块数据 3.0:秩序互联网与主权区块链[M]. 北京:中信出版集团,2017.

[2] 张仕斌,万武南,张金全. 应用密码学[M]. 西安:西安电子科技大学出版社,2009.

[3] Li H, Dong X. Sequential multiple signature scheme based on wavelet domain digital watermarking[J]. Advanced Materials Research, 2013(7):622 - 625.

[4] Ohta K, Okamoto T. Multisignature schemes secure against active insider attacks[J]. IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences, 1999, E82 - A(1):21 - 31.

[5] 曹阳. 基于身份的 ELGamal 多重数字签名方案[J]. 科技通报,2015,31(5):30 - 34.

[6] William Stallings. 密码编码学与网络安全—原理与实践[M]. 5 版. 王张宜,译. 北京:电子工业出版社,2011.

[7] 卡哈特. 金名. 密码学与网络安全[M]. 北京:清华大学出版社,2005.

[8] 胡向东,魏琴芳. 应用密码学教程[M]. 北京:电子工业出版社,2005.

[9] 王世志,马紫宁. 基于混合密钥数字签名在移动 OA 系统的研究[J]. 电子科技,2016,29(2):167 - 168,172.

[10] 冯泽宇,巩博儒,赵运磊. 基于离散对数的数字签名标准对比研究[J]. 计算机工程,2016,42(2):145 - 149.

[11] 陈力,葛万成. 椭圆曲线加密算法的边信道攻击[J]. 通信技术,2014,47(9):1062 - 1065.

[12] 刘小东. 椭圆曲线密码算法在 FPGA 上的设计研究[D]. 北京:北京航空航天大学,2010.

[13] 潘晓君. 一种新的基于椭圆曲线的数字签名方案[J]. 计算机系统应用,2008(1):35 - 37.

[14] Bruce Schneier.. 应用密码学:协议、算法与 C 源程序[M]. 2 版. 吴世忠,译. 北京:机械工业出版社,2014.

[15] 王常林,吴斌. 基于 AES 算法和改进 ECC 算法的混合加密方案[J]. 科学技术与工程,2009(18):5379 - 5382,5391.

[16] 傅喆,栗青霞,王换换. 一种改进的双向认证的动态密码[J]. 电子科技,2014,27(1):150 - 152.

(上接第 18 页)

[2] 杜怿,邹春花,朱孝勇,等. 初级永磁型游标直线电机绕组连接及其电磁特性比较[J]. 电工技术学报,2017,32(3):130 - 138.

[3] 陈修亮,车倍凯. 永磁同步电机矢量控制解耦方法的研究[J]. 电气技术,2013(4):37 - 40.

[4] 吕飞,秦福星,张松涛,等. 永磁同步直线电机矢量控制仿真研究[J]. 船电技术,2012,32(1):25 - 28.

[5] 唐小利. 永磁同步直线电机的矢量控制系统研究[J]. 电子技术与软件工程,2017(1):112 - 115.

[6] 尚敬,年晓红,刘可安,等. 负载转矩前馈的电励磁同步电机定子磁链定向矢量控制[J]. 电机与控制学报,2015,19(11):25 - 31.

[7] 周长攀,苏健勇,杨贵杰,等. 基于双零序电压注入 PWM 策略的双三相永磁同步电机矢量控制[J]. 中国电机工程学报,2015,35(10):2522 - 2533.

[8] 朱军,程志磊,汪旭东,等. 一种永磁同步电机电流直接反馈矢量控制[J]. 电机与控制学报,2015,19(6):35 - 40.

[9] 杨贵,彭显刚. 永磁同步电机的状态解耦控制研究[J]. 黑龙江电力,2015,37(4):326 - 330.

[10] 龚寄,骆拓. 永磁同步电机矢量控制中的坐标变换和解耦[J]. 装备制造技术,2016(7):152 - 154.

[11] 赵卓鹏,贾石峰. 电流滞环跟踪 PWM 逆变器控制仿真研究[J]. 电气传动自动化,2011,33(2):1 - 3,18.

[12] 陈斌,杨文焕,吴帅,等. 一种新型恒频滞环电流控制策略研究[J]. 电子科技,2015, 28(10):151 - 154.

[13] 孙凌杰,徐珠勇. 基于 Matlab 的 SVPWM 波形仿真实现[J]. 机电技术,2013(3):75 - 77.

[14] 李少龙,赵琴,李文龙,等. 基于滑模控制的三相 SVPWM 逆变器研究[J]. 电子科技,2016, 29(6):124 - 128.

[15] 周立波,马晓红,袁旭峰,等. 基于 SVPWM 的逆变器控制[J]. 贵州电力技术,2015, 18(9):37 - 41.