doi :10.3969/j.issn.1671-1122.2017.12.004

区块链系统下的多方密钥协商协议

唐春明，高隆

（广州大学数学与信息科学学院，广东广州 510000）

摘　要：密钥协商协议是在公开的信道上，两个或者多个参与者之间进行的共享密钥机制，以保证通信安全和对敏感信息的加密。通信主体需要相互信任，并且需要一个可信中心对彼此身份进行认证，以安全进行密钥协商。为防御针对中心进行攻击或者中心以权谋私，文章给出了在区块链系统下的多方密钥协商协议，利用区块链存储数据只能增加不能删除与更改的特性，使得协议具有更高的安全性。

关键词：多方密钥协商协议；双线性对；区块链；可信第三方

中图分类号：TP309.1　　**文献标识码：**A　　**文章编号：**1671-1122（2017）12-0017-05

中文引用格式：唐春明，高隆 . 区块链系统下的多方密钥协商协议 [J]. 信息网络安全，2017（12）：17-21.

英文引用格式：TANG Chunming, GAO Long. Multi-parties Key Agreement Protocol in Block Chain[J].Netinfo Security,2017(12):17-21.

Multi-parties Key Agreement Protocol in Block Chain

TANG Chunming, GAO Long

(*School of Mathematics and Information Science*, *Guangzhou University*, *Guangzhou Guangdong* 510000, *China*)

Abstract: The key agreement protocol is a shared key mechanism between two or more participants in a public channel to ensure the secure communication and encryption of sensitive information. Communication agents need to trust each other, and a trusted center is needed to authenticate each other to negotiate the key securely. In order to resist the attack on the trusted center and the abuse of power of the trusted center, this paper gives a multi-parties key agreement protocol in block chain system, which uses the characteristics that when store data, data only can increase, but can not be deleted and changed, which makes the protocol more secure.

Key words: multi-parties key agreement protocol; bilinear pairing; block chain; trusted third party

收稿日期：2017-8-28

基金项目：国家自然科学基金 [11271003]；广东省自然科学基金重大基础研究培育项目 [2015A030308016]；广东省教育厅基础研究重大项目 [2014KZDXM044]；教育部高等学校博士学科点专项科研基金联合资助课题（博导类联合）[20134410110003]

作者简介：唐春明（1972—），男，湖南，教授，博士，主要研究方向为信息安全、密码学；高隆（1991—），男，湖南，博士研究生，主要研究方向为信息安全、密码学。

通信作者：唐春明 395033429@qq.com

0 引言

随着计算机技术的快速发展以及互联网时代的兴起，如何在开放的网络中保证信息安全已成为一个重要的研究课题。目前，在公开的网络中保证信息安全的基本手段是对通信主体进行身份认证和对通信数据进行加密处理。对通信数据进行加密处理的关键在于通信双方要拥有一个共同的密钥，密钥协商正是解决这个问题的基本方法。

密钥协商是两个或者多个参与者在公开的信道中，以信息交互的方式来共同生成一个保密的会话密钥。1976 年以前的通信理念是在通信开始之前，进行通信的双方或者多方需要秘密协商出一个只有通信主体才知道的私密密钥，该密钥用来对通信数据进行加密解密，以防止通信数据被他人截取或者修改。1976 年第一个现代密钥交换协议 Diffie-Hellman[1] 被提出，打破了人们的传统观念，使得用户可以在完全公开的信道上进行秘密共享。

Diffie-Hellman 协议的安全性基于有限域上离散对数的难解性，但该协议没有进行认证，容易受到中间人攻击。为了弥补没有认证这一漏洞，学者提出了认证密钥协商协议。

密钥协商协议的认证方式可以划分为基于 PKI 认证方式和基于身份认证方式。但无论基于何种认证方式，协议都需要一个可信第三方对用户身份进行认证，这样容易造成针对中心的攻击或可信中心以权谋私。区块链技术的出现弥补了这一缺陷 [2]，可信中心只负责公私钥的分发，使得协议过程更加透明并且可以溯源。本文根据文献 [3] 和文献 [4] 引入保证金和奖惩机制，即在协议开始前所有用户需要给系统缴纳一定的保证金，如果协议的任何一方出现问题，或者在协议中途有参与者突然中断协议，那么其钱款都将转给诚实的其他参与者。本文根据区块链系统的交易模式进行多方密钥协商，采用 MTI/CO[5] 中的认证方式把文献 [6] 的方案扩展到多方。

1 预备知识

1.1 Diffie-Hellman 密钥协商方案

公开域参数包括群 $(G,\cdot)$ 和阶为 q 的元素 $g\in G$。假设有 A,B 两个参与者进行协商。

1）A 选取一个随机数 $a(0\leqslant a\leqslant q-1)$，计算 $K_A=g^a$ 并将 K_A 发送给 B。

2）B 选取一个随机数 $b(0\leqslant b\leqslant q-1)$，计算 $K_B=g^b$ 并将 K_B 发送给 A。

3）A 计算 $K_A=(g^b)^a$，B 计算 $K_B=(g^a)^b$，显然 $K=(g^a)^b=(g^b)^a=g^{ab}$ 为共享密钥。

计算 Diffie-Hellman 问题通常表示为 CDH，这个困难问题基于有限域上离散对数的难解性，即 $g^x=u$，求解 x 是困难的。基于椭圆曲线的 Diffie-Hellman 协议也是基于有限域上离散对数的难解性，即 $nP=m$，P 是椭圆曲线上的基点，求解 n 是困难的。

1.2 MTI/CO 认证协议

由于 Diffie-Hellman 协议没有进行认证，故许多可认证的密钥协商协议被提出。这里介绍 MTI/CO 认证协议中的认证方式，其过程如下：

1）参与者 A 和参与者 B 能够得到对方的公钥 g^b 和 g^a。

2）A 选取一个随机数 x，计算 $K_A=g^{bx}$ 并发送给 B。

3）B 选取一个随机数 y，计算 $K_B=g^{ay}$ 并发送给 A。

4）A 计算会话密钥 $K_1=K_B{}^{a^{-1}x}=g^{aya^{-1}x}=g^{xy}$，$B$ 计算会话密钥 $K_2=K_A{}^{b^{-1}y}=g^{bxb^{-1}y}=g^{xy}$，这样就得到了共享会话密钥 $K=K_1=K_2=g^{xy}$。

1.3 双线性映射

令 G_1,G_2 和 G_T 为 3 个阶为素数 q 的乘法循环群，g_1,g_2,g_3 分别为 3 个循环群的生成元。令 $e:G_1\times G_2\rightarrow G_T$ 是一个具有以下性质的映射：

1）双线性。对于所有 $g_1\in G_1,g_2\in G_2,a,b\in Z_q$，有 $e(g_1{}^a,g_2{}^b)=e(g_1,g_2)^{ab}$。

2）非退化性。存在 $g_1\in G_1,g_2\in G_2$，满足 $e(g_1,g_2)\neq 1$。即对 G_1，G_2 中的任何元素，通过这个映射都不会得到 G_T 中的单位元。

3）可计算性。对于任意 $g_1\in G_1,g_2\in G_2$，存在有效的算法计算 $e(g_1,g_2)$。

1.4 密钥协商协议的安全性

因为密钥协商协议是在公开的网络中，所有参与者通过信息交互的方式共同生成一个保密的会话密钥，所以协议必须具有一定的安全性。密钥协商协议需要满足的基本安全属性如下 [7]：

1）已知密钥安全。由于每次生成的保密会话密钥中都含有每个参与者随机产生的随机数作为短私钥，所以每次

生成的会话密钥都是唯一的，即使以前使用过的会话密钥发生了泄露，由于短私钥的暂时性，攻击者也不可能知道目前使用的会话密钥。

2）完美前向保密性。即使一个参与者或者多个参与者使用的私钥长期泄露，也不会影响在此之前生成的会话密钥，这就是完美前向保密性。

3）密钥不可控制性。由于会话密钥是各参与者共同协商产生，其中包含随机生成的值，因此无论哪方都不能对协商的会话密钥预先控制其选定的值。

4）抵抗密钥泄露攻击。假设 *A* 的私钥长期泄露，那么攻击者能够假扮 *A* 欺骗其他用户，但是不能扮演其他参与者欺骗 *A*。

5）密钥共享可知性。协议必须在所有参与者都知晓进行密钥协商协议的情况下才能够进行，任意一个参与者或者多个参与者不知晓都不能进行密钥协商协议。

2 区块链简介

2.1 区块链定义

区块链是比特币的基础支撑技术 [8,9]，本质上是一个共享的可靠数据库，这个数据库的维护是去中心化与去信任的。区块链的核心思想是让系统中的每个参与节点通过求解某些 Hash 函数的值来产生数据块，每个数据块中包含了一定时间内系统所有的交流信息数据；验证节点利用 Hash 函数生成信息特征以验证数据块中交易数据的有效性，并且和下一个数据块链接，由此形成区块链（Block Chain）。记录信息是由系统中所有的验证节点共同验证其真伪的。

区块链技术不是一种特定的技术，而是一类类似于 NoSQL（非关系型数据库）的技术解决方案的统称，它可以用多种计算机语言和架构来实现。目前区块链的共识机制有很多，常见的有工作量证明（Proof of Work，POW），权益证明 [10]（Proof of Stake，POS）和股份授权证明机制 [11]（Delegate Proof of Stake，DPOS）等。

2.2 区块链特征

结合区块链的定义，区块链具有以下 4 个特征：

1）去中心化。整个系统中没有一个中心化的管理机构，所有参与节点之间的地位都是平等的，信息传输不再需要一个中心点中转，而是系统中的每个节点根据共识协议进行点对点和自由安全的信息传输，且任意一个或者多个节点（节点数量不超过界限）出现问题都不会影响整个系统的运作。去中心化最主要的一点是所有交易记录都在系统中的所有节点进行了备份。

2）去信任。日常社会活动中，如果没有一个权威机构去证明，那么基本上不会存在可以信任的产品，但这种方式往往会增加交易成本，且会降低效率，更严重的是容易滋生腐败，造成不公平的交易。由于区块链中的数据只能增加不能删除，一旦生成不能修改且每个节点都会备份，因此数据更加透明。区块链系统中每个节点之间进行数据交换不需要彼此信任，且在一定时间内，一些节点也无法联合起来去欺骗其他节点。

3）集体维护。由于系统中没有一个中心管理机构，因此系统中的数据块是由所有具有维护功能的节点共同维护，这就是共识机制。这些维护节点并不具有特殊性，所有节点都可以参与。

4）可靠数据库。系统中的每个节点都能获得一份完整的数据副本，系统的抗灾冗余性增强。系统规定，除非能够同时操控系统中超过 51% 的节点去修改数据，才能改变整个系统数据，对单个节点上的数据修改是没有意义的。因此参与区块链系统的节点越多且节点的计算能力越强，系统的数据安全性就越高。

2.3 区块链分类

根据应用场景与需求的不同，文献 [12] 将区块链分为 3 种模式：公有链、私有链和联盟链。

1）公有链。顾名思义，公有链信息是完全公开的，任何人都可以参与交易与维护。这种区块链模式非常适合互不认识的陌生个体。其典型应用是比特币区块链、以太坊区块链。事实上，这种公共特性也是公有链这种区块链模式最吸引人的地方。

2）私有链。权限仅在一个组织手中，只能由内部少数人使用，信息不公开。想使用区块链时必须要进行验证与授权。

3）联盟链。若干组织合作维护一条区块链，区块链的使用是带有权限的管理，相关信息会得到保护。该模式区块链适用于大型商业活动，彼此信任已经建立，更希望

得到交易的隐私性。

2.4 超级账本区块链交易流程

超级账本区块链交易流程为：Alice 进入超级账本客户端，向成员管理服务发送注册身份请求，成员管理服务返回身份证明与对应私钥。身份证明与对应私钥存储在本地文件系统当中。当 Alice 要发送交易时，由超级账本客户端读取 Alice 的身份证明和私钥，私钥用来对交易消息进行签名，交易的验证则由随机选择出来的 4 个验证节点构成的fabric网络使用PBFT共识算法来执行。当验证通过时，交易记录写入账本，且永远无法更改。

3 协议过程

3.1 文献 [6] 方案简介

文献 [6] 介绍了一个简单的一轮三方协商协议。其中，参与者 A,B,C 分别随机选择 $a,b,c\in Z_p^*$：

1）A 计算 g^a 并分别发送给 B 和 C。

2）B 计算 g^b 并分别发送给 A 和 C。

3）C 计算 g^c 并分别发送给 A 和 B。

4）在收到其他参与者的信息后，A 计算 $K_A=e(g^b,g^c)^a$，B 计算 $K_B=e(g^a,g^c)^b$，C 计算 $K_C=e(g^a,g^b)^c$，得出 $K_A=K_B=K_C=K=e(g,g)^{abc}$ 为会话密钥。

文献 [6] 方案采用 MTI/CO 认证方式过程如下：

1）A,B,C 能够知道每个参与者的公钥 g^a,g^b,g^c。

2）A 选取一个随机数 x，计算 g^{xb},g^{xc} 分别发送给 B 和 C。

3）B 选取一个随机数 y，计算 g^{ya},g^{yc} 分别发送给 A 和 C。

4）C 选取一个随机数 z，计算 g^{za},g^{zb} 分别发送给 A 和 B。

5）A,B,C 在收到其他参与者发送的消息后，分别计算会话密钥 $K_A=e(g^{yaa^{-1}},g^{zaa^{-1}})^x=e(g,g)^{xyz}$，$K_B=e(g^{xbb^{-1}},g^{zbb^{-1}})^y=e(g,g)^{xyz}$，$K_C=e(g^{xcc^{-1}},g^{ycc^{-1}})^z=e(g,g)^{xyz}$。很明显，会话密钥 $K_{ABC}=K_A=K_B=K_C=e(g,g)^{xyz}$。

本文是多方密钥协商协议，是将上述三方扩展到多方，首先介绍一下有可信第三方的多方密钥协商协议。

3.2 有可信第三方的多方密钥协商协议

令 G_1 和 G_2 是两个阶为素数 q 的乘法循环群。令 $e:G_1\times G_1\rightarrow G_2,g$ 是 G_1 的生成元；$sig_i(m)$ 表示用户签名；E_{PK_i} 表示用户的公钥加密算法；H 为 Hash 函数；S 为协议中唯一服务器；pw_i 是参与者与服务器的共享口令，只有参与者与服务器知道；E_{pw} 表示用口令 pw 进行加密；T 表示时戳；g^{x_i} 为每个参与者的公钥，x_i 为每个参与者的私钥，自己保存；ID_i 表示参与者的身份。

假设有 n 个用户 $\{U_1,U_2,\cdots,U_n\}$ 参与协商，$r_i\in Z_q^*$，过程如下：

第一轮：参与者 U_i 选择一个随机数，计算 $Z_i=g^{r_ix_{i-1}}$，$M_i=g^{r_ix_{i-2}}$，将 $(m_i',sig_i(H(m_i')))$，$(m_i'',sig_i(H(m_i'')))$ 分别发送给参与者 U_{i-1},U_{i-2}。其中，$m_i'=ID_i\|ID_{i-1}\|Z_i\|T$，$m_i''=ID_i\|ID_{i-2}\|M_i\|T$。

第二轮：参与者收到上一轮发来的消息，先验证签名，然后计算自己的份额 $k_i=e(g^{r_{i+1}x_ix_i^{-1}},g^{r_{i+2}x_ix_i^{-1}})^{r_i}=e(g,g)^{r_ir_{i+1}r_{i+2}}$，再计算 $C_i=E_{pw_i}(k_i)$，并且把 $(m_i''',sig_i(H(m_i''')))$ 发送给服务器，其中 $m_i'''=ID_i\|ID_s\|C_i\|T$。

第三轮：服务器收到上一轮发来的消息，先验证签名，再利用与每个用户共享的 pw_i 解密得到 k_i，然后计算 $K_i=E_{pw_i}(\prod k_j)(1\leqslant j\leqslant n,i\neq j)$，把 K_i 分别发送给每个参与者。

第四轮：每个参与者接收到 K_i 后，解密得到 $\prod k_j(1\leqslant j\leqslant n,i\neq j)$，再各自计算会话密钥 $K=k_i\prod k_j=e(g,g)^{r_1r_2r_3+r_2r_3r_4+\cdots+r_nr_1r_2}$。

3.3 区块链系统下的多方密钥协商协议

如果上述有可信第三方的多方密钥协商协议在区块链系统下进行，则过程如下：

令 G_1 和 G_2 是两个阶为素数 q 的乘法循环群，令 $e:G_1\times G_1\rightarrow G_2,g$ 是 G_1 的生成元；$sig_i(m)$ 表示用户签名；E_{PK_i} 表示用户的公钥加密算法；H 为 Hash 函数。

第一轮：用户 U_i 利用随机数生成器生成随机数当做自己选择的私钥 s_i 且保存，计算 g^{s_i} 发送给其他用户 $U_j(1\leqslant j\leqslant n,j\neq i)$，发送的消息为 $sig_i(H(m_i))$ 和 $H(g^{s_i})$，其中 $m_i=E_{PK_j}(g^{s_i})$。这里相当于用户把自己选择的公钥发送给了系统中的每个用户，没有授权的用户是看不到的，其中 $H(g^{s_i})$ 一样要写入区块链账本。

第二轮：U_i 收到上一轮发来的消息，先验证签名，再解密得到每个用户的 g^{s_i}，然后选择一个随机数 r_i 计算 $Z_i=g^{r_is_{i-1}},M_i=g^{r_is_{i-2}}$，将 $sig_i(H(m_i'))$ 和 $H(Z_i)$，$sig_i(H(m_i''))$ 和 $H(M_i)$，其中 $m_i'=E_{PK_{i-1}}(Z_i),m_i''=E_{PK_{i-2}}(M_i)$，分别发送给用户 U_{i-1}，U_{i-2}。这里除了交易记录要写进区块链账本，后面的 $H(Z_i),H(M_i)$ 也要写入账本当中。

第三轮：用户 U_i 按照第二轮的方式得到

$Z_{i+1}=g^{r_{i+1}s_i}$,$M_{i+2}=g^{r_{i+2}s_i}$ 后，分别计算自己的份额 $k_i=e(g^{r_{i+1}s_is_i^{-1}},g^{r_{i+2}s_is_i^{-1}})^{r_i}=e(g,g)^{r_ir_{i+1}r_{i+2}}$,将消息 $sig_i(m_i''')$和$H(k_j)(i\neq j,i,j=1,2,\cdots,n)$,其中 $m_i''''=E_{PK_j}(k_j)$, 分别发送给用户 $U_j(1\leqslant j\leqslant n,j\neq i)$。

第四轮：用户 U_i 得到 k_i 后，计算会话密钥 $K=\prod_{i=1}^{n}k_i=e(g,g)^{r_1r_2r_3+r_2r_3r_4+\cdots+r_nr_1r_2}$。

4 安全性与效率分析

4.1 安全性分析

由于本文协议的会话密钥是由每个参与者的由随机数生成的短私钥构成，故每次协议生成的密钥都是唯一的，且每次重新开始协议，用户的短私钥都会不一样，故本文协议满足已知密钥安全性、完美前向保密性和密钥不可控制性。此外，本文协议采用签名认证，故能抵抗密钥泄露攻击和满足密钥共享可知性。

本文协议利用了 MTI/CO 认证，在第二轮中，若有敌手能够获得 M_i,Z_i，那么在第三轮中，他们在不知道用户第一轮所选随机数作为私钥的情况下，计算的份额只能是 $k_i'=e(g^{r_ir_{i+1}s_i},g^{r_ir_{i+2}s_i})=e(g,g)^{r_ir_{i+1}r_{i+2}s_i^2}$，而不是每个用户计算出来的份额 $k_i=e(g^{r_{i+1}s_is_i^{-1}},g^{r_{i+2}s_is_i^{-1}})^{r_i}=e(g,g)^{r_ir_{i+1}r_{i+2}}$，也就得不到最后的会话密钥。如果没有 MTI/CO 认证方式，与 U_i 相关的用户 U_{i+1},U_{i+2} 能够计算出 U_i 计算的份额，那么就可能受到内部成员的角色扮演攻击。

本文方案引入了区块链系统，每次交易都是有记录的，且每个用户还交了保证金。例如，在第一轮中，用户 U_i 对参与密钥协商的每个用户发起交易，发送的是 g^{s_i}。如果交易获得批准写入账本，同时写入账本的还有 $H(g^{s_i})$。那么在第一轮结束后，用户可以查验账本中的 $H(g^{s_i})$ 与写入账本的 $H(g^{s_i})$ 是否相等，如果不相等则可以终止协议，并且查看交易记录是哪个交易出了问题，从而知道是哪个地方出了问题或者是哪个用户不诚信，从而把不诚信用户的保证金扣除，分发给诚信用户。

当然这里对区块链技术的利用更多的是它存储数据只能读取不可更改的特性，以及可以溯源查找是哪个方面出现问题以减少一定的损失。

4.2 效率分析

进行一次密钥协商协议，第一轮中，一个参与者计算了一次，发起 $n-1$ 次交易（发送次数）；第二轮中参与者计算了一次（计算 Z_i、M_i），发送了两次交易；第三轮中计算了一次（计算自己的份额），发送了 $n-1$ 次交易；第四轮中，每个参与者在收到别人的份额后，只需计算最终的会话密钥。因此一个参与者在一次密钥协商协议中的通信轮数为 3 轮，发送交易次数为 $2n$ 次，计算次数为 4 次。

本文协议还存在不足。例如，在第三轮中，参与者发送自己的份额时没有采取更深的保护措施，存在一定的不安全性。

5 结束语

本文是按照区块链系统的交易模式构造的密钥协商协议，对可信第三方的依赖降低，协议过程更加公开、透明，且协议过程引入了 MTI/CO 认证方式，使得协议更加安全。本文还利用区块链的存储性质防止中心作恶。但本文协议只是利用了区块链存储只能增加不能篡改和删除的特性，利用区块链构造更好的协议将是下一步的工作。（责编 马珂）

参考文献：

[1] DIFFIE W，HELLMAN M. New Directions in Cryptography[J].IEEE Transactions on Information Theory,1976, 22(6):644-654.

[2] 谢辉，王健．区块链技术及其应用研究 [J]. 信息网络安全 ,2016(9):192-195.

[3] ANDRYCHOWICZ M, DZIEMBOWSKI S, MALINOWSKI D, et al. Secure Multiparty Computations on Bitcoin[J]. Communications of the Acm, 2016, 59(4):76-84.

[4] KIAYIAS A, ZHOU Hongsheng, ZIKAS V. Fair and Robust Multi-party Computation Using a Global Transaction Ledger[A]// Advances in Cryptology-EUROCRYPT 2016[M]. Heidelberg :Springer, Berlin, Heidelberg,2016:705-734..

[5] MATSYMOTO T , TAKASHIMA Y , IMAI H. On Seeking Smart Public-key Distribution System[J]. The Transations of the IECE of Japan , 1986(86): 99-106.

[6] JOUX A. A One Round Protocol for Tripartite Diffie-Hellman[J]. Journal of Cryptology, 2004, 17(4):263-276.

[7] BLAKE-WILSON S, JOHNSON D, MENEZES A. Key Agreement Protocols and their Security Analysis[A]// Crytography and Coding [M]. Heidelberg:Springer, Berlin, Heidelberg, 1997：30-45.

[8] NAKAMOTO S. Bitcoin: A Peer-to-peer Electronic Cash System [EB/OL]. https://bitcoin.org/ bitcoin. pdf, 2017-8-1.

[9] 王皓，宋祥福，柯俊明．等．数字货币中的区块链及其隐私保护机制 [J]. 信息网络安全 ,2017(7):32-39.

[10] LARIMER D. Transactions as Proof-of-stake [EB/OL]. https://bravenewcoin.com/assets/Uploads/TransactionsAsProofOfStake10.pdf, 2017-8-1.

[11] 韩璇，刘亚敏．区块链技术中的共识机制研究 [J]. 信息网络安全 ,2017(9):147-152.

[12] 张健．区块链：定义未来金融与经济新格局 [M]. 北京：机械工业出版社，2016.