# 基于 SM2 数字签名的区块链匿名密钥交换协议

黄佩达[1], 林 超[1], 伍 玮[2], 何德彪[3]

[1]福建师范大学 计算机与网络空间安全学院 福州 中国 350117
[2]福建师范大学 数学与统计学院 福州 中国 350117
[3]武汉大学 国家网络安全学院 武汉 中国 430072

**摘要** 区块链技术因其去中心化、匿名性、不可篡改、不可伪造等优点, 已经成为我国的一项前沿技术, 在各领域得到广泛的应用。虽然用户可利用区块链发布匿名交易, 有效隐藏交易双方的身份信息, 但双方交易完成后传输交易相关数据可能破坏匿名性。这是因为在数据传输过程中, 为了保证双方通信安全, 往往使用认证密钥交换协议认证双方身份, 计算会话密钥建立安全信道。由于传统的认证密钥交换协议涉及双方的长期公私钥对信息, 所以将泄露交易双方的身份信息。虽然区块链匿名密钥交换可基于交易双方的历史链上交易完成密钥交换, 有效保障交易双方的匿名性, 但现有区块链匿名密钥交换协议主要基于国外密码算法设计, 难以适用于国产区块链平台, 不符合我国密码核心技术自主可控的要求。为丰富国产商用密码算法在区块链匿名密钥交换方面的研究, 满足区块链交易后双方匿名安全通信的需求, 本文以 SM2 数字签名算法和区块链为基础, 构造非交互式和交互式两种区块链匿名密钥交换协议。并在 CK 安全模型中证明非交互式的协议满足会话密钥安全, 交互式的协议满足有前向安全性的会话密钥安全。最后通过理论分析和编程实现结果表明, 本文协议在没有比现有协议消耗更多的计算开销与通信代价的前提下, 可适用于国产化区块链平台。

**关键词** 密钥交换协议；SM2 数字签名；区块链；CK 安全模型
**中图法分类号** TP309.7 DOI 号 10.19363/J.cnki.cn10-1380/tn.2024.05.02

# Blockchain Anonymous Key Exchange Based on SM2 Digital Signature Protocol

HUANG Peida[1], LIN Chao[1], WU Wei[2], HE Debiao[3]

[1] College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, China
[2] School of Mathematics and Statistics, Fujian Normal University, Fuzhou 350117, China
[3] School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China

**Abstract** Blockchain technology has become a frontier technology in China and is widely used in various fields due to its advantages of decentralization, anonymity, immutability and unforgeability. Although users can use blockchain to publish anonymous transactions and effectively hide the identity information of both parties to the transaction, the transmission of transaction-related data after the completion of the transaction between the two parties may destroy the anonymity. This is because during data transmission, in order to secure the communication between the two parties, the authentication key exchange protocol is often used to authenticate the identity of both parties and calculate the session key to establish a secure channel. Since the traditional authentication key exchange protocol involves long-term public-private key pair information of both parties, it will disclose the identity information of both parties of the transaction. Although blockchain anonymous key exchange can complete key exchange based on the historical on-chain transactions of both parties to the transaction and effectively guarantee the anonymity of both parties to the transaction, the existing blockchain anonymous key exchange protocol is mainly designed based on foreign cryptographic algorithms, which is difficult to apply to domestic blockchain platforms and does not meet the requirement of independent and controllable core cryptographic technology in China. To enrich the research of domestic commercial cryptographic algorithms in blockchain anonymous key exchange and meet the demand for anonymous and secure communication between two parties after blockchain transactions, this paper constructs two blockchain anonymous key exchange protocols, non-interactive and interactive, based on SM2 digital signature algorithm and blockchain. And it is proved in the CK security model that the non-interactive protocol satisfies the session key security and the interactive protocol satisfies the session key security with forward security. Finally, the theoretical analysis and programming implementation results show that the protocol in this paper can be suitable for domestic blockchain platforms without consuming more computational overhead and communication costs than existing protocols.

**通讯作者：** 林超, 博士, 副教授, Email: cschaolin@163.com。
本课题得到国家自然科学基金(No. 62102089, No. 62032005, No. 61872089, No. 61972294)、中央高校基本科研业务费专项资金(No. 2042021kf1030)、湖北省自然科学基金 (No. 2017CFA007)、福建省自然科学基金(No. 2020J02016)资助。
收稿日期: 2022-07-10；修改日期: 2022-11-02；定稿日期: 2024-01-17

**Key words** key exchange protocol; SM2 digital signature; blockchain; CK security model

# 1 引言

区块链技术因具有去中心化、匿名、不可篡改、不可伪造等特点, 已经成为我国的一项前沿技术, 在各领域得到广泛的应用。为了满足区块链的国产化需求, 国内工业界和学术界采用 SM2、SM3、SM9 等商用密码算法设计了聚龙链、趣链等国产区块链平台。

现有的国产区块链平台支持用户以匿名的形式在区块链上发布交易, 但链上的交易完成后, 交易双方需要在链下传输交易相关信息, 以确定交易细节。由于直接传输信息无法保障交易后双方数据的安全通信, 面临数据隐私泄露、篡改、删除等问题。虽然采用现有认证密钥交换协议建立安全信道, 利用安全信道传输信息可保障用户身份真实性和传输消息的安全性, 但会暴露区块链上的用户匿名身份与现实身份之间的关联性, 破坏区块链用户的匿名性, 严重侵犯用户的隐私。

近年来, Patrick 等人[1]提出了基于比特币的匿名密钥交换协议, 使用比特币的交易签名中的随机数, 作为密钥交换过程中的随机数, 并利用交易中的数字签名确认了密钥交换双方的身份, 解决了传统认证密钥交换中的身份隐私泄露问题。然而, 文献[1]的方案未给出形式化的安全性证明, 并采用国际算法 ECDSA[2]设计, 无法直接应用于国产区块链平台。因此, 亟需设计可证明安全且适用于国产区块链平台的匿名密钥交换协议, 既保证国产区块链平台用户交易后数据的安全传输, 又保护区块链用户身份的匿名性。本文主要基于商用密码 SM2 数字签名, 重新设计区块链匿名密钥交换协议, 使其适用于使用 SM2 公钥密码算法的国产区块链平台, 并且在 CK (Canetti Krawczyk, CK)安全模型中给出了形式化的安全性证明。

## 1.1 本文贡献

本文借鉴文献[1]的区块链匿名密钥交换协议设计思路, 利用 SM2 数字签名算法, 提出两种匿名密钥交换协议。其中一种是高效的非交互式密钥交换协议, 另一种是具有前向安全的交互式密钥交换协议。这两种密钥交换协议可适用于物联网、金融、政务等不同应用场景, 满足安全性、高效性等应用需求。

本方案验证了区块链匿名密钥交换协议的正确性, 并形式化地证明了协议的安全性: 在 CK 安全模型中, 基于判定性 Diffie-Hellman 问题证明了非交互式密钥交换协议满足会话密钥安全, 以及交互式密钥交换协议满足拥有前向安全性的会话密钥安全。

本文与其他同类型协议进行功能对比, 并通过理论性能分析和 BouncyCastle 算法库仿真模拟, 分析本文协议与基于 ECDSA 的匿名认证密钥交换协议的性能情况。结果表明, 本文协议在没有消耗更多计算开销与通信开销的前提下, 可有效支撑国产区块链平台的匿名密钥交换需求。

## 1.2 相关工作

1976 年, Diffie 和 Hellman[3]最早提出了密钥交换的概念。密钥交换可以通过参与方的交互计算会话密钥, 双方使用会话密钥加密信息, 保证通信的安全。然而, 文献[3]的密钥交换协议未验证参与者的身份, 所以仅能抵抗被动攻击。

为了抵抗主动攻击, Bellare 和 Rogaway[4]提出认证密钥交换, 认证用户身份, 解决了主动攻击的问题。但传统的认证密钥交换协议需要使用公钥基础设施等可信第三方认证参与者身份, 会破坏用户在区块链平台中的匿名性, 因此不适用于区块链这一去中心化的匿名应用场景。

为了保障用户的匿名性, Patrick 等人[1] 2015 年结合 ECDH[5]和 YAK[6]两种设计思路, 基于比特币提出两种认证密钥交换协议, 使用 ECDSA 中的随机数和公开的签名作为密钥交换的参数, 降低通信开销。虽然该方案可保证比特币场景用户双方的安全匿名通信, 但是没有给出形式化的安全性证明, 并且基于国外密码算法设计, 不满足核心技术自主可控的需求。

此外 Yao 等人[7]基于共同利益和 Bloom 过滤器, 在有共同利益的陌生人之间建立信任, 完成密钥交换。同时基于 BPR 模型[8]证明了该方案的安全性。该方案虽然可以匿名的完成密钥交换协议, 但是无法与指定的目标用户密钥交换, 并且需要密钥交换双方预先拥有相同的秘密值。

为了保障用户的匿名性的同时检测和阻止中间人攻击, Bui 等人[9]2017 年利用公共账本的一致性等特点设计了密钥交换协议。由于参与密钥交换的双方在公共账本中公开密钥交换的参数, 所以双方可以在公开账本上查询相关参数, 确认参与的是否为同个密钥交换过程, 从而阻止中间人攻击。但该方法虽然能够检测中间人攻击, 但无法抵抗假冒攻击, 不能确保系统的安全。

Wu 等人[10]2022 年基于区块链提出了五种去中

心化的认证密钥交换协议, 这五种协议分别有不同的安全性质, 可满足不同类型的安全需求。虽然可以满足身份认证、匿名性、前向安全性等需求, 但是该方案的密钥交换过程借助区块链交易完成, 协议运行耗时受到区块链交易花费的时间影响, 效率较低。

### 1.3 本文结构

第 2 节简要回顾本文涉及的 SM2 数字签名算法、零知识证明、安全假设、CK 安全模型等预备知识; 第 3 节介绍基于 SM2 数字签名的区块链上的非交互式密钥交换和交互式密钥交换协议的具体构造; 第 4 节证明了协议的正确性和安全性; 第 5 节对比本文协议与其他协议的功能, 理论分析各方案的性能, 并与基于 ECDSA 的区块链匿名密钥交换协议进行性能对比; 第 6 节总结了本文的工作。

## 2 预备知识

本节简要回顾 SM2 数字签名、零知识证明、安全假设、CK 安全模型等预备知识。

### 2.1 SM2 数字签名算法

SM2 数字签名算法是《SM2 椭圆曲线公钥密码算法》规范中的数字签名算法, 因其高安全、高效率而广泛用于消息传输, 可有效保证消息传输过程中消息的真实性、可靠性和不可否认性。SM2 数字签名主要包含以下四个算法:

**系统参数生成:**该算法输入参数 $\lambda$, 输出系统参数 $pp=(E,a,b,q,\mathbb{G},n,G,\mathcal{H})$。其中 $E$ 是有限域上由 $a$ 和 $b$ 定义的一条椭圆曲线。$\mathbb{G}$ 是阶为 $n$ 的基点 $G$ 生成的循环群。$\mathcal{H}$ 安全哈希函数 $\mathcal{H}:\{0,1\}^*\to\mathbb{Z}_n^*$。

密钥生成:该算法输入系统参数 $pp$, 随机选取 $d\in\mathbb{Z}_n^*$, 计算 $P=dG$, 输出用户的私钥 $sk=d$、公钥 $pk=P$。

签名:该算法输入系统参数 $pp$、用户私钥 $sk=d$ 和签名消息 $m$。随机选取 $k\in\mathbb{Z}_n^*$, 计算 $K=kG=(x_K,y_K)$、$e=\mathcal{H}(m)$ 和 $r=(e+x_K)(mod\ n)$. 若 $r=0$ 或 $r+k=n$, 则重新选取 $k$ 再计算, 否则计算 $s=(1+d)^{-1}(k-rd)(mod\ n)$. 若 $s\neq 0$, 则输出数字签名 $\sigma=(r,s)$。

验证:算法输入系统参数 $pp$、用户公钥 $pk=P$、签名消息 $m$ 和待验证数字签名 $\sigma=(r,s)$, 若 $r,s\notin\mathbb{Z}_n^*$, 则输出 0, 否则计算 $t=(r+s)\ (mod\ n)$。若 $t=0$, 则输出 0, 否则计算 $e'=\mathcal{H}(m)$、$K'=sG+tP=(x'_K,y'_K)$ 和 $r'=(e'+x'_K)\ (mod\ n)$。若 $r'=r$, 则输出 1 表示交易有效, 否则输出 0 表示无效。

### 2.2 零知识证明

零知识证明[11]指证明者能够在不向验证者提供除了论断本身外任何有用信息的情况下, 使验证者相信某个论断是正确的。零知识证明至少由证明者和验证者参与。证明者是零知识证明的一个参与方, 证明某个断言真实性的同时不泄露任何其他信息。验证者是零知识证明的另一个参与方, 验证证明者提出的断言以及证明是否正确。证明者向验证者发送承诺, 验证者选择随机数, 向证明者发起挑战, 证明者结合承诺并针对挑战做出应答。使用 Fiat-Shamir 变换[13]可以将交互式零知识证明转换成非交互式零知识证明, 减少通信的过程并提高效率。

零知识证明包含以下 3 个特性:

1)正确性: 验证者接受的正确的断言的概率不可忽略。

2)可靠性: 证明者成功证明某个错误断言的概率可忽略。

3)零知识性: 验证者只能判断出断言的正确性, 而无法获得其他任何知识。

### 2.3 安全假设

**定义 1.**(Decisional Diffie-Hellman(DDH)问题)已知 $(G,aG,bG,Z)$, $G\in\mathbb{G}$, $Z\in\mathbb{G}$, 判断 $Z=abG$ 或 $Z=cG$,其中 $c$ 是 $\mathbb{Z}_n^*$ 中的随机数。

定义概率多项式时间(Probabilistic Polynomial-Time, $\mathcal{PPT}$)算法 $\mathcal{D}$ 成功解决 DDH 问题的优势为:

$$Adv(\lambda)=|Pr[\mathcal{D}(G,aG,bG,abG)=1]-Pr[\mathcal{D}(G,aG,bG,cG)=1]|$$

DDH 安全假设: 对任意 $\mathcal{PPT}$ 算法 $\mathcal{D}$ 成功解决 DDH 问题的优势 $Adv(\lambda)$ 可忽略。

### 2.4 CK 安全模型

CK 模型由 Canetti 和 Krawczyk[14]于 2001 年提出。CK 模型中的密钥交换协议是由消息驱动的协议。消息驱动的协议由外部调用触发协议, 通过参与方运行, 包含数个交互过程, 协议参与方处理传入的消息, 并生成输出消息发送给其他参与方, 其他参与方收到消息后触发后续协议。

CK 模型中定义了非认证链路模型(Unauthenticated Links Model, UM)和认证链路模型(Authenticated Links Model, AM)两个模型。其中 UM 中的攻击者是一个概率多项式时间的攻击者, 完全控制着通信链路。攻击者可以监听传输的信息, 决定哪些信息和何时到达目的地, 并且能任意的改变这些信息, 或者注入自己生成的信息。攻击者还控制所有协议事

件的调度, 包括协议的调用和消息的传递。本文采用 UM 模型证明协议的安全性。

攻击者除了可以控制通信链路和控制协议事件的调用之外, 还可以通过以下 3 种查询来获取协议参与者存储器中的信息:

$Corrupt(P_i)$. 攻击者在任何时候腐化参与方 $P_i$, 攻击者得到长期密钥 $sk$ 和在参与方存储器中与会话相关的信息。攻击者可以冒充参与方 $P_i$, 参与方 $P_i$ 完全被攻击者控制, 可以任意的偏离协议规范。

$SessionKey(P_i,s)$. 攻击者提供一个参与方 $P_i$ 和一个已完成的会话 $s$, 获得会话 $s$ 的会话密钥 $SK$。

$SessionState(P_i,s)$. 攻击者提供一个参与方 $P_i$ 和未完成的会话 $s$, 获得会话 $s$ 的内部状态。

除此之外, 攻击者还可以使用 $SessionExpiration(P_i,s)$ 提供一个参与方 $P_i$ 和已完成的会话 $s$, 使会话 $s$ 过期, 从参与方 $P_i$ 的存储器里删除会话 $s$ 的会话密钥 $SK$。

定义 2. 匹配会话。密钥交换参与方 $P_i$ 内部的密钥交换协议输入为 $(P_i,P_j,s,role)$ 的四元组, 其中 $P_i$ 和 $P_j$ 为参与密钥交换的两个参与方, $s$ 为会话标识, $role$ 代表参与方的身份,包含 $initiator$ 和 $responder$ 两种身份。其中 $initiator$ 代表会话的发起者, $responder$ 代表会话的回应者。若 $P_i$ 的输入为 $(P_i,P_j,s,initiator)$, $P_j$ 的输入为 $(P_j',P_i',s',responder)$, 其中 $P_i=P_i'$, $P_j=P_j'$, $s=s'$, 则称它们的会话为匹配会话。

定义 3. 会话暴露。若攻击者执行以下查询, 则称会话 $s$ 为本地暴露:

(1) 在会话 $s$ 过期前使用 $Corrupt(P_i)$ 查询。

(2) 对会话 $s$ 使用查询。

(3) 对会话 $s$ 使用 $SessionState(P_i,s)$ 查询。

如果一个会话或其匹配会话本地暴露, 称该会话为会话暴露。

定义 4. 会话密钥安全。对于 UM 中任意攻击者 $\mathcal{A}$, 满足以下条件时, 称该方案在 UM 中是会话密钥安全的。

(1) 两个未被腐化的参与者完成了匹配会话, 并并输出了相同的会话密钥。

(2) 在以下游戏中如果对于任意 $\mathcal{PPT}$ 攻击者 $\mathcal{A}$, 优势 $Adv_{\mathcal{A}}(\lambda)$ 可忽略。

CK 安全模型可通过攻击者 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 之间的游戏定义, 该游戏包含以下几个阶段。

系统建立阶段. 挑战者利用安全参数 $\lambda$, 生成多个会话参与方 $P$ 的公私钥对 $(pk,sk)$, 并将公钥 $pk$ 发送给攻击者。

询问阶段 1. 攻击者调用密钥交换协议, 并适应性地向挑战者询问 $Corrupt(P_i)$、$SessionKey(P_i,s)$ 和 $SessionState(P_i,s)$, 但是不能使用 $SessionExpiration(P_i,s)$ 令会话过期。

挑战阶段. 攻击者选择一个已完成、未到期并且未暴露的会话 $s$ 作为测试会话。$SK$ 为该会话的会话密钥。挑战者随机选择一位比特 $b\in\{0,1\}$, 如果 $b=0$ 返回会话密钥 $SK$, 如果 $b=1$ 返回与会话密钥同分布的随机值。

询问阶段 2. 攻击者调用密钥交换协议, 并可以适应性地向挑战者询问, 但不能暴露测试会话。

猜测阶段. 攻击者输出对 $b$ 的猜测 $b'$。若 $b=b'$ 则攻击者在上述游戏中获胜。

定义攻击者 $\mathcal{A}$ 在游戏中获胜的优势为:

$$Adv_{\mathcal{A}}(\lambda)=|Pr[b=b']-1/2|$$

定义 5. 满足前向安全性的会话密钥安全对于 UM 中任意攻击者 $\mathcal{A}$,满足以下条件时, 称该方案在 UM 中是满足前向安全性的会话密钥安全的。

(1) 两个未被腐化的参与者完成了匹配会话, 并并输出了相同的会话密钥。

(2) 在以下游戏中如果对于任意 $\mathcal{PPT}$ 攻击者 $\mathcal{A}$, 优势 $Adv_{\mathcal{A}}(\lambda)$ 可忽略。

CK 安全模型可通过攻击者 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 之间的游戏定义, 该游戏包含以下几个阶段。

系统建立阶段. 挑战者利用安全参数 $\lambda$, 生成多个会话参与方 $P$ 的公私钥对 $(pk,sk)$, 并将公钥 $pk$ 发送给攻击者。

询问阶段 1. 攻击者调用密钥交换协议, 并适应性地向挑战者询问 $Corrupt(P_i)$、$SessionKey(P_i,s)$ 和 $SessionKey(P_i,s)$ $SessionState(P_i,s)$, 但是可以使用 $SessionExpiration$ $(P_i,s)$ 令会话过期。

挑战阶段. 攻击者选择一个已完成并且未暴露的会话 $s$ 作为测试会话。$SK$ 为该会话的会话密钥。挑战者随机选择一位比特 $b\in\{0,1\}$, 如果 $b=0$ 返回会话密钥 $SK$, 如果 $b=1$ 返回与会话密钥同分布的随机值。

询问阶段 2. 攻击者调用密钥交换协议, 并可以适应性地向挑战者询问, 但不能暴露测试会话。

猜测阶段. 攻击者输出对 $b$ 的猜测 $b'$。若 $b=b'$ 则攻击者在上述游戏中获胜。

定义攻击者 $\mathcal{A}$ 在游戏中获胜的优势为:

$$Adv_{\mathcal{A}}(\lambda)=|Pr[b=b']-1/2|$$

## 3 方案构造

本节基于SM2数字签名算法设计非交互/交互两种区块链匿名密钥交换协议。方案流程和算法具体构造如下:

### 3.1 方案流程

本方案包括用户 *Alice*、用户 *Bob* 和区块链三个实体, 系统流程如图 1 所示, 使用流程如下: 区块链首先调用初始化算法确定系统参数 $pp$, 将系统参数 $pp$ 分享给其他实体。用户 *Alice* 和 *Bob* 分别调用密钥对生成算法产生公私钥对 $(pk_A,sk_A)$ 和 $(pk_B,sk_B)$。然后, 用户 *Alice* 和 *Bob* 分别在区块链上发布交易内容 $T_A$、$T_B$, 即 *Alice* 和 *Bob* 分别利用私钥调用交易签名算法对交易签名, 签名分别为 $(r_A,s_A)$、$(r_B,s_B)$。交易 $T_A$、$T_B$ 及交易签名上链后, 用户 *Alice* 和 *Bob* 可以基于交易签名进行密钥交换: 执行非交互式密钥交换协议或交换式密钥交换协议计算会话密钥 $SK$。

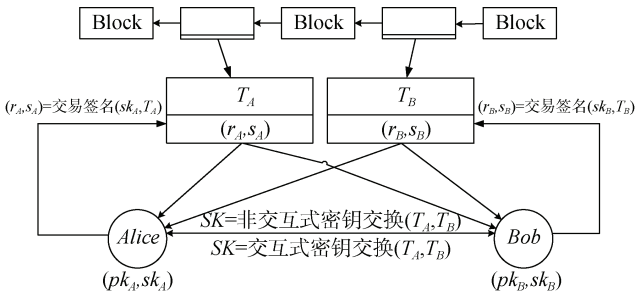


**图 1 系统流程**

**Figure 1 System flow**

### 3.2 算法构造

为了算法描述, 本文统一描述两种协议的共同部分(初始化、密钥对生成、交易签名、交易验证 4 个算法), 并分别描述非交互式与交互式 2 个密钥交换协议。

初始化算法: 算法输入安全参数 $\lambda$, 随机选取大素数 $q$, 确定非奇异椭圆曲线 $E:y^2=x^3+ax+b(mod\ q)$ (其中, $a,b\in\mathbb{Z}_q^*$), 在 $E$ 所有点 (包含无穷远点) 中选取素数 $n$ 阶循环群 $\mathbb{G}$ 以及生成元 $G\in\mathbb{G}$。选取安全哈希函数 $\mathcal{H}:\{0,1\}^*\to\mathbb{Z}_n^*$、零知识证明函数 $ZKP(X,G,x)$、验证函数 $VERZKP$、密钥派生函数 $KDF$ 和解压函数 $uncompress$。算法输出系统参数 $pp=(E,a,b,q,\mathbb{G},n,G,\mathcal{H},ZKP,VerZKP,KDF,uncompress)$。本文参数使用与 SM2 椭圆曲线公钥密码算法相同的椭圆曲线参数。

**表 1 符号说明**

**Table 1 Symbol**

| | |
|---|---|
| $uncompress(x,sign)$ | 根据 $x$ 轴的坐标和符号, 解压还原椭圆曲线中的点 |
| $ZKP(X,G,x)$ | 零知识证明函数, 以零知识形式证明 $X=xG$ |
| $\pi$ | 零知识证明函数生成的证明 |
| $VERZKP(X,G,\pi)$ | 零知识证明验证函数, 验证零知识证明的正确性, 相信证明者确实拥有 $x$ 满足 $X=xG$ |
| $T_A$ | 区块链中 *Alice* 的交易 |
| $(r,s)$ | 区块链交易中的签名 |
| $d_A$ | *Alice* 的私钥 |
| $k_A$ | 实际 *Alice* 交易签名中的随机数和交易私钥 |
| $\hat{k}_A$ | 估计 *Alice* 交易签名中的随机数和交易私钥 |
| $Q_A$ | 实际 *Alice* 的交易公钥 |
| $\hat{Q}_A$ | 估计 *Alice* 的交易公钥 |
| $w_A$ | *Alice* 密钥交换中的临时私钥 |
| $W_A$ | *Alice* 密钥交换中的临时公钥 |
| $x_{AB}$ | *Alice* 和 *Bob* 的共同秘密值 |
| $KDF$ | 密钥派生函数 |
| $SK$ | 会话密钥 |

密钥对生成算法: 算法输入系统参数 $pp$, 随机选取 $d\in\mathbb{Z}_n^*$, 计算 $P=dG$, 算法输出用户的私钥 $sk=d$、公钥 $pk=P$。

交易签名算法: 算法输入系统参数 $pp$、用户私钥 $sk=d$ 和交易内容 $T$, 执行如下运算:

A.1 随机选取随机数 $k\in\mathbb{Z}_n^*$, 并计算 $K=kG=(x_K,y_K)$;

A.2 计算 $e=\mathcal{H}(T)$ 和 $r=(e+x_K)(mod\ n)$. 若 $r=0$ 或 $r+k=n$, 重新选取 $k$ 再计算;

A.3 计算 $s=(1+d)^{-1}(k-rd)(mod\ n)$. 若 $s=0$, 返回第一步重新选取随机数, 否则输出签名 $\sigma=(r,s)$。

交易验证算法: 算法输入系统参数 $pp$、用户公钥 $pk=P$、交易内容 $T$ 和待验证交易签名 $\sigma=(r,s)$, 执行如下运算:

B.1 若 $r,s\notin\mathbb{Z}_n^*$, 则输出 0 表示无效;

B.2 计算 $t=(r+s)(mod\ n)$。若 $t=0$, 则输出 0 表示无效;

B.3 计算 $e'=\mathcal{H}(T)$, $K'=sG+tP=(x'_K,y'_K)$;

B.4 计算 $r'=(e'+x'_K)\ (mod\ n)$。若 $r'=r$, 则输出 1 表示交易有效, 否则输出 0 表示无效。

非交互式密钥交换: 协议输入系统参数 $pp$, 用户 *Alice* 和 *Bob* 在区块链上分别发布的交易 $T_A$, $T_B$ 以及其签名 $(r_A,s_A)$, $(r_B,s_B)$。*Alice* 和 *Bob* 执行以下

计算:

*Alice*:

C.1 使用私钥计算 *Alice* 交易签名中随机数 $k_A=(s_A(1+d_A)+r_Ad_A)(mod\ n)$;

C.2 计算 $x_B=(r_B-\mathcal{H}(T_B))(mod\ n)$;

C.3 计算交易公钥 $\hat{Q}_B=uncompress(x_B,+)$;

C.4 计算共同秘密 $k_A\hat{Q}_B=(x_{AB},\pm y_{AB})$;

C.5 计算并输出会话密钥 $SK_A=KDF(x_{AB})$;

*Bob*:

C.6 使用私钥计算 *Bob* 交易签名中随机数 $k_B=(s_B(1+d_B)+r_Bd_B)(mod\ n)$;

C.7 计算 $x_A=(r_A-\mathcal{H}(T_A))(mod\ n)$;

C.8 计算交易公钥 $\hat{Q}_A=uncompress(x_A,+)$;

C.9 计算共同秘密 $k_B\hat{Q}_A=(x_{AB},\pm y_{AB})$;

C.10 计算并输出会话密钥 $SK_B=KDF(x_{AB})$。

交互式密钥交换: 协议输入系统参数 $pp$, 用户 *Alice* 和 *Bob* 在区块链上分别发布的交易 $T_A$, $T_B$ 以及其签名 $(r_A,s_A)$, $(r_B,s_B)$。*Alice* 和 *Bob* 执行以下交互:

*Alice*:

D.1 使用私钥计算 *Alice* 交易签名中随机数 $k_A=(s_A(1+d_A)+r_Ad_A)(mod\ n)$;

D.2 计算 $x_B=r_B-\mathcal{H}(T_B)(mod\ n)$;

D.3 计算交易公钥 $Q_A=k_AG=(x_A,y_A)$;

D.4 计算估计交易公钥 $\hat{Q}_A=uncompress(x_A,+)$ 和 $\hat{Q}_B=uncompress(x_B,+)$, 若 $Q_A=\hat{Q}_A$, 则令 $\hat{k}_A=k_A$, 否则 $\hat{k}_A=-k_A$;

D.5 随机选取交易私钥 $w_A\in[1,n-1]$, 计算交易公钥 $W_A=w_AG$, $\pi_A=ZKP(W_A,G,w_A)$, 将 $(W_A,\pi_A)$ 发送给 *Bob*;

*Bob*:

D.6 调用 $VerZKP(W_A,G,\pi_A)$ 验证 $\pi_A$ 的有效性, 若 $VerZKP(W_A,G,\pi_A)=0$ 则退出, 否则进入下一步;

D.7 使用私钥计算 *Bob* 交易签名中随机数 $k_B=(s_B(1+d_B)+r_Bd_B)(mod\ n)$;

D.8 计算 $x_A=(r_A-\mathcal{H}(T_A))(mod\ n)$;

D.9 计算交易公钥 $Q_B=k_BG=(x_B,y_B)$;

D.10 计算估计交易公钥 $\hat{Q}_A=uncompress(x_A,+)$ 和 $\hat{Q}_B=uncompress(x_B,+)$。若 $Q_B=\hat{Q}_B$, 则令 $\hat{k}_B=k_B$, 否则 $\hat{k}_B=-k_B$;

D.11 随机选取交易私钥 $w_B\in[1,n-1]$, 计算交易公钥 $W_B=w_BG$;

D.12 计算 $\pi_B=ZKP(W_B,G,w_B)$, 将 $(W_B,\pi_B)$ 发送给 *Alice*;

D.13 计算共同秘密 $(x_{AB},y_{AB})=(\hat{k}_B+w_B)(\hat{Q}_A+W_A)$。最后计算会话密钥 $SK_B=KDF(x_{AB})$。

*Alice*:

D.14 调用 $VerZKP(W_B,G,\pi_B)$ 验证 $\pi_B$ 的有效性, 若 $VerZKP(W_B,G,\pi_B)=0$ 则退出, 否则计算共同秘密 $(x_{AB},y_{AB})=(\hat{k}_A+w_A)(\hat{Q}_B+W_B)$;

D.15 计算并输出会话密钥 $SK_A=KDF(x_{AB})$。

## 4 安全性分析

本节在 CK 模型中分析了非交互式密钥交换协议和交互式密钥交换协议的安全性。

### 4.1 非交互式密钥交换

定理 1. 在 DDH 安全假设下, 基于 SM2 数字签名的非交互式密钥交换协议在 UM 下的随机谕言模型中满足会话密钥安全。

证明: 如果非交互式密钥交换协议满足定义 4 的两个条件, 则该协议在 UM 下的随机谕言模型中满足会话密钥安全。

(1)在协议的交互过程中, 双方均没有被攻击者腐化。双方分别计算的共同秘密值 $x_{AB}$:

$$\begin{aligned}(x_{AB},y_{AB})&=k_A\hat{Q}_B\\&=(s_A(1+d_A)+r_Ad_A)(s_BG+(r_B+s_B)P_B)\\&=s_As_BG+(s_As_B+r_As_B)d_AG+(s_As_B+r_Bs_A)\\&\quad d_BG+(r_Ar_B+s_As_B+r_Bs_A+r_As_B)d_Ad_BG\end{aligned}$$

$$\begin{aligned}(x_{AB},y_{AB})&=k_B\hat{Q}_A\\&=(s_B(1+d_B)+r_Bd_B)(s_AG+(r_A+s_A)P_A)\\&=s_As_BG+(s_As_B+r_As_B)d_AG+(s_As_B+r_Bs_A)\\&\quad d_BG+(r_Ar_B+s_As_B+r_Bs_A+r_As_B)d_Ad_BG\end{aligned}$$

因此, 双方拥有相等的秘密值 $x_{AB}$, 建立相同的会话密钥 $SK_A=SK_B=KDF(x_{AB})$。

(2)假设在非认证链路模型中, 存在一个攻击者 $\mathcal{A}$ 以不可忽略的优势 $\varepsilon$ 区分测试会话的会话密钥 $SK$ 是真实的还是随机的。则存在输入为 $(pp,D_v)$ 的算法 $\mathcal{D}$, 通过调用 $\mathcal{A}$ 以不可忽略的优势解决 DDH 困难问题。其中 $pp$ 为系统参数, $v\in\{0,1\}$ $D_0=(A=aP,B=bP,C=abP)$, $D_1=(A=aP,B=bP,\ C=cP)$, 其中 $a,b,c\in\mathbb{Z}_n^*$ 且未知。

系统建立阶段. 假设 $\mathcal{A}$ 发起的会话轮数为 $L$。

$\mathcal{D}$ 选择随机数 $r\in[1,L]$。随机选择 $r_A^*$、$s_A^*$、$r_B^*$、$s_B^*\in\mathbb{Z}_n^*$ 作为第 $r$ 轮会话中 *Alice* 和 *Bob* 对交易内容 $T_A$、$T_B$ 的签名。在非第 $r$ 轮会话, 随机选择 $d_A,d_B$ 计算公钥 $P_A=d_AG$、$P_B=d_BG$。第 $r$ 轮会话将困难问题实例 $aG$, $bG$ 作为 *Alice* 和 *Bob* 的公钥 $P_A$、$P_B$。最后 $\mathcal{D}$ 将公钥返回给 $\mathcal{A}$。

询问阶段 1. $\mathcal{D}$ 控制一个记录所有询问和回应的哈希表, 开始哈希表是空的。如果 $\mathcal{A}$ 询问的交易内容 $T$ 已经在表中, 则 $\mathcal{D}$ 根据哈希表中的内容回应, 否则根据以下规则回应: 若 $\mathcal{A}$ 询问第 $r$ 轮会话以外的交易内容 $T$ 的哈希值, 则随机选择 $\mathcal{H}(T)=e\in\mathbb{Z}_n^*$, 并将 $(T,\mathcal{H}(T))$ 加入哈希表。若 $\mathcal{A}$ 询问第 $r$ 轮会话中 *Alice* 或 *Bob* 的交易内容 $T_A$、$T_B$ 对应的哈希值, 则 $\mathcal{D}$ 计算 $(x_{kA},y_{kA})=K=s_AG+(r_A+s_A)P_A$, $\mathcal{H}(T_A)=r_A-x_{kA}$, $(x_{kB},y_{kB})=K=s_BG+(r_B+s_B)P_B$, $\mathcal{H}(T_B)=r_B-x_{kB}$。$\mathcal{D}$ 将 $\mathcal{H}(T_A)$ 或 $\mathcal{H}(T_B)$ 返回给 $\mathcal{A}$, 并将 $(T_A,\mathcal{H}(T_A))$ 和 $(T_B,\mathcal{H}(T_B))$ 加入哈希表。

$\mathcal{A}$ 适应性地向 $\mathcal{D}$ 询问 *Corrupt*$(P)$、*SessionKey*$(P,s)$ 和 *SessionState*$(P,s)$。除第 $r$ 轮会话以外, 若 $\mathcal{A}$ 使用 *Corrupt*$(P)$ 腐化参与者 $P$, 则 $\mathcal{D}$ 将参与者 $P$ 的所有信息发送给 $\mathcal{A}$。若 $\mathcal{A}$ 使用 *SessionKey*$(P,s)$ 查询参与者 $P$ 的会话密钥, 则 $\mathcal{D}$ 把会话 $s$ 的会话密钥 *SK* 发送给 $\mathcal{A}$。若 $\mathcal{A}$ 使用 *SessionState*$(P,s)$ 查询参与者 $P$ 的内部状态, 则 $\mathcal{D}$ 将参与者 $P$ 的内部状态发送给 $\mathcal{A}$。

挑战阶段. 在第 $r$ 轮会话中, $\mathcal{A}$ 输入 (*Alice*, *Bob*,$s$) 调用 *Alice* 和 *Bob* 的会话, *Alice* 发布交易 $(Alice,s,(r_A^*,s_A^*))$。*Bob* 收到 $(Alice,s,(r_A^*,s_A^*))$ 后, 发布交易 $(Bob,s,(r_B^*,s_B^*))$。

如果 $\mathcal{A}$ 选择会话 $(Alice,Bob,s)$ 作为测试会话, 那么向 $\mathcal{A}$ 提供 $s_A^*s_B^*G+(s_A^*s_B^*+r_A^*s_B^*)P_A+(s_A^*s_B^*+r_B^*s_A^*)P_B+(r_A^*r_B^*+s_A^*s_B^*+r_B^*s_A^*+r_A^*s_B^*)C$ 作为询问应答。

询问阶段 2. $\mathcal{A}$ 继续适应性地向 $\mathcal{D}$ 询问 *Corrupt*$(P)$、*SessionKey*$(P,s)$ 和 *SessionState*$(P,s)$, 但是不能使测试会话暴露。

猜测阶段. 如果会话 $(Alice,Bob,s)$ 会话暴露, 或者 $\mathcal{A}$ 选择第 $r$ 轮会话外的会话作为测试会话, 或者 $\mathcal{A}$ 没有选择测试会话就终止了, 那么 $\mathcal{D}$ 随机输出比特 $b\in\{0,1\}$ 然后终止。如果 $\mathcal{A}$ 中止并输出比特 $b$, 那么 $\mathcal{D}$ 中止并且输出相同的比特 $b$。

优势分析: 情况 1: $\mathcal{A}$ 选择的测试会话 $s$ 为 $\mathcal{D}$ 随机选择的第 $r$ 轮会话。若 $\mathcal{D}$ 的输入为 $D_0=(A=aP,B=bP,C=abP)$, 则 $\mathcal{A}$ 的询问应答就是 *Alice* 和 *Bob* 在会话 $s$ 中真实的会话密钥。如果 $\mathcal{D}$ 的输入为 $D_1=(A=aP,B=bP,C=cP)$, 则给 $\mathcal{A}$ 的询问应答就是随机值。若测试会话中 $\mathcal{A}$ 正确区分会话密钥和随机值的概率是 $1/2+\varepsilon$, 则 $\mathcal{D}$ 正确区分会话密钥和随机值的概率也等于 $1/2+\varepsilon$。因此, $\mathcal{D}$ 有不可忽略的优势解决 DDH 困难问题。

情况 2: $\mathcal{A}$ 选择的测试会话 $s$ 和 $\mathcal{D}$ 随机选择的会话不同。$\mathcal{D}$ 输出一个随机比特后结束会话, 这时 $\mathcal{D}$ 正确区分会话密钥和随机值的概率是 $1/2$。

$\mathcal{A}$ 选择第 $r$ 轮会话作为测试会话的概率为 $1/L$, 因此, $\mathcal{D}$ 解决困难问题的概率为 $(1/2+\varepsilon)(1/L)+(1/2)(1-(1/L))=1/2+\varepsilon/L$, 说明 $\mathcal{D}$ 解决 DDH 安全假设的优势为 $\varepsilon/L$。

## 4.2 交互式密钥交换

定理 2.在 DDH 安全假设下, 基于 SM2 数字签名的交互式密钥交换协议在 UM 中满足带有前向安全性的会话密钥安全。

证明: 如果非交互式密钥交换协议满足定义 5 的两个条件, 则该协议在 UM 中满足带有前向安全性的会话密钥安全。

(1)在协议的交互过程中, 双方均没有被攻击者腐化。双方分别计算的共同秘密值 $x_{AB}$:

$$\begin{aligned}(x_{AB},y_{AB})&=(\hat{k}_A+w_A)(\hat{Q}_B+W_B)\\&=\hat{k}_A\hat{Q}_B+\hat{k}_AW_B+w_A\hat{Q}_B+w_AW_B\\&=(s_A(1+d_A)+r_Ad_A)(s_BG+(r_B+s_B)P_B)\\&\quad+(s_A(1+d_A)+r_Ad_A)w_BG\\&\quad+w_A(s_BG+(r_B+s_B)P_B)+w_Aw_BG\\&=s_As_BG+(s_As_B+r_As_B)d_AG+(s_As_B+r_Bs_A)d_BG\\&\quad+(r_Ar_B+s_As_B+r_Bs_A+r_As_B)d_Ad_BG\\&\quad+s_Aw_BG+s_Bw_AG+(r_A+s_A)d_Aw_BG\\&\quad+(r_B+s_B)d_Bw_AG+w_Aw_BG\end{aligned}$$

$$\begin{aligned}(x_{AB},y_{AB})&=(\hat{k}_B+w_B)(\hat{Q}_A+W_A)\\&=\hat{k}_B\hat{Q}_A+\hat{k}_BW_A+w_B\hat{Q}_A+w_BW_A\\&=(s_B(1+d_B)+r_Bd_B)(s_AG+(r_A+s_A)P_A)\\&\quad+(s_B(1+d_B)+r_Bd_B)w_AG\\&\quad+w_B(s_AG+(r_A+s_A)P_A)+w_Aw_BG\\&=s_As_BG+(s_As_B+r_As_B)d_AG+(s_As_B+r_Bs_A)d_BG\\&\quad+(r_Ar_B+s_As_B+r_Bs_A+r_As_B)d_Ad_BG\\&\quad+s_Aw_BG+s_Bw_AG+(r_A+s_A)d_Aw_BG\\&\quad+(r_B+s_B)d_Bw_AG+w_Aw_BG\end{aligned}$$

因此, 双方拥有相等的秘密值 $x_{AB}$, 建立相同的会话密钥 $SK_A=SK_B=KDF(x_{AB})$。

(2)假设在认证链路模型中, 存在一个攻击者 $\mathcal{A}$ 以不可忽略的优势 $\varepsilon$ 区分测试会话的会话密钥 *SK* 是

真实的还是随机的。则存在输入为 $(pp, D_v)$ 的算法 $\mathcal{D}$，通过调用 $\mathcal{A}$ 以不可忽略的优势解决 DDH 困难问题。其中 $pp$ 为系统参数，$v \in \{0,1\}$，$D_0 = (A = aP, B = bP, C = abP)$，$D_1 = (A = aP, B = bP, C = cP)$，其中 $a, b, c \in \mathbb{Z}_n^*$ 且未知。

系统建立阶段. 假设 $\mathcal{A}$ 发起的会话轮数为 $L$，$\mathcal{D}$ 选择随机数 $r \in [1, L]$。随机选择 $d_A, d_B$ 计算公钥 $P_A = d_A G$、$P_B = d_B G$。最后 $\mathcal{D}$ 将公钥返回给 $\mathcal{A}$。

询问阶段 1. $\mathcal{A}$ 适应性地向 $\mathcal{D}$ 询问 $Corrupt(P)$、$SessionKey(P, s)$ 和 $SessionState(P, s)$。除第 $r$ 轮会话以外，若 $\mathcal{A}$ 使用 $Corrupt(P)$ 腐化参与者 $P$，则 $\mathcal{D}$ 将参与者 $P$ 的所有信息发送给 $\mathcal{A}$。若 $\mathcal{A}$ 使用 $SessionKey(P, s)$ 查询参与者 $P$ 的会话密钥，则 $\mathcal{D}$ 把会话 $s$ 的会话密钥 $SK$ 发送给 $\mathcal{A}$。若 $\mathcal{A}$ 使用 $SessionState(P, s)$ 查询参与者 $P$ 的内部状态，则 $\mathcal{D}$ 将参与者 $P$ 的内部状态发送给 $\mathcal{A}$。

挑战阶段. 第 $r$ 轮会话中，输入 $(Alice, Bob, s)$ 调用 *Alice* 和 *Bob* 的会话，*Alice* 调用模拟器生成零知识证明 $\pi_A$，并向 *Bob* 发送 $(Alice, s, (A, (R_A, \pi_A)))$。*Bob* 收到 $(Alice, s, (A, (R_A, \pi_A)))$ 后，调用模拟器生成零知识证明 $\pi_B$，并向 *Alice* 发送 $(Bob, s, (B, (R_B, \pi_B)))$。

如果 $\mathcal{A}$ 选择会话 $(Alice, Bob, s)$ 作为测试会话，那么向 $\mathcal{A}$ 提供 $s_A s_B G + (s_A s_B + r_A s_B) d_A G + (s_A s_B + r_B s_A) d_B G + (r_A r_B + s_A s_B + r_B s_A + r_A s_B) d_A d_B G + s_A B + s_B A + (r_A + s_A) d_A B + (r_B + s_B) d_B A + C$ 作为询问的应答。

询问阶段 2. $\mathcal{A}$ 继续适应性地向 $\mathcal{D}$ 询问 $Corrupt(P)$、$SessionKey(P, s)$ 和 $SessionState(P, s)$，并可以使用 $SessionExpiration(P, s)$ 令测试会话到期，但是不能使测试会话暴露。

猜测阶段. 如果会话 $(Alice, Bob, s)$ 暴露，或者 $\mathcal{A}$ 选择第 $r$ 轮会话外的会话作为测试会话，或者 $\mathcal{A}$ 没有选择测试会话就终止了，那么 $\mathcal{D}$ 随机选择 $b \in \{0,1\}$ 输出然后终止。如果 $\mathcal{A}$ 中止并输出比特 $b$，那么 $\mathcal{D}$ 中止并且输出相同的比特 $b$。

因为零知识证明具有零知识性，*Alice* 和 *Bob* 可以调用模拟器 simulator 生成零知识证明 $\pi$，同时没有向 $\mathcal{A}$ 透露任何知识。

优势分析: 情况 1: $\mathcal{A}$ 选择的测试会话 $s$ 和 $\mathcal{D}$ 随机选择的会话相同。如果 $\mathcal{D}$ 的输入为 $D_0 = (A = aP, B = bP, C = abP)$，则给 $\mathcal{A}$ 的询问应答就是 *Alice* 和 *Bob* 在会话 $s$ 中真实的会话密钥。如果 $\mathcal{D}$ 的输入为 $D_1 = (A = aP, B = bP, C = cP)$，则给 $A$ 的询问应答就是随机值。在测试会话中 $\mathcal{A}$ 正确区分会话密钥和随机值的概率是 $1/2 + \varepsilon$。因此，$D$ 正确区分会话密钥和随机值的概率也等于 $1/2 + \varepsilon$，这说明 $\mathcal{D}$ 有不可忽略的优势解决 DDH 困难问题。

情况 2: $\mathcal{A}$ 选择的测试会话 $s$ 和 $\mathcal{D}$ 随机选择的会话不同。$\mathcal{D}$ 输出一个随机比特后结束会话，这时 $\mathcal{D}$ 正确区分会话密钥和随机值的概率是 $1/2$。

$\mathcal{A}$ 选择第 $r$ 轮会话作为测试会话的概率为 $1/L$，因此，$\mathcal{D}$ 解决困难问题的概率为 $(1/2 + \varepsilon)(1/L) + (1/2)(1 - (1/L)) = 1/2 + \varepsilon/L$，说明 $\mathcal{D}$ 解决 DDH 安全假设的优势为 $\varepsilon/L$。

## 5 功能对比与性能分析

### 5.1 功能对比

将本文方案与 SM2 的密钥交换方案、文献[7]、文献[9]、文献[10]、文献[1]进行对比，对比结果如表 2 所示。

**表 2 密钥交换方案功能对比**

**Table 2 Features comparison of key exchange schemes**

| 方案 | 身份认证 | 会话密钥安全 | 前向安全 | 匿名 | 国密 | 可证明安全 | 安全模型 |
|---|---|---|---|---|---|---|---|
| SM2 密钥交换 | ✓ | ✓ | | | ✓ | ✓ | CK |
| [7]中密钥交换 | ✓ | ✓ | | | | ✓ | BPR[8] |
| [9]中密钥交换 | | ✓ | | ✓ | | | 无 |
| [10]中 DAKE1 | | ✓ | | | | | 无 |
| [10]中 DAKE2 | | ✓ | ✓ | | | | 无 |
| [10]中 DAKE3 | ✓ | ✓ | ✓ | | | | 无 |
| [10]中 DAKE4 | ✓ | ✓ | ✓ | | | | 无 |
| [10]中 DAKE5 | ✓ | ✓ | ✓ | | | | 无 |
| [1]中非交互密钥交换 | ✓ | ✓ | | ✓ | | | 无 |
| [1]中交互密钥交换 | ✓ | ✓ | ✓ | ✓ | | | 无 |
| 本文非交互密钥交换 | ✓ | ✓ | | ✓ | ✓ | ✓ | CK |
| 本文交互密钥交换 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | CK |

由表 2 对比可以看出, SM2 密钥交换缺少匿名功能。SM2 密钥交换协议需要借助公钥基础设施认证密钥交换双方的身份。公钥基础设施与用户的现实身份绑定, 在区块链匿名场景下会泄露用户的隐私, 因此无法满足匿名性。而文献[9]中密钥交换没有对身份进行认证, 无法抵抗假冒攻击。

文献[10]中的 DAKE1 和 DAKE2 虽然可以完成密钥协商, 但是缺少身份认证的功能。同时 5 种 DAKE 协议都无法实现用户的匿名性, 并且没有形式化的安全性证明。

而文献[1]中的密钥交换协议虽然满足匿名性, 但是不适用于国产区块链平台, 并且缺少形式化的安全性证明。

### 5.2 性能分析

本节主要将本文协议与文献[1]和[7]进行性能分析与对比。

为了清晰描述理论分析理论结果, 后文使用 $T_{em}$ 表示椭圆曲线上的乘法运算用时, 使用 $T_{eadd}$ 表示椭圆曲线上的加法运算用时, 使用 $T_{inv}$ 表示 $\mathbb{Z}_q^*$ 上的模逆运算用时, 使用 $T_m$ 表示 $\mathbb{Z}_q^*$ 上的乘法运算用时, 使用 $T_H$ 表示安全的哈希运算用时, 使用 $T_c$ 表示字符串对比用时, 使用 $k$ 代表文献[7]中密钥交换双方共同利益的个数, 使用 $T_{ZKP}$ 表示零知识证明的运算用时。

如表 3 所示, 文献[7]中密钥交换在算法运行过程中需要执行 4 次区块链上的交易, 而文献[1]中密钥交换和本文密钥交换的区块链交易可在密钥交换算法运行前完成, 因此不影响密钥交换协议的运行时间。区块链的交易耗时远大于本地计算耗时, 可见与文献[7]中密钥交换方案相比, 文献[1]中和本文密钥交换方案的效率更高, 在实际应用中有明显的优势。而文献[1]中非交互式密钥交换和本文非交互式密钥交换都需要 1 次椭圆曲线上的乘法运算, 3 次有限域上的乘法运算和 1 次安全哈希运算, 但 SM2 非交互式密钥交换无需模逆运算。交互式密钥交换中, 文献[1]中的方案与本文方案均需要进行 3 次椭圆曲线上的乘法运算, 1 次椭圆曲线上的加法运算, 4 次有限域上的乘法运算, 2 次零知识证明运算。而文献[1]中的方案需要 1 次模逆运算和 1 次安全哈希运算, 而本文方案无需模逆运算, 但需要 2 次安全哈希运算。因为本文方案与文献[1]中的方案在椭圆曲线上的运算数量相同, 而模逆运算和安全哈希运算等运算相对于椭圆曲线上的运算相比开销较小, 因此本文方案与文献[1]中的方案计算开销相当。

**表 3 区块链密钥交换方案性能比较**

**Table 3 Performance comparison of blockchain key exchange schemes**

| 方案 | 区块链交易次数 | 用户通信次数 | 运行效率 |
|---|---|---|---|
| [7]中密钥交换 | 4 | 0 | $(5T_H+6T_c)k+T_H$ |
| [1]中非交互式密钥交换 | 0 | 0 | $T_{em}+3T_m+T_{inv}+T_H$ |
| [1]中交互式密钥交换 | 0 | 2 | $3T_{em}+T_{eadd}+4T_m+T_{inv}+T_H+2T_{ZKP}$ |
| 本文非交互式密钥交换 | 0 | 0 | $T_{em}+3T_m+T_H$ |
| 本文交互式密钥交换 | 0 | 2 | $3T_{em}+T_{eadd}+4T_m+2T_H+2T_{ZKP}$ |

为了得到实际的比较结果, 在相同测试环境下, 对本方案和方案[1]进行编程实现。具体测试设备为个人笔记本电脑, 配置为 16GB 内存, 64 位 Windows 10 操作系统, 使用 BouncyCastle 算法库, 椭圆曲线参数选用 SM2 椭圆曲线公钥密码算法中推荐的椭圆曲线参数。交易与交易签名由算法模拟产生, 两个密钥交换方案基于同一交易执行协议, 各自均执行 1000 次。

实验结果如图 2 所示, 其中横坐标表示各方案中对应算法, 纵坐标表示算法运行时间(单位为 ms)。本方案的非交互式密钥交换算法和交互式密钥交换算法用时分别为 1.13 ms 和 6.22 ms。方案[1]的非交互式密钥交换算法和交互式密钥交换算法用时分别为 1.15 ms 和 6.25 ms。可见与方案[1]相比, 本方案在没有增加计算开销与通信开销的情况下, 可满足国产区块链平台的匿名密钥交换需求。

## 6 总结

用户利用区块链完成交易后, 需要建立安全信道保证后续通信的安全。虽然区块链匿名密钥交换可以同时提供身份认证、匿名保护等功能, 但现有协议大都基于国外密码算法设计, 无法满足密码产品安全可控的需求。本文利用 SM2 椭圆曲线数字签名算法, 设计了适用于国产区块链的高效非交互式密钥交换协议和高安全交互式密钥交换协议, 并在 CK 模型中证明了两个协议的安全性。最后, 通过功能对比、性能评估和仿真实验对比, 验证了本文协议的实用性。

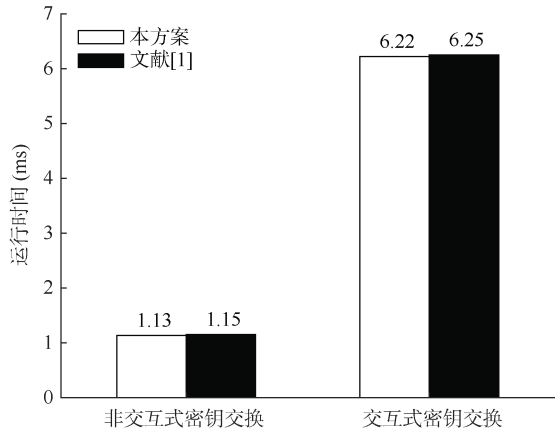


**图 2　方案运行时间比较**

**Figure 2　Comparison on the running time of schemes**

## 参考文献


[1] McCorry P, Shahandashti S F, Clarke D, et al. Authenticated Key Exchange over Bitcoin[C]. *The Second International Conference on Security Standardisation Research - Volume 9497*, 2015: 3-20.

[2] Johnson D, Menezes A, Vanstone S. The Elliptic Curve Digital Signature Algorithm (ECDSA)[J]. *International Journal of Information Security*, 2001, 1(1): 36-63.

[3] Diffie W, Hellman M. New Directions in Cryptography[J]. *IEEE Transactions on Information Theory*, 1976, 22(6): 644-654.

[4] Bellare M, Rogaway P. Entity Authentication and Key Distribution[C]. *The 13th Annual International Cryptology Conference on Advances in Cryptology*, 1993: 232-249.

[5] Miller V S. Use of elliptic curves in cryptography[C]. *Conference on the theory and application of cryptographic techniques*, 1985: 417-426.

[6] Hao F. On Robust Key Agreement Based on Public Key Authentication[C]. *The 14th international conference on Financial Cryptography and Data Security*, 2010: 383-390.

[7] Yao H L, Wang C F. A Novel Blockchain-Based Authenticated Key Exchange Protocol and Its Applications[C]. *2018 IEEE Third International Conference on Data Science in Cyberspace*, 2018: 609-614.

[8] Bellare M, Pointcheval D, Rogaway P. Authenticated Key Exchange Secure Against Dictionary Attacks[M]. *Advances in Cryptology — EUROCRYPT 2000*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000: 139-155.

[9] Bui T, Aura T. Key Exchange with the Help of a Public Ledger[C]. *Cambridge International Workshop on Security Protocols*, 2017: 123-136.

[10] Wu Q, Luo Y, Zhao Y, et al. DAKEs: Decentralized Authenticated Key Exchange Protocols via Blockchain for Smart City[J]. *Wireless Communications and Mobile Computing*, 2022, 2022: 3314051.

[11] Blum M, Feldman P, Micali S. Non-interactive zero-knowledge and its applications[M]. Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali. 2019: 329-349.

[12] State Cryptography Administration. Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves[S/OL]. 2020.12.

[13] Fiat A, Shamir A. How to Prove Yourself: Practical Solutions to Identification and Signature Problems[C]. *Proceedings on Advances in cryptology—CRYPTO'86*, 1987: 186-194.

[14] Canetti R, Krawczyk H. Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels[M]. *Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001: 453-474.


**黄佩达**　于 2021 年在北方工业大学信息安全专业获得学士学位。现在福建师范大学网络空间安全专业攻读硕士学位。研究领域为公钥密码学、区块链隐私保护。Email: huangpeida@foxmail.com

**林超**　于 2020 年在武汉大学网络空间安全专业获得博士学位。现任福建师范大学计算机与网络空间安全学院副教授。研究领域为应用密码学、区块链隐私保护。Email: cschaolin@163.com

**伍玮**　于 2011 年在澳大利亚伍伦贡大学信息安全专业获得博士学位。现任福建师范大学数学与统计学院教授。研究领域为密码学、信息安全。Email: weiwu@fjnu.edu.cn

**何德彪**　于 2009 年在武汉大学应用数学专业获得博士学位。现任武汉大学国家网络安全学院教授。研究领域为公钥密码学、网络与信息安全。Email: hedebiao@whu.edu.cn