基于 SM2 的标识认证密钥交换协议

王晓虎[1], 林 超[1], 伍 玮[2]

[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

摘要 会话密钥(Session Secret Key, SSK)可在远程实现各方之间的安全通信, 在实际的开放网络部署中具有重要地位。传统 SSK 主要是基于公钥基础设施的认证密钥交换(Authenticated Key Exchange, AKE)协议构建的, 因涉及证书的颁发、更新、撤销等繁琐操作, 面临昂贵的计算、通信和存储开销。虽然基于标识(Identity, ID)的 AKE(ID-AKE)协议可解决这个问题, 但目前的大部分 ID-AKE 协议均基于国外密码算法设计, 尚未见基于国产商用密码算法的 ID-AKE 协议在国内外刊物上正式发表, 不符合我国密码核心技术自主可控的要求。SM2 认证密钥交换(Authenticated Key Exchange From SM2, SM2-AKE)协议因具有高安全和高效率的特性, 在商用密码中得到广泛应用。但证书管理开销问题仍未被解决, 这将极大限制了 SM2-AKE 协议的应用与推广。文章于标识密码(Identity-based Cryptography, IBC)体系下采用类 Schnorr 签名密钥生成方法, 基于 SM2 设计了一种标识认证密钥交换 (SM2-ID-AKE)协议, 并在 CDH 安全假设和随机谕言模型下证明了该协议的安全性。最后的理论分析和仿真实验结果表明, 与现有的 ID-AKE 协议相比, 文章协议至少节省 66.67%的通信带宽和 34.05%的计算开销, 有效降低和减轻了系统的代价和负担, 更能够适应网络通讯部署等领域下不同用户的安全通信服务需求。

关键词 标识密码; SM2; 认证密钥交换
中图法分类号 TP309 DOI 号 10.19363/J.cnki.cn10-1380/tn.2024.03.07

SM2-based Identity-based Authentication Key Exchange Protocol

WANG Xiaohu[1], LIN Chao[1], WU Wei[2]

[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

Abstract The session secret key (SSK) plays a crucial role in the deployment of realistic open networks by allowing secure communication among parties at a remote location. Traditional session secret key is mainly built based on the authenticated key exchange (AKE) protocol of public key infrastructure (PKI), which faces expensive computation, communication and storage overheads due to the cumbersome operations involved in certificate issuance, renewal and revocation. Despite the fact that this issue can be resolved by the identity-based (ID) authenticated key exchange (ID-AKE) protocol, the bulk of ID-based authenticated key exchange protocols in use currently are designed based on foreign cryptographic methods. Additionally, there has been no formal publication of an ID-based authenticated key exchange protocol based on domestic commercial cryptographic algorithms in either local or foreign journals, which does not meet the independent and controllable requirements of China's core cryptographic technology. Because of its superior efficiency and high level of security, the authenticated key exchange from SM2 (SM2-AKE) protocol is frequently used in commercial cryptography. However, the issue with management overhead of certificate has not been resolved, which greatly limits the application and promotion of the authenticated key exchange protocol from SM2. This work uses the Schnorr-like signature's key generation technique in the context of the ID-based cryptography (IBC) system, to build the ID-based authenticated key exchange protocol (SM2-ID-AKE) from SM2. The security of the proposal is proved under the computational Diffie-Hellman (CDH) security assumption and random oracle model. The final theoretical analysis and simulation results demonstrate that, in comparison to the existing ID-based authenticated key exchange protocols, the proposed protocol saves at least 66.67% of the communication bandwidth and 34.05% of the computational overhead. This indeed effectively reduces the cost and burden of the system and will be better adapt to the security communication service needs of various users in the field of network communication deployment.

Key words identity-based cryptography; SM2; authenticated key agreement

通讯作者: 林超, 博士, 副教授, Email: linchao91@fjnu.edu.cn。
本课题得到国家自然科学基金项目 (No. 62032005, No. 62102089, No.U21A20466, No. 62372108) 资助。
收稿日期: 2022-06-17; 修改日期: 2022-09-22; 定稿日期: 2023-11-01

1 引言

国家密码管理局颁布的 SM2 椭圆曲线公钥密码算法是一种椭圆曲线公钥密码算法[1], 包括数据加密、数字签名和认证密钥交换(Authenticated Key Exchange, AKE)三类算法。其中, SM2 认证密钥交换协议因具有高安全和高效率的特性, 在商用密码中得到广泛应用。SM2 认证密钥交换协议主要包括系统初始化、用户密钥对生成和密钥交换三个阶段。通信双方可通过这三个阶段共同协商当前通信的会话密钥。

虽然 SM2 认证密钥交换协议安全高效且简单易用, 还能作为网络运营商技术标准化和技术安全性的参考模板, 但该协议基于公钥基础设施(Public Key Infrastructure, PKI)体系设计, 涉及证书的颁发、更新、撤销等内容, 需要昂贵的计算、通信和存储开销。这些开销随着用户数量增加而呈线性增长, 尤其是在用户量巨大的云计算和大数据背景下会更加显著。因此, 证书管理开销将成为 SM2 认证密钥交换协议广泛应用与推广的主要制约因素。

为了降低传统公钥系统的证书管理开销, Shamir[2]推出了标识密码(Identity-based Cryptography, IBC)的理念。该体系中, 用户公用信息不再由证书机构颁发, 而是与用户自身的唯一标识挂钩, 如身份证号、电话号码、IP 地址等。用户私有信息则通过可信第三方密钥生成中心(Key Generator Center, KGC)获取。以此便可保证, 仅拥有私钥的用户可查看标识加密的消息。随着标识密码学的不断发展, 国内外学者提出了一系列基于标识(Identity, ID)的 AKE(ID-AKE)协议, 而这些协议均是基于国外密码算法设计, 不符合我国密码核心技术自主可控的要求。目前尚未见基于国产商用密码算法的 ID-AKE 协议在国内外刊物上正式发表。

1.1 相关工作

本节从密钥交换方式和安全模型的角度介绍 ID-AKE 及其安全证明的发展进程。

密钥交换方式: 自 1984 年 Shamir 基于 ID 的密码学概念提出以来, ID-AKE 得到了广泛研究。Okamoto 等[3-4]使用与 Shamir 相同的密钥对构建方式, 提出类 ID-AKE 方案。2001 年, Boneh 和 Franklin[5]提出基于 Weil 线性对的标识加密方案。在 2002 年, Smart[6]基于文献[5]中的 IBE 方案在双线性对的假设下提出 ID-AKE 协议, 而此后的大部分 ID-AKE 协议也均是基于双线性对构建的。2007 年, Chen 等[7]提出将内置决策函数整合到协议中的方法。该函数能将安全性证明中的困难决策问题转换为简单的决策问题。同年, Zhu 等[8]提出无双线性对的 ID-AKE 协议。此后, 国内外学者又提出一系列无对(Bilinear Pairing-free)的 ID-AKE 协议[9-11]。2013 年, Brzuska 等[12]将 ID-AKE 应用到 EMV 系统, 使卡片和读卡器之间能够建立起安全通道。2019 年, Tomida 等[13]通过构造通讯双方的非对称双线性对, 提高了协议效率。到 2021 年, Tsai 等[14]提出具有高效撤销机制的抗泄漏 ID-AKE(Leakage-Resilient ID-AKE, LR-ID-AKE)协议。该协议能够有效地从系统中撤销密钥泄露的用户。

安全模型: 1997 年, Blake-Wilson 等[15]提出 BJM97 模型。该模型适用于公钥密码环境下 AKE 协议的安全性证明, 但并不能保证完美前向安全性。2001 年, Canetti 和 Krawczyk[16]提出 CK01 模型。该模型刻画了会话密钥安全的定义, 可用于密钥交换协议的标准化安全性证明。此后, Chen 等[17]基于 BJM97 安全模型提出 ID-BJM 模型, 该模型可适用于 IBC 环境。2007 年, LaMacchia 等[18]在 CK01 模型基础上, 提出增强型 CK(Enhanced Canetti-Krawczyk, eCK)模型。2009 年, Wang 等[19]基于 BJM97 提出另一种 IBC 环境下的 ID-mBJM 安全模型。ID-mBJM 和 ID-BJM 大致相同, 但由于前者不允许对参与方进行 Corrupt 查询, 导致其不满足后者的抗密钥泄露模仿(Key Compromise Impersonation, KCI)性。同年, Huang 和 Cao[20]将 eCK 模型扩展到基于标识的公钥密码体制, 提出 ID-eCK(ID-based Enhanced Canetti-Krawczyk)模型。随后, Wu 等[21]和 Wariki 等[22]分别在 2019 年和 2022 年基于 ID-eCK 提出改进的安全模型——基于身份的连续泄漏扩展 Canetti-Krawczyk (Identity-based Continuous-leakage Extended Canetti-Krawczyk, ID-CL-eCK) 模型和两个可捕获攻击者行为的类 ID-eCK 模型。

1.2 文章贡献

文章于 IBC 体系下采用类 Schnorr 签名[23]密钥生成方法, 结合 SM2 认证密钥交换协议, 提出基于 SM2 的标识认证密钥交换 (SM2-ID-AKE)协议。该协议满足以下特性:

高效性: 文章通过理论分析和仿真实验, 证明 SM2-ID-AKE 协议与现有的 ID-AKE 协议相比, 至少可节省 66.67%的通信带宽和 34.05%的计算开销。该协议能有效降低和减轻了通讯系统的代价和负担, 使其更能适应网络通讯部署等领域下不同用户的安全通信服务需求。

安全性: 文章在 ID-eCK 模型下证明新协议的安全性, 具体规约到椭圆曲线循环加法群下的 CDH 安

全假设。另外, 文章通过六种情形下各方行为细节的分析, 进一步证明了 SM2-ID-AKE 协议的安全性。

实用性: 目前大部分 ID-AKE 协议均基于国外密码算法设计, 尚未见基于国产商用密码算法的 ID-AKE 协议在国内外刊物上公开发表。为丰富国产商用密码算法在ID-AKE方面的研究, 文章构造了新的 SM2-ID-AKE 协议, 可为 SM2 在 ID-AKE 协议方面的扩展提供理论参考。

1.3 文章主体结构

文章在第二节回顾 IBC 体系、椭圆曲线群、安全假设、ID-eCK 安全模型的形式化定义等预备知识。第三节具体描述 SM2-ID-AKE 协议。在第四节, 定义协议安全性并通过安全模型分析协议安全性。在第五节分析所提协议性能表现并进行实验模拟实现。最后第六节总结文章工作。

2 预备知识

本节简要回顾 IBC 系统、椭圆曲线群、安全假设、ID-AKE、ID-eCK 模型等预备知识。

2.1 基于标识的密码系统

基于标识的密码学体系因避免了繁琐的数字证书管理, 在物联网等轻量级领域具有广泛的应用前景。该系统采用电子邮件地址、身份证、护照号等用户唯一标识符作为用户的公有信息, 用户私钥则由公众可信第三方生成并安全发放。系统的可信机构是唯一的, 是基于标识的密码系统的建立者, 一般称为 PKG 或 KGC。为了方便描述, 文章统一采用 KGC。

2.2 椭圆曲线群

文章协议的架构均建立于椭圆曲线上定义的群。现对该群群律作如下描述: 取一素数 p, 则其有限域 $\mathbb{F}_p$ 满足:

1) 若 $a,b\in\mathbb{F}_p$, 则 $a+b=r\left(\mathrm{mod}\,p\right)$, 其中 $0\leqslant r\leqslant p-1$。

2) 若 $a,b\in\mathbb{F}_p$, 则 $a\cdot b=r\left(\mathrm{mod}\,p\right)$, 其中 $0<r\leqslant p-1$。

3) 若 $a\in\mathbb{F}_p$ 且 $a\neq 0$, 则存在唯一的 $c\in\mathbb{F}_p$, 满足 $a\cdot c=1\left(\mathrm{mod}\,p\right)$。

若存在元素 $a,b\in\mathbb{F}_p$ 满足 $\Delta=4a^3+27b^2\neq 0$ 判别式, 则可定义基于 $\mathbb{F}_p$ 的椭圆曲线 $\mathrm{E}(\mathbb{F}_p)$ 为 $\mathbb{F}_p$ 中满足维尔斯特拉斯等式 $y=x^3+ax+b$ 的点集附加无穷远点 O, 即为 $\mathbb{G}=\{(x,y)\,|\,x,y\in\mathbb{F}_p,\text{且}y^2=x^3+ax+b\}\cup\{\mathrm{O}\}$。而椭圆曲线群 $\mathbb{G}$ 上的几何加法满足如下运算律: 假设点 $P,Q\in\mathbb{G}$, 过点 P 和点 Q 的直线为 L, L 交 $\mathrm{E}(\mathbb{F}_p)$ 于第三点 R'。过 R' 对 x 轴作垂线交曲线 $\mathrm{E}(\mathbb{F}_p)$ 于点 R, 即满足运算律 $P+Q=R$。群 $\mathbb{G}$ 中的数量乘法则满足以下运算律: $tP=\underbrace{P+P+\ldots+P}_{t\text{次}}$。

2.3 安全假设

计算型 Diffie-Hellman(Computational Diffie-Hellman, CDH)困难问题: 对于未知的 $a,b\in\mathbb{Z}_p^*$, 给定 $g,g^a,g^b\in\mathbb{G}$, 计算 g^{ab}。

定义 1. (CDH 安全假设)给定 $g,g^a,g^b\in\mathbb{G}$, 对于任意的 $a,b\in\mathbb{Z}_p^*$, 任何概率多项式时间(Pro-babilistic Polynomial Time, $\mathcal{PPT}$)的攻击者 $\mathcal{M}$ 计算出 g^{ab} 的概率均是可忽略不计的。为方便起见, 定义 $\mathcal{M}$ 计算 g^{ab} 的成功优势为 $\mathrm{Adv}_{\mathcal{M}}=\Pr[\mathcal{M}(g,g^a,g^b)=g^{ab}]$。

2.4 ID-AKE 协议的形式化定义

ID-AKE 协议一般由以下三个多项式时间算法组成:

Setup. 算法输入系统安全参数 λ, 输出系统公私钥对(P_{pub}, P_{pri})。

Extract. 算法输入系统公私钥对(P_{pub}, P_{pri})和用户标识 ID_i, 输出用户 ID_i 对应的密钥对(d_i, L_i)。

Exchange. 算法输入协商双方的私钥信息(d_{A}, L_{A})、(d_{B}, L_{B})和身份标识 ID_{A}、ID_{B}, 输出用户 A 和 B 相同的共享密钥。

2.5 基于 ID-eCK 模型安全性证明

两方 ID-AKE 协议的安全模型主要包括 BJM 修改类和 eCK 修改类两种。文章将在 ID-eCK 模型下证明协议的安全性, 因此以下主要回顾 ID-eCK 模型的内容[24]。

2.5.1 协议参与者

在用户集合中, 每个用户均拥有长期公钥-私钥对 $(pk_{\mathrm{U}},sk_{\mathrm{U}})$ 和唯一标识(如 U), 密钥对的私钥由 KGC 产生, 而公钥 pk_{U} 则由唯一标识产生。

每个用户均模拟为 $\mathcal{PPT}$ 的图灵机, 以并行地方式参与多项式会话。文章将会话 $\Pi_{\mathrm{U,V}}^{i}$ 定义为用户 U 发起的与用户 V 进行的第 i 次会话。

2.5.2 敌手的能力

敌手 $\mathcal{M}$ 作为 $\mathcal{PPT}$ 的图灵机, 可随意窃听、延

迟、重放、修改和插入消息。敌手通过以上方式掌控全部会话网络。通过以下模拟可表现敌手 $\mathcal{M}$ 拥有的能力:

EphemeralKeyReveal ($\Pi^i_{\mathrm{U,V}}$): 敌手 $\mathcal{M}$ 获取 $\Pi^i_{\mathrm{U,V}}$ 的临时私钥。

SessionKeyReveal($\Pi^i_{\mathrm{U,V}}$): 谕言机根据 $\Pi^i_{\mathrm{U,V}}$ 是否生成了会话密钥决定发送给敌手 $\mathcal{M}$ 该会话密钥(Session Secret Key, SSK)还是空值。

StaticKeyReveal(U): 敌手 $\mathcal{M}$ 获取 U 的长期私钥。此时敌手仍无法完全掌控 U 。

KGCStaticKeyReveal: 模拟完美前向安全。谕言机向敌手 $\mathcal{M}$ 发送 KGC 主私钥。

EstablishParty(U): 此询问中敌手 $\mathcal{M}$ 可自适应地注册一个合法参与方 U 。敌手可根本上掌控参与方 U 并获取其长期私钥。

Send($\Pi^i_{\mathrm{U,V}}, m$): 通过向通信会话 $\Pi^i_{\mathrm{U,V}}$ 发送 m , 敌手 $\mathcal{M}$ 收到该会话的相关回答。

Test($\Pi^i_{\mathrm{U,V}}$): 敌手 $\mathcal{M}$ 对未被询问过的会话 $\Pi^i_{\mathrm{U,V}}$ 发起仅一次的 Test 询问。Test 谕言机随机选择一位比特 $b\in\{0,1\}$ 。若 $b=1$, 则返回会话 $\Pi^i_{\mathrm{U,V}}$ 的真实 SSK; 若 $b=0$, 则随机返回一个与该 SSK 均匀同分布的值。

定义 2. (匹配会话) 执行一次通信会话协议后得到统一会话识别符 SID 的两个会话 $\Pi^i_{\mathrm{U,V}}$ 和 $\Pi^j_{\mathrm{V,U}}$, 它们互为对方的匹配会话。SID 包含 $\Pi^i_{\mathrm{U,V}}$ 或 $\Pi^j_{\mathrm{V,U}}$ 发送和接收的消息值与双方角色的顺序值。

定义 3. (新鲜性) 若用户 U 和用户 V 共同建立了会话 $\Pi^i_{\mathrm{U,V}}$, 则当该会话达到以下条件时, 称 $\Pi^i_{\mathrm{U,V}}$ 是新鲜的:

(1) 会话 $\Pi^i_{\mathrm{U,V}}$ 及其匹配会话的 SSK 未被查询过。

(2) 在 $\Pi^i_{\mathrm{U,V}}$ 有匹配会话的情况下, $\Pi^i_{\mathrm{U,}I'}$ 的临时私钥和 U 的长期私钥以及 $\Pi^i_{\mathrm{U,V}}$ 的临时私钥和 V 的长期私钥未被查询过。

(3) 在 $\Pi^i_{\mathrm{U,V}}$ 无匹配会话的情况下, U 的长期私钥和 $\Pi^i_{\mathrm{U,V}}$ 的临时私钥以及 V 的长期私钥未被查询过。

定义 4. (ID-eCK 安全性) 事件 $\mathrm{E_{succ}}$ 是指任意敌手 $\mathcal{M}$ 对某新鲜会话进行了一次 Test 查询, 并正确猜出 b 的值的事件。敌手 $\mathcal{M}$ 攻击协议的优势定义为 $\mathrm{Adv}^{\mathrm{AKE}}(\mathcal{M})=\left|2\Pr\left[\mathrm{E_{succ}}\right]-1\right|$。若对于任意 $\mathcal{PPT}$ 的敌手 $\mathcal{M}$, $\mathrm{Adv}^{\mathrm{AKE}}(\mathcal{M})$ 是可忽略的, 则称该 AKE 协议在 ID-eCK 模型下安全。

3 协议及流程

3.1 SM2-ID-AKE 协议

本协议是基于 SM2 认证密钥交换协议改进和优化的, 因此本协议与 SM2 使用的系统参数相同。SM2-ID-AKE 协议包含: 系统初始化(Setup)、用户密钥提取(Extract)和密钥交换(Exchange)三个多项式算法。具体构造如下:

系统初始化(Setup). 该算法主要用于产生系统主公私钥对以及整个认证密钥交换协议过程所需参数, 其中主要包括: KGC 公私钥对(P_{pub} , P_{pri})、椭圆曲线相关参数 ($q,\mathbb{F}_q,a,b,n,G$)、安全的密码杂凑函数($\mathrm{H}(\cdot),\mathrm{H}_{256}(\cdot),\mathrm{KDF}(\cdot)$)等。具体生成过程如下:

算法输入安全参数 λ , 随机选取大素数 q , 确定非奇异椭圆曲线 $\mathrm{E}: y^2=x^3+ax+b\left(\mathrm{mod}\,q\right)$ (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 $\mathrm{H}:\{0,1\}^*\to\mathbb{Z}_n^*$, $\mathrm{H}_{256}:\{0,1\}^*\to\{0,1\}^{256}$, KDF: $\{0,1\}^*\to\{0,1\}^{klen}$ 。另外, 以 Hash(·) 表示以上任一种安全密码杂凑函数。

系统主公钥 P_{pub} 和系统主私钥 P_{pri} 生成过程如下:

步骤 1: KGC 从集合 $\{1,2,\cdots,n-1\}$ 中随机选取整数 d_{K} 作为主私钥 $P_{\mathrm{pri}}=d_{\mathrm{K}}$, 其中 n 表示 SM2 密码运算所使用的椭圆曲线点群的阶;

步骤 2: KGC 根据所选主私钥 d_{K} , 计算 $P_{\mathrm{K}}=\left[d_{\mathrm{K}}\right]G=(x_{\mathrm{K}},y_{\mathrm{K}})$ 并公布系统主公钥 $P_{\mathrm{pub}}=P_{\mathrm{K}}$, 其中 G 为 SM2 数字签名系统参数中椭圆曲线点群的基点, $\left[d_{\mathrm{K}}\right]G$ 表示点乘运算, $\left(x_{\mathrm{K}},y_{\mathrm{K}}\right)$ 表示主公钥 P_{pub} 的横纵坐标。

用户密钥提取(Extract). 该算法主要用于产生用户的密钥对, 是本协议的主要创新点。假设用户 i 具有长度 $entlen_i$ 比特的可辨别标识 ID_i , 记 $ENTL_i$ 是由整数 $entlen_i$ 转换而成的两个字节, 则 KGC 为用户 i 生成私钥信息和公开参数过程如下:

步骤 1: 从集合 $\{1,2,\cdots,n-1\}$ 中随机选取整数 l_i ; 计算得到用户私钥的第一部分 $L_i=\left[l_i\right]G=(x_{l_i},y_{l_i})$,

其中, (x_{l_i}, y_{l_i}) 表示 L_i 的横纵坐标;

步骤 2: 将点 L_i 的坐标 x_{l_i}, y_{l_i} 的数据类型转换成比特串后计算 $h_i = \mathrm{H}(ENTL_i \| \mathrm{ID}_i \| x_{l_i} \| y_{l_i})$, 符号 $\|$ 表示比特串连接;

步骤 3: 计算得到用户私钥的第二部分 $d_i = l_i + h_i \cdot d_{\mathrm{K}} \pmod q$, 其中, $\pmod q$ 表示模 n 运算;

步骤 4: 最终得到用户 i 的私钥信息 (d_i, L_i), 并将其以安全信道的方式发送给用户 i;

步骤 5: 用户 i 接收到 (d_i, L_i), 先验证 $d_i G = L_i + \mathrm{H}(ENTL_i \| \mathrm{ID}_i \| x_{l_i} \| y_{l_i}) P_{\mathrm{K}}$ 的正确性以判断 (d_i, L_i) 的合法性, 后确定私钥信息 (d_i, L_i) 及其公开参数 $P_i = d_i G$。记用户 A 和用户 B 的私钥信息分别为 $(d_{\mathrm{A}}, L_{\mathrm{A}})$, $(d_{\mathrm{B}}, L_{\mathrm{B}})$, 对应的公开参数分别为 $P_{\mathrm{B}} = d_{\mathrm{B}} G$, $P_{\mathrm{B}} = d_{\mathrm{B}} G$。用户 A 和用户 B 的身份可辨标识、部分椭圆曲线系统参数和公钥信息的杂凑值分别为 $Z_{\mathrm{A}} = \mathrm{H}_{256}(ENTL_{\mathrm{A}} \| \mathrm{ID}_{\mathrm{A}} \| a \| b \| x_G \| y_G \| x_{\mathrm{A}} \| y_{\mathrm{A}})$ 和 $Z_{\mathrm{B}} = \mathrm{H}_{256}(ENTL_{\mathrm{B}} \| \mathrm{ID}_{\mathrm{B}} \| a \| b \| x_G \| y_G \| x_{\mathrm{B}} \| y_{\mathrm{B}})$, 其中 a, b 为椭圆曲线方程参数, x_G, y_G 为基点 G 的坐标, $x_{\mathrm{A}}, y_{\mathrm{A}}$ 和 $x_{\mathrm{B}}, y_{\mathrm{B}}$ 分别为 P_{A} 和 P_{B} 的坐标。

密钥交换(Exchange). 该算法主要用于用户 A 和 B 协商获得相同的密钥, 设用户 A 和 B 协商获得密钥数据的长度为 $klen$ 比特, 用户 A 为发起方, 用户 B 为响应方, 记 $w = (\log_2(n)/2) - 1$。具体过程如下:

步骤 1: 用户 A 执行以下过程:

A.1 从集合 $\{1, 2, \cdots, n-1\}$ 中随机选取整数 r_{A};

A.2 通过计算 $R_{\mathrm{A}} = [r_{\mathrm{A}}]G = (x_1, y_1)$ 得到椭圆曲线点 R_{A}, 其中, (x_1, y_1) 表示 R_{A} 的横纵坐标;

A.3 将 R_{A} 发送给用户 B;

步骤 2: 用户 B 执行以下过程:

B.1 从集合 $\{1, 2, \cdots, n-1\}$ 中随机选取整数 r_{B};

B.2 通过计算 $R_{\mathrm{B}} = [r_{\mathrm{B}}]G = (x_2, y_2)$ 得到椭圆曲线点 R_{B}, 其中, (x_2, y_2) 表示 R_{B} 的横纵坐标;

B.3 从 R_{B} 中取出元素 x_2, 计算 $\overline{x}_2 = 2^w + (x_2 \,\&\, (2^w - 1))$;

B.4 计算 $t_{\mathrm{B}} = (d_{\mathrm{B}} + \overline{x}_2 \cdot r_{\mathrm{B}}) \pmod n$;

B.5 验证 R_{A} 是否满足椭圆曲线方程, 若不满足则协商失败; 否则从 R_{A} 中取出元素 x_1 计算 $\overline{x}_1 = 2^w + (x_1 \,\&\, (2^w - 1))$;

B.6 计算 $V = [h \cdot t_{\mathrm{B}}](L_{\mathrm{A}} + \mathrm{H}(ENTL_{\mathrm{A}} \| \mathrm{ID}_{\mathrm{A}} \| x_{l_{\mathrm{A}}} \| y_{l_{\mathrm{A}}}) P_{\mathrm{K}} + [\overline{x}_1] R_{\mathrm{A}}) = (x_V, y_V)$, 若 V 是无穷远点, 则 B 协商失败; 否则将 x_V, y_V 的数据类型转换成比特串;

B.7 计算 $K_{\mathrm{B}} = \mathrm{KDF}(x_V \| y_V \| Z_{\mathrm{A}} \| Z_{\mathrm{B}}, klen)$;

B.8 (选项) 将 R_{A} 的坐标 x_1, y_1 和 R_{B} 的坐标 x_2, y_2 的数据类型转换成比特串, 计 $S_{\mathrm{B}} = \mathrm{Hash}(0\mathrm{x}02 \| y_V \| \mathrm{Hash}(x_V \| Z_{\mathrm{A}} \| Z_{\mathrm{B}} \| x_1 \| y_1 \| x_2 \| y_2))$;

B.9 将 R_{B} (选项 S_{B})发送给用户 A;

步骤 3: 用户 A 执行以下过程:

A.4 从 R_{A} 取出元素 x_1, 计算 $\overline{x}_1 = 2^w + (x_1 \,\&\, (2^w - 1))$;

A.5 计算 $t_{\mathrm{A}} = (d_{\mathrm{A}} + \overline{x}_1 \cdot r_{\mathrm{A}}) \pmod n$;

A.6 验证 R_{B} 是否满足椭圆曲线方程, 若不满足则协商失败; 否则从 R_{B} 中取出元素 x_2, 计算 $\overline{x}_2 = 2^w + (x_2 \,\&\, (2^w - 1))$;

A.7 计算 $U = [h \cdot t_{\mathrm{A}}](L_{\mathrm{B}} + \mathrm{H}(ENTL_{\mathrm{B}} \| \mathrm{ID}_{\mathrm{B}} \| x_{l_{\mathrm{B}}} \| y_{l_{\mathrm{B}}}) P_{\mathrm{K}} + [\overline{x}_2] R_{\mathrm{B}}) = (x_U, y_U)$, 若 U 是无穷远点, 则 A 协商失败; 否则将 x_U, y_U 的数据类型转成比特串;

A.8 计算 $K_{\mathrm{A}} = \mathrm{KDF}(x_U \| y_U \| Z_{\mathrm{A}} \| Z_{\mathrm{B}}, klen)$;

A.9 (选项) 将 R_{A} 的坐标 x_1, y_1 和 R_{B} 的坐标 x_2, y_2 的数据类型转换成比特串, 计算 $S_1 = \mathrm{Hash}(0\mathrm{x}02 \| y_U \| \mathrm{Hash}(x_U \| Z_{\mathrm{A}} \| Z_{\mathrm{B}} \| x_1 \| y_1 \| x_2 \| y_2))$, 并校验 $S_1 = S_{\mathrm{B}}$ 正确性, 若不正确则 K_{BA} 确认失败;

A.10(选项)计算 $S_{\mathrm{A}} = \mathrm{Hash}(0\mathrm{x}03 \| y_U \| \mathrm{Hash}(x_U \| Z_{\mathrm{A}} \| Z_{\mathrm{B}} \| x_1 \| y_1 \| x_2 \| y_2))$ 并将 S_{A} 发送给用户 B。

步骤 4: 用户 B 执行以下过程:

B.10 (选项) 计算 $S_2 = \mathrm{Hash}(0\mathrm{x}03 \| y_V \| \mathrm{Hash}(x_V \| Z_{\mathrm{A}} \| Z_{\mathrm{B}} \| x_1 \| y_1 \| x_2 \| y_2))$ 并校验 $S_2 = S_{\mathrm{A}}$ 正确性, 若不正确则 K_{AB} 确认失败。

3.2 系统模型

本协议包括可信第三方 KGC、密钥交换参与方 A 和参与方 B 三个实体。协议流程如下图 1 所示: KGC 首先执行 Setup 算法计算其主公私钥对; 然后用户 A 和用户 B 将其身份标识传至 KGC; 收到身份标识后, KGC 调用 Extract 算法计算出二者的私钥信息, 并将对应的私钥信息发送给参与方; 最终参与方按 Exchange 算法进行密钥交换并协商出共享密钥 $K_{\mathrm{AB}} = K_{\mathrm{BA}}$。

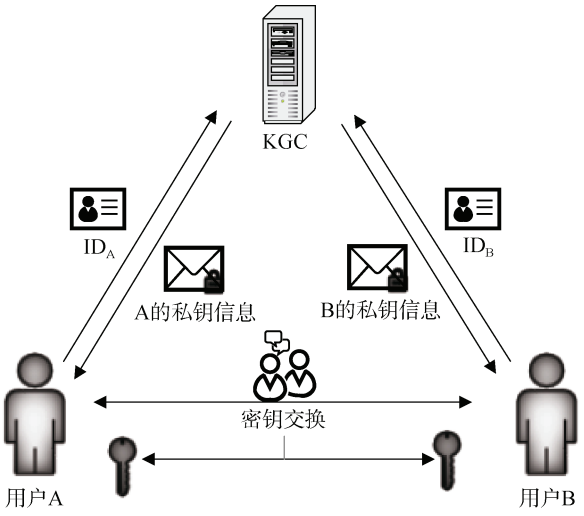

图 1 SM2-ID-AKE 系统模型

Figure 1 SM2-ID-AKE system model

4 安全性证明

本节在 ID-eCK 模型下证明新协议的安全性, 具体规约到椭圆曲线循环加法群下的 CDH 安全假设。

定理 1. (SM2-ID-AKE 协议的 ID-eCK 安全) 假定 H() 和 $\mathrm{H}_{256}()$ 是随机谕言机, 且 CDH 安全假设成立, 则 SM2-ID-AKE 协议在 ID-eCK 模型下是安全的。

证明 将安全参数设为 k、每个诚实参与者可激活的最大会话数目设为 $q_s(k)$。$n(k)$ 表示为敌手 $\mathcal{M}$ 最多可激活的诚实参与者数目。敌手仅有伪造攻击、密钥复制攻击和纯粹以 50% 的概率猜测的方式辨别收到的是随机串还是真实会话密钥, 且此前敌手已向 Test($\Pi^i_{\mathrm{U,V}}$)发出查询。下面讨论前两种情况:

(1) 伪造攻击: 敌手 $\mathcal{M}$ 于可获取到 Z_{A}、Z_{B} 和 R_{A} 的条件下, 在挑战阶段对随机谕言机进行关于元组 $(x_i \| y_i \| Z_{\mathrm{A}} \| Z_{\mathrm{B}}, klen)$ 的查询, 其中 $i \in \{\mathrm{U},\mathrm{V}\}$。

(2) 密钥复制攻击: 敌手使 Test 会话的非匹配会话拥有和 Test 会话相同会话密钥, 再对该会话进行 SSK 的查询。

但最终分析来看, 后者并不可行。原因是随机谕言机 H 不会为非匹配的两次会话询问返回相同的会话标识, 因此密钥复制攻击成功的可能性是可忽略的。

由新鲜性的概念, 我们可根据伪造攻击按 Test 会话是否存在匹配会话的两种情况进行具体讨论。

4.1 不存在 Test 会话的匹配会话

考虑以下两种子情况:

情形 1: 敌手 $\mathcal{M}$ 已掌握 A 的长期私钥且无法通过查询获得 Test 会话的临时私钥;

情形 2: 敌手 $\mathcal{M}$ 未掌握 A 的长期私钥且可通过查询获得 Test 会话的临时私钥。

以下具体讨论这两种情形:

情形 1:

模拟器 $\mathcal{S}$ 的操作: 设 CDH 问题实例 $X = aG$, $Y = bG$, 且 $a,b \in \mathbb{Z}_q^*$, $X,Y \in \mathrm{E}(\mathbb{F}_q)$。$\mathcal{S}$ 的目标是利用实例求得结果 $\mathrm{CDH}(X,Y) = abG$。

算法 $\mathcal{S}$ 作为模拟器设定以下条件: 假设敌手 $\mathcal{M}$ 将攻击 Test 会话 $\Pi^m_{\mathrm{A,B}}$ 且成功的概率不可忽略; 设定参与者 B 的公钥为 $P_{\mathrm{B}} = h_{\mathrm{B}}P_{\mathrm{K}} - \bar{x}_2 R_{\mathrm{B}} = h_{\mathrm{B}}bG - \bar{x}_2 R_{\mathrm{B}}$, 其中 $b \in \mathbb{Z}_q^*$; 按规定设定其他 $n(k)-1$ 个参与者的公私钥对; 设定 Y 作为 KGC 的主公钥。

关于参与者 B 的询问, $\mathcal{S}$ 以模拟嵌入或取随机值的方式回应; 关于其他 $n(k)-1$ 个参与者的询问, $\mathcal{S}$ 按规定返回真实值。

对于随机谕言机查询的一致性, 文章使用陷门测试技术[25]来维护。这种方法的优势在于, 可证明协议在标准的 CDH 安全假设下是安全且无需 Gap 假设, 使证明更加简洁易懂。为方便描述, 后文设定参与者 B 为协议会话 $\Pi^m_{\mathrm{A,B}}$ 的相应方。当回应询问时, $\mathcal{S}$ 具体作以下模拟:

H($ENTL_i \| \mathrm{ID}_i \| x_{l_i} \| y_{l_i}$) 询问: $\mathcal{S}$ 模拟 H 为随机谕言机, 维护初始为空的列表 Λ_H。记录元组 $(ENTL_i \| \mathrm{ID}_i \| x_{l_i} \| y_{l_i}, l_i, h_i)$。$\mathcal{M}$ 询问关于 $\mathrm{ID}_i \in \{0,1\}^*$ 的 H 查询, S 回应如下:

(1) 若 Λ_H 中已存在 $(ENTL_i \| \mathrm{ID}_i \| x_{l_i} \| y_{l_i})$, 则 $\mathcal{S}$ 输出 h_i。

(2) 否则, 若 $\mathrm{ID}_i = \mathrm{B}$, 模拟器 $\mathcal{S}$ 随机选取 $b \in \mathbb{Z}_q^*$, 计算 $P_{\mathrm{B}} = h_{\mathrm{B}}P_{\mathrm{K}} - \bar{x}_2 R_{\mathrm{B}} = h_{\mathrm{B}}bG - \bar{x}_2 R_{\mathrm{B}}$, $h_{\mathrm{B}} = \dfrac{P_{\mathrm{B}} + \bar{x}_2 R_{\mathrm{B}}}{P_{\mathrm{K}}} = \dfrac{d_{\mathrm{B}} + \bar{x}_2 r_{\mathrm{B}}}{b}$ 然后在列表 Λ_H 中记录 $(ENTL_{\mathrm{B}} \| \mathrm{B} \| x_{l_{\mathrm{B}}} \| y_{l_{\mathrm{B}}}, \perp, h_{\mathrm{B}})$。

(3) 否则, $\mathcal{S}$ 选择随机数 $d_i \in \mathbb{Z}_q^*$, 计算 $P_i = d_i G$, $h_i = \dfrac{P_i - L_i}{P_{\mathrm{K}}}$, 并在列表 Λ_H 中记录 $(ENTL_i \| \mathrm{ID}_i \| x_{l_i} \| y_{l_i}, l', h_i)$。

KDF ($x_i \| y_i \| Z_i \| Z_j, klen$) 询问: 模拟器 $\mathcal{S}$ 以元组 $(x_i \| y_i \| Z_i \| Z_j, klen, h)$ 维护列表 Λ_{KDF}, 列表初试为空。$\mathcal{S}$ 一般情况下按协议规定进行模拟并返回输出, 但若询问格式为 $(x_U \| y_U \| Z_{\mathrm{C}} \| Z_{\mathrm{B}}, klen)$ 且 C

可能为恶意会话对象, 则$\mathcal{S}$按模拟值进行返回。

(1) 若$(x_U \| y_U \| Z_C \| Z_B, klen)$已经在列表元组中存在, 则$\mathcal{S}$输出$h$。

(2) 否则, $\mathcal{S}$在列表Λ_{send}中查找形如$(x_U \| y_U \| Z_C \| Z_B, klen, *)$的条目。若找到, $\mathcal{S}$计算$\overline{U} = \frac{U}{h} - d_C h_B P_K = (\overline{x}_U, \overline{y}_U)$, 其中, $U = (x_U, y_U)$是此条目前两条串联比特值组成的点。随后$\mathcal{S}$判断U值是否正确生成, 若正确生成则$U \in \mathbb{G}$成立。注意: U值是否正确生成等价于$U = [h \cdot t_C](L_B + \text{H}(ENTL_B \| \text{ID}_B \| x_{l_B} \| y_{l_B}) P_K + [\overline{x}_2] R_B) = (x_U, y_U)$, 又等价于$\overline{U} = r_C d_K G$。另外, $\mathcal{S}$还检查$Z_C = \text{H}_{256}(ENTL_C \| \text{ID}_C \| a \| b \| x_G \| y_G \| x_C \| y_C)$以及$Z_B = \text{H}_{256}(ENTL_B \| \text{ID}_B \| a \| sb \| x_G \| y_G \| x_B \| y_B)$是否成立。

(i) 若以上两条件检查后均成立, 则$\mathcal{S}$返回给$\mathcal{M}$在Λ_{send}中的值k_{CB}且在Λ_{KDF}保存$(x_U \| y_U \| Z_C \| Z_B, klen)$元组。

(ii) 若以上两个检查均不成立, 则模拟器$\mathcal{S}$发送给$\mathcal{M}$随机选取的$h \in \{0,1\}^{klen}$并将含h的新元组$(x_U \| y_U \| Z_C \| Z_B, klen, h)$存入表$\Lambda_{\text{KDF}}$中。

(3) 若无此条目存在, 算法$\mathcal{S}$发送给$\mathcal{M}$随机选取的$h \in \{0,1\}^{klen}$并将含h的新元组$(x_U \| y_U \| Z_C \| Z_B, klen, h)$存入表$\Lambda_{\text{KDF}}$中。

EstablishParty(ID_i)询问: $\mathcal{M}$注册ID_i, 但由算法$\mathcal{S}$代理操作。代理过程为, $\mathcal{S}$向H询问值$ENTL_i \| \text{ID}_i \| x_{l_i} \| y_{l_i}$, 后给$\mathcal{M}$发送$\text{ID}_i$对应的长期私钥$d_i = h_i d_k + l_i$。

KGCStaticKeyReveal 询问: 此情况下模拟器$\mathcal{S}$失败(见定义 3)。

StaticKeyReveal(ID_i)询问: 若$\text{ID}_i = \text{B}$, 模拟器$\mathcal{S}$失败($\mathcal{M}$不能查询 B 的长期私钥)。否则, $\mathcal{S}$随机选$a, b \in \mathbb{Z}_q^*$, 使$d_i = a$, $h_i = b$, 并计算$L_i = aG - bd_K G = (x_{l_i}, y_{l_i})$, 并将$c = \text{H}(ENTL_i \| \text{ID}_i \| x_{l_i} \| y_{l_i})$发送给敌手, 敌手可验证$\text{H}(ENTL_i \| \text{ID}_i \| x_{l_i} \| y_{l_i}) = c$, 即敌手可信任$d_i = a$, $\mathcal{S}$将相应的私钥d_i返回给敌手$\mathcal{M}$。

EphemeralKeyReveal($\Pi^{m}_{\text{ID}_i,\text{ID}_j}$)询问: 若$\Pi^{m}_{\text{ID}_i,\text{ID}_j}$为 Test 会话(即$\Pi^{m}_{\text{ID}_i,\text{ID}_j} = \Pi^{m}_{\text{A,B}}$), 则模拟器$\mathcal{S}$因暴露 Test 会话临时私钥而失败, 模拟终止; 否则, 模拟器$\mathcal{S}$发给$\mathcal{M}$所存临时私钥。

Send($\Pi^{m}_{\text{ID}_i,\text{ID}_j}$, R_j)询问: 维护列表Λ_{send}, 记录元组$(R_i, R_j, \text{ID}_i, \text{ID}_j, k)$。

(1) 若$\Pi^{m}_{\text{ID}_i,\text{ID}_j}$为 Test 会话, 即$\Pi^{m}_{\text{ID}_i,\text{ID}_j} = \Pi^{m}_{\text{A,B}}$, 则算法$\mathcal{S}$向$\mathcal{M}$发送$X$。

(2) 若$\text{ID}_i = \text{B}$, (为方便起见, 记$\text{ID}_j = \text{C}$且$R_j = R_c$), 则

(i) $\mathcal{S}$随机选择$r_B \in \mathbb{Z}_q^*$, 返回$R_B = r_B G$给敌手$\mathcal{M}$。

(ii) $\mathcal{S}$在列表Λ_{KDF}查找形如$(*\|*\|Z_C \| Z_B, klen)$的条目。若找到, $\mathcal{S}$计算$\overline{U} = \frac{U}{h} - d_C h_B P_K = \frac{}{\overline{x}_1 h_B} = (\overline{x}_U, \overline{y}_U)$, 其中, $U = (x_U, y_U)$是此条目前两个串联比特值组成的点。随后$\mathcal{S}$判断U值是否正确生成, 若正确生成则$U \in \mathbb{G}$成立。注意: U值是否正确生成等价于$U = [h \cdot t_C](L_B + \text{H}(ENTL_B \| \text{ID}_B \| x_{l_B} \| y_{l_B}) P_K + [\overline{x}_2] R_B) = (x_U, y_U)$, 又等价于$\overline{U} = r_C d_K G$。另外, $\mathcal{S}$还检查$Z_C = \text{H}_{256}(ENTL_C \| \text{ID}_C \| a \| b \| x_G \| y_G \| x_C \| y_C)$以及$Z_B = \text{H}_{256}(ENTL_B \| \text{ID}_B \| a \| b \| x_G \| y_G \| x_B \| y_B)$是否成立($Z_A$, Z_B是此条目第一个值中后两个串联比特)。若以上两个检查均通过, 则算法$\mathcal{S}$返回给$\mathcal{M}$在Λ_{KDF}中所存值h, 并在Λ_{send}中保存含h的新元组$(x_U \| y_U \| Z_C \| Z_B, klen, h)$; 否则, 算法$\mathcal{S}$发送给$\mathcal{M}$随机选取的值$k \in \{0,1\}^{klen}$并在$\Lambda_{\text{send}}$中保存含$k$的新元组$(x_U \| y_U \| Z_C \| Z_B, klen, k)$。

(iii) 若没有这样的条目, 则模拟器$\mathcal{S}$返回给$\mathcal{M}$随机选择的值$k \in \{0,1\}^{klen}$且在Λ_{send}中保存含k的新元组$(x_U \| y_U \| Z_C \| Z_B, klen, k)$。

(3) 否则($\text{ID}_i \neq \text{B}$), $\mathcal{S}$遵循协议规定返回响应。

SessionKeyReveal($\Pi^{m}_{\text{ID}_i,\text{ID}_j}$)询问: 若$\Pi^{m}_{\text{ID}_i,\text{ID}_j}$为 Test 会话, 即$\Pi^{m}_{\text{ID}_i,\text{ID}_j} = \Pi^{m}_{\text{A,B}}$, 则模拟器$\mathcal{S}$因敌手$\mathcal{M}$查询 Test 会话的会话密钥时无法返回而终止; 否则, 模拟器$\mathcal{S}$发送给$\mathcal{M}$在Λ_{send}中的k值。

Test($\Pi^{m}_{\text{ID}_i,\text{ID}_j}$)询问: 若$\Pi^{m}_{\text{ID}_i,\text{ID}_j}$非 Test 会话, 则算法$\mathcal{S}$的模拟终止; 否则, 模拟器$\mathcal{S}$随机选择一位比特$b \in \{0,1\}$。若$b = 1$, 则返回$\Pi^{m}_{\text{ID}_i,\text{ID}_j}$的真实 SSK;

若 $b=0$, 则随机返回一个与该 SSK 均匀同分布的值。

若某时刻 $\mathcal{M}$ 以不可忽略的概率成功地攻击了 Test 会话, 由于伪造攻击的属性, 其必定已询问了 KDF 含 $U^*=\left[h\cdot t_{\mathrm{A}}\right](L_{\mathrm{B}}+\mathrm{H}(ENTL_{\mathrm{B}}\|\mathrm{ID}_{\mathrm{B}}\|x_{l_{\mathrm{B}}}\|y_{l_{\mathrm{B}}})P_{\mathrm{K}}+\left[\overline{x}_2\right]R_{\mathrm{B}}^*)=(x_U,y_U)$ 的值, 其中 R_{B}^* 由 $\mathcal{M}$ 生成。模拟器 $\mathcal{S}$ 随机选择一个 Λ_{KDF} 中的条目 U^* 并且作如下计算以解决 CDH(aG, bG)问题:

$\mathcal{S}$ 先计算

$$\begin{aligned}U^*&=[h\cdot t_{\mathrm{A}}](L_{\mathrm{B}}+\mathrm{H}(ENTL_{\mathrm{B}}\|\mathrm{ID}_{\mathrm{B}}\|x_{l_{\mathrm{B}}}\|y_{l_{\mathrm{B}}})P_{\mathrm{K}}\\&\quad+[\overline{x_2}]R_{\mathrm{B}}^*)\\&=[h\cdot t_{\mathrm{A}}](P_{\mathrm{B}}+[\overline{x_2}]R_{\mathrm{B}}^*)\\&=[h\cdot t_{\mathrm{A}}](h_{\mathrm{B}}P_{\mathrm{K}}-[\overline{x_2}]R_{\mathrm{B}}+[\overline{x_2}]R_{\mathrm{B}}^*)\\&=[h\cdot(d_{\mathrm{A}}+[\overline{x_1}]r_{\mathrm{A}})]h_{\mathrm{B}}P_{\mathrm{K}}\\&=h\cdot(d_{\mathrm{A}}h_{\mathrm{B}}P_{\mathrm{K}}+[\overline{x_1}]h_{\mathrm{B}}r_{\mathrm{A}}d_{\mathrm{K}}G)\end{aligned}$$

然后 $\mathcal{S}$ 计算

$$\begin{aligned}\overline{U}&=\frac{U/h-d_{\mathrm{A}}h_{\mathrm{B}}P_{\mathrm{K}}}{\overline{x_I}h_{\mathrm{B}}}\\&=abG\end{aligned}$$

最后, $\mathcal{S}$ 以如下概率解决了 CDH 问题:

$$\Pr[\mathcal{S}]\geqslant\frac{1}{q_s(k)n(k)^2t(k)}p_1(k),$$

此式中, 设定敌手 $\mathcal{M}$ 对 KDF 谕言机进行询问的次数最多为 $t(k)$ 次, 设定情形 1 发生且 $\mathcal{M}$ 成功攻破协议的事件概率为 $p_1(k)$。

由此可知, 若存在一个敌手 $\mathcal{M}$ 能以不可忽略的概率攻破协议, 则必存在一个算法 $\mathcal{S}$, 其解决 CDH 困难问题的概率不可忽略。而这显然和 CDH 安全假设相矛盾。

情形 2:

模拟器 $\mathcal{S}$ 的操作: 设 CDH 问题实例 $X=aG$, $Y=bG$, 且 $a,b\in\mathbb{Z}_q^*$, $X,Y\in\mathrm{E}(\mathbb{F}_q)$。$\mathcal{S}$ 的目标是利用实例求得结果 $\mathrm{CDH}(X,Y)=abG$。

算法 $\mathcal{S}$ 作为模拟器设定以下条件: 假设敌手 $\mathcal{M}$ 将攻击 Test 会话 $\Pi_{\mathrm{A,B}}^m$ 且成功的概率不可忽略; 设定参与者 A 的公钥为 $P_{\mathrm{A}}=X=a'G$、B 的公钥为 $P_{\mathrm{B}}=X=a^*G$, 其中 $a^*,a'\in\mathbb{Z}_q^*$; 按规定设定其他 $n(k)-2$ 个参与者的公私钥对; 设定 Y 作为 KGC 的主公钥。

关于参与者 A、B 的询问, $\mathcal{S}$ 以模拟嵌入或取随机值的方式回应; 关于其他 $n(k)-2$ 个参与者的询问, $\mathcal{S}$ 按规定返回真实值。

以下只描述算法 $\mathcal{S}$ 不同于情形 1 的应答。

$\mathrm{H}(ENTL_i\|\mathrm{ID}_i\|x_{l_i}\|y_{l_i})$ 询问: $\mathcal{S}$ 模拟为随机谕言机, 维护初始为空的列表 Λ_H, 记录元组 $(ENTL_i\|\mathrm{ID}_i\|x_{l_i}\|y_{l_i},l_i,h_i)$。$\mathcal{S}$ 模拟此谕言机的情形几乎和情形 1 一样, 除了当 $\mathcal{M}$ 查询 $\mathrm{H}(ENTL_{\mathrm{A}}\|\mathrm{A}\|x_{l_{\mathrm{A}}}\|y_{l_{\mathrm{A}}})$ 时, $\mathcal{S}$ 回应如下:

(1) 若 $\mathrm{ID}_i=\mathrm{A}$, 模拟器 S 随机选取 $a\in\mathbb{Z}_q^*$, 计算 $P_{\mathrm{A}}=X=a'G$, $h_{\mathrm{A}}=\dfrac{P_{\mathrm{A}}+\overline{x}_2R_{\mathrm{A}}}{P_{\mathrm{K}}}=\dfrac{a'+\overline{x}_2r_{\mathrm{A}}}{b'}$, 然后在列表 Λ_H 中记录 $(ENTL_{\mathrm{A}}\|\mathrm{A}\|x_{l_{\mathrm{A}}}\|y_{l_{\mathrm{A}}},\perp,h_{\mathrm{A}})$。

KDF $(x_i\|y_i\|Z_i\|Z_j,klen)$ 询问: 模拟器 $\mathcal{S}$ 以元组 $(x_i\|y_i\|Z_i\|Z_j,klen,h)$ 维护列表 Λ_{KDF}, 列表初试为空。当敌手 $\mathcal{M}$ 查询 KDF 条目 $(x_V\|y_V\|Z_{\mathrm{A}}\|Z_{\mathrm{B}},klen)$ 时, $\mathcal{S}$ 作以下回应:

(2) 若 $(x_V\|y_V\|Z_{\mathrm{A}}\|Z_{\mathrm{B}},klen)$ 已经在列表元组中存在, 则 $\mathcal{S}$ 输出 h。

(3) 若无此条目存在, 算法 $\mathcal{S}$ 发送给 $\mathcal{M}$ 随机选取的 $h\in\{0,1\}^{klen}$ 并将含 h 的新元组 $(x_V\|y_V\|Z_{\mathrm{A}}\|Z_{\mathrm{B}},klen,h)$ 存入表 Λ_{KDF} 中。

当敌手 $\mathcal{M}$ 查询非 KDF $(x_V\|y_V\|Z_{\mathrm{A}}\|Z_{\mathrm{B}},klen)$ 时, 算法 $\mathcal{S}$ 对此谕言机的模拟基本和情形 1 一致。

Send($\Pi_{\mathrm{ID}_i,\mathrm{ID}_j}^m$, R_j)询问: $\mathcal{S}$ 维护列表 Λ_{send}, 记录元组 $(R_i,R_j,\mathrm{ID}_i,\mathrm{ID}_j,k)$。

若 $\mathrm{ID}_i=\mathrm{B}$ 和 $\mathrm{ID}_j=\mathrm{A}$ ($\mathrm{ID}_i=\mathrm{A}$ 和 $\mathrm{ID}_j=\mathrm{B}$ 相似处理), 则

(i) $\mathcal{S}$ 随机选取 $r_{\mathrm{B}}\in\mathbb{Z}_q^*$, 返回 $R_{\mathrm{B}}=r_{\mathrm{B}}\mathrm{G}$ 给敌手 $\mathcal{M}$。

(ii) 模拟器 $\mathcal{S}$ 在 Λ_{send} 中保存含随机选择的值 $k\in\{0,1\}^{klen}$ 的新元组 $(x_U\|y_U\|Z_{\mathrm{C}}\|Z_{\mathrm{B}},klen,k)$。

(4) 除此之外, 算法 $\mathcal{S}$ 的操作和情形 1 一致。

EphemeralKeyReveal($\Pi_{\mathrm{ID}_i,\mathrm{ID}_j}^m$)询问: 模拟器 $\mathcal{S}$ 返回给 $\mathcal{M}$ 所存临时私钥。

若某时刻 $\mathcal{M}$ 以不可忽略的概率成功地攻击了 Test 会话, 其必定已询问了 KDF 含 $V^*=\left[h\cdot t_{\mathrm{B}}\right](L_{\mathrm{A}}+\mathrm{H}(ENTL_{\mathrm{A}}\|\mathrm{ID}_{\mathrm{A}}\|x_{l_{\mathrm{A}}}\|y_{l_{\mathrm{A}}})P_{\mathrm{K}}+\left[\overline{x}_1\right]R_{\mathrm{A}})=(x_V,y_V)$ 的值, 其中 R_{A} 由算法 $\mathcal{S}$ 模拟输出。模拟器 $\mathcal{S}$ 随机选择一个 Λ_{KDF} 中的条目 V^* 并且作如下计算以解决 CDH(aG, bG)问题:

$\mathcal{S}$ 先计算

$$V^* = [h\cdot t_{\mathrm{B}}](L_{\mathrm{A}} + \mathrm{H}(ENTL_{\mathrm{A}} \| \mathrm{ID}_{\mathrm{A}} \| x_{l_{\mathrm{A}}} \| y_{l_{\mathrm{A}}})P_{\mathrm{K}} + [\overline{x_1}]R_{\mathrm{A}})$$
$$= [h\cdot t_{\mathrm{B}}][\overline{x_1}]R_{\mathrm{A}}$$
$$= [h(d_{\mathrm{B}} + [\overline{x_2}]R_{\mathrm{B}})][\overline{x_1}]R_{\mathrm{A}}$$
$$= h(d_{\mathrm{B}}[\overline{x_1}]R_{\mathrm{A}} + [\overline{x_1}][\overline{x_2}]r_{\mathrm{A}}r_{\mathrm{B}}G)$$

然后 $\mathcal{S}$ 计算

$$\overline{V} = \frac{\frac{V}{h} - [\overline{x_2}]h_{\mathrm{A}}R_{\mathrm{B}}P_{\mathrm{K}}}{h_{\mathrm{A}}} = abG$$

最终 $\mathcal{S}$ 以如下概率解决了 CDH 问题:

$$\Pr[\mathcal{S}] \geqslant \frac{1}{q_s(k)n(k)^2 t(k)} p_2(k),$$

此式中, 设定敌手 $\mathcal{M}$ 对 KDF 谕言机进行询问的次数最多为 $t(k)$ 次, 设定情形 2 发生且 $\mathcal{M}$ 成功攻破协议的事件概率为 $p_2(k)$。

由此可知, 若存在一个敌手 $\mathcal{M}$ 能以不可忽略的概率攻破协议, 则必存在一个算法 $\mathcal{S}$, 其解决 CDH 困难问题的概率不可忽略。而这显然和 CDH 安全假设相矛盾。

4.2 存在 Test 会话的匹配会话

由于此情形中 Test 会话拥有其匹配会话, 因此可按新鲜性列出以下四种可能子情况:

情形 3: $\mathcal{M}$ 已掌握 Test 会话及匹配会话的临时私钥且无法通过查询获得二者的长期私钥;

情形 4: $\mathcal{M}$ 已掌握 Test 会话及匹配会话的长期私钥且无法通过查询获得二者的临时私钥;

情形 5: $\mathcal{M}$ 已掌握 Test 会话的长期私钥及匹配会话的临时私钥;

情形 6: $\mathcal{M}$ 已掌握 Test 会话的临时私钥及匹配会话的长期私钥;

以下按这四种情形具体讨论:

情形 3:

模拟器 $\mathcal{S}$ 的操作: 设 CDH 问题实例 $X = aG$, $Y = bG$, 且 $a,b \in \mathbb{Z}_q^*$, $X,Y \in \mathrm{E}(\mathbb{F}_q)$。$\mathcal{S}$ 的目标是利用实例求得结果 $\mathrm{CDH}(X,Y) = abG$。

算法 $\mathcal{S}$ 作为模拟器设定以下条件: 假设敌手 $\mathcal{M}$ 将攻击 Test 会话 $\Pi_{\mathrm{A,B}}^m$ 且成功的概率不可忽略; 设定参与者 A 的公钥为 $P_{\mathrm{A}} = X = a'G$、B 的公钥为 $P_{\mathrm{B}} = X = a^*G$, 其中 $a^*, a' \in \mathbb{Z}_q^*$; 按规定设定其他 $n(k)-2$ 个参与者的公私钥对; 设定 Y 作为 KGC 的主公钥。

模拟器 $\mathcal{S}$ 对 A, B 询问的操作与情形 2 一致, 在此不再赘述。

若某时刻 $\mathcal{M}$ 以不可忽略的概率成功地攻击了 Test 会话, 由于伪造攻击的属性, 其必定已询问了 KDF 含 $U^* = [h\cdot t_{\mathrm{A}}](L_{\mathrm{B}} + \mathrm{H}(ENTL_{\mathrm{B}} \| \mathrm{ID}_{\mathrm{B}} \| x_{l_{\mathrm{B}}} \| y_{l_{\mathrm{B}}})P_{\mathrm{K}} + [\overline{x_2}]R_{\mathrm{B}}) = (x_U, y_U)$ 的值, 其中 R_{A}, R_{B}^* 由模拟器生成且 $\mathcal{S}$ 掌握 r_{A}, r_{B}。模拟器 $\mathcal{S}$ 随机选择一个 Λ_{KDF} 中的条目 U^* 并且作如下计算以解决 $\mathrm{CDH}(aG, bG)$ 问题:

$$U^* = [h\cdot t_{\mathrm{A}}](L_{\mathrm{B}} + \mathrm{H}(ENTL_{\mathrm{B}} \| \mathrm{ID}_{\mathrm{B}} \| x_{l_{\mathrm{B}}} \| y_{l_{\mathrm{B}}})P_{\mathrm{K}} + [\overline{x_2}]R_{\mathrm{B}})$$
$$= [h\cdot t_{\mathrm{A}}](P_{\mathrm{B}} + [\overline{x_2}]R_{\mathrm{B}})$$
$$= [h\cdot t_{\mathrm{A}}](h_{\mathrm{B}}b^*G - [\overline{x_2}]R_{\mathrm{B}} + [\overline{x_2}]R_{\mathrm{B}})$$
$$= [h(d_{\mathrm{A}} + [\overline{x_1}]R_{\mathrm{A}})]h_{\mathrm{B}}b^*G$$
$$= h(h_{\mathrm{B}}a'b^*G + [\overline{x_1}]h_{\mathrm{B}}R_{\mathrm{A}}P_{\mathrm{K}})$$

然后 $\mathcal{S}$ 计算

$$\overline{V} = \frac{\frac{V}{h} - [\overline{x_1}]h_{\mathrm{B}}R_{\mathrm{A}}P_{\mathrm{K}}}{h_{\mathrm{B}}} = abG$$

最终 $\mathcal{S}$ 以如下概率解决了 CDH 问题:

$$\Pr[\mathcal{S}] \geqslant \frac{1}{q_s(k)n(k)^2 t(k)} p_3(k),$$

此式中, 设定敌手 $\mathcal{M}$ 对 KDF 谕言机进行询问的次数最多为 $t(k)$ 次, 设定情形 3 发生且 $\mathcal{M}$ 成功攻破协议的事件概率为 $p_3(k)$。

由此可知, 若存在一个敌手 $\mathcal{M}$ 能以不可忽略的概率攻破协议, 则必存在一个算法 $\mathcal{S}$, 其解决 CDH 困难问题的概率不可忽略。而这显然和 CDH 安全假设相矛盾。

情形 4:

给定 CDH 实例 $(R_{\mathrm{A}}, R_{\mathrm{B}})$, $R_{\mathrm{A}}, R_{\mathrm{B}} \in \mathrm{E}(\mathbb{F}_q)$, 构造 $\mathrm{CDH}(R_{\mathrm{A}}, R_{\mathrm{B}})$ 问题的算法 $\mathcal{S}$。

算法 $\mathcal{S}$ 作为模拟器设定以下条件: $\mathcal{S}$ 假设 $\mathcal{M}$ 将选择被给予会话中的一个作为 Test 会话, 而另外一个作为其匹配会话, 而两个会话均为 $\mathcal{S}$ 随机选取; 设定匹配会话拥有者为 B, 而 Test 会话拥有者为 A; 分别设定 R_{A}、R_{B} 作为 Test 会话及其匹配会话的临时公钥。另外, 由算法 $\mathcal{S}$ 设定以下条件: 按规定设定 KGC 主私钥和 $n(k)$ 个参与者的公私钥对。

由于模拟器 $\mathcal{S}$ 掌握了全部参与者的长期私钥以及 KGC 主私钥, $\mathcal{S}$ 的模拟较易体现, 不再赘述。

若某时刻 $\mathcal{M}$ 以不可忽略的概率成功地攻击了 Test 会话, 由于伪造攻击的属性, 其必定已询问了 KDF 含 $V^* = [h\cdot t_{\mathrm{B}}](L_{\mathrm{A}} + \mathrm{H}(ENTL_{\mathrm{A}} \| \mathrm{ID}_{\mathrm{A}} \| y_{l_{\mathrm{A}}})P_{\mathrm{K}} +$

$[\overline{x_1}]R_A)=(x_V,y_V)$ 的值。算法 $\mathcal{S}$ 随机选择一个 Λ_{KDF} 中的条目且作如下计算以解决 CDH(aG , bG)问题:

$$\begin{aligned}V^*&=[h\cdot t_B](L_A+\mathrm{H}(ENTL_A\|\mathrm{ID}_A\|x_{l_A}\|y_{l_A})P_K+[\overline{x_1}]R_A)\\&=[h\cdot t_B][\overline{x_1}]R_A\\&=[h(d_B+[\overline{x_2}]R_B)][\overline{x_1}]R_A\\&=h(d_B[\overline{x_1}]R_A+[\overline{x_1}][\overline{x_2}]r_Ar_BG)\end{aligned}$$

然后 $\mathcal{S}$ 计算

$$\begin{aligned}\overline{V}&=\frac{\frac{V}{h}-d_B[\overline{x_1}]R_A}{[\overline{x_2}][\overline{x_1}]}\\&=r_Ar_BG\end{aligned}$$

最终 $\mathcal{S}$ 以如下概率解决了 CDH 问题:

$$\Pr[\mathcal{S}]\geqslant\frac{2}{q_s(k)^2t(k)}p_4(k),$$

此式中, 设定敌手 $\mathcal{M}$ 对 KDF 谕言机进行询问的次数最多为 $t(k)$ 次, 设定情形 4 发生且 $\mathcal{M}$ 成功攻破协议的事件概率为 $p_4(k)$。

由此可知, 若存在一个敌手 $\mathcal{M}$ 能以不可忽略的概率攻破协议, 则必存在一个算法 $\mathcal{S}$, 其解决 CDH 困难问题的概率不可忽略。而这显然和 CDH 安全假设相矛盾。

情形 5 和情形 6:

证明与情形 1 相似, 在此省略。

综上所述, CDH 问题的算法 $\mathcal{S}$ 的成功概率为

$$\Pr[\mathcal{S}]\geqslant\max\{\max_{i=1,2,3,5,6}\frac{1}{q_s(k)n(k)^2t(k)}$$

$$p_i(k),\frac{2}{q_s(k)^2t(k)}p_4(k)\}。$$

若存在一个敌手 $\mathcal{M}$ 能在上述六种情况之一以不可忽略的概率攻破协议, 则必存在一个算法 $\mathcal{S}$, 其解决 CDH 困难问题的概率不可忽略。而这显然和 CDH 安全假设相矛盾。由于攻破 SM2-ID-AKE 协议的困难性可归约到攻破 CDH 问题的困难性上, 因此可得 SM2-ID-AKE 协议的安全性基于 CDH 安全假设。

证毕。

5 性能分析

本节从安全模型、安全假设、通信代价和计算开销四个方面, 分析和对比 SM2-ID-AKE 协议与同类型协议的安全性和性能, 并通过仿真对比各协议的实际性能。

5.1 理论分析

首先从理论上比较文章协议和相关的 ID-AKE 协议, 对比结果见表 1。其中, 协议[14,21,26]均基于双线性对构造, 协议[26]中的验签计算也需要一次双线性对运算。因此协议[14]、[21]和[26]分别需要 15、4 和 1 次高耗时的双线性对运算, 而协议[11]和 SM2-ID-AKE 协议无需双线性对运算。

为清晰描述理论分析结果, 下文对于计算开销方面将点乘运算次数设定为 M、将模指数运算次数设定为 E、将单个实体的双线性对运算次数设定为 P; 在通讯代价方面将安全参数 λ 的长度设定为 $|\lambda|$、将群 $\mathbb{G}_1$ 中元素的大小分别设定为 $|\mathbb{G}_1|$。

在计算开销和通信代价方面, SM2-ID-AKE 协议的计算开销和无双线性对或较少双线性对的 AKE 协议总体相当, 而与含多对的协议相比则具有显著优势。同时, 在 SM2-ID-AKE 协议的协商阶段, 双方需发送的数据仅为各自的临时公钥, 通讯代价仅为 2 个 $\mathbb{G}$ 中的元素长度; 而相比下, 其他协议的通讯代价包括临时公钥以及计算共享密钥时所需的中间值, 通讯代价均较高。

表 1 标识认证密钥交换协议性能比较

Table 1 Performance comparison of identity-based Authenticated key exchange protocols

协议	安全模型	困难假设	通信代价	计算开销
协议[14]	G_{RID}−CL−eCK	DL+CDH	6$\|\mathbb{G}_1\|$	15P+33E
协议[21]	ID-CL-eCK	DL+CDH	6$\|\mathbb{G}_1\|$	4P+27E
协议[11]	启发式	NA	4$\|\mathbb{G}_1\|$+7$\|\lambda\|$	16M
协议[26]	ID-eCK-PFS	q-SDH	10$\|\mathbb{G}_1\|$+4$\|\lambda\|$	1P+17M
本协议	ID-eCK	CDH	2$\|\mathbb{G}_1\|$	1E+15M

(注: M 指点乘运算次数; E 指模指数运算次数; P 指双线性对运算次数; $|\lambda|$ 指安全参数 λ 的长度; $|\mathbb{G}_1|$ 指群 $\mathbb{G}_1$ 中元素的大小; NA 指无)

在安全性方面, 除协议[11]外, SM2-ID-AKE 协议与其他所有对比协议的安全性证明均依赖随机谕言模型。协议[11]仅为启发式证明, 而文章协议与协议[14]、[21]和[26]的安全性均在类 ID-eCK 模型中证

明。其中, 文章协议的安全性可规约至 CDH 困难问题, 协议[14,21]的安全性可规约至 DL 和CDH 困难问题, 协议[26]的安全性可规约至 q-SDH 困难问题。协议[14,21]能够抗侧信道攻击, 但这些协议中均存在一次或多次高耗的双线性对运算。因此, 在与其他协议保持相同安全性的情况下, SM2-ID-AKE 协议可在计算开销和计通信代价方面占有较大优势。

5.2 实验仿真

本节对协议进行编程仿真, 测试协议中各个算法的运行时间。文章采用 MIRACL(Multiprecision Integer and Rational Arithmetic C/C++ Library)库作为仿真过程中的函数调用工具; 因密码学应用中满足加密特质的椭圆曲线具有特殊性, 其仿射方程为 $y^2 = x^3 + ax + b$ 且需满足 $\Delta = 4a^3 + 27b^2 \neq 0$, 故文章也采用这种经典的椭圆曲线实例, 并设定该椭圆曲线的群元素大小为 $|\mathbb{G}_1| = 256$ bits。文章仿真实验所搭建的软硬件环境如下: 硬件为一台装备 16.0 GB 机带 RAM 的联想台式主机, 装备中央处理器的规格为 Intel(R) Core(TM) i7-10700 CPU @ 2.90GHz 2.90 GHz; 主机搭载的操作系统版本为 64 位的 Windows 10 家庭中文版; 编程所用软件为 Visual Studio 2022; 所用编程语言为 C 语言, 版本为 ISO C11 标准。文章仿真结果如图 2 所示, 其中各数据为某轮二十次运行结果的平均值。

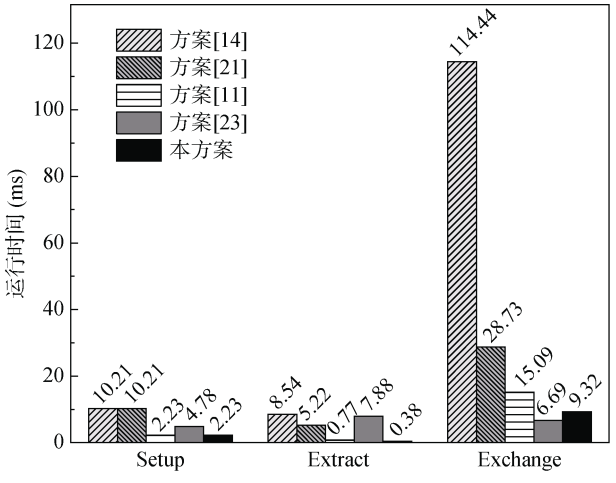

图 2 各协议运行时间比较

Figure 2 Comparison on the running time of protocols

图 2 中, 纵坐标表示算法运行时间(单位为 ms), 横坐标表示各协议中对应算法。SM2-ID-AKE 协议的 Setup 算法、Extract 算法和 Exchange 算法的用时分别为 2.23 ms、0.38 ms 和 9.32 ms, 通信代价为 128 字节; 协议[14]的 Setup 算法、Extract 算法和 Exchange 算法的用时分别为 10.21ms、8.54 ms 和 114.44 ms, 通信代价为 384 字节; 协议[21]的 Setup 算法、Extract 算法和 Exchange 算法的用时分别为 10.21 ms、5.22 ms 和 28.73 ms, 通信代价为 384 字节; 协议[11]的 Setup 算法、Extract 算法和 Echange 算法的用时分别为 2.23 ms、0.77 ms 和 15.09 ms, 通信代价为 480 字节; 协议[26]的 Setup 算法、Extract 算法和 Exchange 算法的用时分别为 4.78 ms、7.88 ms 和 6.69 ms, 通信代价为 728 字节。可见, 与对比协议中用时最少的协议[11]和带宽最少的协议[25]相比, SM2-ID-AKE 协议的用时降低了 34.05%, 带宽节省了 66.67%字节。

6 结束语

文章根据 IBC 体制下的类 Schnorr 签名机制, 结合 SM2 认证密钥交换协议, 提出了 SM2-ID-AKE 协议。该协议既减少了 PKI 体系证书分发带来的大量计算、通讯和存储开销, 又能符合当代国产自主化的发展需求。在 ID-eCK 模型和 CDH 安全假设下证文章证明了 SM2-ID-AKE 协议的安全性。最后, 通过理论分析和仿真实验验证了协议的实用性。

参考文献

[1] Beijing Huada Xinan Technology Co., Ltd., Chinese People's Liberation Army Information Engineering University, Chinese Academy of Sciences Data and Communication Protection Research and Education Center. Information Security Technology SM2 Elliptic Curve Public Key Cryptographic Algorithm Part 1: General Provisions[M]. National Quality Supervision of the People's Republic of China General Administration of Inspection and Quarantine, Standardization Administration of China, 2016: 48.
(北京华大信安科技有限公司, 中国人民解放军信息工程大学, 中国科学院数据与通信保护研究教育中心. 信息安全技术 SM2 椭圆曲线公钥密码算法 第 1 部分: 总则[M]. 中华人民共和国国家质量监督检验检疫总局, 中国国家标准化管理委员会, 2016: 48.)

[2] Shamir A. Identity-based cryptosystems and signature schemes[C]. *Workshop on the theory and application of cryptographic tecniques. Springer, Berlin, Heidelberg*, 1984: 47-53.

[3] Okamoto E, Tanaka K. Key distribution system based on identification information[J]. *IEEE Journal on selected areas in communications*, 1989, 7(4): 481-485.

[4] Okamoto E. Key distribution systems based on identification information[C]. *Conference on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg,* 1987: 194-202.

[5] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[C]. *Annual international cryptology conference. Springer, Berlin, Heidelberg*, 2001: 213-229.

[6] Smart N P. Identity-based authenticated key agreement protocol

based on Weil pairing[J]. *Electronics letters*, 2002, 38(13): 630-632.

[7] Chen L, Cheng Z, Smart N P. Identity-based key agreement protocols from pairings[J]. *International Journal of Information Security*, 2007, 6(4): 213-241.

[8] Zhu R, Yang G, Wong D. An efficient identity-based key exchange protocol with KGS forward secrecy for low-power devices[J]. *Theoretical Computer Science*, 2007, 378(2): 198-207.

[9] Fiore D, Gennaro R. Making the Diffie-Hellman protocol identity-based[C]. *Cryptographers' track at the RSA conference. Springer, Berlin, Heidelberg*, 2010: 165-178.

[10] Ni L, Chen G, Li J, et al. Strongly secure identity-based authenticated key agreement protocols without bilinear pairings[J]. *Information Sciences*, 2016, 367: 176-193.

[11] Huo S, Yang W, Li J, et al. New Identity-based Authentication and Key Agreement Scheme in Ad hoc Networks[J]. *COMPUTER SCIENCE*, 2018, 45(S1): 380-382.
(霍士伟, 杨文静, 李景智, 等. 一种新的基于身份的 Ad hoc 认证和密钥协商方案[J]. *计算机科学*, 2018, 45(Z6): 380-382.)

[12] Brzuska C, Smart N P, Warinschi B, et al. An analysis of the EMV channel establishment protocol[C]. *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. 2013: 373-386.

[13] Tomida J, Fujioka A, Nagai A, et al. Strongly secure identity-based key exchange with single pairing operation[C]. *European Symposium on Research in Computer Security. Springer*, Cham, 2019: 484-503.

[14] Tsai T, Chuang Y, Tseng Y, et al. A leakage-resilient ID-based authenticated key exchange protocol with a revocation mechanism[J]. *IEEE Access*, 2021, 9: 128633-128647.

[15] Blake-Wilson S, Johnson D, Menezes A. Key agreement protocols and their security analysis[C]. *IMA international conference on cryptography and coding. Springer, Berlin, Heidelberg*, 1997: 30-45.

[16] Canetti R, Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels[C]. *International conference on the theory and applications of cryptographic techniques. Springer, Berlin, Heidelberg*, 2001: 453-474.

[17] Chen L, Kudla C. Identity based authenticated key agreement protocols from pairings[C]. *16th IEEE Computer Security Foundations Workshop*, 2003: 219-233.

[18] LaMacchia B, Lauter K, Mityagin A. Stronger security of authenticated key exchange[C]. *International conference on provable security. Springer, Berlin, Heidelberg*, 2007: 1-16.

[19] Wang S, Cao Z, Choo K R, et al. An improved identity-based key agreement protocol and its security proof[J]. *Information Sciences*, 2009, 179(3): 307-318.

[20] Huang H, Cao Z. An ID-based authenticated key exchange protocol based on bilinear Diffie-Hellman problem[C]. *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, 2009: 333-342.

[21] Wu J, Tseng Y, Huang S. An identity-based authenticated key exchange protocol resilient to continuous key leakage[J]. *IEEE Systems Journal*, 2019, 13(4): 3968-3979.

[22] Wariki K, Fujioka A, Sasaki T, et al. Malicious Private Key Generators in Identity-Based Authenticated Key Exchange[J]. *The Institute of Electronics, Information and Communication Engineers*, 2022,1(1): 18-21.

[23] Goh E J, Jarecki S, Katz J, et al. Efficient signature schemes with tight reductions to the Diffie-Hellman problems[J]. *Journal of Cryptology*, 2007, 20(4): 493-514.

[24] Daniel R M, Rajsingh E B, Silas S. An efficient eCK secure identity based Two Party Authenticated Key Agreement scheme with security against active adversaries[J]. *Information and Computation*, 2020, 275: 104630.

[25] Cash D, Kiltz E, Shoup V. The Twin Diffie–Hellman Problem and Applications[J]. *Journal of Cryptology*, 2009, 22(4): 470-504.

[26] Wang F, Chen M. An Identity-based Authenticated Key Agreement Scheme with Perfect Forward Secrecy[J]. *Journal of Cryptologic Research*, 2020, 7(1): 56-68.
(王霏, 陈明. 完美前向安全的基于身份认证密钥协商方案[J]. *密码学报*, 2020, 7(1): 56-68.)

王晓虎 于 2021 年在河南财经政法大学软件工程专业获得学士学位。现在福建师范大学网络空间安全专业攻读硕士学位。研究领域为密码学、区块链隐私保护。Email: wangxiaohu49@163.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, CCF 专业会员。研究领域为应用密码学、区块链隐私保护。Email: linchao91@fjnu.edu.cn

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