基于 CSIDH 的认证密钥交换协议

张亚峰 陈辉焱 陈昱帆
(北京电子科技学院密码科学与技术系 北京 100070)

摘 要 针对 Galbraith 等提出的基于超奇异同源的认证密钥交换协议存在的安全问题,通过使用 NAXOS 技巧,并将通信双方静态密钥的 Diffie-Hellman 值添加到会话密钥的计算中,提出一个新的基于 CSIDH 的两轮认证密钥交换协议,并给出安全性证明。该协议是目前第一个基于 CSICDH 问题假设,且在 eCK 模型下可证明安全的认证密钥交换协议。经对比,该协议具有更强的安全属性,具体表现在可抵抗最大暴露攻击和自适应性攻击等方面。

关键词 认证密钥交换 eCK 模型 Diffie-Hellman 群作用 超奇异椭圆曲线 同源

中图分类号 TP3 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2024.10.056

AUTHENTICATION KEY EXCHANGE PROTOCOL BASED ON CSIDH

Zhang Yafeng Chen Huiyan Chen Yufan
(*Department of Cryptography and Technology, Beijing Electronic Science and Technology Institute, Beijing 100070, China*)

Abstract To solve the security problems in existing of the supersingular isogeny-based authentication key exchange protocol proposed by Galbraith, this paper proposes a new two-round authentication key exchange protocol based on CSIDH by using NAXOS techniques, and adding the Diffie-Hellman value of the static key of the two communicating parties to the calculation of the session key. Its proof of security was given. This protocol was currently the first authentication key exchange protocol based on the CSICDH problem assumption and provably secure under the eCK model. By comparison, the protocol has stronger safety attribute, which is specifically manifested in the ability to resist maximum exposure attacks and adaptive attacks.

Keywords Authentication key exchange protocol eCK model Diffie-Hellman Group action Supersingular elliptic curve Isogeny

0 引 言

1997 年,Shor 发表了在多项式时间内运行的关于计算大整数因子分解和离散对数的量子算法[1],这意味着当大型量子计算机问世,基于 RSA 的密码系统和 Diffie-Hellman 的密钥交换等加密体制就会遭到破坏。为了解决这个威胁,许多研究者将注意力集中在后量子密码的研究上,其目标是找到既可以在经典计算机上实现,同时也能保证对经典计算机和量子计算机安全的新的密码原语。在不安全通道上建立密钥是一种重要的密码技术,而认证和密钥建立是建立安全通信的基本步骤[2]。近年来对这方面的研究导致了认证密钥交换协议 AKE(Authenticated Key Exchange)的出现。而在后量子时代,我们希望能有一个可以抵抗量子对手攻击的 AKE 协议。为了构建安全的抗量子攻击防御系统。一种方法是通过将具有后量子安全的公钥加密或密钥封装机制与签名结合起来实现这一目标,但由此产生的显式身份验证方案会带来巨大的计算消耗;另一种方法是基于已建立的通用框架从量子安全的公钥加密或密钥封装机制来构造隐式 AKE[3]。

目前已有两种基于超奇异椭圆曲线同源的密码方案被认为是抗量子的:一种是 2011 年由 Feo 等[4]提出

收稿日期:2021-03-30。**张亚峰**,硕士生,主研领域:公钥密码学。**陈辉焱**,教授。**陈昱帆**,硕士生。

的基于超奇异同源的 Diffie-Hellman 结构 SIDH(Supersingular Isogeny Diffie-Hellman);另一种是 2018 年由 Castryck 等[5]提出的基于交换的超奇异同源的 Diffie-Hellman 结构 CSIDH(Commutative Supersingular Isogeny Diffie-Hellman)。虽然 SIDH 和 CSIDH 实现了针对敌手被动安全的会话密钥建立,但后续在进一步构造可证明安全的基于同源的 AKE 方面进展甚微,这与基于经典困难问题,如大整数因子分解、椭圆曲线离散对数和双线性对等的 AKE 协议的发展形成了鲜明的对比。原因在于尽管 SIDH 和 CSIDH 在形式上类似于 Diffie-Hellman,但其代数结构不能像经典协议一样具有多种构造方式。即使结构可以转换,最终的协议也可能是不安全的,如 Terada 等[7]提出的将 SIDH 和 CSIDH 实例化所得到密钥交换协议在离线字典攻击下是不安全的。因此近几年许多学者提出的基于同源的认证密钥交换协议[6,12-14,18]大多是基于某些通用框架构造的方式来获得的。

本文在 Lee 等[9]提出的 NAXOS + 协议基础上,提出了基于 CSIDH 的认证密钥交换协议,该协议是目前第一个基于 CSICDH 问题假设,并在 eCK 模型[11]下可证明安全的 AKE 协议。相较于 Galbraith 所提出的协议[12],该协议使用了 NAXOS 技巧, 并将静态密钥的 Diffie-Hellman 值添加到会话密钥的计算中,使得协议在计算 Diffie-Hellman 假设下的 eCK 模型中被证明是安全的,并对协议的一些安全属性,如抗未知密钥共享攻击、抗冒充攻击、抗中间人攻击、抗重放攻击和弱前向安全性等进行了简要的形式化分析。通过与其他基于超奇异同源的 AKE 协议对比分析可发现,本协议分别在安全性或计算效率上存在部分优势,具体表现在是否能抵抗最大暴露攻击和密钥泄露模拟攻击,是否允许敌手对任意静态公钥进行注册以及所需同源计算的次数等方面。

1　预备知识

1.1　椭圆曲线及其代数基础

设 E 为有限域$\mathbb{F}_p$上的一条超奇异椭圆曲线,当且仅当$\#E(\mathbb{F}_p)=p+1$。代数闭包$\mathbb{F}_p$上任意两条具有相同 j-不变量的椭圆曲线都是同构的,因此我们可以利用同构来定义椭圆曲线之间的等价关系,并利用该类中曲线的 $j-$不变量来识别等价类。令 E_1 和 E_2 为定义在$\mathbb{F}_p$上的两条椭圆曲线,定义从 E_1 到 E_2 的同源为态射 $\phi:E_1\to E_2$,使得 $\phi(0_{E_1})=0_{E_2}$,其中 0_{E_1} 和 0_{E_2} 分别为 E_1 和 E_2 的无限远点。给定同源映射的核,可通过 Vélu's formulae[10]来计算同源 ϕ,其计算复杂度为 $O(l\cdot\log(p)^2)$。

设 R 为任意整环,K 是它的商域。设 M 是 R-模 K 的 R-子模,$M\neq(0)$,并且存在元素 $0\neq a\in R$ 使得 $aM\subseteq R$。我们便称 M 是 R 的一个分式理想,由一个元素生成的分式理想叫做主分式理想。由于每个戴德金整环的全部分式理想形成乘法群 $I(R)$,显然主分式理想形成它的一个子群 $P(R)$,叫作 R 的主分式理想类群。它们都是交换群,其商群 $C(R)=I(R)/P(R)$ 叫作 R 的理想类群[8]。每个分式理想 $\mathfrak{a}$ 在 $C(R)$ 中的像,叫作是 $\mathfrak{a}$ 所在的理想类。两个分式理想 $\mathfrak{a}$ 和 $\mathfrak{b}$ 属于同一个理想类,当且仅当他们差一个主分式理想。理想类群 $\mathcal{CL}(O_K)$ 为虚二次序 O_K 的分式理想模上主分式理想的等价类,由于自同态环 $End_p(E)$ 始终与虚二次域上的序 O_K 同构,因此定义 $\mathcal{ELL}(\mathcal{O},\pi)$ 为 $\mathbb{F}_p$ 上满足 $End_p(E)\cong\mathcal{O}$ 的 E 的集合,其中 π 对应于 E 的 Frobenius 自同态[17]。

1.2　群作用

若 G 为交换群而 X 为一个集合,则 G 在 X 上的一个群作用[16]是一个二元函数 $G\cdot X\to X$,其中 $g\in G$ 和 $x\in X$ 的像写作 $g\cdot x$,满足如下两条公理:

(1) $(g\cdot h)\cdot x=g\cdot(h\cdot x)$ 对于所有的 $g,h\in G$ 和 $x\in X$ 成立。

(2) $e\cdot x=x$ 对于每个 $x\in X$ 成立(e 代表 G 的幺元)。

从这两条公理, 可以看出对于每个 $g\in G$, 映射 $x\in X$ 到 $g\cdot x$ 的函数是一个双射。

取 $\mathcal{ELL}(\mathcal{O},\pi)$ 中的椭圆曲线 $E:y^2=x^3+Ax+B$,通过向量 $\boldsymbol{v}\in\mathbb{Z}^d$ 来定义理想类,我们的目标是计算 $\phi(\boldsymbol{v})\cdot E\in\mathcal{ELL}(\mathcal{O},\pi)$。

$$\phi(\boldsymbol{v})\cdot E=\Big(\prod_{i=1}^{d}[\mathfrak{l}_i]^{v_i}\Big)\cdot E \tag{1}$$

由群作用的结合律,可以通过因子 $[\mathfrak{l}_i]$ 或 $[\mathfrak{l}_i]^{-1}$ 来逐渐计算式(1),称该操作为跳跃, 其对应着阶为 l_i 的 $E\to E_1$ 的同源。式(1) 的计算由 $\sum_{i=1}^{d}|v_i|$ 在椭圆曲线之间的跳跃组成。使用符号:

$$(l,b,\Delta)=l\mathbb{Z}+\frac{b+\sqrt{\Delta}}{2}\mathbb{Z} \tag{2}$$

表示素理想 $\mathfrak{l}_i$。由于 $\left(\frac{\Delta}{l}\right)=1$, 素数 l 是分歧的,因此 $lO_K=(l,b,\Delta)(l,-b,\Delta)$,其中 $(l,-b,\Delta)=[(l,b,\Delta)]^{-1}$。

为了计算椭圆曲线 $E_1=[(l,b,\Delta)]\cdot E$，通过使用 SEA 算法[17]。该群作用存在一个阶为 $N_{\mathfrak{Q}}^{K}(l,b,\Delta)=l$ 的$\mathbb{F}_p$上的可分同源 $\psi:E\to E_1$。$E_2=[(l,-b,\Delta)]\times E$ 同理。E_1和 E_2的 j-不变量可由方程：

$$\Phi_l(x,j(E))=0(\mathrm{mod})p \tag{3}$$

的根得出，其中 Φ_l为阶为 l 的模多项式。当 l 不整除 Δ_π的导子，该方程有两个根，可以取其中一个根 $\hat{j}$，应用 Elikes 算法[17]计算同源的椭圆曲线 $\hat{E}$，进而确定哪个根是曲线 E_1的 j-不变量。

1.3 CSIDH

下面对 CSIDH[5]进行简要描述，其相关的基础代数结构已在前面做出介绍，在此只讨论与本文所构造协议相关的部分。

参数设置：首先确定一个大素数 $p=4\cdot\ell_1\cdots\ell_n-1$，其中$\ell_1,\cdots,\ell_n$为互不相同的小奇素数。由于素数 p 满足 $p\equiv3(\mathrm{mod}4)$，因此可轻易的在$\mathbb{F}_p$上构造出超奇异椭圆曲线，并且在实现中可使用蒙哥马利曲线的形式来表示曲线。每次协议执行所使用的曲线都是取素域为$\mathbb{F}_p$上的，并具有自同态环 $\mathcal{O}=\mathbb{Z}[\pi]$的超奇异椭圆曲线 $E_0:y^2=x^3+x$。

密钥生成：Alice 随机选取 n 元组$(e_1,\cdots,e_n)$作为私钥，其中 $e_i\in\{-t,t\}$。从而可得理想类 $\mathfrak{a}=[\mathfrak{l}_1^{e_1}\cdots\mathfrak{l}_n^{e_n}]\in\mathcal{CL}(\mathcal{O})$，其中$\mathfrak{l}_i=(l_i,\pi-1)$。Alice 计算 $E_A=\mathfrak{a}E_0$，并将曲线 E_A的蒙哥马利系数 A 作为其公钥，对于 Bob 同理。

密钥交换：假设 Alice 和 Bob 分别拥有密钥对$(\mathfrak{a},E_A)$，$(\mathfrak{b},E_B)$。收到 Bob 的公钥 $B\in\mathbb{F}_q\setminus\{-2,2\}$后，验证 E_B是否在环 $\mathcal{E}\ell\ell_p(\mathcal{O},\pi)$中。若不是，则终止，否则通过理想类群作用计算 $\mathfrak{a}E_B=\mathfrak{a}\mathfrak{b}E_0$。Bob 同样通过自己的私钥 $\mathfrak{b}$ 和 Alice 的公钥 A 来计算 $\mathfrak{b}E_A=\mathfrak{b}\mathfrak{a}E_0$。双方可得共享密钥 S，其中 S 为双方共同计算出的曲线形式为 $y^2=x^3+Sx^2+x$ 的蒙哥马利系数。

1.4 基于 CSIDH 的困难问题

本节给出基于 CSIDH 的计算困难问题。为了使表达尽可能简单，默认每个曲线都由其蒙哥马利系数来表示。

问题一：Decisional-CSIDH problem(CSIDDH)：在 CSIDH 中，令 $\mathfrak{a}$，$\mathfrak{b}$，$\mathfrak{t}\xleftarrow{R}\mathcal{CL}(\mathcal{O})$，$b\xleftarrow{R}\{0,1\}$，$E_A=\mathfrak{a}E_0$，$E_B=\mathfrak{b}E_0$。若 $b=0$ 时，$E_Z=\mathfrak{t}E_0$，否则 $E_Z=\mathfrak{a}\mathfrak{b}E_0$。将 E_A、E_B、E_Z作为输入，对任意概率多项式时间算法 $\mathcal{A}$，定义其解决 CSIDDH 的优势为：

$$Adv_{\mathcal{CL}(\mathcal{O})}^{\text{Dec-CSIDH}}(\mathcal{A})=\left|Pr[\mathcal{A}(E_A,E_B,E_Z)=b]-\frac{1}{2}\right| \tag{4}$$

换句话说，如果对手以微不足道的概率成功地区分正确计算的会话密钥和随机密钥，那么该决策问题就很难被解决。

问题二：Computational-CSIDH problem(CSICDH)，在 CSIDH 中，令 $\mathfrak{a}$，$\mathfrak{b}\xleftarrow{R}\mathcal{CL}(\mathcal{O})$，$b\xleftarrow{R}\{0,1\}$，$E_A=\mathfrak{a}E_0$，$E_B=\mathfrak{b}E_0$。给定 E_Z满足 $E_Z=\mathfrak{a}\mathfrak{b}E_0$。将 E_A、E_B作为输入，对任意概率多项式时间算法 $\mathcal{A}$，定义其解决 CSICDH 的优势为：

$$Adv_{\mathcal{CL}(\mathcal{O})}^{\text{Com-CSIDH}}(\mathcal{A})=|Pr[\mathcal{A}(E_A,E_B)=E_Z]| \tag{5}$$

1.5 eCK 安全模型

本节简要回顾 eCK 模型[11]。在该模型中，使用符号 P 来表示由 n 个用户组成的集合，其中用户被建模成多项式时间的概率图灵机，且每个用户 $U_i\in P$ 都拥有静态密钥对(ssk_i,spk_i)，其中静态公钥 spk_i通过证书颁发机构 CA 与其身份绑定在一起，以便其他用户确认其身份。

会话：协议被调用的实例被称为会话，由形式为(U_A,U_B,I)或(U_B,U_A,R,X_A)的输入消息来激活。其中 I 和 R 代表发起者和响应者，为角色标识符，U_A和 U_B为用户标识符。若用户 U_A被消息(U_A,U_B,I)激活，那么 U_A被称作会话的发起者。对应地，若用户 U_B被消息(U_B,U_A,R,X_A)激活，那么 U_B被称作会话的响应者。发起者 U_A输出 X_A，那么就可能收到由响应者 U_B发出的消息(U_A,U_B,I,X_A,X_B)。如果会话 sid 的第一个坐标为 U_A，那么 U_A为会话 sid 的拥有者，如果会话 sid 的第二坐标是 U_A，那么 U_A为会话 sid 的预期会话者。如果会话拥有者计算出对应的会话密钥，则该会话已完成。已完成会话(U_A,U_B,I,X_A,X_B)的匹配会话是(U_B,U_A,R,X_A,X_B)，反之亦然。

敌手模型：敌手 $\mathcal{A}$ 由多项式时间的概率图灵机所建模，可向诚实的一方以及随机预言集合 $\mathcal{H}$ 进行预言查询：$Send(message)$。发送的消息具有形式：(U_A,U_B,I)，(U_B,U_A,R,X_A)，(U_A,U_B,I,X_A,X_B)。

为了捕捉秘密信息的潜在暴露方式，敌手 $\mathcal{A}$ 被允许执行以下几个询问：

(1) $EstablishParty(U)$：根据敌手的选择，额外注册添加一个不在用户集 P 中的用户 U。相对于 P 中的用户，由 $EstablishParty(U)$查询注册的用户被称为不诚实的。我们假设敌手能够完全控制不诚实的一方。

(2) $StaticKeyReveal(U)$：揭示诚实用户 U 的静态私钥。

(3) *EphemeralKeyReveal*(*sid*):揭示由诚实方拥有的属于会话 *sid* 的临时私钥。

(4) *SessionKeyReveal*(*sid*):揭示由诚实方拥有的完整会话 *sid* 的会话密钥。

由于对手可能会对测试会话发起不同程度的破坏,可能能够轻易地解决挑战。为了使安全定义有意义,规定对手应该只对未损坏的会话进行测试询问。因此安全实验必须为 AKE 规定一个"新鲜性"的概念,该概念定义了会话未被损坏的含义。

定义 1(新鲜性)　用 *sid* 来表示诚实用户 U_A、U_B 之间的完整会话 $T_{sid}=(U_A,U_B,role,X,Y)$,令 sid^* 和 sid^e 表示 *sid* 的匹配会话和等价会话。会话 *sid* 是新鲜的当且仅当不满足以下条件:

(1) 敌手 $\mathcal{A}$ 执行 *SessionKeyReveal*(sid^e)。

(2) 若 sid^* 存在,敌手 $\mathcal{A}$ 执行 *SessionKeyReveal*(sid^*)。

(3) 敌手 $\mathcal{A}$ 执行 *StaticKeyReveal*(U_A) 和 *EphemeralKeyReveal*(sid^e)。

(4) 若 sid^* 存在,敌手 $\mathcal{A}$ 执行 *StaticKeyReveal*(U_B) 和 *SessionKeyReveal*(sid^*)。

(5) 若 sid^* 不存在,敌手 $\mathcal{A}$ 执行 *StaticKeyReveal*(U_B)。

对于协议的安全性,考虑以下安全性实验:开始给定敌手 $\mathcal{A}$ 一组诚实的用户,并执行以上的所描述的任意询问。在实验过程中,敌手 $\mathcal{A}$ 执行如下的询问:*Test*(sid^*)。该询问可以在任何阶段对已完成的、新鲜的会话进行作用。随机选取 $b\in_U\{0,1\}$,若 $b=0$ 返回会话密钥,$b=1$ 则返回随机密钥。

该询问用来刻画会话密钥的语义安全,在会话过程中敌手只能进行一次 *Test* 询问。敌手 $\mathcal{A}$ 给出他的猜测 b'时实验停止,如果此刻测试会话 sid^* 仍然是新鲜的,并且敌手 $\mathcal{A}$ 的猜测是正确的($b=b'$),那么敌手 $\mathcal{A}$ 将赢得游戏。

定义 2(eCK 模型安全)　其中敌手 $\mathcal{A}$ 关于该协议的 AKE 安全优势定义为:

$$Adv_{\Pi}^{\mathrm{AKE}}(\mathcal{A})=\left|Pr[b=b']-\frac{1}{2}\right| \tag{6}$$

$Pr[b=b']$为敌手成功区分等长的会话密钥和随机密钥的概率,如果对于任意多项式时间的敌手 $\mathcal{A}$,概率 $Adv_{\Pi}^{\mathrm{AKE}}(\mathcal{A})$都是可忽略的,则称协议是安全的。

2　基于 CSIDH 密钥交换协议的构造

在本节中提出了一个基于 CSIDH 的两轮认证密钥交换协议,并进行了详细的描述,然后对该协议的相关安全属性进行了简要的分析。

2.1　协议描述

本节提出了基于 CSICDH 困难问题的两轮 AKE 协议。

公共参数:除 1.3 小节中已知的参数设定外,另给定两独立散列函数 $H_1:\{-t,\cdots,t\}^{2n}\to\{-t,\cdots,t\}^n$ 和 $H_2:\{0,1\}^*\to\{0,1\}^{\lambda}$,$\lambda$ 为安全参数。

用户注册:用户 U_A随机选取 n 元整数组$\{e_1,\cdots,e_n\}$作为静态私钥来代表理想类群 $\mathfrak{a}=\mathfrak{l}_1^{e_1}\cdots\mathfrak{l}_n^{e_n}\in\mathcal{CL}(\mathcal{O})$,其中 e_i为$\{-t,\cdots,t\}$的随机抽样,$2t+1\geqslant\sqrt[n]{\#|\mathcal{CL}(\mathcal{O})|}$。与其相对应的静态公钥用曲线 $E_A=\mathfrak{a}\times E_0$的蒙哥马利系数 A 来表示,可得密钥对$(\mathfrak{a},E_A)$。相应地,用户 U_B的密钥对记为$(\mathfrak{b},E_B=\mathfrak{b}\times E_0)$。定义 U_A作为协议的发起者,U_B作为协议的响应者。当一方向认证中心注册其静态公钥时,认证中心检查公钥是否为超奇异椭圆曲线,并颁发相关证书。假设每当一个新的会话启动时,每一方都通过证书来获得另一方的公钥。

发起:对于任意会话 *sid*, 用户 U_A秘密随机选取临时密钥$(e'_1,\cdots,e'_n)$,其中 $e'_i\in\{-t,t\}$。通过 NAXOS 技巧对私钥对(esk_{U_A},sk_{U_A})进行变换, 即:

$H_1(esk_{U_A},sk_{U_A})=H_1(e'_1,\cdots,e'_n,e_1,\cdots,e_n)=(x_1,\cdots,x_n)$

对应的临时公钥为 $E_X=[\mathfrak{l}_1^{x_1}\cdots\mathfrak{l}_n^{x_n}]E_0=\mathfrak{x}E_0$。用户 U_A将 E_X发送给 U_B。在此, $H_1(esk_{U_A},sk_{U_A})$并不被认为是一个临时密钥,因为 $H_1(esk_{U_A},sk_{U_A})$可以在任何需要的时候从 esk_{U_A}和 sk_{U_A}计算得到。

响应:在收到用户 U_A的消息后,U_B首先检查 E_X是否为超奇异椭圆曲线。然后同发起阶段, 用户 U_B秘密随机选取临时密钥,通过 NAXOS 技巧对私钥对进行变换, 即 $H_1(esk_{U_B},sk_{U_B})=H_1(\cdots,\cdots)=\{y_1,\cdots,y_n\}$。对应的临时公钥为 $E_Y=[\mathfrak{l}_1^{y_1}\cdots\mathfrak{l}_n^{y_n}]=\mathfrak{y}E_0$,然后将 E_Y发送给 U_A。

协商完成:同样的在收到用户 U_B的消息后,首先检查 E_Y是否为超奇异椭圆曲线。然后双方进行会话密钥的计算。

对于发起者 U_A:

$\sigma_A=(U_A,U_B,j(\mathfrak{a}E_B),j(\mathfrak{a}E_Y),j(\mathfrak{x}E_B),j(\mathfrak{x}E_Y))$

对于响应者 U_B:

$\sigma_B=(U_A,U_B,j(\mathfrak{b}E_A),j(\mathfrak{y}E_A),j(\mathfrak{b}E_X),j(\mathfrak{y}E_X))$

显然 $\sigma_A=\sigma_B$,因此会话 $T_{\mathrm{sid}}=(U_A,U_B,R_{ole},X,Y)$的会话密钥 $K_{AB}=H(\sigma_A)$。

U_A (a,E_A)		U_B (b,E_B)
$esk_{U_A}\leftarrow\{-t,\cdots,t\}^n$		
$H_1(esk_{U_A},sk_{U_A})=\{x_1,\cdots,x_n\}$		
$E_X=[\mathfrak{l}_1^{x_1}\cdots\mathfrak{l}_n^{x_n}]E_0=\mathfrak{x}E_0$	$\xrightarrow{E_X}$	
		$esk_{U_B}\leftarrow\{-t,\cdots,t\}^n$
		$H_1(esk_{U_B},sk_{U_B})=\{y_1,\cdots,y_n\}$
	$\xleftarrow{E_Y}$	$E_Y=[\mathfrak{l}_1^{y_1}\cdots\mathfrak{l}_n^{y_n}]E_0=\mathfrak{y}E_0$
$\sigma_A=(U_A,U_B,j(aE_B),j(aE_Y),j(\mathfrak{x}E_B),j(\mathfrak{x}E_Y))$		
$\sigma_B=(U_A,U_B,j(bE_A),j(\mathfrak{y}E_A),j(bE_X),j(\mathfrak{y}E_X))$		
$H_2(\sigma_A)=K_{AB}=H_2(\sigma_B)$		

2.2 协议的安全属性

本协议除了实现通信双方的隐式认证及 eCK 模型下部分攻击类型的抵抗之外，还可额外抵抗未知密钥共享攻击、冒充攻击、中间人攻击、重放攻击和弱前向安全性等[19]。本节对部分安全属性进行简要的形式化分析。

抗未知密钥共享攻击：当用户 U_A 与另一方 U_B 共同协商生成一个会话密钥时，由于通信双方的身份标识符包含在密钥导出函数中，因此最终协议抵抗未知密钥共享攻击。

抗冒充攻击：假设 CSICDH 问题是困难的，那么只有用户 U_A 和 U_B 能够计算会话密钥 $K(\sigma)$。若敌手试图模仿用户 U_A，显然无法正确计算值 $j(aE_B)$，因为除用户 U_A 外没有任何人可以计算获得 a。同理，在 CSICDH 困难问题假设下该协议可抵抗中间人攻击。

抗重放攻击：在该协议中，参与者 U_A 和 U_B 在每次会话中都需要重新生成临时密钥：$esk\leftarrow\{-t,\cdots,t\}^n$，并通过给定散列函数 H_1 来计算新的 n 元组，进而得到会话密钥。由于每次会话生成的会话密钥都是不同的，因此协议有效防止了重放攻击。

弱前向安全性：在该协议中，会话密钥并不完全由参与者双方的静态公私钥计算得到，而是包含了当前会话的临时私钥。假设用户 U_A 在与 U_B 完成匹配并已得到会话密钥 $K(\sigma)$ 后，存在敌手获得了 U_A 的私钥。但由于敌手不知道会话 *sid* 中所包含的临时私钥 $\mathfrak{x}$，进而无法计算获得 $j(\mathfrak{x}E_B)$ 和 $j(\mathfrak{x}E_Y)$。因此新协议具有弱的完美前向安全性。

注：进行公钥验证可有效防止如无效曲线攻击[15]等潜在攻击方式，而不会泄露任何关于密钥本身的信息。

3 协议的安全性分析

本节在 eCK 模型下证明该协议的安全性。由于篇幅所限，对部分证明过程进行了简化。

定理 1 对于给定的随机预言机 H_1 和 H_2，假设 CSICDH 问题成立，则协议 2.1 在 eCK 模型下是可证明安全的。具体来说，假设参与协议的用户数量为 n 且任意两个用户之间至多有 l 个会话，对任意多项式时间内，至多能进行 $q=q_{H_1}+q_{H_2}$ 次随机预言查询的敌手 $\mathcal{A}$，存在可解决 CSICDH 的模拟算法 $\mathcal{S}$ 使得：

$$Adv_{\mathrm{CSICDH}}^{\mathrm{AKE}}(\mathcal{S})\geqslant\frac{1}{2}\left(\frac{2(1-(n+q_{H_1})/2^{\lambda-1})}{q_{H_2}n^2}+\frac{(1-(l+q_{H_1})/2^{\lambda-1})}{2q_{H_2}nl}\right)Adv_{\Pi}^{\mathrm{AKE}}(\mathcal{A}) \tag{7}$$

证明：由于测试会话的会话密钥是通过对 6 元组 σ 的计算得到的，即 $K=H_2(\sigma)$，因此对手只有以下三种方法来从随机字符串中区分会话密钥 K：

（1）A_1 伪造攻击：敌手 $\mathcal{A}$ 在某时刻对 σ 进行随机预言查询 $H_2(\sigma)$。

（2）A_2 密钥复制攻击：敌手 $\mathcal{A}$ 成功建立与测试会话具有相同会话密钥的另一个会话。

（3）A_3 猜测攻击：敌手正确猜出会话密钥 K。

显然在安全参数 λ 下，敌手正确猜出会话密钥的概率是可忽略的。如果随机预言不产生碰撞，那么密钥复制攻击是不可能的，因为会话密钥的相等意味着相应的 6 元组 σ 相等（通过 H_2 被散列产生会话密钥）。而 σ 决定了会话内容，相同的 σ 意味着该会话应该是测试会话的匹配会话或等效会话。由于不允许敌手 $\mathcal{A}$ 通过查询来揭示匹配会话或等效会话的任何会话密钥，又因为不同的 AKE 会话必须有不同的 6 元组 σ。因此，如果随机预言不产生碰撞（碰撞概率为 $O(l^2/2^{\lambda})$），敌手必须发动伪造攻击。显然：

$$Adv_{\Pi}^{\mathrm{AKE}}(\mathcal{A})\leqslant\frac{1}{2}\Pr[A_1] \tag{8}$$

接下来，证明如果敌手可以发动一次成功的伪造攻击，那么可以构造一个使用 $\mathcal{A}$ 作为子程序的 CSICDH 求解模拟算法 $\mathcal{S}$。剩下的大部分证明都致力于 $\mathcal{S}$ 的构造。

定义以下两个事件：

E_1：在测试会话具有匹配会话的前提下，敌手 $\mathcal{A}$ 对测试会话进行伪造攻击。

E_2：在测试会话没有匹配会话的前提下，敌手 $\mathcal{A}$ 对测试会话进行伪造攻击。

因此有：

$$\Pr[A_1]\leqslant\Pr[E_1]+\Pr[E_2] \tag{9}$$

对事件 E_1 的分析：

模拟者 $\mathcal{S}$ 准备 n 个用户并随机分配密钥对，并将

至少以 $2/n^2$ 的概率独立地随机选择测试会话 sid 以及匹配会话 sid^*。将它们的临时公钥设置为 E_A 和 E_B,这里我们假定会话 sid 和 sid^* 分别归用户 U_A 和 U_B 所有。在此情况下,若敌手 $\mathcal{A}$ 成功地进行了伪造攻击,那么说明模拟者 $\mathcal{S}$ 成功的解决了 CSICDH 问题。

下面模拟 $\mathcal{A}$ 对 $\sigma=(U_A,U_B,*,Z,*,*)$ 进行 H_2 查询,由于无法检查等式 $E_Z=CDH(E_A,E_B)$ 是否成立,因此 $\mathcal{S}$ 将在对随机预言 H_2 发出的 q_{H_2} 次查询的结果中随机挑选一个值。敌手 $\mathcal{A}$ 若要成功区分模拟实验和真实实验,唯一的方法是向 $(esk_{\mathrm{sid}},sk_{U_A})$ 和 $(esk_{\mathrm{sid}^*},sk_{U_B})$ 进行随机预言 H_1 查询,验证 E_A 和 E_B 是否成立。由于 sid 是新鲜会话,且 eCK 模型不允许敌手在测试会话中同时对某个用户以及属于该用户的会话 sid 进行 $StaticKeyReveal(U)$ 和 $EphemeralKeyReveal(sid)$ 查询。由于 H_1 是抗碰撞的,因此敌手正确得到 $H_1(esk_{\mathrm{sid}},sk_{U_A})$ 或 $H_1(esk_{\mathrm{sid}^*},sk_{U_B})$ 的概率至多为 $(n+q_{H_1})/2^{\lambda-1}$。因此 $\mathcal{S}$ 和 $\mathcal{A}$ 的优势存在以下关系:

$$Adv^{\mathrm{AKE}}_{\mathrm{CSI\text{-}CDH}}(S)\geqslant\frac{2}{q_{H_2}n^2}(1-(n+q_{H_1})/2^{\lambda-1})Adv^{\mathrm{AKE}}_{\Pi^+}(\mathcal{A}) \tag{10}$$

对事件 E_2 的分析:

模拟者 $\mathcal{S}$ 在 n 个用户中随机选取一个用户 U_B,假设 $\mathcal{S}$ 不知道其静态私钥,从而无法获得相应静态公钥。为了在多项式时间内解决 CSICDH 问题,$\mathcal{S}$ 将对由 U_B 发起的,并由 U_C 参与的会话进行如下处理,其中用户 C 已经完全被敌手 $\mathcal{A}$ 控制。$\mathcal{S}$ 随机选择 esk_{sid^*} 作为 U_B 的临时私钥使其静态公钥。

在对敌手 $\mathcal{A}$ 的模拟过程中,sid 是预期目标用户 U_B 的测试会话的概率为 $1/nl$,$\mathcal{A}$ 对 $\sigma=(U_A,U_B,*,*,Z,*)$ 或 $\sigma=(U_A,U_B,*,Z,*,*)$ 进行 H_2 查询。同样的,由于无法检查等式 $E_Z=CDH(E_A,E_B)$ 是否成立,因此 $\mathcal{S}$ 将在对随机预言 H_2 发出的 m_2 次查询的结果中随机挑选一个值。$\mathcal{A}$ 对 $(esk_{\mathrm{sid}},sk_{U_A})$ 进行 H_1 查询,并验证 E_A 是否成立。同理,该事件发生的概率至多为 $(n+q_{H_1})/2^{\lambda-1}$,因此 $\mathcal{S}$ 和 $\mathcal{A}$ 的优势存在以下关系:

$$Adv^{\mathrm{AKE}}_{\mathrm{CSICDH}}(\mathcal{S})\geqslant\frac{1}{q_{H_2}nl}(1-(l+q_{H_1})/2^{\lambda-1})Adv^{\mathrm{AKE}}_{\Pi}(\mathcal{A}) \tag{11}$$

4　对比及总结

4.1　效率分析

为满足更多的安全属性,在协议设计过程中难免会导致额外的计算量。与协议 Gal_2[12] 相比,本协议需要多进行 1 次哈希运算和 2 次同源计算,但 CSIDH 算法在进行公钥的生成和验证时计算速度快、空间占用小,在双方交互过程中没有额外的可能造成安全隐患的信息,被传送等特点,如 $\phi(P)$,并且曲线定义在 $\mathbb{F}_p$ 上。因此本协议不仅满足更多的安全属性,而且具有参数生成高效的优势,并进一步节省了信息传输所需要的宽带。

目前基于同源的密码体制大多是在蒙哥马利曲线 $E_a:y^2=x^3+ax^2+x$ 上实现,因为它们可提供快速有效的同源计算。在 SIDH 方案实现的基础上,通过进一步限制条件参数:令 $p=7\bmod 8$,通过利用 2-挠点计算恢复蒙哥马利曲线的系数。

在射影坐标下,对于 2-挠点 $P=(X:Z)$,令 ϕ 为 ℓ -同源,$\ker\phi=\langle P\rangle$。因此 $P'=\phi(P)=(X':Z')$,其中 $X'=X(\prod_{i=1}^{d}(XX_i-Z_iZ))^2$,$Z'=Z(\prod_{i=1}^{d}(XZ_i-X_iZ))^2$,$x_i=X_i/Z_i$ 为 $[i]P$ 的 x-坐标,$1\leqslant i\leqslant d$。对于 ℓ -同源,$P'=\phi\langle P\rangle=(X':Z')$ 计算成本为 $(4d)M+2S+(6d)a$,其中 M、s、a 分别表示 $\mathbb{F}_p$ 中乘法、平方和加法的运算成本。然后通过方程 $a'=-(\alpha'^2-1)/\alpha'$ 恢复曲线 $E_{a'}$ 的系数,在射影坐标下该方程被表示为 $a'=(A':C')=((X_\alpha+Z_\alpha)^2:(X_\alpha-Z_\alpha)^2-(X_\alpha+Z_\alpha)^2)$,需要 $2S+3a$ 的计算成本。

4.2　协议对比

本节分别从安全性能和计算效率等方面将本文协议与其他基于超奇异同源的 AKE 协议进行简单的对比,结果如表 1 所示。

表 1　基于超奇异同源的认证密钥交换协议对比

协议	假设	模型	Key Reg.	MEX	KCI	Isog.
Gal_1[12]	SICDH	CK	Honest	×	×	6
Gal_2[12]	SICDH	BR	Honest	×	√	8
Longa[13]	SIDDH	CK	Arbitrary	√	×	12
SIAKE_2[18]	SIDDH	CK^+	Arbitrary	√	√	11
本文	CSICHD	eCK	Arbitrary	√	√	10

其中:“Key Reg.”表示协议所支持的静态公钥注册类型,“Arbitrary”表示允许任意类型注册,而“Honest”则表示只允许诚实的注册者,该项反映了协议是否抗自适应性攻击。“MEX”表示最大暴露攻击(Maximal-Exposure Attacks),“KCI”表示密钥泄露模拟攻击(Key Compromise Impersonation)。符号“√”表示协议

可抵抗该攻击性质,而“×”则相反;“Isog.”形式化地表示了协议所需的同源计算次数。

5 结 语

针对 Galbraith 等提出的一个基于 SICDH 问题假设,AKE 协议存在易于遭受最大暴露攻击,不能抵抗自适应性攻击等缺点,本文通过使用 NAXOS 技巧,并将通信双方静态密钥的 Diffie-Hellman 值添加到会话密钥的计算中,提出了一个新的基于 CSIDH 的两轮认证密钥交换协议,并给出了安全性证明。该协议避免了 SIDH 上存在的代数结构问题,是目前第一个基于 CSICDH 问题假设,并在 eCK 模型下可证明安全的 AKE 协议。经对比,该协议具有更强的安全属性,具体表现在能够抵抗最大暴露攻击和密钥泄露模拟攻击,且允许敌手对任意静态公钥进行注册,这意味着能够抵抗自适应性攻击。下一步工作是通过利用具有强安全性的抗量子伪随机函数,将长密钥和短密钥交替用作密钥派生函数和伪随机函数的输入,构造出在标准模型下可证明安全的认证密钥交换协议。

参 考 文 献

[1] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Journal on Computing,1999,41(2):7011.

[2] Boyd C, Mathuria A, Stebila D. Protocols for authentication and key establishment[M]. Heidelberg: Springer,2020.

[3] Hvelmanns K, Kiltz E, Schge S. Generic authenticated key exchange in the quantum random oracle model[M]. Cham: Springer,2020.

[4] Feo L D, Jao D, Plût J. Towards quantum resistant cryptosystems from supersingular elliptic curve isogenies[J]. Journal of Mathematical Cryptology,2014,8(3):209 - 247.

[5] Castryck W, Lange T, Martindale C, et al. CSIDH: An efficient post-quantum commutative group action[C]//24th International Conference on the Theory and Application of Cryptology and Information Security,2018:395 - 427.

[6] Kock B, Gjøsteen K, Veroni M. Practical isogeny-based key-exchange with optimal tightness[C]//27th International Conference on Cryptography,2020:451 - 479.

[7] Terada S, Yoneyama K. Password-based authenticated key exchange from standard isogeny assumptions[C]//13th International Conference on Provable Security,2019:41 - 56.

[8] 冯克勤. 交换代数基础[M]. 北京:高等教育出版社,1985.

[9] Lee J, Park J H. Authenticated key exchange secure under the computational Diffie-Hellman assumption[EB/OL]. [2021 - 03 - 21]. https://eprint.iacr.org/2008/344.pdf.

[10] Vélu J. Isogénies entre courbes elliptiques[J]. C. R. Acad. Sci. Paris, Sér A-B,1971, 273:238 - 241.

[11] Lamacchia B, Lauter K, Mityagin A. Stronger security of authenticated key exchange[C]//International Conference on Provable Security,2007:73.

[12] Galbraith S D. Authenticated key exchange for SIDH[EB/OL]. [2021 - 03 - 21]. https://eprint.iacr.org/2018/266.pdf.

[13] Longa P. A note on post-quantum authenticated key exchange from supersingular isogenies[EB/OL]. [2021 - 03 - 21]. https://eprint.iacr.org/2018/267.pdf.

[14] Fujioka A, Takashima K, Terada S, et al. supersingular isogeny Diffie-Hellman authenticated key exchange[EB/OL]. [2021 - 03 - 21]. https://eprint.iacr.org/2018/730.pdf.

[15] Antipa A, Brown D R, Menezes A, et al. Validation of elliptic curve public keys[C]//6th International Workshop on Theory and Practice in Public Key Cryptography,2003: 211 - 223.

[16] Couveignes J M. Hard homogeneous spaces[EB/OL]. [2021 - 03 - 21]. https://eprint.iacr.org/2006/291.pdf.

[17] Galbraith S D. Mathematics of public key cryptography[J]. Computers & Security,2012,20(7):612 - 619.

[18] Xu X, Xue H Y, Wang K P. Strongly secure authenticated key exchange from supersingular isogenies[C]//25th International Conference on the Theory and Application of Cryptology and Information Security,2019:278 - 308.

[19] 李子臣,张亚泽,张峰娟. 一种新型基于 Binary-LWE 的认证密钥交换协议[J]. 计算机应用与软件,2017,34(11): 284 - 289.

(上接第 334 页)

[14] Wang Q, Chen M, Nie F. Detecting coherent groups in crowd scenes by multiview clustering[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence,2018,42(1): 46 - 58.

[15] 宋悦. 不完整多视觉数据聚类分析[D]. 西安:西安电子科技大学,2019.

[16] 姬名书. 基于稀疏嵌入框架的不完全多视图聚类[D]. 南昌:南昌大学,2019.

[17] Yang Y, Wang H. Multi-view clustering: A survey[J]. Big Data Mining and Analytics,2018,31(2): 83 - 107.

[18] Zhan K, Niu C,Chen C. Graph structure fusion for multiview clustering[J]. IEEE Transactions on Knowledge and Data Engineering,2018,31(10): 1984 - 1993.