基于同源的抗量子群密钥交换协议

樊雪君[1],王 龙[1],徐 秀[2],宋宁宁[1],范 晶[1],王 怡[1]
(1.华北计算机系统工程研究所,北京 100083;2.中国信息通信研究院,北京 100191)

摘 要:面对越来越多的基于群成员协同操作的需求,群密钥交换协议在近期的研究中受到了广泛的关注。基于同源的密码协议是抗量子密码中的重要组成部分,因此文章主要关注基于同源的群密钥交换协议。针对超奇异同源的困难问题,提出了两个2轮的基于超奇异同源的群密钥交换协议,均是针对 Burmester-Desmedt(BD)协议的优化。此外,为了证明协议的安全性,分别针对两个优化版本的群密钥交换协议给出了安全性证明。通过与现有的协议进行比较,可发现所提出的两个协议在通信量和计算复杂度上都有所降低。

关键词:抗量子;超奇异同源;SIDH;密钥交换协议
中图分类号:TP309.7 **文献标识码**:A **DOI**:10.19358/j.issn.2096-5133.2022.05.001
引用格式:樊雪君,王龙,徐秀,等. 基于同源的抗量子群密钥交换协议[J].信息技术与网络安全,2022,41(5):1-8.

Group key exchange protocols from supersingular isogenies

Fan Xuejun[1], Wang Long[1], Xu Xiu[2], Song Ningning[1], Fan Jing[1], Wang Yi[1]
(1.National Computer System Engineering Research Institute of China, Beijing 100083, China;
2.China Academy of Information and Communication Technology, Beijing 100191, China)

Abstract: Group key exchange(GKE) protocols get much attention in current research with increasing applicability in numerous group-oriented and collaborative applications. Isogeny-based cryptosystem is one of the significant components of post-quantum cryptography, so this paper mainly considers the group key exchange protocol based on isogeny. In this paper, we propose two schemes on supersingular isogenies. They all have two rounds. They are optimizations of Burmester-Desmedt(BD) protocol without authentication. We give formal proofs for their security. We also give a comparison of our methods and these existing GKE protocols. Compared with the existing protocols, the results show that our methods are more efficient in the view of communication and computation time.

Key words: post quantum; supersingular isogeny; SIDH; key exchange protocol

0 引言

基于同源的密码协议是抗量子密码中的重要组成部分,它依赖于计算给定椭圆曲线之间同源的困难性,该困难问题在量子算法攻击下的时间复杂度是(亚)指数级别的。目前基于同源的密钥交换协议有三类:OIDH(基于常曲线同源的密钥交换协议)、SIDH(基于超奇异同源的密钥交换协议)和 CSIDH(基于可交换的超奇异同源的密钥交换协议)。相比于其他抗量子密码协议,基于同源的密码体制的优势是密钥长度短,劣势是协议效率低。本文主要考虑了基于同源的群密钥交换协议,从调整协议的模型的角度来讨论基于同源的密钥交换协议的加速。

1 研究背景及研究内容

1.1 研究背景

群密钥交换(GKE)协议允许多个参与方在公共网络上协商共享密钥,现已被广泛地应用于现实世界的交互网络中,比如 Ad-hoc 网络和无线传感网络等。目前大部分的群密钥交换方案[1-3]都是从两方的密钥交换协议扩展而来的。

但是目前针对抗量子的群密钥交换方案还比较少。Apon 等人[4]将 BD 协议推广到环 LWE 问题上,得到了格上的群密钥交换协议。基于同源的群密钥

交换协议也逐渐得到关注，Furukawa 等人[5]提出了两个基于超奇异同源的多方密钥交换协议。第一个是 SIDH 协议的变形，域的特征变为 $p=f\cdot\prod_{i=1}^{n} l_i^{e_i}\pm 1$，参与方的数量会影响 p 的选取。第二个是传统 BD 协议[1]的变形，但其乘法运算的数量较多，降低了协议的效率。Azarderakhsh 等人[6]构造了 n 方群密钥交换协议，每个用户在发送下一条信息之前都必须使用自己的私钥信息进行计算，即提供了隐式认证，但是该方案也有很多缺陷：第一，如果参与方的数量 n 发生了变化，则有限域的特征 $p=f\cdot\prod_{i=1}^{n} l_i^{e_i}\pm 1$ 也需要更改；第二，方案每个用户需要计算 $n-1$ 个同源和 $(n-1)n$ 个点的像，单个用户传输的比特数可达到 $O(\lambda n^2)$（λ 是安全参数）量级，故方案的计算复杂度和通信量较高；第三，该方案没有安全性证明。因此，研究基于超奇异同源的群密钥交换协议是非常有意义的。

1.2 本文工作及结构

本文提出了两个 2 轮的基于超奇异同源的抗量子群密钥交换协议。第一个是对基于超奇异同源的 BD 协议—SIBD 协议[5]的加速。由于 BD 协议中单个用户的通信量较高，研究者们便考虑了树形的 BDII 模型[7]，故本文的第二个方案便是 SIDH 和 BDII 协议[3]的结合。在这两个 GKE 协议中，本文都更换了会话密钥的计算方式，使用有限域中的加减法而不是乘除法来进行计算，从而提高了整个协议的计算效率，使其可以被微型处理器接受。此外本文还给出了两个方案针对被动攻击者的安全性证明，最后对协议的轮数、通信量以及计算复杂度进行了分析。与现有的基于超奇异同源的 GKE 协议[5]比较，本文所提协议具有较小的计算复杂度和较高的通信效率。

2 基础知识

2.1 SIDH 协议

2.1.1 SIDH 协议形式

De Feo 等人[8]利用 $\mathbb{F}_{p^2}$ 上的超奇异椭圆曲线构造了 SIDH 协议。由于 $\mathbb{F}_{p^2}$ 上的超奇异椭圆曲线的自同态环是非交换的，故 SIDH 协议的量子攻击复杂度为指数时间[9]。

SIDH 协议[6]使用了有理点的个数有很多小素数做因子的超奇异曲线，这样曲线有很多小次数的同源，从而可提高计算效率。特别地，取超奇异椭圆曲线 $E/\mathbb{F}_{p^2}$，其中 $p=l_A^{e_A}l_B^{e_B}\cdot f\pm 1$ 是素数，l_A 和 l_B 是小素数，f 是使得 p 是素数的调节因数，则 $\#E/(\mathbb{F}_{p^2})=(l_A^{e_A}l_B^{e_B}\cdot f)^2$。$E[l_A^{e_A}]$（或 $E[l_B^{e_B}]$）是 $\mathbb{F}_{p^2}$ 有理的，且包含 $l_A^{e_A-1}(l_A+1)$（或 $l_B^{e_B-1}(l_B+1)$）个阶为 $l_A^{e_A}$（或 $l_B^{e_B}$）的循环子群，这些循环子群对应了不同构的同源。令 $E[l_A^{e_A}]=\langle P_A,Q_A\rangle$，$E[l_B^{e_B}]=\langle P_B,Q_B\rangle$，$(E,P_A,Q_A,P_B,Q_B)$ 是公共参数，SIDH 协议的具体执行过程如图 1 所示。

Alice 和 Bob 通过密钥交换分别获得曲线 E_{AB} 和 E_{BA}，且 $E_{AB}\cong E_{BA}\cong E/\langle[m_A]P_A+[n_A]Q_A,[m_B]P_B+[n_B]Q_B\rangle$，因此协议双方可共享 E_{AB} 和 E_{BA} 的 j-不变量。

值得注意的是，Alice 的私钥 m_A、n_A 不能同时被 l_A 整除，以保证 $\ker\psi_A=l_A^{e_A}$，对 Bob 的私钥 m_B、n_B 也有类似要求。在具体执行过程中，一般取 $l_A=2$，$l_B=3$。且为了减少标量乘的计算、提高协议的效率，会不失一般性地取 $m_A=m_B=1$，且 n_A 和 n_B 分别在 $\mathbb{Z}/l_A^{e_A}\mathbb{Z}$ 和 $\mathbb{Z}/l_B^{e_B}\mathbb{Z}$ 中随机均匀选取。

图 2 给出了更直观的协议双方进行的操作。

值得一提的是，基于 SIDH 协议构造的密钥封装协议 SIKE[10]已经被提交到 NIST 算法竞赛中，并成

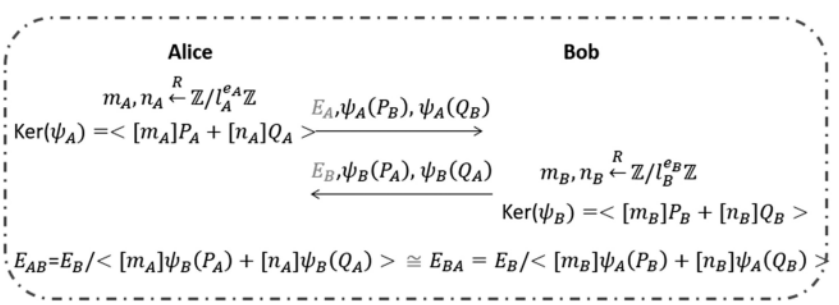

图 1 基于 $\mathbb{F}_{p^2}$ 上的超奇异椭圆曲线的密钥交换协议(SIDH)

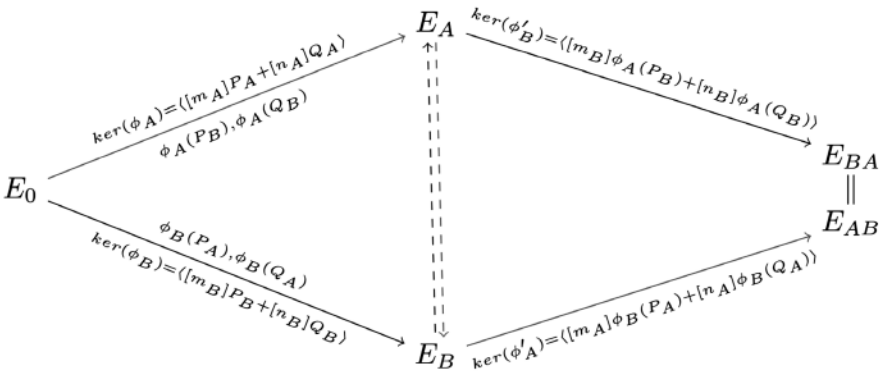

图 2 SIDH 协议的直观执行图

为第三轮候选算法。

2.1.2 SIDH 协议的基本困难问题

首先利用 DH 语言来描述一下 SIDH 协议，以便后续安全性证明中使用。

设$\{t,s\}=\{0,1\}$，记公钥参数为$\mathfrak{g}=(E_0;P_0,Q_0,P_1,Q_1)$和$\mathfrak{e}=(l_0;l_1,e_0,e_1)$。定义超奇异椭圆曲线的集合及曲线和点构成三元组的集合：

$SSEC_p=\{$定义在$\mathbb{F}_{p^2}$上超奇异椭圆曲线$E:E(\mathbb{F}_{p^2})\simeq(\mathbb{Z}_{l_0^{e_0}l_1^{e_1}f})^2\}$

$SSEC_A=\{(E;P_t^{'},Q_t^{'})|E\in SSEC_p,(P_t^{'},Q_t^{'})$是$E[l_t^{e_t}]$的基$\}$

$SSEC_B=\{(E;P_s^{'},Q_s^{'})|E\in SSEC_p,(P_s^{'},Q_s^{'})$是$E[l_s^{e_s}]$的基$\}$

记$\mathfrak{a}=k_a$且$\mathfrak{b}=k_b$，则可以定义：

$\mathfrak{g}^{\mathfrak{a}}=(E_A;\phi_A(P_t),\phi_A(Q_t))\in SSEC_A$

其中$R_A=P_s+[k_a]Q_s,\phi_A:E_0\rightarrow E_A=E_0/\langle R_A\rangle$。

$\mathfrak{g}^{\mathfrak{b}}=(E_B;\phi_B(P_s),\phi_B(Q_s))\in SSEC_B$

其中$R_B=P_t+[k_b]Q_t,\phi_B:E_0\rightarrow E_B=E_0/\langle R_B\rangle$。

$(\mathfrak{g}^{\mathfrak{b}})^{\mathfrak{a}}=j(E_{BA})$

其中$R_{BA}=\phi_B(P_s)+[k_a]\phi_B(Q_s),\phi_{BA}:E_B\rightarrow E_{BA}=E_B/\langle R_{BA}\rangle$。

$(\mathfrak{g}^{\mathfrak{a}})^{\mathfrak{b}}=j(E_{AB})$

其中$R_{AB}=\phi_A(P_t)+[k_b]\phi_A(Q_t),\phi_{AB}:E_A\rightarrow E_{AB}=E_A/\langle R_{AB}\rangle$。

值得注意的是，本文定义$\mathfrak{g}^{\mathfrak{a}}$和$\mathfrak{g}^{\mathfrak{b}}$是群，而定义$(\mathfrak{g}^{\mathfrak{b}})^{\mathfrak{a}}$和$(\mathfrak{g}^{\mathfrak{a}})^{\mathfrak{b}}$是$j$-不变量。这并不是出现了错误，只是将 SIDH 协议的形式与传统的 Diffie-Hellman(DH)密钥交换协议的形式结合起来。利用上述符号，便可发现 SIDH 协议的形式与 DH 协议形式几乎完全相同。公共参数为$\mathfrak{g}$和$\mathfrak{e}$，Alice 选择私钥$\mathfrak{a}$并发送$\mathfrak{g}^{\mathfrak{a}}$给 Bob，Bob 选择私钥$\mathfrak{b}$并发送$\mathfrak{g}^{\mathfrak{b}}$给 Alice，最终共享密钥为$j=(\mathfrak{g}^{\mathfrak{b}})^{\mathfrak{a}}=(\mathfrak{g}^{\mathfrak{a}})^{\mathfrak{b}}$。基于符号定义，本文描述两个关于超奇异同源的标准假设：

定义 1 (SI-DDH 假设[7]) 给定公共参数$\mathfrak{g}$和$\mathfrak{e}$，定义两个分布D_0和D_1：

$D_1:=\{\mathfrak{e},\mathfrak{g},\mathfrak{g}^{\mathfrak{a}},\mathfrak{g}^{\mathfrak{b}},(\mathfrak{g}^{\mathfrak{a}})^{\mathfrak{b}}|\mathfrak{a}\leftarrow\mathbb{Z}_{l_s^{e_s}},\mathfrak{b}\leftarrow\mathbb{Z}_{l_t^{e_t}}\}$

$D_0:=\{\mathfrak{e},\mathfrak{g},\mathfrak{g}^{\mathfrak{a}},\mathfrak{g}^{\mathfrak{b}},(\mathfrak{g}^{\mathfrak{s}})^{\mathfrak{t}}|\mathfrak{a},\mathfrak{s}\leftarrow\mathbb{Z}_{l_s^{e_s}},\mathfrak{b},\mathfrak{t}\leftarrow\mathbb{Z}_{l_t^{e_t}}\}$

SI-DDH 问题指的是，随机给定一个分布D_b，其中$b\leftarrow\{0,1\}$，猜测b的值。对于多项式时间的算法$\mathcal{A}$，定义其解决 SI-DDH 问题的优势为：

$$Adv_{\mathcal{A}}^{SIDDH}=2|Pr[b'=b|b'\leftarrow\mathcal{A}(\sigma_b\leftarrow D_b),b\leftarrow\{0,1\}]-1/2|$$

则 SI-DDH 假设指的是，对于任意多项式时间的算法$\mathcal{A}$，解决 SI-DDH 问题的优势都是可忽略的。

2.2 SIBD 协议的安全模型

针对群密钥交换协议的安全性，由于本文是以 SIDH 协议为基础构造的群密钥交换协议，因此本文考虑文献[11]中的认证链接攻击者模型。在证明过程中假设所有协议的参与方都是诚实的。

假设协议中共有n个参与方$\mathcal{U}=\{U_1,U_1,\cdots,U_n\}$，每个参与者都可以同时运行多个事件。记参与者$U$的第$i$个事件为$\prod_U^i$，会话标识为 sid，会话参与者标识为 pid。

GKE 模型的安全性是由一系列挑战者和攻击者$\mathcal{A}$之间的游戏定义的。在游戏过程中，敌手$\mathcal{A}$可以通过询问下列问题解决某个挑战：

Execute($\prod_U^i$)：返回诚实执行$\prod_U^i$过程中的交互信息。这是被动攻击所执行的。

RevealKey($\prod_U^i$)：当事件$\prod_U^i$被接受，便输出群会话密钥。

Corrupt(U_i)：该询问泄露 U_i 的静态密钥。如果敌手未进行 Corrupt 询问，则参与者是诚实的。

Test($\prod_U^i$)：在接受事件 $\prod_U^i$ 中进行该询问，该询问在整个执行过程中只能出现一次。

在安全性证明的过程中，允许敌手 $\mathcal{A}$ 执行 Test 询问。令 κ 是当前会话过程中的会话密钥，挑战者随机选取 $b\in\{1,0\}$，若 $b=1$ 则向敌手发送当前的会话密钥；否则便向敌手发送密钥空间中的随机元素。如果敌手在会话 s 过期之前就向相应的 oracle 询问了 s 或者 $\prod_U^i$，则称参与方 $\prod_U^i$ 的会话都是本地公开的。如果 s 在过期之前，s 或者其匹配会话 s' 是本地公开的，则称 s 被暴露；否则，证 s 是新鲜的会话。

在 Test 询问的前后，攻击者都可以进行自适应的查询，即询问挑战者关于测试会话以外的其他问题。最后，攻击者 $\mathcal{A}$ 猜测比特 b'，令 $\mathrm{Succ}^{\mathcal{A}}(\lambda)$ 是挑战者 $\mathcal{A}$ 猜对 $b=b'$ 的概率，其中 λ 是安全参数，则定义：

$$\mathrm{Adv}^{\mathcal{A}}(\lambda)=\max\{0,|\Pr[\mathrm{Succ}^{\mathcal{A}}(\lambda)]-\frac{1}{2}|\}$$

定义 2 (Session－Key 安全) 设密钥交换协议的安全参数为 λ，若对于任意多项式时间的敌手 $\mathcal{A}$，均满足：若未被 Corrupt 询问的两方完成了匹配会话，则会话便输出相同的密钥，且 $\mathrm{Adv}^{\mathcal{A}}(\lambda)$ 是可忽略的。则称该密钥交换协议是 Session－Key 安全的。

3 改进的基于超奇异同源的群密钥交换协议

本节将 SIDH 协议分别与 BD 协议和 BDII 协议结合，并利用加法运算代替会话密钥计算过程中的乘法运算，从而得到了更高效的 2 轮群密钥交换协议。

3.1 改进的 SIBD 协议

Furukawa 等人[5]以 SIDH 协议为基础推广 BDI 协议，从而得到了 SIBD 协议。本文将其会话密钥计算过程中的乘除法更换为加减法，从而优化了 SIBD 协议，还给出了抵抗被动攻击的安全性证明。

群密钥交换协议中的公共参数与 SIDH 协议的公共参数相同，设协议中共有 n 个参与方，依次标号为 $1,2,\cdots,n$，记 $U_{n+1}=U_1$，则 n 个参与方可构成一个环形。当 n 是奇数时，可以使其中某个参与者虚拟地扮演两个角色。因此可只考虑 n 是偶数的情况。下面为改进的 SIBD 协议流程。

第 1 轮：每个用户 U_i 随机选取 $k_i\in\mathbb{Z}_{l_s^{e_s}}$ 作为私钥，计算 $R_i=P_s+k_iQ_s$，其中 $s=i(\mathrm{mod}\ 2)$。然后计算同源 $\phi_i:E\to E_i=E/\langle R_i\rangle$，令 $\mathrm{pk}_i^1=(E_i,\phi_i(P_{1-s}),\phi_i(Q_{1-s}))$，$\mathrm{sk}_i^1=k_i$，将 pk_i^1 广播给 U_{i-1} 和 U_{i+1}。

第 2 轮：每个用户 U_i 收到相邻两方发送来的公钥 pk_{i-1}^1 和 pk_{i+1}^1，利用收到的公钥和自己的私钥 sk_i^1 执行 SIDH 协议，可得 $K_i^L=j_{i-1,i}$ 和 $K_i^R=j_{i,i+1}$，其中 $j_{i-1,i}$ 和 $j_{i,i+1}$ 分别代表了 $E_{i-1}/\langle\phi_{i-1}(P_s)+k_i\phi_{i-1}(Q_s)\rangle$ 和 $E_{i+1}/\langle\phi_{i+1}(P_s)+k_i\phi_{i+1}(Q_s)\rangle$ 的 j－不变量。最后，用户 U_i 向所有参与方广播 $\mathrm{pk}_i^2=u_i=j_{i,i+1}-j_{i-1,i}$。

计算会话密钥：每个用户 U_i 利用哈希函数 $H:\{0,1\}^*\to\{0,1\}^\lambda$，其中 λ 是安全参数，计算会话密钥 $K_i=H(nj_{i-1,i}+(n-1)u_i+(n-2)u_{i+1}+\cdots+2u_{i-3}+u_{i-2})$，可以验证，对于任意 i，均有：

$$K_i=H(j_{1,2}+\cdots+j_{n,1})=K$$

需要强调，相比于有限域中的乘法，加法计算的复杂度可以被忽略，这便是改进的 SIBD 协议效率提高的主要原因。关于安全强度，GKE 协议中最基本的安全性要求便是 SK－安全(SK－security)，即对被动攻击者来说会话密钥不可区分。

定理 1 在 SI－DDH 的假设下，改进的 SIBD 协议在随机谕言机模型下是安全的，并且可以达到前向安全性。即如果存在 n 个用户，敌手 $\mathcal{A}$ 询问 q_E 次 Execute，该协议满足 $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{GKE}}(q_E)\leqslant 2n\mathrm{Adv}_{\mathcal{A}}^{\mathrm{SIDDH}}+\frac{2nq_E}{p}$。

证明：由于协议中没有静态密钥，故敌手可以忽略 Corrupt 询问，因此该协议满足前向安全性。

现假设存在敌手 $\mathcal{A}$ 可以攻击改进的 SIBD 协议，证明可以构造区分器 $\mathcal{D}$ 以不可忽略的优势解决 SI－DDH 问题。敌手 $\mathcal{A}$ 可以询问 Execute、RevealKey 和 Test。设 $T=(\mathrm{pk}_i^1,\mathrm{pk}_i^2)$ 是一次执行过程的记录，K 是该过程得到的会话密钥，则可定义两个分布 Real 和 Fake。其中 Real 是真实协议执行产生的分布，而 Fake 中的 pk_i^2 是在 $\mathbb{F}_{p^2}$ 中随机选取且满足 $\sum_i \mathrm{pk}_i^2=0$。记 $\mathrm{g}^{l_i}=(E_i,\phi_i(P_{1-s}),\phi_i(Q_{1-s}))$，$\phi_i:E\to E_i=E/\langle P_s+l_iQ_s\rangle$，

则：

$$\text{Real}=\left\{\begin{array}{l}\mathfrak{k}_1,\cdots,\mathfrak{k}_n\in\mathbb{Z}_{\ell_s^{e_s}};\\ pk_1^1=\mathfrak{g}^{\mathfrak{k}_1},\cdots,pk_n^1=\mathfrak{g}^{\mathfrak{k}_n},\\ K_1^R=K_2^L=j(\mathfrak{g}^{\mathfrak{k}_1\mathfrak{k}_2}),\cdots,K_n^R=K_1^L=j(\mathfrak{g}^{\mathfrak{k}_n\mathfrak{k}_1});\\ pk_1^2=K_1^R-K_1^L,\cdots,pk_n^2=K_n^R-K_n^L;\\ T=(pk_1^1,\cdots,pk_n^1;pk_1^2,\cdots,pk_n^2);\\ K=H(nj(\mathfrak{g}^{\mathfrak{k}_{i-1}\mathfrak{k}_i})+(n-1)pk_i^2+(n-2)pk_{i+1}^2+\cdots+pk_{i-2}^2)\end{array}:(T,K)\right\}$$

$$\text{Fake}=\left\{\begin{array}{l}\mathfrak{k}_1,\cdots,\mathfrak{k}_n\in\mathbb{Z}_{\ell_s^{e_s}};\\ pk_1^1=\mathfrak{g}^{\mathfrak{k}_1},\cdots,pk_n^1=\mathfrak{g}^{\mathfrak{k}_n},\\ K_1^R=K_2^L=j(\mathfrak{g}^{\mathfrak{s}_1\mathfrak{s}_2}),\cdots,K_n^R=K_1^L=j(\mathfrak{g}^{\mathfrak{s}_n\mathfrak{s}_1}):\mathfrak{s}_1,\cdots,\mathfrak{s}_n\in\mathbb{Z}_{\ell_s^{e_s}};\\ pk_1^2=K_1^R-K_1^L,\cdots,pk_n^2=K_n^R-K_n^L;\\ T=(pk_1^1,\cdots,pk_n^1;pk_1^2,\cdots,pk_n^2);\\ K=H(nj(\mathfrak{g}^{\mathfrak{k}_{i-1}\mathfrak{k}_i})+(n-1)pk_i^2+(n-2)pk_{i+1}^2+\cdots+pk_{i-2}^2)\end{array}:(T,K)\right\}$$

断言 1 对于任意敌手 $\mathcal{A}$，有 $|\Pr[(T,K)\leftarrow\text{Real}:\mathcal{A}(T,K)=1]-\Pr[(T,K)\leftarrow\text{Fake}':\mathcal{A}(T,K)=1]|\leqslant \text{Adv}_{\mathcal{A}}^{\text{SIDDH}}+\frac{1}{p}$，**其中：**

$$\text{Fake}'=\left\{\begin{array}{l}\mathfrak{k}_1,\cdots,\mathfrak{k}_n\in\mathbb{Z}_{\ell_s^{e_s}};\\ pk_1^1=\mathfrak{g}^{\mathfrak{k}_1},\cdots,pk_n^1=\mathfrak{g}^{\mathfrak{k}_n},\\ K_1^R=K_2^L=j(\mathfrak{g}^{\mathfrak{k}_1\mathfrak{k}_2}),\cdots,K_{n-1}^R=K_n^L=j(\mathfrak{g}^{\mathfrak{k}_{n-1}\mathfrak{k}_n}),\\ K_n^R=K_1^L=j(\mathfrak{g}^{\mathfrak{s}_n\mathfrak{s}_1});\mathfrak{s}_1,\mathfrak{s}_n\in\mathbb{Z}_{\ell_s^{e_s}};\\ pk_1^2=K_1^R-K_1^L,\cdots,pk_n^2=K_n^R-K_n^L;\\ T=(pk_1^1,\cdots,pk_n^1;pk_1^2,\cdots,pk_n^2);\\ K=H(nj(\mathfrak{g}^{\mathfrak{k}_{i-1}\mathfrak{k}_i})+(n-1)pk_i^2+(n-2)pk_{i+1}^2+\cdots+pk_{i-2}^2)\end{array}:(T,K)\right\}$$

证明：设存在一个针对 SI-DDH **问题的区分器** $\mathcal{D}$。$\mathcal{D}$ **调用敌手** $\mathcal{A}$，**输入与** SIDH **协议中相同的** $(\mathfrak{g}^{\mathfrak{a}},\mathfrak{g}^{\mathfrak{b}},\mathfrak{g}^{\mathfrak{c}})$，**根据分布** Dist′ **生成** (T,K)，**然后输出敌手** $\mathcal{A}$ **的输出结果。其中：**

$$\text{Dist}'=\left\{\begin{array}{l}\mathfrak{k}_1,\cdots,\mathfrak{k}_n\in\mathbb{Z}_{\ell_s^{e_s}};\\ pk_1^1=\mathfrak{g}^{\mathfrak{a}},pk_2^1=\mathfrak{g}^{\mathfrak{k}_2},\cdots,pk_{n-1}^1=\mathfrak{g}^{\mathfrak{k}_{n-1}},pk_n^1=\mathfrak{g}^{\mathfrak{b}},\\ K_1^R=K_2^L=j(\mathfrak{g}^{\mathfrak{a}\mathfrak{k}_2}),K_2^R=K_3^L=j(\mathfrak{g}^{\mathfrak{k}_2\mathfrak{k}_3}),\cdots,\\ K_{n-2}^R=K_{n-1}^L=j(\mathfrak{g}^{\mathfrak{k}_{n-2}\mathfrak{k}_{n-1}}),\\ K_{n-1}^R=K_n^L=j(\mathfrak{g}^{\mathfrak{k}_{n-1}\mathfrak{b}}),K_n^R=K_1^L=j(\mathfrak{g}^{\mathfrak{c}});\\ pk_1^2=K_1^R-K_1^L,\cdots,pk_n^2=K_n^R-K_n^L;\\ T=(pk_1^1,\cdots,pk_n^1;pk_1^2,\cdots,pk_n^2);\\ K=H(nj(\mathfrak{g}^{\mathfrak{k}_{i-1}\mathfrak{k}_i})+(n-1)pk_i^2+(n-2)pk_{i+1}^2+\cdots+pk_{i-2}^2)\end{array}:(T,K)\right\}$$

如果 $\mathfrak{l}_i$ **是随机的，则分布** Real **与分布** $\{\mathfrak{a},\mathfrak{b}\in\mathbb{Z}_{l_s^{e_s}};(T,K)\leftarrow\text{Dist}':(T,K)\}$ **在统计意义下是等价的。此外，除了一个** $\frac{1}{p}$ **的因子，分布** Fake′ **与分布** $\{\mathfrak{a},\mathfrak{b}\in\mathbb{Z}_{l_s^{e_s}},\mathfrak{c}\neq\mathfrak{a}\mathfrak{b};(T,K)\leftarrow\text{Dist}':(T,K)\}$ **在统计意义下是等价的。因此通过** SI-DDH **问题的归约可以得到分布** Real **和** Fake′ **在统计意义下是等价的。**

断言 2 对于任意敌手 $\mathcal{A}$，**均有** $|\Pr[(T,K)\leftarrow\text{Fake}':\mathcal{A}(T,K)=1]-\Pr[(T,K)\leftarrow\text{Fake}:\mathcal{A}(T,K)=1]|\leqslant(n-1)\text{Adv}_{\mathcal{A}}^{\text{SIDDH}}+\frac{n-1}{p}$。

证明：仿照断言 1 中的结论，定义分布

$$\text{Fake}^{(1)}=\left\{\begin{array}{l}\mathfrak{k}_1,\cdots,\mathfrak{k}_n\in\mathbb{Z}_{\ell_s^{e_s}};\\ pk_1^1=\mathfrak{g}^{\mathfrak{k}_1},\cdots,pk_n^1=\mathfrak{g}^{\mathfrak{k}_n};K_1^R=K_2^L=j(\mathfrak{g}^{\mathfrak{k}_1\mathfrak{k}_2});\\ K_2^R=K_3^L=j(\mathfrak{g}^{\mathfrak{s}_2\mathfrak{s}_3}),\cdots,K_n^R=K_1^L=j(\mathfrak{g}^{\mathfrak{s}_n\mathfrak{s}_1});\mathfrak{s}_1,\cdots,\mathfrak{s}_n\in\mathbb{Z}_{\ell_s^{e_s}};\\ pk_1^2=K_1^R-K_1^L,\cdots,pk_n^2=K_n^R-K_n^L;\\ T=(pk_1^1,\cdots,pk_n^1;pk_1^2,\cdots,pk_n^2);\\ K=H(nj(\mathfrak{g}^{\mathfrak{k}_{i-1}\mathfrak{k}_i})+(n-1)pk_i^2+(n-2)pk_{i+1}^2+\cdots+pk_{i-2}^2)\end{array}:(T,K)\right\}$$

便可得：

$$|\Pr[(T,K)\leftarrow\text{Fake}:\mathcal{A}(T,K)=1]-\Pr[(T,K)\leftarrow\text{Fake}^{(1)}:\mathcal{A}(T,K)=1]|\leqslant\text{Adv}_{\mathcal{A}}^{\text{SIDDH}}+\frac{1}{p}$$

然后利用 hybrid **方法可以得到：**

$$|\Pr[(T,K)\leftarrow\text{Fake}':\mathcal{A}(T,K)=1]-\Pr[(T,K)\leftarrow\text{Fake}:\mathcal{A}(T,K)=1]|\leqslant(n-1)\text{Adv}_{\mathcal{A}}^{\text{SIDDH}}+\frac{n-1}{p}$$

断言 3 对于任意敌手 $\mathcal{A}$，**均有** $|\Pr[(T,K_0)\leftarrow\text{Fake};K_1\leftarrow\mathbb{F}_{p^2};b\leftarrow\{0,1\}:\mathcal{A}(T,K_b)=b]|=\frac{1}{2}$。

证明：因为 $\text{pk}_1^2+\text{pk}_2^2+\cdots+\text{pk}_n^2=0$，**所以在记录** T **中得不到任何关于会话密钥** $K=H(j_{1,2}+\cdots+j_{n,1})$ **的信息。故可得：**

$$|\Pr[(T,K_0)\leftarrow\text{Fake};K_1\leftarrow\mathbb{F}_{p^2};b\leftarrow\{0,1\}:\mathcal{A}(T,K_b)=b]|=\frac{1}{2}$$

综合以上三个断言可知：

$$\text{Adv}_{\mathcal{A}}^{\text{GKE}}=|2\Pr[\mathcal{A}\text{wins}]-1|=2|\Pr[(T,K_0)\leftarrow\text{Real},K_1\leftarrow\mathbb{F}_{p^2},b\leftarrow\{0,1\}:\mathcal{A}(T,K_b)=b]-\frac{1}{2}|=2|\Pr[T,K_0]\leftarrow\text{Real},K_1\leftarrow\mathbb{F}_{p^2},b\leftarrow\{0,1\}:\mathcal{A}(T,K_b)=b]-\Pr[T,K_0]\leftarrow\text{Fake},K_1\leftarrow\mathbb{F}_{p^2},b\leftarrow\{0,1\}:\mathcal{A}(T,K_b)=b]|$$

总结上述结论，可得 $\text{Adv}_{\mathcal{A}}^{\text{GKE}}\leqslant 2n\text{Adv}_{\mathcal{A}}^{\text{SIDDH}}+\frac{2n}{p}$。

q_E **次询问的过程都是类似的，因此** $\text{Adv}_{\mathcal{A}}^{\text{GKE}}(q_E)=2|\Pr[T,K_0]\leftarrow\text{Real},K_1\leftarrow\mathbb{F}_{p^2},b\leftarrow\{0,1\}:\mathcal{A}(T,K_b)=b]-\Pr[T,K_0]\leftarrow\text{Fake},K_1\leftarrow\mathbb{F}_{p^2},b\leftarrow\{0,1\}:\mathcal{A}(T,K_b)=$

$b]|\leqslant 2n\mathrm{Adv}_{\mathcal{A}}^{\mathrm{SIDDH}}+\frac{2nq_E}{p}$。

定理 1 证毕。

3.2 改进的 SIBDII 协议

由于 BD 协议的通信量较高，故考虑使用树形结构的 BDII 协议。在广播版本中，BDII 协议的每个用户的通信量和计算复杂度均为 $O(\log(n))$，故本节结合 SIDH 协议给出优化的 SIBDII 协议。协议中 n 个用户被标识为 $1,2,\cdots,n$(n 为偶数)，且用户按照其标识被依次放置于树形结构上(如图 3 所示)。

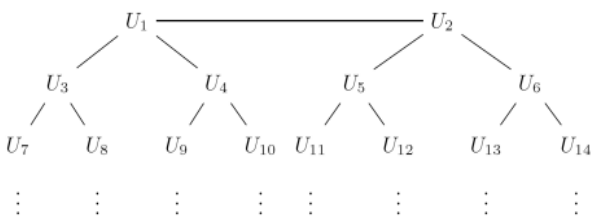

图 3 BDII 协议中的二元树

从图 3 中可以发现，用户 U_i 位于树的第$\lfloor\log_2(i+1)\rfloor$层。记用户 U_i 的父母、左孩子和右孩子的标识分别为 $\mathrm{parent}(i)$、$l_{\mathrm{child}}(i)$和 $r_{\mathrm{child}}(i)$，U_1 和 U_2 分别是对方的父母。则树上所有除叶子节点之外的节点均有一个父母和两个孩子。令 $\mathrm{ancestors}(i)$为用户 U_i 的所有祖先的标识构成的集合，其中 $i\in\mathrm{ancestors}(i)$但 $1,2\notin\mathrm{ancestors}(i)$。为了保证用户 U_i 和 $U_{\mathrm{parent}(i)}$在公共曲线 E 的两个不同子集中进行计算，令 $s(1)=0$，$s=s(i)=s(\mathrm{parent}(i))+1\pmod 2$用于标识两个不同的子集。改进的 SIBDII 协议的公共参数与 SIDH 的参数相同，其具体执行过程如下：

第 1 轮：用户 U_i 随机选择私钥 $k_i\in\mathbb{Z}_{l_s^{e_s}}$并计算 $R_i=P_s+k_iQ_s$，以$\langle R_i\rangle$为核计算同源 $\phi_i:E\to E_i=E/\langle R_i\rangle$，令 $\mathrm{pk}_i^1=(E_i,\phi_i(P_{1-s}),\phi_i(Q_{1-s}))$，$\mathrm{sk}_i^1=k_i$，并将 pk_i^1 广播给父母和两个孩子。

第 2 轮：用户 U_i 收到父母及其两个孩子的公钥 $\mathrm{pk}_{\mathrm{parent}(i)}^1$，$\mathrm{pk}_{l_{\mathrm{child}}(i)}^1$和 $\mathrm{pk}_{r_{\mathrm{child}}(i)}^1$，并利用这些公钥和自己的私钥 sk_i^1 执行 SIDH 密钥交换协议，可得$K_i^P=j_{\mathrm{parent}(i),i}=E_{\mathrm{parent}(i)}/\langle\phi_{\mathrm{parent}(i)}(P_s)+k_i\phi_{\mathrm{parent}(i)}(Q_s)\rangle$，$K_i^L=j_{i,l_{\mathrm{child}}(i)}=E_{l_{\mathrm{child}}(i)}/\langle\phi_{l_{\mathrm{child}}(i)}(P_s)+k_i\phi_{l_{\mathrm{child}}(i)}(Q_s)\rangle$和 $K_i^R=j_{i,r_{\mathrm{child}}(i)}=E_{r_{\mathrm{child}}(i)}/\langle\phi_{r_{\mathrm{child}}(i)}(P_s)+k_i\phi_{r_{\mathrm{child}}(i)}(Q_s)\rangle$。然后用户 U_i 计算 $\mathrm{pk}_i^2=(u_{l_{\mathrm{child}}(i)},u_{r_{\mathrm{child}}(i)})=(j_{\mathrm{parent}(i),i}-j_{i,l_{\mathrm{child}}(i)},j_{\mathrm{parent}(i),i}-j_{i,r_{\mathrm{child}}(i)})$，并将结果广播给其后代。

会话密钥计算：用户 U_i 利用哈希函数 $H:\{0,1\}^*\to\{0,1\}^\lambda$，其中 λ 为安全参数，计算会话密钥 $K_i=H(j_{\mathrm{parent}(i),i}+\sum_{m\in\mathrm{ancestors}(i)}X_m)$，其中 $X_m=j_{\mathrm{parent}(\mathrm{parent}(m)),\mathrm{parent}(m)}-j_{\mathrm{parent}(m),m}$。

容易验证，对于任意 i 均有 $K_i=H(j_{1,2})=K$。值得注意的是，在改进的 SIBDII 协议中，仍使用加法运算来计算会话密钥，从而提高了整个协议的效率。

定理 2 在 SI-DDH 假设下，改进的 SIBDII 群密钥交换协议在随机谕言机模型下可抵抗被动攻击，并且满足前向安全性。即如果有 n 个参与者，敌手攻击 k 次会话过程，询问 q_E 次 Execute，则该方案满足 $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{GKE}'}(q_E)\leqslant k(n-1)\mathrm{Adv}_{\mathcal{A}}^{\mathrm{SIDDH}}$。

证明：由于协议中没有静态密钥，敌手可以忽略 Corrupt 询问，故该协议满足前向安全性。

假设改进的 SIBDII 群密钥交换协议存在敌手 $\mathcal{A}$，可以构造区分器 $\mathcal{D}$ 调用 $\mathcal{A}$，以不可忽略的概率解决 SI-DDH 问题。敌手 $\mathcal{A}$ 可以询问 Execute、RevealKey 和 Test。设 $T=(\mathrm{pk}_i^1,\mathrm{pk}_i^2)$是一次执行过程的记录，$K$ 是该过程得到的会话密钥，则可定义两个分布 Real 和 Fake。其中Real 是真实协议执行产生的分布，而 Fake 中的 pk_i^2 是在 $\mathbb{F}_{p^2}$ 中随机选取的。记 $\mathfrak{g}^{l_i}=(E_i,\phi_i(P_{1-s}),\phi_i(Q_{1-s}))$，$\phi_i:E\to E_i=E/\langle P_s+l_iQ_s\rangle$。

$$\mathrm{Real}=\left\{\begin{array}{l}\mathfrak{k}_1,\cdots,\mathfrak{k}_n\in\mathbb{Z}_{l_s^{e_s}};\quad pk_1^1=\mathfrak{g}^{\mathfrak{k}_1},\cdots,pk_n^1=\mathfrak{g}^{\mathfrak{k}_n};\\ K_1^P=K_2^P=j(\mathfrak{g}^{\mathfrak{k}_1\mathfrak{k}_2}),\ \text{and for } 3\leq i\leq\frac{n}{2}-1\\ K_i^L=K_{2i+1}^P=j(\mathfrak{g}^{\mathfrak{k}_i\mathfrak{k}_{2i+1}}),K_i^R=K_{2i+2}^P=j(\mathfrak{g}^{\mathfrak{k}_i\mathfrak{k}_{2i+2}}),\\ pk_1^2=(K_1^P-K_1^L,K_1^P-K_1^R),\cdots,pk_n^2=(K_n^P-K_n^L,K_n^P-K_n^R);\\ T=(pk_1^1,\cdots,pk_n^1;pk_1^2,\cdots,pk_n^2);\\ K=H(K_i^P+\sum_{m\in\mathrm{ancestors}(i)}(K_{\mathrm{parent}(m)}^P-K_m^P))\end{array}:(T,K)\right\}$$

$$\mathrm{Fake}=\left\{\begin{array}{l}\mathfrak{k}_1,\cdots,\mathfrak{k}_n\in\mathbb{Z}_{l_s^{e_s}};\quad pk_1^1=\mathfrak{g}^{\mathfrak{k}_1},\cdots,pk_n^1=\mathfrak{g}^{\mathfrak{k}_n};\\ K_1^P=K_2^P=j(\mathfrak{g}^{\mathfrak{s}_1\mathfrak{s}_2}),\ \text{and for } 3\leq i\leq\frac{n}{2}-1:\\ K_i^L=K_{2i+1}^P=j(\mathfrak{g}^{\mathfrak{s}_i\mathfrak{s}_{2i+1}}),K_i^R=K_{2i+2}^P=j(\mathfrak{g}^{\mathfrak{s}_i\mathfrak{s}_{2i+2}}),\mathfrak{s}_1,\cdots,\mathfrak{s}_n\in\mathbb{Z}_{l_s^{e_s}};\\ pk_1^2=(K_1^P-K_1^L,K_1^P-K_1^R),\cdots,pk_n^2=(K_n^P-K_n^L,K_n^P-K_n^R);\\ T=(pk_1^1,\cdots,pk_n^1;pk_1^2,\cdots,pk_n^2);\\ K=H(K_i^P+\sum_{m\in\mathrm{ancestors}(i)}(K_{\mathrm{parent}(m)}^P-K_m^P))\end{array}:(T,K)\right\}$$

使用 hybrid 方法计算$|\Pr[T,K_0]\leftarrow\mathrm{Real},K_1\leftarrow\mathbb{F}_{p^2},b\leftarrow\{0,1\}:\mathcal{A}(T,K_b)=b]-\Pr[T,K_0]\leftarrow\mathrm{Fake},K_1\leftarrow\mathbb{F}_{p^2},$

$b\leftarrow\{0,1\}:\mathcal{A}(T,K_b)=b]|$

需要定义分布：

$$\mathrm{Fake}^1=\left\{\begin{array}{l}\mathfrak{k}_1,\cdots,\mathfrak{k}_n\in\mathbb{Z}_{\ell^{\mathfrak{g}}_{\mathfrak{g}}};\quad pk_1^1=\mathfrak{g}^{\mathfrak{k}_1},\cdots,pk_n^1=\mathfrak{g}^{\mathfrak{k}_n};\\ K_1^P=K_2^P=j(\mathfrak{g}^{\mathfrak{s}_1\mathfrak{s}_2}),\mathfrak{s}_1,\cdots,\mathfrak{s}_n\in\mathbb{Z}_{\ell^{\mathfrak{g}}_{\mathfrak{g}}};\\ \text{for } 3\le i\le\dfrac{n}{2}-1:\\ K_i^L=K_{2i+1}^P=j(\mathfrak{g}^{\mathfrak{k}_i\mathfrak{k}_{2i+1}}),K_i^R=K_{2i+2}^P=j(\mathfrak{g}^{\mathfrak{k}_i\mathfrak{k}_{2i+2}});\\ pk_1^2=(K_1^P-K_1^L,K_1^P-K_1^R),\cdots,pk_n^2=(K_n^P-K_n^L,K_n^P-K_n^R);\\ T=(pk_1^1,\cdots,pk_n^1;pk_1^2,\cdots,pk_n^2);\\ K=H(K_i^P+\sum_{m\in\mathrm{ancestors}(i)}(K_{\mathrm{parent}(m)}^P-K_m^P))\end{array}\right\}:(T,K)$$

断言 4 对于任意敌手 $\mathcal{A}$，均有 $|\Pr[(T,K_0)\leftarrow\mathrm{Fake};K_1\leftarrow\mathbb{F}_{p^2};b\leftarrow\{0,1\}:\mathcal{A}(T,K_b)=b]|=\frac{1}{2}$。

断言 5 对于任意敌手 $\mathcal{A}'$，有 $|\Pr[(T,K)\leftarrow\mathrm{Real}:\mathcal{A}'(T,K)=1]-\Pr[(T,K)\leftarrow\mathrm{Fake}^1:\mathcal{A}'(T,K)=1]|=\frac{k}{2}\mathrm{Adv}_{\mathcal{A}}^{\mathrm{SIDDH}}$，其中 k 是敌手攻击会话过程数目的上界。

证明：会话过程可匹配的概率为 $\frac{1}{k}$，故可构造区分器 $\mathcal{D}$ 解决 SI-DDH 问题(算法 1)，其最终的攻击优势为：

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{SIDDH}}=\frac{\mathrm{Adv}_{\mathcal{A}'}}{k}=\frac{2|\Pr[(T,K)\leftarrow\mathrm{Real}:\mathcal{A}'(T,K)=1]-\Pr[(T,K)\leftarrow\mathrm{Fake}^1:\mathcal{A}'(T,K)=1]|}{k}$$

断言 6 对于任意敌手 $\mathcal{A}$，均有 $|\Pr[(T,K)\leftarrow\mathrm{Fake}:\mathcal{A}'(T,K)=1]-\Pr[(T,K)\leftarrow\mathrm{Fake}^1:\mathcal{A}'(T,K)=1]|=k(n-\frac{3}{2})\mathrm{Adv}_{\mathcal{A}}^{\mathrm{SIDDH}}$。

总结上述三个断言，可得：

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{GKE}}=|2\Pr[\mathcal{A}\mathrm{wins}]-1|=2|\Pr[(T,K_0)\leftarrow\mathrm{Real},K_1\leftarrow\mathbb{F}_{p^2},b\leftarrow\{0,1\}:\mathcal{A}(T,K_b)=b]-\frac{1}{2}|=2|\Pr[T,K_0]\leftarrow\mathrm{Real},K_1\leftarrow\mathbb{F}_{p^2},b\leftarrow\{0,1\}:\mathcal{A}(T,K_b)=b]-\Pr[T,K_0]\leftarrow\mathrm{Fake},K_1\leftarrow\mathbb{F}_{p^2},b\leftarrow\{0,1\}:\mathcal{A}(T,K_b)=b]|\le k(n-1)\mathrm{Adv}_{\mathcal{A}}^{\mathrm{SIDDH}}$$

定理 2 证毕。

4 协议比较

4.1 复杂度分析

改进的 SIBD 协议是 BD 协议的变形，本文更换了会话密钥的计算方式，将 j-不变量之间的乘法变为加法。原 SIBD 协议[5]中需要 $\frac{n^2+n}{2}$ 次乘法，而改进的SIBD 协议中只需要 $(n-1)$ 次乘法和 n 次加法。改进的 SIBDII 协议是 BDII 协议的变形，其计算复杂度为 $O(\log(n))$。

一个群密钥交换协议的通信复杂度是由协议的轮数及各用户每次交互信息的大小决定的。选择参考文献[9]中的参数，在 λ 比特安全强度下，p 的比特长度应为 6λ，则 $\mathbb{F}_{p^2}$ 中元素的比特长度为 12λ。由于曲线是定义在 $\mathbb{F}_{p^2}$ 上的，故曲线和点的表示都需要 12λ bit(见表1)。

表 1 群密钥交换协议的比较

协议	单个用户交互信息量	计算复杂度
SIBD	$(48n-48)\lambda$	$3\mathrm{Iso}+\frac{n^2+n}{2}M$
改进 SIBD	$(12n+60)\lambda$	$3\mathrm{Iso}+(n-1)M+nA$
改进 SIBDII	$(12\lfloor\log_2(n+1)\rfloor+96)\lambda$	$4\mathrm{Iso}+(\lfloor\log_2(n+1)\rfloor+1)A$

注：1)为了方便比较，树形结构中每个用户在一次密钥协商中交互信息的大小，本文取的是上界，用户 U_i 每次交互信息的大小实际为 $(12\lfloor\log_2(i+1)\rfloor+96)\lambda$ bit。

2)表中 Iso 代表计算一次同源需要的计算量，M 代表有限域 $\mathbb{F}_{p^2}$ 中一次乘法的计算量，A 代表有限域 $\mathbb{F}_{p^2}$ 中一次加法的计算量。为了方便阐述，视平方的运算量与乘法的运算量相等。

表 1 中结果是以一个用户为单位来计算通信复杂度和计算复杂度的。而对于一次密钥交换过程中所有用户交互的总信息量来说，改进的 SIBD 协议中所有用户交互信息的总和为 $(12\lfloor\log_2(n+1)\rfloor+96)n\lambda$ bit，改进的 SIBDII 协议中所有用户交互信息的总和为 $\sum_{i=1}^{n}[(12\lfloor\log_2(i+1)\rfloor+96)\lambda]$ bit。

4.2 环形结构和树形结构的比较

通过两类群密钥交换协议的通信复杂度和计算复杂度的比较可以发现：在树形结构的群密钥交换协议中，每个用户的通信复杂度和计算复杂度都是 $O(\log(n))$ 级别的；而在环形结构的群密钥交换协议中，通信复杂度和计算复杂度都是 $O(n)$ 级别的(其中 n 为用户数量)。这是否意味着基于树形结构的群密钥交换协议更好呢？本小节主要比较了环形结构和树形结构在应用场景和计算性能等方面的表现。

首先假定协议的各个参与方的计算能力相当。否则，若存在一个可信用户 U_i，其计算能力远大于

其他用户的计算能力，则可以使用环形结构的变形：用户 U_i 与其他 $n-1$ 个用户分别交互获得密钥，进行计算后再统一广播给其他参与方。此时用户 U_i 的计算复杂度是其他用户的 $n-1$ 倍。在通信复杂度方面，记 B 是广播所需通信量，P 是点对点交互所需的通信量，则用户 U_i 的通信量是 $2B+(n-1)P$，其他用户的通信量为 $2P$。

在计算复杂度方面，如果各个参与方的计算能力相当，环形结构的计算复杂度为 $O(n)$ 量级，而树形结构的计算复杂度为 $O(\log(n))$ 量级，因此树形结构更优。在通信复杂度上，环形结构中用到了广播的通信模式，而树形结构中用到的是多方传播的通信模式。由于协议的参与方数量有限，因此此处不区分广播和多方传播的通信复杂度，则有如下比较（见表 2）。

表 2 树形结构和环形结构中单用户通信量比较

结构	发送消息	接收消息
树形结构	$3P+B$	$3P+\log_2(i)B$
环形结构	$2P+B$	$2P+(n-1)B$

总之，尽管使用了环形结构的 BD 协议具有很好的代数结构，但是由于其总体的通信复杂度高，故很少被应用于实际场景中[12]。

5 结论

本文主要利用 SIDH 协议构造了两个改进的群密钥交换协议。通过安全性证明，本文所提出的协议可以归约到 SI-DDH 问题，因此在量子攻击下是安全的，此外，通过与现有的基于超奇异同源的群密钥交换协议比较，所提协议的计算复杂度和通信量都更低。

参考文献

[1] BURMESTER M, DESMEDT Y. A secure and efficient conference key distribution system[C]//Advances in Cryptology-Eurocrypt'94, 1994: 275-286.

[2] BURMESTER M, DESMEDT Y. A secure and scalable group key exchange system[J]. Information Processing Letters, 2005, 94(3): 137-143.

[3] BURMESTER M, DESMEDT Y. Efficient and secure conference-key distribution[C]//International Workshop on Security Protocols. Springer-Verlag, 1996.

[4] APON D, DACHMAN-SOLED D, GONG H, et al. Constant-round group key exchange from the ring-LWE assumption[C]//International Conference on Post-Quantum Cryptography, Chongqing, China, 2019: 189-205.

[5] FURUKAWA S, KUNIHIRO N, TAKASHIMA K. Multi-party key exchange protocols from supersingular isogenies[C]//2018 International Symposium on Information Theory and Its Applications (ISITA), 2018.

[6] FUJIOKA A, TAKASHIMA K, TERADA S, et al. Supersingular isogeny diffie - hellman authenticated key exchange[C]//International Conference on Information Security and Cryptology, 2018: 177-195.

[7] KIM Y, PERRIG A, TSUDIK G. Tree-based group key agreement[J]. ACM Transactions on Information and System Security, 2004, 7(1): 60-96.

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

[9] COSTELLO C, LONGA P, NAEHRIG M. Efficient algorithms for supersingular isogeny diffie-hellman[C]//Advances in Cryptology-CRYPTO 2016, 2016: 572-601.

[10] JAO D, AZARDERAKHSH R, CAMPAGNA M, et al. Supersingular isogeny key encapsulation(NIST Round 2)[J]. IEEE Transactions on Computers, 2020.

[11] CANETTI R, KRAWCZYK H. Analysis of key-exchange protocols and their use for building secure channels[C]//International Conference on the Theory & Application of Cryptographic Techniques: Advances in Cryptology. Springer Berlin Heidelberg, 2001: 453-474.

[12] YVO D, TANJA L, MIKE B. Scalable authenticated tree based group key exchange for Ad-Hoc groups[C]//Financial Cryptography and Data Security, 11th International Conference, 2007: 104-118.

（收稿日期：2021-09-11）

作者简介：

樊雪君（1993-），女，博士，主要研究方向：后量子密码学、信息安全。

王龙（1990-），通信作者，男，硕士，高级工程师，主要研究方向：信息安全。E-mail：peakwl@qq.com。

徐秀（1992-），女，博士，主要研究方向：密码学、信息安全。

版权声明

经作者授权，本论文版权和信息网络传播权归属于《信息技术与网络安全》杂志，凡未经本刊书面同意任何机构、组织和个人不得擅自复印、汇编、翻译和进行信息网络传播。未经本刊书面同意，禁止一切互联网论文资源平台非法上传、收录本论文。

截至目前，本论文已经授权被中国期刊全文数据库（CNKI）、万方数据知识服务平台、中文科技期刊数据库（维普网）、JST 日本科技技术振兴机构数据库等数据库全文收录。

对于违反上述禁止行为并违法使用本论文的机构、组织和个人，本刊将采取一切必要法律行动来维护正当权益。

特此声明！

《信息技术与网络安全》编辑部

中国电子信息产业集团有限公司第六研究所