

椭圆曲线上高效可完全模拟的不经意传输协议

宋佳烁, 李祯祯, 丁海洋, 李子臣

(北京印刷学院数字版权保护技术研究中心, 北京 102600)

摘要: 不经意传输协议是安全多方计算的一个关键技术, 是当前网络与信息安全研究的热点。基于双线性对及椭圆曲线上的困难问题, 分别设计了半诚实模型下和标准恶意模型下的安全高效 N 选 1 不经意传输协议。在半诚实模型下设计了一个椭圆曲线上的不经意传输协议, 该协议只需 2 轮交互, 接收方需要 2 次双线性对运算和 1 次椭圆曲线倍点运算, 发送方需要 n 次椭圆曲线倍点运算和 n 次模幂运算, 协议的安全可规约到椭圆曲线上的离散对数问题; 构建了基于椭圆曲线上双线性对的零知识证明方案, 并设计了一个恶意模型下的不经意传输协议, 该协议只需 3 轮交互, 接收者需要 3 次双线性对运算和 3 次椭圆曲线倍点运算, 发送者需要 $n+1$ 次椭圆曲线倍点运算和 $n+1$ 次模幂运算, 协议能在标准恶意模型下抵抗参与者的恶意攻击行为。实验结果得到在半诚实模型下协议平均运行时间需要 0.787 9 s, 在标准恶意模型下协议平均运行时间需要 1.205 6 s, 进一步论证协议的速度。

关键词: 不经意传输; 完全模拟; 双线性对; 零知识证明; 安全多方计算

中图分类号: TP309

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2023012

Efficient and fully simulated oblivious transfer protocol on elliptic curve

SONG Jiashuo, LI Zhenzhen, DING Haiyang, LI Zichen

Digital Rights Management Research Center, Beijing Institute of Graphic Communication, Beijing 102600, China

收稿日期: 2022-03-24; **修回日期:** 2022-10-13

通信作者: 宋佳烁, 694248412@qq.com

基金项目: 国家自然科学基金 (61370188); 北京市教委科研计划 (KM202010015009, KM202110015004); 北京印刷学院博士启动金项目 (27170120003/020); 北京印刷学院科研创新团队项目 (Eb202101); 北京印刷学院校内学科建设项目 (21090121021); 北京印刷学院重点教改项目 (22150121033/009); 北京印刷学院科研基础研究一般项目 (Ec202201)

Foundation Items: The National Natural Science Foundation of China (61370188), Beijing Municipal Education Commission Scientific Research Project (KM202010015009, KM202110015004), Beijing Institute of Graphic Communication Doctoral Funding Project (27170120003/020), Beijing Institute of Graphic Communication Research Innovation Team Project (Eb202101), Intramural Discipline Construction Project of Beijing Institute of Graphic Communication (21090121021), Key Educational Reform Project of Beijing Institute of Graphic Communication (22150121033/009), General Research Project of Basic Research of Beijing Institute of Graphic Communication (Ec202201), The BIGC Project (Ec202201) and the Initial Funding for the Doctoral Program of BIGC (27170122006)

引用格式: 宋佳烁, 李祯祯, 丁海洋, 等. 椭圆曲线上高效可完全模拟的不经意传输协议[J]. 网络与信息安全学报, 2023, 9(1): 158-166.

Citation Format: SONG J S, LI Z Z, DING H Y, et al. Efficient and fully simulated oblivious transfer protocol on elliptic curve[J]. Chinese Journal of Network and Information Security, 2023, 9(1): 158-166.

Abstract: Oblivious transfer protocol, an important technology in secure multi-party computation, is the research hotspot on network and information security. Based on the bilinear pairs and the difficult problems on elliptic curves, an efficient 1-out-of- N oblivious transfer protocol in the semi-honest model and in the standard malicious model were proposed respectively. The protocol in semi-honest model was designed. It only needed two rounds of interaction. The receiver needed two times of bilinear pair arithmetic and one time of multi point arithmetic, and the sender needed n times of multi point arithmetic and n times of modular exponentiation. The security of the protocol was based on the discrete logarithm problem on elliptic curves. A zero-knowledge proof protocol and the oblivious transfer protocol in the standard malicious model were proposed respectively. The oblivious transfer protocol only needed four rounds of interaction. The receiver needed three times of bilinear pair arithmetic and three times of multi point arithmetic, and the sender needed $n+1$ times of multi point arithmetic and $n+1$ times of modular exponentiation. Besides, it can resist malicious behaviors of the party. The results show that the average running time of the protocol in the semi-honest model and in the standard malicious model were 0.787 9 s and 1.205 6 s respectively, which can further demonstrate the efficiency of the protocol.

Keywords: oblivious transfer, fully simulation, bilinear pairing, zero-knowledge proof, secure multi-party computation

0 引言

随着物联网、大数据和云计算的快速发展,网络社会给人们的生活带来了极大便利,但同时带来了很大的隐私保护问题,尤其是大数据流通市场存在很多风险。为了在提供便利的同时保证人们的隐私,密码学者提出了很多隐私计算技术,如安全多方计算^[1]、不经意传输协议^[2]等。例如,如今流行的购物平台(如淘宝、京东等),会对用户的浏览记录和购物记录进行数据采集,然后通过机器学习智能优化用户的首页及搜索结果,然而当涉及购买私密物品时,会给购物者带来很多不便与尴尬。如果某购物平台使用不经意协议,用户可以在搜索和购买商品的同时,实现真正的选择性购物,保护自己的隐私。

1981年,Rabin^[2]首次提出不经意传输(OT, oblivious transfer)的概念,并设计了一个基于二次剩余计算的不经意传输协议,该协议共有两个参与方,分别是接收方 R 和发送方 S ,接收方 R 有 $1/2$ 的概率能得到发送方 S 发送的消息。1985年,Even等^[3]首次提出了2选1随机不经意传输(1-out-of-2 OT)协议,接收方通过该协议能够随机获得发送方发送的两个信息中的一个。1995年,Beaver^[4]首次提出2选1选择不介意传输协议(chosen 1-out-of-2 OT)的概念,接收方可以通过该协议选择获得发送方发送的两条消息中的一个,但是不能获得另外一个消息的任何内

容。Beaver提出的不经意传输定义被广泛接受并成为2选1不经意传输协议的标准概念,通常记为 OT_2^1 。从此不经意传输开始快速发展,被广泛应用到各种密码学协议中。到目前为止,不经意传输具有广泛的应用场景,如安全多方计算^[5,6]、私人信息检索^[7-8]、隐私保护数据挖掘^[9]、合同签订^[10-12]、公平数据交换^[13]和不经意传输系统^[14]等。

1986年,Brassard等^[15]首次将 OT_2^1 拓展为 OT_n^1 。2001年,Naor和Pinkas^[16]在随机预言机模型(radom oracle model)下设计了一个基于判定Diffie-Hellamn困难问题假设的2轮 OT_n^1 协议,具有较高的效率。之后,Aiello等^[17]基于同态公钥加密方案构造了一个2轮 OT_n^1 协议。2008年,Lindell^[18]基于cut-and-choose技术构建出一种不经意传输协议,该协议效率较高且具有一定安全性,但是存在不可忽略的传播错误消息的概率。2012年,Chou等^[19]提出了一种基于身份的不经意传输协议,但是该不经意传输协议只能实现身份的认证,且需要第三方进行身份密钥的分发。2013年,徐彦蛟等^[20]对其进行改进,由发送方进行密钥的生成与分发,但认证功能只能保护消息在信道传播时的双方隐私。2021年,Esmailzade等^[21]提出了一种基于同态加密构建不经意传输协议的通用结构,但是同态加密需要的算法计算开销太大。此外,以上所有协议都不能抵抗恶意接收者,只能保证隐私性或发送方的安全。1990年,Bellare将数据通过公共文件传输的方

法,提出了非交互式的不经意传输^[22]和零知识证明^[23]方案。2004年,Tzeng^[24]基于离散对数问题设计了一种不经意传输协议,运算效率较高,且结合零知识证明和随机预言机模型实现了恶意模型下的协议模拟,但是离散对数问题为了达到一定的安全要求,需要的通信开销较大,实际应用难度较大。2014年,Garay等^[25]构造了一个具有通用可组合安全的线性复杂度 OT_n^1 协议,但是该协议需要参与方预先商讨公共参考串信息。2016年,魏晓超等^[26]基于双模加密机制提出了一个高效可完全模拟的 OT_n^1 协议,该协议使用DH元组的概念,在零知识证明阶段对大量的DH元组进行零知识证明且需要公共参考串的参与,因此计算开销和通信开销较大。2017年,赵川等^[27]对其方案进行改进,提出一种基于cut-and-choose技术的双向不经意传输协议,该协议具有较低的交互轮数,并在2021年基于该技术提出一种安全多方计算协议^[28]。综上所述,现有的 OT_n^1 协议主要存在两个问题:一是目前安全多方计算使用的不经意传输协议基本上只保证协议的正确性和隐私性,或者抵抗单边恶意协议参与者,不能达到完全模拟;二是基于公钥密码体制的不经意传输协议在实际使用中效率较低,通信开销较大。

本文基于双线性对提出了一种椭圆曲线上可完全模拟的 OT_n^1 协议,协议使用零知识证明确保协议的可完全模拟,接收者的选择是无条件安全的,发送方消息的安全性基于椭圆曲线上的离散对数问题。该协议运算速率快,计算开销和通信开销均为 $O(n)$,交互轮数为常数,接收者只需要计算两次双线性对运算,发送方需要计算 n 次倍点运算和 n 次模幂运算。协议使用恒定的公用参数,避免了初始化公共参数的资源消耗。最终对该协议进行模拟,实验结果表明,该协议可以正确运行且十分高效。

1 基础知识

1.1 双线性对

令 G_1 和 G_2 分别是阶为 q 的加法群,其中 q 是一个大素数。 G_T 是有限域 F_p^* 上的乘法群,则定义映射 $e:G_1 \times G_2 \rightarrow G_T$ 为双线性对,该映射满足以下特性。

双线性性:对任意 $P \in G_1, Q \in G_2, n \in \mathbb{Z}$,有 $e([n]P, Q) = e(P, [n]Q) = e(P, Q)^n$ 。

非退化性:一定存在 $P \in G_1$ 和 $Q \in G_2$,使得 $e(P, Q) \neq 1_{G_T}$,其中 1_{G_T} 表示 G_T 中的单位元。

可计算性:存在有效的多项式时间算法计算出双线性对的值。

1.2 困难问题

1) ECDLP(椭圆曲线上的离散对数)问题: $p > 3$ 是一个素数, E 是有限域 Z_p 上的椭圆曲线, G 是 $E_p(a, b)$ 的生成元, $Y \in E_p(a, b)$,对于 Y 和 G ,求满足方程 $xG=Y, 0 \leq x \leq \text{ord}(G)-1$ 的唯一整数 x 是困难的。

2) ECDDH(椭圆曲线可决定性的Diffie-Hellman)问题: G 是有限域 Z_p 上的椭圆曲线, g 是 $E_p(a, b)$ 的生成元。对 $a, b, r \in [1, q-1]$,区分 $Y_1=(g, [a]g, [b]g, [ab]g)$ 和 $Y_1=(g, [a]g, [b]g, [c]g)$ 是困难的。

1.3 1-out-of- n 不经意传输

不经意传输共有两个参与者,分别为消息的接收者 R 和发送方 S 。参与者按照行为方式分为半诚实参与者和恶意参与者:按照协议要求执行但是想获得额外信息的参与者是半诚实参与者;为了获取额外信息不惜破坏协议进行的参与者为恶意参与者。一个1-out-of- n 不经意传输(OT_n^1)协议应满足如下3个要求。

(1) 正确性

发送方 S 拥有 n 个消息记为 $\{m_1, m_2, \dots, m_n\}$,其中 $n \geq 2$ 。接收者 R 想要获取这 n 个秘密中的第 σ 个。如果发送方和接收者能按照协议要求完成该协议,则最终接收者可以正确获得 m_σ 。

(2) 接收者 R 的隐私安全

接收者 R 的不同选择 σ 和 σ' 经过加密后得到的结果对于信息发送方来说是不可区分的。对于发送方来说,如果加密后的 σ 是接近随机的字符串,则说明接收者的选择是安全的。

(3) 发送方 S 的隐私安全

发送方 S 将加密后的消息 $\{c_1, c_2, \dots, c_n\}$ 发送接收者,接收者 R 只能获得选择的消息 m_σ ,对其他消息 $m_i, i \neq \sigma$ 一概不知。其对于接收者 R 来说,如果加密后的消息 $c_i, i \neq \sigma$ 接近随机的字符串,则说明发送方的选择是安全的。

在理想模型下，一个可信第三方可以帮助接收者和发送方执行此协议。接收者将自己的选择 σ 发送给可信第三方，发送方将自己含有的数据 $\{m_1, m_2, \dots, m_n\}$ 发送给可信第三方，然后可信第三方将 m_σ 发送给接收者。在协议理想化执行的过程中，发送方不知道接收方的选择 σ ，接收者也对发送方含有的剩余信息一无所知。

1.4 零知识证明

20 世纪 80 年代初，Goldwasser 提出了零知识证明的概念。1987 年，Goldreich 等给出了如何利用零知识证明将任意可抵御半诚实参与者的 MPC 协议转换为可抵御恶意参与者的 MPC 协议。

零知识证明协议共含有两个参与方，分别是证明者 P 和验证者 V 。零知识证明可以使验证者 V 在不知道证明者 P 的秘密 S 的情况下验证证明者含有秘密 S 。一个零知识证明协议应满足如下要求。

- 1) 完备性 (completeness): 如果证明者 P 含有秘密 S ，那么一定能通过验证者的验证。
- 2) 可靠性 (soundness): 如果证明者 P 不含有秘密 S ，那么 P 通过验证者 V 的概率可以忽略。
- 3) 零知识性 (zero-knowledge): 在零知识证明的过程中，证明者 P 不会直接透露给验证者 V 有关秘密 S 的信息，即验证者 V 在协议过程中获取秘密 S 的概率是可以忽略的。

WIPK (witness indistinguishable proof of knowledge) 是零知识证明的一种，WIPK 不仅能够让被证明者信服证明者含有秘密，而且在证明的过程中，不同的秘密对应的交互数据对于被证明者来说是不可区分的。在该不经意传输协议中，接收者 R 含有的秘密 σ 的值域为 $[1, n]$ ，所以接收者 R 使用 WIPK 向发送方 S 证明含有秘密 $\sigma \in [1, n]$ 。

1.5 安全性定义

1.5.1 计算不可区分

对于两个分布总体 $X = \{X(a, n) | a \in \{0, 1\}^*, n \in N\}$ 和 $Y = \{Y(a, n) | a \in \{0, 1\}^*, n \in N\}$ ，如果对每一个概率性多项式时间图灵机 (PPTM, probabilistic polynomial-time machine) D ，存在一个可忽略的函数 $\mu(\cdot)$ ，对于每个 $a \in \{0, 1\}^*$ 和每个 $n \in N$ ，都有 $|\Pr[D(X(a, n))=1] - \Pr[D(Y(a, n))=1]| \leq \mu(n)$ ，那么称 X 和 Y 是不可区分的，用 $X \stackrel{c}{=} Y$ 表示。

1.5.2 完全模拟 (fully-simulation)

令 $f: \{0, 1\}^* \times \{0, 1\}^* \rightarrow \{0, 1\}^* \times \{0, 1\}^*$ 是一个理想模型下的安全两方计算函数，其中 $f = (f_1, f_2)$ ， π 是一个真实模型下的安全两方计算协议，如果对于真实环境下存在一对至少有一个是诚实的非均匀概率期望多项式时间图灵机 $A = (A_1, A_2)$ ，都在理想环境下存在一对至少有一个是诚实的非均匀概率期望多项式时间图灵机 $B = (B_1, B_2)$ ，使 $\{\text{IDEAL}_{f, B(x, y)}\}_{x, y} \stackrel{c}{=} \{\text{REAL}_{\pi, A(x, y)}\}_{x, y}$ ，则称 π 能在恶意模型下安全地计算 f ，其中 $|x| = |y|$ 。

2 半诚实模型下的不经意传输协议

本节提出一个能够抵抗半诚实参与者的安全不经意传输协议。协议中的半诚实参与者能够按照要求执行协议，但是在协议的运行过程中想要获得额外的信息。

假设存在 3 个阶为 q 的群 $(G_1, +)$ 、 $(G_2, +)$ 和 $(G_T, +)$ 。其中 q 是一个大素数， G_1 是 $E(F_{q d_1})$ (d_1 能整除群的嵌入次数) 的 N 阶子群， G_2 是 $E(F_{q d_2})$ (d_2 能整除群的嵌入次数) 的 N 阶子群，那么 G_T 是 $E(F_{q k})$ (k 是能整除群的嵌入次数) 的 N 阶子群。 P 是 G_1 的生成元， Q 是 G_2 的生成元。即使 $e(P, Q)$ 的值可以计算，接收方的选择也是安全的，所以系统参数 (P, Q, G_1, G_2) 是可以循环使用的。

半诚实模型下的不经意传输协议流程如图 1 所示。假设所有的消息在 F_{qk}^* 域上，且发送方拥有 n 个秘密 $(m_1, m_2, \dots, m_n)$ ，但只想接收方 R 获得选择的秘密，故接收方 R 随机选择并公开 $\{P_1, P_2, \dots, P_n\}$ 。

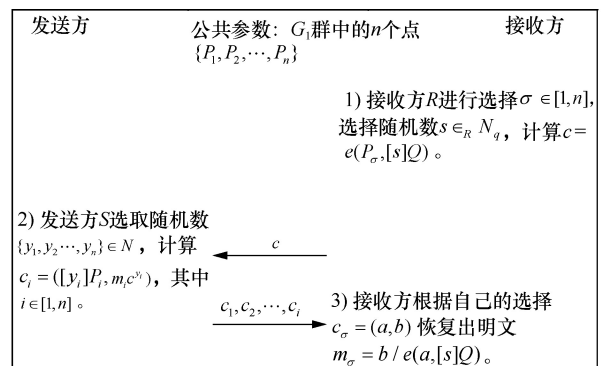


图1 半诚实模型下的不经意传输协议流程
Figure 1 Flow chart of OT protocol under Semi-Honest model

2.1 协议的正确性

如果协议双方都诚实按照协议执行,可以保证 R 能够正确得到 m_σ 。当 $i=\sigma$ 时,对协议进行正确性推导。

$$\begin{aligned} m_i &= m_i \cdot e(P_\sigma, [s]Q)^{y_i} / e([y_i]P_i, \\ [s]Q) &= m_i \cdot e(P_\sigma, Q)^{s \cdot y_i} / e(P_i, Q)^{s \cdot y_i} = m_\sigma \end{aligned} \quad (1)$$

2.2 协议的效率分析

2.2.1 实验结果

本文基于 Windows 平台使用 python 语言(版本为 3.9)实现了该半诚实模型下的不经意传输协议,硬件属性为 CPU-i7-9700f, GPU-2060, RAM16 GB。设置发送方拥有 5 条秘密信息,长度均不大于 160 bit,接收者随机进行选择,对该协议进行百次运行并取平均值。实验结果表明,该协议的正确率为 100%,平均运行时间为 0.7879 s,平均通信开销为 960 bit。

2.2.2 理论分析

通常来说,一个协议的效率共有 3 个影响因素:轮数、计算开销和通信开销。

(1) 轮数

该协议只有必要的两轮交互:一是接收者 R 要进行选择并且要发送给 S ,二是 S 要响应 R 的请求。接收者 R 只发送给发送方 S 一条消息,即接收者的选择。发送方发送给接收者 n 条消息,即加密后的 n 个秘密。

(2) 计算开销

该协议最耗时的运算即双线性对运算、多倍点运算和幂运算。接收者 R 共需要 2 次双线性对运算和 1 次多倍点运算,发送方 S 共需要进行 n 次多倍点运算和 n 次幂运算。

(3) 通信开销

在等同于使用 1 024 bit 密钥的 RSA 加密的安全性下,椭圆曲线加密的密钥以及密文群元素大小均为 160 bit,故该不经意传输协议所需要的通信开销为 $360n+160$ bit,可加密消息最大长度为 160 bit,其中 n 为消息的总数。如加密长度大于 160 bit 的消息,可通过该协议传输加密所需密钥或使用哈希函数加密消息。

2.3 协议的安全性分析

定理 1 在该协议中,接收者 R 的选择 σ 是无条件安全的。

证明 根据协议可知,接收者的选择 σ 经过加密之后的结果为 $c=e(P_\sigma, [s]Q)$ 。在加密 σ 的过程中,接收者会产生一个随机数 s 。发送方 S 可以计算得到所有的 $e(P_i, Q)$ (其中 $i=1,2,\dots,n$),但是发送方并不知道接收者产生的随机数 s ,也就不能确定接收者的选择 i 。综上所述,即使发送方算力再强,也不能从加密后的信息中获取关于 σ 的任何信息,所以接收方 R 的选择是无条件安全的。

定理 2 在该协议中,如果接收者 R 是半诚实的且 ECDDH 问题是困难的,那么只能得到其选择的秘密,对其他未选择的秘密一无所知,即不能从其他项得到相关秘密信息。

证明 在该协议中,发送方发送的秘密信息为 $c_i=(a=[y_i]P_i, b=m_i c^{y_i})$ 。其中, y_i 为发送方用于加密公钥和消息的整数, a 为 y_i 的加密结果, b 为 m_i 的加密结果。如果对于接收者 R 来说, (P, Q, c_i) ($i \neq \sigma$) 与 (P, Q, a_r, b_r) 计算不可区分,那么说明 R 从 c_i ($i \neq \sigma$) 中得不到有关 m_i 的任何信息,即 m_i 是安全的。

首先定义一个模拟机 S ,然后模拟发送方生成秘密信息 $E_i=(P, Q, [y_i]P_i, m_i c^{y_i})$,其中 P 是 G_1 的生成元, Q 是 G_2 的生成元, y_i 是 E_q 域上的随机整数。然后产生随机信息 $X=(r_1, r_2, r_3, r_4)$,其中 r_3 是 G_1 上的随机点, r_4 是 G_T 上的随机数。可以看出, $E_i=(P, Q, [y_i]P_i, m_i c^{y_i})$ 类似于 ECDDH 困难问题中的 Y_1 ,而 $X=(P, Q, P_R, m_i c^{r_4})$ 类似于其中的 Y_2 。

接下来定义一个 PPTM D 用于区分 E_i 和 X 的高效规约算法 $\mathfrak{B}_1(p, q, s, t)$ 。

1) 取随机整数 r , 计算 $(p, Q, t, m_i c^b)$, 其中 Q 是 G_2 的生成元。

2) 使用 D 对 (p, t) 进行区分。如果 $\mathfrak{B}_1$ 输入 Y_1 , 那么 $(p, t)=(P, [ab]P)$ 。如果 $\mathfrak{B}_1$ 输入 Y_2 , 那么 $(p, t)=(p, [c]p)$ 。

3) 使用 D 对 $(p, s, t, m_i c^b)$ 进行区分。如果 $\mathfrak{B}_1$ 输入 Y_1 , 那么 $(p, s, t, m_i c^b)=(P, [b]P, [ab]P, m_i c^b)$ 。如果 $\mathfrak{B}_1$ 输入 Y_2 , 那么 $(p, s, t, m_i c^b)=(P, [b]P, [c]P, m_i c^r)$ 。

4) 如果 D 通过步骤 2)、步骤 3) 判断规约算法输入的是 Y_1 , 则输出 1; 否则输出 0。

如果概率多项式模拟机 D 区分 E_i 和 X 的概率是 ε , 那么假设模拟机 D 解决 ECDLP 困难问题

的概率为 ε_1 , 解决 ECDDH 困难问题的概率为 ε_2 , 且由 $\mathfrak{B}_1$ 可知

$$|\Pr[\mathfrak{B} = 1] - \Pr[\mathfrak{B} = 0]| = \varepsilon = \varepsilon_1 + \varepsilon_2$$

由于 ECDLP 和 ECDDH 是椭圆曲线上的困难问题, 所以 ε 可以忽略, 综上所述, 该协议能够保证发送方的隐私。

3 恶意模型下的不经意传输协议

为了使得上述协议能够在真实情况下运行, 将其拓展到恶意敌手模型 (malicious model) 下。恶意敌手模型下, 被恶意敌手攻陷的参与者可能在协议的运行中, 做出任意违背协议的指令, 如拒绝参

加协议、替换自己的输出、中断协议的执行等, 更加贴近协议真实运行情况。例如, 在 n 选 1 不经意传输协议中, 一个被攻陷的接收者可能通过特定的构造使得 $c_i = m_i \cdot c^{y_i}$ 中的 m_i 不安全。为了预防这种攻击, 要确保 c 是按照协议的要求去构建的, 即 $c = e(P_{\sigma}, [s]Q)$ 。目前共有两种方案可以解决这个问题, 一是使用 WIPK; 二是使用随机预言机模型。

然而, 随机预言机模型只存在于理想条件下, 故本节基于 WIPK 和椭圆曲线的双线性对提出一种恶意敌手模型下的不经意传输协议, 流程如图 2 所示。

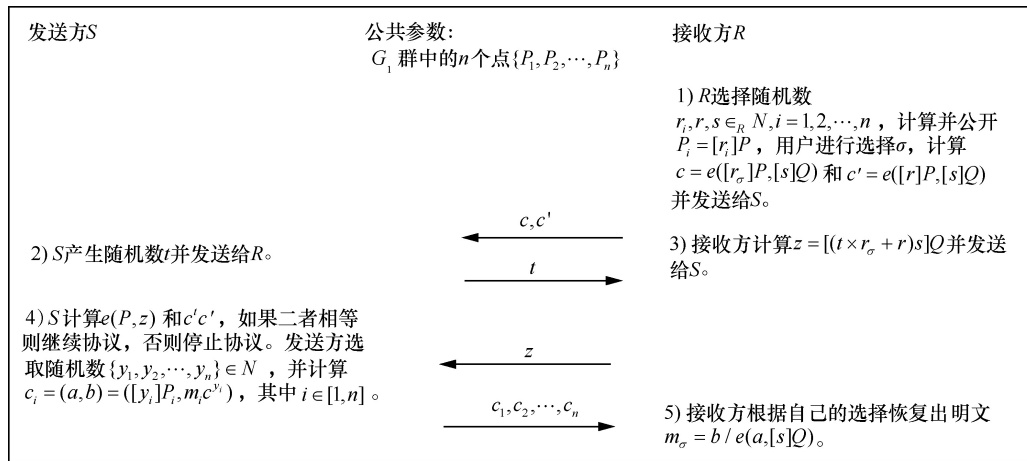


图 2 恶意敌手模型下的不经意传输协议流程

Figure 2 Flow chart of OT protocol under malicious model

3.1 协议正确性分析

由于双线性对的特殊性 $e([n]P, Q) = e(P, [n]Q) = e(P, Q)^n$, 有 $[e(r_{\sigma})P, [s]Q]^t \cdot e([r]P, [s]Q) = e(P, Q)^{(t \times r_{\sigma} + r)s} = e(P, [(t \cdot r_{\sigma} + r)s]Q)$, 因此该零知识证明是正确的。

3.2 不经意传输协议效率分析

3.2.1 实验结果

本文对恶意敌手模型下的不经意传输协议进行了模拟实现, 硬件软件属性同 2.2.1 节, 发送方拥有 5 条秘密信息, 长度均不大于 160 bit, 接收者随机进行选择, 对该协议进行百次运行并取平均值。实验结果表明, 该协议的正确率为 100%, 平均运行时间为 1.205 6 s, 平均通信开销为 1 440 bit。

3.2.2 理论分析

(1) 轮数

在能抵抗恶意接收者的不经意传输协议中,

协议共需要 4 轮交互完成不经意传输, 其中零知识证明需 2 轮, 不经意传输需 2 轮。

(2) 计算开销

R 需要进行 3 次双线性对算和 3 次倍点运算, S 需要计算 $n+1$ 次多倍点运算和 $n+1$ 次模幂运算。

(3) 通信开销

在恶意模型下的协议中, R 发送给 S 的通信开销为 480 bit, S 发送给 R 的通信开销为 $320n+160$ bit, 其中 n 为消息的总数。

与其他不经意传输协议的比较结果如表 1 所示, ML 是传输消息的长度, n 是发送方含有消息的总数。其中文献[15、16、25、26、27]中的协议能够做到保证参与者隐私或者单边模拟运行, 而本文协议可以实现完全模拟, 安全性较高。文献[21]能够达到通用可组合安全, 但是需要公共字符串的存在。文献[27]与

表1 与其他不经意传输协议的比较结果
Table 1 Comparison results with other OT protocols

协议	安全等级	困难问题	轮数	$R \rightarrow S$ 数据大小/bit	$S \rightarrow R$ 数据大小/bit	计算复杂度
Brassard ^[15]	单边模拟	QRA	3	$1\ 024 + n \cdot ML \cdot 1024$	$n \cdot ML \cdot 1\ 024$	$O(n)$
Naor ^[16]	单边模拟	DDH	2	1024	$n \cdot ML + 1024(n+1)$	$O(n)$
Garay ^[21]	UC	DDH	3	1024	$1\ 024n$	$O(n)$
Tzeng ^[25]	保护隐私	DDH	3	1024	$2\ 048n$	$O(n)$
Chou ^[26]	保护隐私	BCDH	3	160×3	$160 + n \cdot ML$	$O(n)$
徐彦蛟 ^[27]	保护隐私	BCDH	2	160×3	$n \cdot ML$	$O(n)$
魏晓超 ^[28]	完全模拟	DDH	3	$2\ 048n + 1\ 024$	$2\ 048n$	$O(n)$
本文协议	完全模拟	ECDDH	5	480	$160 + 320 \cdot n$	$O(n)$

注：① 将安全系数统一为密钥长度 1 024 bit 的 RSA 加密或者 160 bit 的 ECC 加密。

② 对于 k -out-of- n OT 协议，本文对比时将 k 的值设置为 1。

文献[26]不同的是密钥由接收者产生并分发，减少了第三方的参与和通信开销，但只通过身份认证实现了非安全信道中的双方隐私保护。文献[28]实现了恶意模型下的安全模拟，但是基于 DDH 假设的不经意传输所需要的通信较大。本文协议基于 ECDDH 困难问题，在同样的安全等级下需要的密钥和密文长度较短，算法效率高。

3.3 安全性证明

定理 3 在恶意模型下，该协议能够达到完全模拟安全。

证明 在该不经意传输协议中， c 是用户的选择加密之后的结果。在零知识证明的过程中， R 计算 c' 和 $[(t \cdot r_\sigma + r)s]Q$ 并与 S 进行了三轮交互，用于验证 R 含有秘密，即选择 σ 。假设证明过程中的倍点运算由模拟器 S 的一个理想函数计算，接下来对两种腐败情况进行分析。

情况 1 假设存在敌手 A ，其控制腐化的参与者 S ，标记为 S^* 。

首先构建一个理想环境下的模拟机 S 来获取 S^* 的输入，模拟机 S 构造如下。

步骤 1 S 在给定输入 $\{r_i, r, s\}$ ， $i=1, 2, \dots, n$ 下，选择随机数 r' 计算 $c = e([r']P, [s]Q)$ 和 $c' = e([r]P, [s]Q)$ 并发送给 A 。

步骤 2 A 产生随机数 t 并发送给 S 。

步骤 3 S 计算 $[(t \cdot r' + r)s]Q$ 发送给 A 并开始记录 A 的所有倍点运算及结果，此时 S 通过零知识证明认证。 A 计算并发送 $c_i = ([y_i]P_i, m_i c^{y_i})$ ， $i \in [1, n]$ 给 S ；由于倍点运算由 S 计算，所以 S 可以获得

S 的所有输入 $(m_1, m_2, \dots, m_i)$ 。

步骤 4 S 将 $(m_1, m_2, \dots, m_i)$ 输入给理想环境中的不经意传输函数并与诚实的 R 进行交互，然后中止。

可知模拟机 S 的视图 $O_1 = ((m_1, m_2, \dots, m_i), e([r_\sigma]P, [s]Q), e([r]P, [s]Q), ((t \cdot r_\sigma + r)s)Q)$ ，真实情况下敌手 A 的视图为 $O_2 = ((m_1, m_2, \dots, m_i), e([r_\sigma]P, [s]Q), e([r]P, [s]Q), ((t \cdot r_\sigma + r)s)Q)$ ，在二者的视图中不同且含有接收者隐私的值为 c 和 z 。

接下来，证明两个视图中的 c 和 z 计算不可区分。由定理 1 可知，发送方从 c 中获取到 σ 的值是不可能的。

定义一个用来区分理想环境和现实执行中的 z 的高效规约算法 $\mathfrak{B}_2(P, Q)$ 。

- 1) 生成随机整数 r_σ, s, r, t 。
- 2) 生成随机整数 R_1, R_2, R_3 。
- 3) 计算 $c = e([r_\sigma]P, [s]Q)$ ， $c' = e([r]P, [s]Q)$ 。
- 4) 计算 $z = [(t \cdot r_\sigma + r)s]Q$ 和 $z' = [R_3]Q$ 。
- 5) 随机选取 $x = \mathcal{U}(0, 1)$ ，当 $x=1$ 时输出 (c, c', z) ，否则输出 (c, c', z') 。

最终使用 PPTM 对 $\mathfrak{B}_2$ 的输出进行区分。当 $x=1$ 时， $\mathfrak{B}_2$ 的输出对应的是真实情况下的敌手视图，当 $x=0$ 时， $\mathfrak{B}_2$ 对应的是理想情况下的模拟器视图。假如存在 PPTM D 能够以不可忽略的概率 ε 区分 O_1 和 O_2 ，那么存在一个多项式概率图灵机能够以 ε 的概率区分 (c, c', z) 和 (c, c', z') ，也就是能够以 ε 的概率解决 ECDDH 困难问题。由于 ECDDH 困难问题无法在多项式时间下解决，因此理想环境中模拟机 S 的视图以及真实执

行中敌手 $\mathcal{A}$ 的视图不可区分, 即在参与者 S 被腐化后该协议仍然能安全执行。

情况 2 假设存在敌手 $\mathcal{A}$, 其控制腐化的参与者 R , 标记为 R^* 。

首先构建一个理想模型下的模拟机 $\mathcal{S}$ 获取 R 的输入, 模拟机 $\mathcal{S}$ 构造如下。

步骤 1 模拟机 $\mathcal{S}$ 开始记录敌手 $\mathcal{A}$ 的倍点运算。在接收到 $\mathcal{A}$ 发来的 c 和 c' 后, 对于所有 P 的倍点, 计算 $e(P_i, [s]Q)$ 并与 c 比较, 将相等时的值 P_i 与敌手 $\mathcal{A}$ 公开的所有点对比获取敌手的真实输入 σ 。

步骤 2 $\mathcal{S}$ 按照协议要求进行零知识证明。如果验证失败, 则停止该不经意传输协议。如果验证成功, 则 $\mathcal{S}$ 将 σ 发送给理想环境中的不经意传输理想函数与诚实的发送方交互获得 m_σ 。

步骤 3 对于 $i = \sigma$, $\mathcal{S}$ 计算 $\overline{c_\sigma} = ([y]P_\sigma, m_\sigma C^n)$, 否则 $\overline{c_i} = (a_i, b_i)$, $1 \leq i \neq \sigma \leq n$, $a_i \in {}_R G_1, b_i \in {}_R G_T$ 。最终, $\mathcal{S}$ 发送 $(\overline{c_1}, \dots, \overline{c_n})$ 给敌手 $\mathcal{A}$ 。

接下来, 证明理想情况下模拟机 $\mathcal{S}$ 的视图和真实情况下 $\mathcal{A}$ 的视图是计算不可区分的。由上述模拟机的模拟过程可知, 模拟机 $\mathcal{S}$ 的总视图为 $O_3 = (c, c', t, z, (\overline{c_1}, \dots, \overline{c_n}))$ 。在协议的真实执行过程中, 敌手 $\mathcal{A}$ 的视图为 $(c, c', t, z, (c_1, \dots, c_n))$ 。二者的视图不同点在于除了当 $i = \sigma$ 时, $c_\sigma = \overline{c_\sigma}$, 其余情况下 c_σ 为 m_i 的加密结果, 而 $\overline{c_\sigma}$ 为值域内的随机数。

定义一个用于区分二者视图的高效规约算法 $\mathfrak{B}_3(P, Q, (m_1, \dots, m_n))$ 。

- 1) 选择随机数 $r_i, r, s \in {}_R N, i = 1, 2, \dots, n$, $\sigma \in [1, n]$ 并计算 $c = e([r_\sigma]P, [s]Q)$ 和 $c' = e([r]P, [s]Q)$ 。
- 2) 选择随机数 t 并计算 $z = [(t \cdot r_\sigma + r)s]Q$ 。
- 3) 选择随机数 $y_i \in {}_R N, \overline{y_i} \in {}_R N, i = 1, 2, \dots, n$, 选择随机值 $\overline{b_i} \in {}_R F_{qk}^*$ 。
- 4) 计算 $c_i = ([y_i]P_i, m_i c^{y_i})$ 和 $\overline{c_i} = ([\overline{y_i}]P_i, \overline{b_i})$, $i = 1, 2, \dots, n$, 然后替换 $\overline{c_\sigma}$ 的值为 c_σ 。
- 5) 随机选取 $x = \mathcal{U}(0, 1)$, 当 $x = 1$ 时输出 $(c, c', t, z, (c_1, \dots, c_n))$, 否则输出 $(c, c', t, z, (\overline{c_1}, \dots, \overline{c_n}))$ 。

使用 PPTM 对 $\mathfrak{B}_3$ 的输出结果进行区分。当 $x = 1$ 时, $\mathfrak{B}_3$ 的输出与协议的真实输出相同, 当 $x = 0$ 时, $\mathfrak{B}_3$ 的输出与理想环境下的模拟结果相

同。假如存在一个 PPTM D 能够以不可忽略的概率 ε 区分 $\mathfrak{B}_3$ 的两种输出, 那么存在一个多项式概率图灵机能够以 $\varepsilon/(n-1)$ 的概率解决 ECDLP 困难问题。然而, ECDLP 困难问题无法在多项式时间内解决, 因此真实环境中敌手 $\mathcal{A}$ 的视图和模拟器 $\mathcal{S}$ 的视图是计算不可区分的, 即当接收者 S 被腐化时该协议仍能安全运行。

综上所述, 在恶意模型下, 该协议能够进行完全模拟。

4 结束语

本文提出了一种基于双线性对的不经意传输协议, 结合零知识证明实现了恶意模型下的完全模拟。该协议中接收者 R 的选择是无条件安全的, 发送方 S 的安全性基于 ECDLP 困难问题和 ECDDH 困难问题, 该协议的交互轮数为常数, 通信复杂度和计算复杂度均为 $O(n)$, 且不需要在每次运行时初始化系统参数, 具有效率高、通信开销小的特点。

随着量子计算机的不断发展, 传统的困难问题已经不能抵挡量子攻击, 下一步将设计能够抵挡量子攻击的格上不经意传输协议。

参考文献:

- [1] YAO A C. Protocols for secure computations[C]//Proceedings of 23rd Annual Symposium on Foundations of Computer Science (SFCS 1982). 2008: 160-164.
- [2] RABIN M. How to exchange secrets with oblivious transfer[J]. IACR Cryptology ePrint Archive. 2005. 187.
- [3] SHIMON E, ODED G, LEMPEL A. A randomized protocol for signing contracts[R]. 1985.
- [4] BEAVER D. Precomputing oblivious transfer[M]//Advances in Cryptology — CRYPTO' 95. Berlin Heidelberg: Springer. 1995: 97-109.
- [5] BURRA S S, LARRAIA E, NIELSEN J B, et al. High-performance multi-party computation for binary circuits based on oblivious transfer[J]. Journal of Cryptology, 2021, 34(3): 34.
- [6] RAO C K, SINGH K, KUMAR A. Oblivious stable sorting protocol and oblivious binary search protocol for secure multi-party computation[J]. Journal of High Speed Networks, 2021, 27(1): 67-82.
- [7] JANNATI H, BAHRAK B. An oblivious transfer protocol based on elgamal encryption for preserving location privacy[J]. Wireless Personal Communications, 2017, 97(2): 3113-3123.
- [8] YANG Y G, SUN S J, PAN Q X, et al. Reductions between private information retrieval and oblivious transfer at the quantum level[J]. Optik, 2015, 126(21): 3206-3209.
- [9] ASHAROV G, LINDELL Y, SCHNEIDER T, et al. More efficient oblivious transfer extensions[J]. Journal of Cryptology, 2017, 30(3):

- 805-858.
- [10] CHOU Y H, TSAI I M, KO C M, et al. Quantum oblivious transfer and fair digital transactions[C]//Proceedings of 2006 12th Pacific Rim International Symposium on Dependable Computing (PRDC'06). 2006: 121-128.
- [11] 曲亚东, 侯紫峰, 韦卫. 基于不经意传输的合同签订协议[J]. 计算机研究与发展, 2003(4): 615-619.
- QU Y D, HOU Z F, WEI W. A Protocol for Signing Contracts Based on Oblivious Transfer[J]. Journal of Computer Research and Development, 2003(4): 615-619.
- [12] STANEKOVÁ L, STANEK M. Fast contract signing with batch oblivious transfer[M]//Communications and Multimedia Security. Berlin Heidelberg: Springer. 2005: 1-10.
- [13] TIAN TIAN, LI, . FAPS: a fair, autonomous and privacy-preserving scheme for big data exchange based on oblivious transfer, Ether Cheque and smart contracts[J]. Information Sciences, 2021, 544: 469-484.
- [14] HUSSAIN S, GUO H, LI T, et al. COPS: a complete oblivious processing system[J]. Microprocessors and Microsystems, 2021, 85: 104295.
- [15] BRASSARD G, CREPEAU C, ROBERT J M. All or nothing disclosure of secrets[C]//Advances in Cryptology—CRYPTO' 86. 2007: 234-238.
- [16] NAOR M, PINKAS B. Efficient oblivious transfer protocols[C]//Proceedings of the Twelfth Annual ACM-SIAM Symposium on Discrete Algorithms. 2001: 448-457.
- [17] AIELLO B, ISHAI Y, REINGOLD O. Priced oblivious transfer: How to sell digital goods[M]//Lecture Notes in Computer Science. Berlin Heidelberg: Springer. 2001: 119-135.
- [18] LINDELL Y, PINKAS B. An efficient protocol for secure two-party computation in the presence of malicious adversaries[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin Heidelberg: Springer. 2007: 52-78.
- [19] CHEN Y L, CHOU J S, HOU X W. A novel k-out-of-n oblivious transfer protocols based on bilinear pairings[J]. IACR Cryptol EPrint Arch, 2010, 2010: 27.
- [20] 徐彦蛟, 李顺东, 陈振华. 基于双线性对的高效不经意传输协议[J]. 计算机工程, 2013, 39(6): 166-169, 173.
- XU Y J, LI S D, CHEN Z H. Efficient oblivious transfer protocol based on bilinear pairing[J]. Computer Engineering, 2013, 39(6): 166-169, 173.
- [21] ESMAELZADE S, PAKNIAT N, ESLAMI Z. A generic construction to build simple oblivious transfer protocols from homomorphic encryption schemes[J]. The Journal of Supercomputing, 2022, 78(1): 72-92.
- [22] BELLARE M, MICALI S. Non-interactive oblivious transfer and applications[M]//Advances in Cryptology — CRYPTO' 89 Proceedings. 2007: 547-557.
- [23] BELLARE M, ROGAWAY P. Random oracles are practical: A paradigm for designing efficient protocols[C]//Proceedings of the 1st ACM Conference on Computer and Communications Security. 1993: 62-73.
- [24] TZENG W G. Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters[J]. IEEE Transactions on Computers, 2004, 53(2): 232-240.
- [25] GARAY J A, ISHAI Y, KUMARESAN R, et al. On the complexity of UC commitments[M]//Advances in Cryptology – EUROCRYPT 2014. Berlin Heidelberg: Springer. 2014: 677-694.
- [26] 魏晓超, 蒋瀚, 赵川. 一个高效可完全模拟的 n 取 1 茫然传输协议[J]. 计算机研究与发展, 2016, 53(11): 2475-2481.
- WEI X C, JIANG H, ZHAO C. An efficient 1-out-of-n oblivious transfer protocol with full simulation[J]. Journal of Computer Research and Development, 2016, 53(11): 2475-2481.
- [27] 赵川, 蒋瀚, 魏晓超, 等. Cut-and-Choose 双向不经意传输[J]. 软件学报, 2017, 28(2): 352-360.
- ZHAO C, JIANG H, WEI X C, et al. Cut-and-choose bilateral oblivious transfer[J]. Journal of Software, 2017, 28(2): 352-360.
- [28] 赵川, 徐俊. 基于 Cut-and-Choose 技术的安全多方计算[J]. 计算机研究与发展, 2022, 59(8): 1800-1818.
- CHUAN Z, JUN X. Secure multi-party computation based on Cut-and-Choose technology[J]. Journal of Computer Research and Development, 2022, 59(8): 1800-1818.

[作者简介]



宋佳烁 (1998—), 男, 河北廊坊人, 北京印刷学院硕士生, 主要研究方向为密码学。



李祯祯 (1991—), 女, 河南驻马店人, 北京印刷学院讲师, 主要研究方向为信息安全、网络安全和量子密码学。



丁海洋 (1979—), 男, 河南郑州人, 博士, 北京印刷学院副教授, 主要研究方向为信息隐藏、半色调信息隐藏、数字图像处理。



李子臣 (1965—), 男, 河南温县人, 北京印刷学院教授、博士生导师, 主要研究方向为信息安全、数字水印、数字签名、密码学。