

基于椭圆曲线公钥系统的不经意传输协议

徐彦蛟¹ 李顺东¹ 王道顺² 吴春英¹

(陕西师范大学计算机科学学院 西安 710062)¹ (清华大学计算机科学与技术系 北京 100084)²

摘 要 不经意传输是密码学中的基础协议。使公钥系统具有不经意传输功能有重要的实际意义。利用椭圆曲线公钥系统设计了两个 k -out-of- n 不经意传输协议,协议充分利用公钥系统的优势,不需要预先建立认证通道,同时椭圆曲线公钥系统的高效性使协议具有很高的执行效率。第一个方案直接利用椭圆曲线公钥系统的加密方法和解密方法设计;第二个方案是第一个方案的改进,它保留了原方案的优势,同时降低了执行的开销。椭圆曲线公钥系统的概率加密性可以大大扩展协议的应用范围。两个协议都能够保证发送者和接收者的隐私性,同时能够抵抗冒充攻击、重放攻击以及中间人攻击,因此在不安全的信道传递消息时依然是安全的。

关键词 不经意传输,椭圆曲线,公钥系统,高效,隐私,安全

中图法分类号 TP309 文献标识码 A

Oblivious Transfer Based on Elliptic Curve Public Key Cryptosystems

XU Yan-jiao¹ LI Shun-dong¹ WANG Dao-shun² WU Chun-ying¹

(School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)¹

(Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)²

Abstract Oblivious transfer is a primitive of cryptography. Endowing a public key system with oblivious transfer function has important practical significance. This paper used the elliptic curve cryptosystems to design two k out of n oblivious transfer schemes. These schemes can make full use of the property of public key cryptosystems, and do not need to establish a authentication channel in advance. Based on efficient elliptic curve cryptosystems, these schemes are very efficient. The first scheme is directly constructed from the encryption and decryption property of elliptic curve cryptosystems, and the second improves the first. It keeps the advantages of the first and reduces the overhead cost of the first. Elliptic curve cryptosystem is probabilistic, and oblivious transfer based on it can expand the application of oblivious transfer. The new protocol can protect the privacy of both the receiver and the sender. The new protocols also can prevent impersonation attacks, replay attacks and man-in-the-middle attacks. They can be used in an insecure channel.

Keywords Oblivious transfer, Elliptic curve, Public key cryptosystems, Efficient, Privacy, Secure

1 引言

不经意传输(Oblivious Transfer, OT)是一种用于传递秘密消息的协议,可以保护消息传递双方的隐私,是密码学中的基础协议,常用于构建其他密码协议和应用^[8],如多方保密计算^[12]、隐密关键字搜索等。不经意传输是研究热点课题之一。

不经意传输首先由 Rabin^[1]提出,通过交互的方式实现了发送方发送消息 M ,接收方只有 $1/2$ 的概率获得该消息,同时发送方无法获知接收者是否获取了 M 。随后 Even 提出了 1-out-of-2(OT_2^1)协议^[2,17],实现了对于发送方发送的两条消息 M_0, M_1 ,接收方只能获取其中的一条消息 M_σ ($\sigma \in \{0, 1\}$),无法同时获得,发送方无法确定接收方选择了 M_0 还是 M_1 。 OT_n^k 协议^[3,16,19]是对 OT_2^1 的发展。目前研究最多的是一般

的 OT_n^k 协议^[4-7,9],这方面已经有许多科研成果。

到目前为止,所有不经意传输系统是一个独立的系统,虽然它们都是建立在密码学中的一些加密算法基础之上,但是这些系统无法利用公钥加密系统的认证功能,因此在协议执行前需要建立认证通道,以防止没有获得发送方认可的窃取者冒充接收方获得其中的某些消息,造成协议参与双方的损失。建立认证通道不仅增加了协议执行的开销,同时也使协议执行的安全依赖于认证通道建立方法的安全性,如果认证通道的安全性不高,窃取者依然有机可乘。扩展公钥系统,使其具有 OT_n^k 功能,这样就不需要重新建立不经意传输系统,同时利用公钥系统的认证功能,在执行 OT_n^k 时不需要事先建立认证通道,从整体上减少系统执行的开销,因此设计一种直接建立在公钥系统的 OT_n^k 协议具有重要的实用价值。

本文利用椭圆曲线公钥系统^[13,14]实现了 OT_n^k 协议,由于

到稿日期:2013-02-24 返修日期:2013-06-14 本文受国家自然科学基金(61070189, 61170032, 61272435),陕西师范大学研究生创新基金(2013CXSS043)资助。

徐彦蛟(1988—),男,硕士生,主要研究领域为密码学、信息安全, E-mail: xuyan-jiao@163.com;李顺东(1963—),男,博士,教授,博士生导师,主要研究领域为密码学、信息安全。

这种公钥系统的密文 $c=(c_0, c_1)$ 是一对数据, 其中 c_0 是包含明文 m 的密文项, c_1 是用于与接收者私钥联合使用从 c_0 中恢复出明文 m 的密文项, 因此, 即使接收者拥有解密私钥, 如果只收到 c_0 , 依然无法从 c_0 中恢复出明文 m 。本文设计了两种 OT_n^* 方案, 第一个方案直接利用椭圆曲线公钥系统加密和解密方法设计, 思想简单, 容易理解; 第二个方案是对第一个方案的改进, 保留了原方案的优势, 并降低了原方案执行所需的开销。两个方案能够在保证参与双方隐私性的前提下正确传递消息, 而且协议的执行不需要额外建立认证通道。事实上, 一些加密数据形如 $c=(c_0, c_1)$ 的加密方案, 例如 Boneh 的基于身份的加密方案^[10]以及 ElGamal 加密方案^[11], 都可以采用本文的设计思想实现 OT_n^* 协议。鉴于椭圆曲线公钥系统在相同安全等级下与 RSA 系统和 ElGamal 系统等相比具有运算速度快、网络开销低等优点, 可以提高 OT_n^* 协议的执行效率, 本文选定椭圆曲线公钥系统作为设计 OT_n^* 协议的基础。椭圆曲线公钥系统是一种概率加密系统, 这一性质用来设计 OT_n^* 协议是非常重要的。不经意传输协议所传输的信息由消息的具体内容和消息所在的位置共同决定, 不同位置出现相同消息内容所传递的信息是不同的, 例如多方保密计算^[12]用到的 OT_1^* 协议, 4 个位置代表 4 种情况, 但是每个位置传递的消息只可能是 0 或 1, 在一次传输过程中出现有两个位置所传输的消息相同的情况。在这样的场景下, 采用确定性加密方法设计 OT 协议^[6,9]不能得到有效的执行, 需要额外的处理工作。事实上这样的应用有很多, 例如, Alice 是股票预测专家, 他预测了 n 只股票的涨跌幅度, Bob 是股票投资者, 他想要购买其中 k 只股的预测, 但是他不想让 Alice 知道他想要哪些股票的预测信息, 防止 Alice 知道自己的选择后在下次购买时恶意提高价钱, 因此他们需要执行 OT_n^* 协议。我们知道股票的涨跌幅度是有限制的, 有可能出现两只以上股票的涨跌预测值相同的情况, 这就需要使用以概率加密为基础的 OT_n^* 协议。本文设计的 OT_n^* 有最广泛的应用范围。

2 预备知识

2.1 椭圆曲线公钥系统

椭圆曲线公钥系统^[13,14]所使用的椭圆曲线

$$y^2 = x^3 + ax^2 + bx + c \quad (1)$$

的方程系数 a, b, c 在有限域 F_p (p 是一个大素数) 上取值。方程的判别式 $\Delta = 27c^2 + 4a^3c + 4b^3 - a^2b^2 + 8abc \pmod p \neq 0$, 所有满足方程(1)的点 (x, y) ($x, y \in F_p$) 构成的集合并添加无穷远点 $\mathcal{O}$ 作为单位元, 构成一个加法群 G , 且 G 是一个 Abel 群。 $P_1 + P_2 = P_3 = (x_3, y_3)$, 其中 $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $P_1, P_2, P_3 \in G$ 。

若 $P_1 = \mathcal{O}$, 则 $P_3 = P_2$;

当 P_1, P_2 都不等于 $\mathcal{O}$ 时;

(1) $P_1 \neq P_2, x_1 = x_2 \pmod p$ 时, $P_3 = \mathcal{O}$;

(2) $P_1 \neq P_2, x_1 \neq x_2 \pmod p$ 时, 通过计算

$$\lambda = \frac{x_1 - x_2}{y_1 - y_2}$$

$$x_3 = \lambda^2 - a - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

获得 $P_3 = (x_3, y_3)$;

(3) $P_1 = P_2$ 时, 通过计算

$$\lambda = \frac{3x_1 + 2ax_1 + b}{2y_1}$$

$$x_3 = \lambda^2 - a - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

获得 $P_3 = (x_3, y_3)$ 。

椭圆曲线上的乘法运算定义为加法的重复, 例如 $Q = kP = P + P + \dots + P$ 为 k 个 P 相加, 其中 $P \in G$ 。设群 G 的阶为 $q, k \in \mathbb{Z}_q$, 计算 kP 是容易的, 但是给定 P, Q 求出 k 却是困难的, 这个困难问题称为椭圆曲线上的离散对数问题, 椭圆曲线公钥系统的安全性正是基于这一困难问题。这一公钥系统的应用过程描述如下。

密钥生成: Alice 选定一条椭圆曲线 E , 并选取椭圆曲线上的一点 G 作为基点。Alice 选定一个私钥 $s_a \in \mathbb{Z}_q$, 计算公钥 $K_A = s_a G$, 因此 Alice 的公钥为 (K_A, G) , 公共参数为椭圆曲线 E 。

加密: Bob 想要秘密发送消息 m 给 Alice, 首先 Bob 将 m 编码到 E 上的一点 M , 而后随机选取 $r \in \mathbb{Z}_q$, 计算 $C = (C_0, C_1)$, 其中 $C_0 = M + rK_A, C_1 = rG$, 发送 C 给 Alice。

解密: Alice 收到 C 后计算

$$C_0 - s_a C_1 = M + rK_A - s_a(rG) = M + r s_a G - s_a r G = M$$

恢复出 M , 对 M 译码获得消息 m 。

通过以上执行过程不难发现, 通过 (K_A, G) 以及 (C_1, G) 求出 s_a 和 r 是困难的, 消除 C_0 中的随机因子 $s_a r G$ 是困难的, 因此协议是安全的。为了方便后续的 OT_n^* 叙述, 这里给出如下引理。

引理 1 $\forall P, Q \in G, r, k \in \mathbb{Z}_q, q$ 为群 G 的阶, 则 $k(P + rQ) = kP + krQ$ 成立。

证明: 这个引理是显然的, 由于 G 是 Abel 群, 根据 Abel 群的交换性, 交换 P, rQ 的位置可得:

$$(P + rQ) + \dots + (P + rQ) = P + \dots + P + rQ + \dots + rQ$$

从而, $k(P + rQ) = kP + krQ$ 。

引理 2 $\forall P \in G, a_1, a_2 \in \mathbb{Z}_q$, 当 P 是 G 的生成元时, 如果 $a_1 \neq a_2$, 那么 $a_1 P \neq a_2 P$ 。

证明: 用反证法。假设 $a_1 P = a_2 P$, 那么 $a_1 P - a_2 P = \mathcal{O}$, 即 $(a_1 - a_2)P = \mathcal{O}$, 所以 $a_1 - a_2$ 是 q 的整数倍, 又因为 $|a_1 - a_2| < q$, 因此 $a_1 - a_2 = 0$, 即 $a_1 = a_2$ 与假设矛盾, 因此当 $a_1 \neq a_2$ 时, $a_1 P \neq a_2 P$ 。

引理 3 如果由生成元 G 生成的群 G 的阶 q 为素数, 那么 G 中所有非 $\mathcal{O}$ 元素的阶也为 q , 都可作为群 G 的生成元。

证明: 假设存在非 $\mathcal{O}$ 元素 $X \in G$ 的阶为 $p \neq q$, 根据元素阶的定义, $pX = \mathcal{O}$, 同时由于 G 是生成元, 存在 $a \in \mathbb{Z}_q^*$ 使得 $X = aG$ 成立, 因此 $paG = \mathcal{O}$, 由此得出 pa 是 q 的整数倍, a, q 互素, 则 p 是 q 的整数倍。由于 G 的元素个数为 q , 根据群的封闭性以及元素阶的定义得出 $p \leq q$ 且 $p \neq 0$, 因此 $p = q$, 与假设矛盾, 结论成立。所以, $\forall Y \in G, Y \neq \mathcal{O}$, 都可以通过 $iY (i = 1, \dots, q)$ 遍历 G 中每一个元素, 因此 Y 是 G 的一个生成元。

2.2 OT_n^* 安全模型

OT_n^* 协议是发送者和接收者之间用来传递消息的协议, 发送者同意发送自己拥有的 n 个消息中的 k 个给接收者, 在 OT_n^* 协议执行后能够保证发送者和接受者各自的隐私性。我们假定参与双方是半诚实的, 他们按照协议执行, 但会保留协议执行过程所获取的中间变量, 同时我们假定在网络中存在

消息窃取的第三方,他们通过一些攻击手段试图获取他们想要的信息(不考虑劫持并销毁或篡改协议执行过程中的通信数据从而阻止协议执行的恶意攻击者)。因此一个安全的 OT_n^* 协议必须满足以下性质:

(1) 正确性: 协议执行完毕后接收者能够获得他所选择的 k 个消息。

(2) 发送者隐私性: 协议执行完毕后, 接收者通过发送者发来的 n 个秘密数据、已经获得的 k 个消息以及系统的公共参数, 不能获得自己没有选择的 $n-k$ 个消息中的任何一个。

(3) 接收者隐私性: 协议执行完毕后, 发送者通过系统的公共参数、接收者发来的选择数据, 不能区分出接收者具体选择了哪 k 个消息。

(4) 抗冒名攻击: 发送者发送的信息只能由其认可的接收者获取。

(5) 抗重放攻击性: 攻击者采用网络监听的手段, 获取发送者与接收者间传递的数据, 通过这些数据以及公共参数, 依然无法获知接收者的选择以及发送者拥有的数据。

(6) 抗中间人攻击性: 中间人攻击是指第三方以发送方的身份与接收者通信, 以接收方身份与发送者通信, 在协议执行完毕后, 接收者和发送者无法察觉到第三方的存在。

3 基于椭圆曲线公钥系统的 OT_n^* 协议方案-I

3.1 协议执行过程描述

椭圆曲线公钥系统: 群 G_B 是由椭圆曲线上的基点 G 生成的 q (q 是个大素数) 阶加法群, $s_B \in \mathbb{Z}_q^*$ 为 Bob 的私钥, $K_B = s_B G$ 为 Bob 的公钥, ψ_B 是将明文编码到 G_B 的方法, ψ_B^{-1} 为译码方法, Bob 公钥系统的公共参数为 $\langle G_B, q, G, \psi_B, \psi_B^{-1} \rangle$ 。

初始化:

Alice 持有私密消息 $m_1, \dots, m_n \in \{0, 1\}^*$, 并将其编码到群 G_B 上的点 $\{M_1, \dots, M_n\}$ 。Bob 的选择 $\sigma_1, \dots, \sigma_k \in \{1, \dots, n\}$ 。

信息交互:

(1) Alice 随机选取 $t_0, r_1, \dots, r_n \in \mathbb{Z}_q^*$, $r_i \neq r_j$ ($i \neq j$), 计算 $C_i = (C_{i1}, C_{i2})$ ($i=1, \dots, n$)

其中 $C_{i1} = M_i + r_i t_0 K_B$, $C_{i2} = r_i G$, 发送 $\{C_1, \dots, C_n\}$ 给 Bob。

(2) Bob 收到 Alice 发来的 $\{C_1, \dots, C_n\}$, 随机选取 $a_1, \dots, a_k \in \mathbb{Z}_q^*$, $a_i \neq a_j$ ($i \neq j$), 根据自己的选择 $\{\sigma_1, \dots, \sigma_k\}$, 以及 C_{σ_i} 中的 $C_{\sigma_i, 2}$ 计算

$$D_i = C_{\sigma_i, 2} + a_i G, i=1, \dots, k$$

发送 $\{D_1, \dots, D_k\}$ 给 Alice。

(3) Alice 收到 Bob 发来的 $\{D_1, \dots, D_k\}$, 计算

$$R = t_0 K_B, D_i = t_0 D_i (i=1, \dots, k)$$

发送 $R, \{D_1, \dots, D_k\}$ 给 Bob。

获取消息:

Bob 收到 $R, \{D_1, \dots, D_k\}$ 后, 利用自己的私钥 s_B 以及 a_i 计算

$$C_{\sigma_i, 1} - s_B D_i + a_i R = M_{\sigma_i}, i=1, \dots, k$$

利用译码方法恢复出消息 $m_{\sigma_i} = \psi_B^{-1}(M_{\sigma_i})$ 。

3.2 协议-I 的正确性

在协议的执行过程中, 其正确性体现在以下等式成立:

$$C_{\sigma_i, 1} - s_B D_i + a_i R = M_{\sigma_i}$$

那么根据椭圆曲线公钥系统加密解密方法以及引理 1, 很容易

证明以上等式成立, 这是因为:

$$\begin{aligned} & C_{\sigma_i, 1} - s_B D_i + a_i R \\ &= C_{\sigma_i, 1} - s_B t_0 D_i + a_i R \\ &= C_{\sigma_i, 1} - s_B t_0 (C_{\sigma_i, 2} + a_i G) + a_i t_0 K_B \\ &= C_{\sigma_i, 1} - s_B t_0 C_{\sigma_i, 2} - s_B t_0 a_i G + a_i t_0 K_B \\ &= M_{\sigma_i} + t_0 r_{\sigma_i} K_B - s_B t_0 C_{\sigma_i, 2} - s_B t_0 a_i G + a_i t_0 s_B G \\ &= M_{\sigma_i} + t_0 r_{\sigma_i} s_B G - s_B t_0 r_{\sigma_i} G \\ &= M_{\sigma_i} \end{aligned}$$

因此协议执行完毕后, Bob 能够获得自己所选择的全部消息。

3.3 协议-I 的安全性

整个协议的执行过程的安全性依赖于椭圆曲线公钥系统的安全性。从另一个角度来看, 这个协议的执行过程等价于 Alice 利用 Bob 的公钥系统分 n 次加密 n 个消息, 其中只有 k 个密文是完全的密文, 其余的密文都是不完整的, 因此根据前面的分析, 即使 Bob 拥有解密密钥也无法正确地恢复出其余的消息, 我们根据以下定理详细地证明协议的安全性。

定理 1 接收者的选择是无条件安全的, 即协议执行完毕后发送者不能知道接收者的具体选择。

证明: 根据上面协议的执行过程, Alice 如果能够区分出 Bob 的选择, 他一定能够通过 D_i 区分出 $C_{\sigma_i, 2}$, 即存在概率多项式时间算法 $\mathcal{A}$, 通过 D_i 分辨出 $C_{\sigma_i, 2}$ 的概率

$$\Pr[\mathcal{A}(D_i) = C_{\sigma_i, 2} \mid D_i = C_{\sigma_i, 2} + a_i G] > \epsilon$$

是不可忽略的概率, 那么利用 $\mathcal{A}$ 攻破椭圆曲线公钥系统, 因为以上的区分过程等价于直接从椭圆曲线密文 $c = (c_0, c_1)$ 中的 c_0 , 在没有私钥 s 以及密文 c_1 的辅助下直接恢复出明文, 显然这与椭圆曲线公钥系统的安全性不符, 因此假设不成立。综上所述, 协议执行完毕后发送者不能知道接收者的具体选择。

定理 2 接收者只能打开 k 个密文, 即发送者其余的 $n-k$ 个消息接收者无法获得。

证明: 根据协议的执行过程以及椭圆曲线公钥系统的加密解密算法, 如果 Bob 想要在 C_{i1} 中计算出明文 m_i 的编码元 M_i , 他必须能够计算出 $t_0 r_i s_B G$, 由于 s_B 是 Bob 的私钥, 因此 Bob 只需要计算出 $t_0 r_i G$ 。Bob 通过计算 $t_0 C_{i2}$ 或 $r_i R$ 获取 $t_0 r_i G$, 然而 t_0, r_i 对 Bob 是保密的。假设 Bob 能够找到一个概率多项式时间算法 $\mathcal{A}$ 通过 C_{i2}, G 或 R, G 计算出 r_i 或 t_0 , 那么 $\forall P, Q \in G$, 利用算法 $\mathcal{A}$ 就可以计算出 $l \in \mathbb{Z}_q^*$ 使得 $Q = lP$ 成立, 因此 $\mathcal{A}$ 可以解椭圆曲线上的离散对数问题, 显然假设不成立。由于 Bob 在步骤(2)中只能发送 k 个数据, 因此最终只能建立 k 个方程, 根据椭圆曲线上的离散对数问题可知 $t_0 r_i G$ 是未知解, 因此 k 个方程最多能够解出 k 个未知解。综上, 发送者其余的 $n-k$ 个消息接收者无法获得。

定理 3 该协议能够防止冒名攻击、重放攻击以及中间人攻击。

证明: 根据协议的执行过程可知, 采用已经在密钥基础设施中认证的 Bob 公钥 K_B 加密的信息, 必须拥有 Bob 的私钥 s_B 才能解密, 因此该 OT_n^* 协议能够防止冒名攻击。同时, 攻击者通过截取数据 $(C_1, \dots, C_n), (D_1, \dots, D_k), (D_1, \dots, D_n)$ 在没有解密密钥 s_B 的情况下无法恢复出任何 Alice 的消息, 而且攻击者所获取协议执行的数据不比 Alice 多, 因此在 Alice 无法分辨出 Bob 的选择的情况下攻击者也无法分辨出 Bob

的选择,协议能够抵抗重放攻击。最后,由于协议能够有效地抵抗冒充攻击和重放攻击,因此能够抵抗中间人攻击。

4 OT_n^I 协议-II

协议-I是直接利用椭圆曲线公钥系统加密的方法设计的,思想简单,容易理解和实现。但是方案 I 还存在一些不足:Alice 的运算量远大于 Bob 的运算量,同时数据传输的轮数较多、需要相互传递的数据量大等。基于以上问题,在保证充分发挥公钥系统的作用的前提下,本文对方案 I 进行了改进。改进后的协议执行步骤如下。

4.1 协议执行描述

协议用到的公钥系统定义如协议-I,其公共参数为 $\langle G_B, q, G, \psi_B, \psi_B^{-1} \rangle$ 。

初始化:

Alice 持有私密消息 $m_1, \dots, m_n \in \{0, 1\}^*$, 并将其编码到群 G_B 上的点 $\{M_1, \dots, M_n\}$ 。Bob 的选择 $\sigma_1, \dots, \sigma_k \in \{0, \dots, n\}$ 。

信息交互:

(1) Bob 计算 $G_i = s_B^{-1} \psi_B(\sigma_i)$, $i = 1, \dots, k$, 其中 $s_B^{-1} \in \mathbb{Z}_q^*$ 为 Bob 的私钥 s_B 的乘法逆元。Bob 发送 $\{G_1, \dots, G_k\}$ 给 Alice。

(2) Alice 收到 $\{G_1, \dots, G_k\}$ 后, 随机选取 $t_0 \in \mathbb{Z}_q^*$, 计算 $C_i = M_i + t_0(\psi_B(i) + K_B)$, $i = 1, \dots, n$

$D_j = t_0(G_j + G)$, $j = 1, \dots, k$

发送 $\{C_1, \dots, C_n\}, \{D_1, \dots, D_k\}$ 给 Bob。

获取信息:

Bob 收到 $\{C_1, \dots, C_n\}, \{D_1, \dots, D_k\}$ 后, 计算

$M_{\sigma_i} = C_{\sigma_i} - s_B D_i$, $i = 1, \dots, k$

恢复 $m_{\sigma_i} = \psi_B^{-1}(M_{\sigma_i})$ 。

4.2 协议-II 的正确性

协议-II 的正确性和一致性体现在以下等式成立:

$M_{\sigma_i} = C_{\sigma_i} - s_B D_i$

根据椭圆曲线公钥系统以及引理 1 显然上式成立, 这是因为:

$$\begin{aligned} C_{\sigma_i} - s_B D_i &= M_{\sigma_i} + t_0(\psi_B(\sigma_i) + K_B) - s_B t_0(s_B^{-1} \psi_B(\sigma_i) + G) \\ &= M_{\sigma_i} + t_0(\psi_B(\sigma_i) + K_B) - t_0(\psi_B(\sigma_i) + K_B) \\ &= M_{\sigma_i} \end{aligned}$$

因此协议执行完毕后, Bob 能够正确且全部恢复出自己选择的消息。

4.3 协议-II 的安全性

定理 4 将任意两个不同的消息 x, y 编码到 G 中的点 $X = \psi_B(x), Y = \psi_B(y)$, 根据 x, y 间的关系求得 $k \in \mathbb{Z}_q^*$ 使 $X = kY$ 成立依然是困难的。

证明: 假设存在概率多项式时间算法 $\mathcal{A}$ 以不可忽略的概率 ξ 根据 x, y 间的关系求得 $k \in \mathbb{Z}_q^*$ 使 $X = kY$ 成立, 即

$$\Pr[\mathcal{A}(x, y) = k \mid X = kY, X = \psi_B(x), Y = \psi_B(y)] > \xi$$

那么一定存在概率多项式时间算法 $\mathcal{B}$ 可以用来解椭圆曲线上的离散对数问题。 $\mathcal{B}$ 通过如下的方法构造: 首先执行译码函数 ψ_B^{-1} 然后执行算法 $\mathcal{A}$, 算法 $\mathcal{A}$ 的输入是 ψ_B^{-1} 的输出, 即对于 $\forall X, Y \in G$, 利用 ψ_B^{-1} 求出 $x = \psi_B^{-1}(X), y = \psi_B^{-1}(Y)$, 而后通过 $\mathcal{A}(x, y) = k$ 使 $X = kY$ 成立, 由于 ψ_B^{-1} 是概率多项式时间算法, 由此算法 $\mathcal{B}$ 便是由两个概率多项式时间算法以概率多项式时间复合而成的, 所以算法 $\mathcal{B}$ 也是概率时间多项式算

法, 由此便找到一个概率多项式时间算法解椭圆曲线上的离散对数问题, 与椭圆曲线上的离散对数问题困难性假设矛盾, 假设不成立。

定理 5 协议-II 能够保证接收者的选择是安全的。

证明: 根据协议执行过程可知, Alice 只能通过 Bob 发来的数据 $\{G_1, \dots, G_k\}$ 区分 Bob 的具体选择, 根据定理 4 可知, 求 $v_{ij} \in \mathbb{Z}_q^*$ 使 $\psi_B(i) = v_{ij} \psi_B(j)$ 成立是困难的, 因此 Alice 无法通过验证 $G_i = v_{ij} G_j$ 是否成立的方法来确定 G_i 是否为第 x 项以及 G_j 是否为第 y 项。根据引理 3 可知, $\psi_B(i) (i = 1, \dots, n)$ 都是群 G_B 的生成元, 所以 $\exists b_{ij} \in \mathbb{Z}_q^*$ 使得 $G_j = b_{ij} \psi_B(i)$ 成立, 在未知 s_B^{-1} 的情况下, Alice 无法准确判断 G_j 是 Bob 由哪个 $\psi_B(i)$ 计算得到的。同时观察到 $b_{ji} = b_{ij}^{-1}$, 因此 Alice 可以尝试通过 G_i 与 $\psi_B(j)$ 求出 b_{ij} , 计算 $E_u^j = b_{ij} \psi_B(u), u = 1, \dots, n$, 如果集合 $\{G_1, \dots, G_k\} \subset \{E_1^j, \dots, E_n^j\}$ 且 $G_i = E_u^j$, 那么 $(u_1, \dots, u_k)$ 有极大概率是 Bob 的选择, 然而通过 G_i 与 $\psi_B(j)$ 求出 b_{ij} 是解椭圆曲线上的离散对数问题, 通过以上办法区分 Bob 的选择是极困难的。综上所述, 对于任意在概率多项式时间算法 $\mathcal{A}$ 在未知 s_B^{-1} 的条件下

$$\Pr[\mathcal{A}(G_1, \dots, G_k) = (\sigma_1, \dots, \sigma_k) \mid G_i = s_B^{-1} \psi_B(\sigma_i)] < \epsilon$$

其中 ϵ 是可忽略的概率值。

定理 6 协议-II 能够保证发送者未被选择的消息的安全。

证明: 根据协议执行过程以及椭圆曲线上的离散对数问题, Bob 要想从 C_i 中恢复出 M_i , 必须拥有 $t_0(s_B^{-1} \psi_B(i) + G)$, t_0 对 Bob 是保密的。假设 Bob 能够找到概率时间算法 $\mathcal{A}$ 通过 $\{D_1, \dots, D_k\}$ 以及 $\{G_1, \dots, G_k\}$ 和 G 求出 t_0 , 即存在一个不可忽略的概率 ξ 使得

$$\Pr[\mathcal{A}(D_1, \dots, D_k, (G_1 + G), \dots, (G_k + G)) = t_0 \mid D_i = t_0(G_i + G), i = 1, \dots, k] > \xi$$

那么 $\forall P, Q \in G, l_1, \dots, l_k \in \mathbb{Z}_q^*$, 求出 $\mathcal{A}(l_1 Q, \dots, l_k Q, l_1 P, \dots, l_k P) = d$, 显然 $Q = dP$, 因此算法 $\mathcal{A}$ 可以用来计算椭圆曲线上的离散对数问题, 与椭圆曲线离散对数困难问题假设矛盾, 因此 Bob 无法通过 t_0 和 $\psi_B(i) + G$ 计算 $t_0(\psi_B(i) + G)$ 。同理求出 v_{ij} 使 $\psi_B(i) + G = v_{ij}(\psi_B(j) + G)$ 成立, 需要能解椭圆曲线上的离散对数问题, 因此 Bob 无法通过计算 $v_{ij} D_j = t_0(\psi_B(i) + G)$ 的方法获取 $t_0(\psi_B(i) + G)$, 综上 Alice 未被选择的消息是安全的。

定理 7 协议-II 能够抵抗冒充攻击、重放攻击以及中间人攻击。

证明: 根据协议中对消息的加密方法 $C_i = M_i + r_0(\psi_B(i) + K)$ 可知, 如果能够正确恢复 M_i , 必须能够消除随机项 $r_0(\psi_B(i) + K)$, 根据协议数据传递, 攻击者只能获取 $D = r_0(b\psi_B(i) + G)$, 其中 $b \in \mathbb{Z}_q^*$ 由攻击者选取, 由于攻击者不知道 Bob 的私钥 s_B , 因此 b 的选取与 s_B 无关, 观察到如果 $\psi_B(i) + K = h(b\psi_B(i) + G)$ 成立, 那么 $r_0(\psi_B(i) + K) = h r_0(b\psi_B(i) + G)$ 同样成立。因此如果能够求出 h , 攻击者可利用 $C_i - hD$ 恢复出 M_i , 然而通过 $\psi_B(i) + K$ 和 $b\psi_B(i) + G$ 求出 h 是困难的, 这是因为假设求出 h 是容易的, 那么解离散对数问题便是容易的, 由于 $\psi_B(i) + K = h(b\psi_B(i) + G)$, 所以 $\psi_B(i) = \frac{s_B - 1}{hb - 1} G$, 攻击者就能解 $\psi_B(i)$ 与 G 间的离散对数问题, 假设不成立, 同时由于攻击者不知道 s_B , 因此他求 h 的能力要低于知道 s_B

时的能力,因此通过 $\psi_B(i)+K$ 和 $b\psi_B(i)+G$ 求出 h 是困难的,协议-II 能够抵抗冒名攻击;同时攻击者通过截取协议执行传递的数据,在不知道 s_B 的情况下无法恢复出 Alice 的任何一条消息,同时所截取的数据只是 Alice 知道的数据的一部分,因此分辨 Bob 的选择不会比 Alice 的分辨能力有优势,因此协议-II 能够抵抗重放攻击。综上所述,协议-II 能够抵抗中间人攻击。

5 协议执行效率分析

新的 OT_n^* 直接建立于认证的公钥系统中,可以利用公钥系统的认证功能,不需要在执行协议之前构建一个认证的通道,可以节省建立认证通道的开销,一般来说认证通道的建立是一项开销比较大的工作。同时,椭圆曲线公钥系统是一种运算速度快、网络带宽消耗低的公钥系统,因此在发送者发送的信息数以及接受者选择的消息数都相同的情况下,本文设计的协议是执行效率较高的一种。接下来我们从以下 3 方面说明两个协议的具体开销,设进行一次椭圆曲线:

1. 协议执行所需要的信息传递的次数,方案 I 需要 3 轮数据传递,方案 II 需要两轮;

2. 计算复杂性,协议执行过程中比较耗时的运算为椭圆曲线群上的乘法运算(简称数乘运算),发送长度为 l bit 的明文消息 m ,方案 I 需要 $rn+n+3k+1$ 次乘法运算,方案 II 需要 $r*n+3k$ 次,其中 $r=\lceil l/L \rceil$, L 为映射到群 G 中的元素的最长明文 bit 长度,后续使用的 r 定义相同;

3. 通信复杂性,协议执行过程中传递的都是群 G 中的元素,本文采用 160bit,方案 I 需要传递 $160((r+1)n+2k)$ bit,方案 II 需要 $160(r*n+2k)$ bit。

Huang 等在文献[9]中同样利用椭圆曲线离散对数问题设计了一个 OT_n^* 协议,同时也指出了他们设计的 OT_n^* 协议相对于基于其他困难问题的 OT_n^* 协议效率的优越性。然而 Huang 的 OT_n^* 协议在执行过程中由于设计算法本身的问题,无法使用椭圆曲线公钥系统的认证功能,在协议执行前需要建立认证通道,该作者也指出需要预先建立认证通道。表 1 给出我们设计方案与 Huang 方案的效率对比。

表 1 效率对比

协议	轮数	计算复杂性 (次)	通信复杂性 (bit)	是否需要建 立认证通道
Ours 方案 I	3	$(n(r+1)+3k+1)$	$160(n(r+1)+2k)$	否
Ours 方案 II	2	$(n*r+3k)$	$160(n*r+2k)$	否
Huang et al. [9]	3	$r*(3k+n)$	$160*r*(n+2k)$	是

通过表 1 中的数据不难发现,由于 Huang 的协议需要建立认证通道,同时如果发送的明文可以一次发送即 $r=1$ 时,我们的方案 II 的开销与 Huang 的协议效率相当,但是当 $r>1$ 时我们方案 II 的效率要高,同时随着 r 的增大,我们方案 II 的效率优势逐渐增大,同时当 $r>\lceil n/3k+1 \rceil$ 时,我们方案 I 也较 Huang 的方案效率高。

综上所述,由于本文设计的方案不需要预先建立认证通道,结合 Huang 在文献[9]中的效率分析,以及本文中的效率对比分析,本文所设计的 OT_n^* 协议是高效的协议。

结束语 本文基于椭圆曲线公钥系统设计了 OT_n^* 协议,

该协议充分发挥公钥系统的功能,使发送者与接收者使用 OT_n^* 协议传递消息时不需要预先构建认证通道,从而降低协议执行的整体开销,同时椭圆曲线公钥系统本身具有的高效性也能提高协议的执行效率,因此总体上本文设计的 OT_n^* 协议是一种非常高效的协议。协议在保证发送者、接收者各自利益的同时,能够有效地防止开放网络中的第三方攻击,因此新的协议可以在不安全的信道执行。椭圆曲线公钥系统是一种概率加密系统,因此拓展了 OT_n^* 的应用范围。

参考文献

- [1] Rabin M O. How to exchange secrets by oblivious transfer, technical report TR-81 [R]. Aiken Computation Laboratory, Harvard University, 1981
- [2] Even S, Goldreich O, Lempel A. A randomized protocol for signing contracts [J]. Communications of the ACM, 1985, 28: 637-647
- [3] Tzeng W-G. Efficient 1-Out-of-n oblivious transfer schemes with universally usable parameters [J]. IEEE Trans. Computers, 2004, 53(2): 232-240
- [4] Qin Jing, Zhao Hua-wei. k out of n Oblivious Transfer Protocols from Bilinear Pairings [J]. Journal of Software, 2010, 1(5): 65-72
- [5] Chang C C, Lee J S. Robust t-out-of-n oblivious transfer mechanism based on CRT [J]. Journal of Network and Computer Applications, 2009, 32(1): 226-235
- [6] Huang H F, Chang C C. A new design for efficient t-out-n oblivious transfer scheme [C]// ANIA 2005. 2005: 28-30
- [7] Yi Mu, Zhang Jun-qi, Vijay Varadharajan. m out of n oblivious transfer [C]// ACISP2002, LNCS 2384. Springer Verlag, 2002: 395-405
- [8] Camenisch J, Dubovitskaya M, Neven G. Oblivious Transfer with Hidden Access Control Policies [C]// PKC 2011, LNCS 6571. Springer press, 2011: 192-209
- [9] Huang H, Chang C C. A new t-out-n oblivious transfer with low bandwidth [J]. Applied Mathematical Sciences, 2007, 1(7): 311-320
- [10] Boneh D, Franklin M. Identity-Based Encryption from the Weil Pairing [C]// Advances in Cryptology-Crypto 2001, LNCS 2442. Springer press, 2002: 354-369
- [11] ElGamal T. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms [J]. IEEE Transactions on Information Theory, 1985, 31(4): 469-472
- [12] Goldreich O. Secure multi-party computation. Available at <http://theory.lcs.mit.edu/oded>
- [13] Enge A. Elliptic curves and their applications to cryptography: An introduction [M]. Norwell, MA, USA: Kluwer Academic Publishers, 1999
- [14] He F, Stein A, Stein S, et al. The Magic of Elliptic Curves and Public-Key Cryptography [J]. Jahresber Dtsch Math, 2012, 114(2): 59-88
- [15] Zeng Bing, Christophe T, Xu Peng, et al. A Practical Framework for t-out-of-n Oblivious Transfer with Security against Covert Adversaries [J]. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 465-479
- [16] Preetha M K, Vasant S, Venkatesan S, et al. A code-based 1-out-

[17] Parakh A. Oblivious Transfer Using Elliptic Curves [J]. Cryptologia, 2007, 31(2): 125-132

[18] Choi S G, Hwang K-W, Katz J. Secure Multi-Party Computation of Boolean Circuits with Applications to Privacy in On-Line Marketplaces[C]// Topics in Cryptology-CT-RSA 2012, LNCS 7178, San Francisco, CA, USA, 2012; 416-432

[19] 王凤和, 胡子濮, 刘振华. 格基不经意传输协议[J]. 通信学报, 2011, 32(2): 125-130

(上接第 168 页)

报监测数据分组至 Sink 的过程中都采用多跳转发机制, 因此由图 4 可看出, 随着节点数增加, 即节点密度 ρ 增加 (0.0032 ~ 0.0048), 各协议 PDF 都相应增加。但 ARPMS 采用预测路由机制, Sink 在移动过程中可能会偏离预定轨道, 从而导致汇报数据即便成功到达预定位置仍有概率失效, 而且 ARPMS 采用任播机制, 选择 Sink 的判据为能耗效率最高而不是汇报成功率最高, 从而也影响了 PDF 的表现。

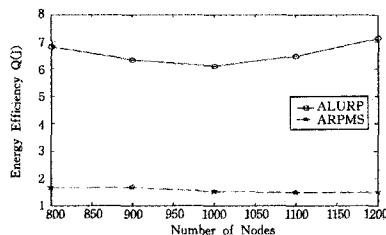


图 5 节点数目和能耗率 Q

由图 5 可知, 尽管 ALURP 的 PDF 优于 ARPMS, 但其能耗效率却很低 (Q 值较高)。这是由于 ALURP 中的 Sink 只要越过其自适应区域 (半径为 40m), 就要时时全网泛洪通知所有节点, 此时能耗 E 值很高, 从而连累 Q 值的表现。

设置节点数目为 1200, 不断调节 Sink 移动速度 V (5 ~ 25m/s), 运行 100s, 实验观察各协议 PDF 和 Q 值, 结果分别如图 6 和图 7 所示。

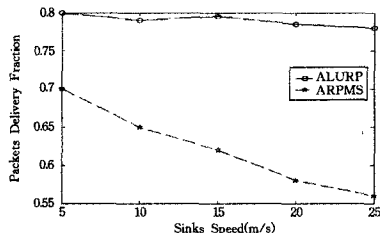


图 6 Sink 速度和数据分组到达率

由图 6 可知, ALURP 的 PDF 表现受 Sink 速度影响很小, 而 ARPMS 采用预测路由机制, 随着 Sink 速度的提高, Δt 时间后 Sink 偏离预定位置的距离 D 值方差增大, 汇报有较大概率失效, 从而影响 PDF 值, 而且 ARPMS 采用的基于能耗效率的任播机制也影响了 PDF 的表现。

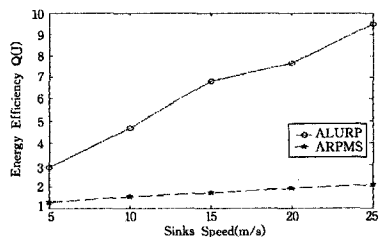


图 7 Sink 速度和能耗率 Q

由图 7 可知, 尽管 ALURP 的 PDF 优于 ARPMS, 但随着 Sink 速度的提高, Sink 的活动范围增大, 超出其自适应区域

的概率增加, 全网泛洪能耗增加很快, 从而导致能耗效率表现较差 (Q 值较大)。而 ARPMS 只在 Sink 改变方向时散播 Sink 位置信息, 与 Sink 移动速度无关, 能耗受 Sink 速度影响较小, 因此具有相对较好的能耗效率 (Q 值较小)。

结束语 提出一种基于预测路由机制的移动 Sink WSN 任播路由协议 (ARPMS)。在 ARPMS 中, Sink 只在移动速度或方向发生改变的时候才需散播其移动信息, 通过 Sink 散播的移动信息, 传感器节点可以计算 (预测) Sink 的当前和将来位置。由于 Sink 无需时时散播位置信息, 从而节省了大量能耗开销。尽管相比传统路由协议 (如经过改进的采用局部泛洪机制的 ALURP 协议), ARPMS 监测数据分组到达率有所下降, 但由于巨大的能耗节省, 其仍然比 ALURP 具有更好的能耗效率 (223% ~ 462%)。

参考文献

- [1] Shah D, Shakkottai S. Oblivious routing with mobile fusion centers over a sensor network[C]//Proceedings of 26th IEEE INFOCOM, 2007; 1541-1549
- [2] Yu J, Jeong E, Jeon G, et al. A dynamic multiagent-based local update strategy for mobile sinks in wireless sensor networks [J]. Proceedings of 11th international conference on computational science and its applications, 2011; 6785(4): 185-196
- [3] 钟智, 罗大庸, 刘少强, 等. 具有移动 sink 的无线传感器网络能量均衡簇路由协议[J]. 控制与决策, 2012, 27(8): 1211-1220
- [4] 郭剑, 孙力娟, 许文君, 等. 基于移动 sink 的无线传感器网络数据采集方案[J]. 通信学报, 2012, 33(9): 176-184
- [5] Kim, J W, In J S, Hur K, et al. An intelligent agent-based routing structure for mobile sinks in WSNs[J]. IEEE Transactions on Consumer Electronics, 2010, 56(4): 2310-2316
- [6] Marta M, Cardei M. Improved sensor network lifetime with multiple mobile sinks[J]. Pervasive and Mobile Computing, 2009, 5(5): 542-555
- [7] Luo J, Hubaux J P. Joint sink mobility and routing to maximize the lifetime of wireless sensor networks: the case of constrained mobility[J]. IEEE/ACM Transactions on Networking, 2010, 18(3): 871-884
- [8] Han S W, Jeong I S, Kang S H. Low latency and energy efficient routing tree for wireless sensor networks with multiple mobile sinks[J]. Journal of Network and Computer Applications, 2013, 36(1): 156-166
- [9] Rao J, Biswas S. Analyzing multi-hop routing feasibility for sensor data harvesting using mobile sinks[J]. Journal of Parallel and Distributed Computing, 2012, 72(6): 764-777
- [10] Li X, Yang J L, Nayak A, et al. Localized geographic routing to a mobile sink with guaranteed delivery in sensor networks[J]. IEEE Journal on Selected Areas in Communications, 2012, 30(9): 1719-1729
- [11] Wang G, Wang T, Jia W, et al. Adaptive location updates for mobile sinks in wireless sensor networks[J]. J Supercomput, 2009, 47(2): 127-145