

基于椭圆曲线的 ElGamal 型位置隐私保护方案

赖慧彬^{1,2}, 许力^{1,2}, 曾雅丽^{1,2}, 朱瑞^{1,2}

(1. 福建师范大学数学与信息学院, 福建 福州 350007;
2. 福建省网络安全与密码技术重点实验室, 福建 福州 350007)

摘要: 针对协作频谱感知场景下用户的位置隐私问题, 提出一种基于椭圆曲线的 ElGamal 型位置隐私保护方案。首先, 次用户通过椭圆曲线上的 ElGamal 公钥密码体制加密原始感知报告后发送给可信第三方; 其次, 可信第三方对加密后的感知报告进行第一次解密, 并且混淆后, 发送给融合中心; 再次, 融合中心进行第二次解密操作后得到原始感知报告; 最后, 分析该方案的安全性。该方案使感知报告的加密方式基于椭圆曲线上的公钥密码体制, 并使可信第三方对感知报告进行混淆, 实现了次用户位置隐私的保护。同时, 与其他方案相比, 该方案有效地降低了通信开销和存储开销。此外, 该方案具有容错机制和动态机制, 增强了方案的实用性。

关键词: 位置隐私保护; 椭圆曲线; ElGamal; 协作频谱感知

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020031

Elliptic curve ElGamal encryption based location privacy-preserving scheme

LAI Huibin^{1,2}, XU Li^{1,2}, ZENG Yali^{1,2}, ZHU Rui^{1,2}

1. College of Mathematics and Informatics, Fujian Normal University, Fuzhou 350007, China
2. Fujian Provincial Key Laboratory of Network Security and Cryptology, Fuzhou 350007, China

Abstract: An elliptic curve ElGamal encryption based location privacy-preserving scheme was proposed to address the location privacy problem of secondary users in collaborative spectrum sensing. Firstly, secondary users encrypted the original sensing reports using the ElGamal public key techniques on the elliptic curve and sent them to the trusted property authority. Secondly, the trusted property authority partially decrypted and randomized sensing

收稿日期: 2019-09-06; 修回日期: 2020-02-18

通信作者: 许力, xuli@fjnu.edu.cn

基金项目: 国家自然科学基金 (61771140, U1905211); 福建省科技厅高校产学研项目 (2017H6005); 企事业合作项目 (DH-1307, DH-1412)

Foundation Items: The National Natural Science Foundation of China (61771140, U1905211), Major Science and Technology Project in Fujian Province, China (2017H6005), IUI Cooperation Project (DH-1307, DH-1412)

论文引用格式: 赖慧彬, 许力, 曾雅丽, 等. 基于椭圆曲线的 ElGamal 型位置隐私保护方案[J]. 网络与信息安全学报, 2020, 6(3): 30-38.

LAI H B, XU L, ZENG Y L, et al. Elliptic curve ElGamal encryption based location privacy-preserving scheme[J]. Chinese Journal of Network and Information Security, 2020, 6(3): 30-38.

reports and then sent the randomized sensing reports to the fusion center. Thirdly, the fusion center finally decrypted and got the original sensing reports. Finally, security of the scheme was analyzed. According to the scheme, the encryption method of sensing reports was based on public key cryptography on elliptic curve. And the trusted property authority randomized encrypted sensing reports. Thus the location privacy of secondary users can be protected. Meanwhile, this scheme effectively reduces communication and storage cost, compared with other schemes. In addition, this scheme also has fault tolerant and dynamic mechanism, which increases the practicability and feasibility.

Key words: location privacy protection, elliptic curve, ElGamal, collaborative spectrum sensing

1 引言

无线频谱是非常珍贵的通信资源。现有的静态频谱分配方案导致频谱资源利用低^[1]，美国联邦通信委员会（FCC，Federal Communications Commission）调查统计发现无线频谱的利用率在15%~85%。而且随着智能手机和平板电脑等移动通信设备的普及，人们对无线频谱资源的需求日益增加^[2]，这使有限的频谱资源更加紧张。为了解决这一问题，Mitola 等^[3]提出了认知无线电（CR，cognitive radio）技术。认知无线网络（CRN，cognitive radio networks）是基于认知无线电技术的一种网络。在认知无线网络中有主用户（PU，primary user）和次用户（SU，secondary user）两类用户。主用户拥有授权频谱，可随时访问自己的频谱资源，目前主用户主要包括卫星通信、电视广播等。次用户只有在主用户空闲时，才能使用主用户的频谱资源^[4]。一旦主用户上线，次用户需立即下线；或者在不干扰主用户正常通信的前提下^[5]，可以和主用户同时使用频谱资源。次用户要想使用空闲频谱，首先需要进行频谱感知^[6]。具有认知功能的次用户通过信号检测方法寻找频谱空洞。由于能量检测方法容易实现且不需要主用户的任何先验信息，已成为认知无线网络中最常用的频谱感知方法。它通过对比接收信号强度（RSS，received signal strength）^[7]和设定的门限值，来判断主用户的频谱资源是否空闲。若小于门限值，则认为主用户不在线，次用户可接入使用频谱；若大于门限值，则认为主用户在线，次用户不可接入使用频谱。

协作频谱感知（CSS，collaborative spectrum sensing）通过收集不同感知区域单个次用户的频谱感知信息并作出综合分析，克服了多径效应、

阴影效应等隐藏终端问题，提高了频谱感知结果的准确性。协作频谱感知场景一般分为集中式和分布式^[8]。在集中式场景下，存在一个中心控制节点，称为融合中心（FC，fusion center）。首先，融合中心通过控制信道发布感知任务；然后，次用户通过统一的频谱感知方式，获得基于自身位置的感知报告，发送给融合中心；接着，融合中心根据融合算法，整合分析频谱感知报告并公布融合结果，次用户根据融合结果申请接入频谱。控制信道是融合中心和次用户之间通信的信道。而在分布式场景下，次用户之间互相分享频谱感知报告，并经过协商分析得出频谱感知结果^[9]。

协作频谱感知在提高感知结果准确性^[10-11]的同时引入了一些安全问题。由于 RSS 值与位置相关，因此攻击者可以从基于 RSS 值的感知报告中推断次用户的位置^[12]，进而对次用户的其他隐私信息进行进一步的推测，如生活习惯、宗教信仰、健康情况等，带来严重的隐私泄露问题^[13]。意识到这些潜在的威胁，次用户可能不愿参与到协作感知中，从而阻碍了认知无线网络的发展。因此，在协作感知场景下，针对次用户位置隐私保护的问题，目前已有的解决方案是隐私保护融合技术。这种技术保证融合中心可以得到融合结果，但不会泄露每个次用户的感知报告。Li 等^[12]提出的位置隐私保护的协作频谱感知（PPSS，privacy preserving collaborative spectrum sensing）方案就是基于这种技术。在他们的方案中，任意两个次用户之间随机生成一组密钥对，最终每个次用户的私钥是由和其他次用户共享的单个密钥累加后决定的。次用户用私钥加密感知报告后发送给融合中心。融合中心通过穷举法解决一个离散对数问题就可以得出最终的融合结果。在这个过程中，融合中心不知道次用户的感知报告，因此保护了

次用户的位置隐私。但由于任意两个次用户之间需要共享一组密钥对，带来较大的通信开销。

Wang 等^[14]提出的 PrimCos (privacy preservation framework for multi-SP collaborative sensing) 方案是基于多个服务提供商下的协作频谱感知场景。每个服务提供商管辖特定次用户群，收集管辖区域内每个次用户的感知报告，多个服务提供商之间协同处理这些感知报告。PrimCos 引入了差分隐私策略来保护次用户的感知报告。

Chen 等^[15]指出，感知报告经过加密发送给融合中心，融合中心需要解密感知报告才能进行融合并得到感知结果。但由于融合中心可能是不可信的，为了让融合中心得到解密后的感知报告后，并不能匹配到感知报告的隶属者，Chen 等从次用户中轮流选择一个次用户作为协助者，并使用改进的 ElGamal 公钥密码体制^[16]，使经过加密的感知报告通过两次解密才能恢复。次用户加密原始感知报告后发送给协助者，协助者先进行打乱感知报告的位置再执行第一次解密操作。第二次解密操作由融合中心执行，融合中心得到原始感知报告后再进行融合。笔者认为，经过打乱操作，融合中心并不知道其解密的感知报告属于哪个次用户。但打乱操作只是改变感知报告的相对位置，其里面的第一项内容还是不变的。因此，半可信的融合中心可以通过窃取加密后的所有感知报告对，再和经过协助者打乱以及第一次解密后的所有感知报告对，比较其第一项内容，匹配感知报告的隶属者。

针对文献[15]方案中存在的不足，本文在此基础上提出了一种椭圆曲线和 ElGamal 算法相结合的位置隐私保护方案。

2 系统模型与假设

2.1 系统模型

本文考虑一种集中式的协作频谱感知场景^[17]，如图 1 所示。该场景包括以下几个实体：融合中心、主用户、次用户和可信第三方 (TPA, trusted property authority)。可信第三方是经过 FCC 授权的实体^[18]，具有强大的计算能力，负责生成系统参数、参与感知报告解密和混淆工作。

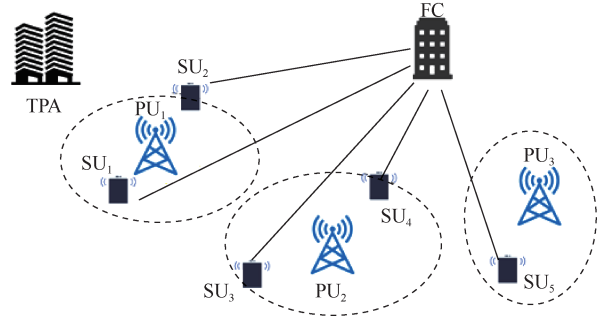


图 1 集中式协作频谱感知场景
Figure 1 Centralized cooperative spectrum sensing

假设 m 个主用户 $PU_i (i=1,2,\dots,m)$ 各自拥有授权频谱， n 个次用户 $SU_j (j=1,2,\dots,n)$ 随机分布在主用户周围，每个次用户都能进行频谱感知，且随时准备接入空闲频谱。集中式协作频谱感知过程如下。

1) 发布感知任务：融合中心通过控制信道通知次用户去感知主用户的信号。

2) 生成感知报告：参照文献[19]，本文采用基于能量检测的频谱感知方式，次用户生成的感知报告用 R_j^i 表示， R_j^i 服从式(1)分布。

$$R_j^i \sim \begin{cases} N(N_0, \frac{N_0^2}{M}), & H_0 \\ N(P_j^i + N_0, \frac{(P_j^i + N_0)^2}{M}), & H_1 \end{cases} \quad (1)$$

其中， H_0 表示频谱空闲， H_1 表示主用户正在使用频谱， N_0 代表噪声功率， P_j^i 表示次用户接收到的主用户信号功率， M 表示信号采样次数。

3) 上传感知报告：次用户通过控制信道发送 R_j^i 给融合中心。

4) 融合感知报告：用 R^i 表示融合结果， R^i 由式(2)确定^[18]。

$$R^i = \sum_{j=1}^n \varpi_j R_j^i \quad (2)$$

其中， ϖ_j 表示 R_j^i 的权重大小，本文采用等增益合并方式^[18]，所有 R_j^i 等权重。

5) 公布融合结果：融合中心通过控制信道广播 R^i 。

2.2 攻击模型与假设

攻击者的目的是获悉次用户的位置信息，攻击者可能来自外部人员，也可能是内部某个恶意次用户，甚至是半可信的融合中心。半可信的融

合中心一方面会“诚实”地融合感知报告，另一方面会“好奇”地伺探次用户的位置信息。融合中心可以通过窃听的方式获得一些信息，然后根据这些信息推断出被攻击者的位置。恶意的次用户不仅想要获得内部其他次用户的位置隐私，同时可能会提交虚假的感知报告扰乱协作频谱感知过程。此外，如果攻击者是次用户，本文允许次用户之间以及次用户和外部人员采取合谋的方式进行攻击。

本文方案的目的是确保融合结果的有效性，同时防止攻击者获得次用户的位置信息。

本文假设次用户在较长一段时间内是静止的，次用户之间有直接的通信信道，此外，恶意次用户的数量不超过次用户总数的一半。

2.3 基于椭圆曲线的 ElGamal 公钥密码算法

2.3.1 椭圆曲线

设 P 是一个大于 3 的素数，则在仿射坐标平面上，有限域 F_p 上的椭圆曲线 E/F_p [20] 由满足方程 $E: y^2 = x^3 + ax + b \bmod p$ 的所有解 $(x, y) \in F_p \cdot F_p$ 以及一个无穷远点 O 组成，如式(3)所示。

$$G = \{(x, y) | y^2 = x^3 + ax + b \bmod p, (x, y) \in F_p \cdot F_p\} \cup \{O\} \quad (3)$$

式中 $a, b \in F_p$ ，且满足 $4a^3 + 27b^2 \neq 0 \bmod p$ 。

选取 E/F_p 上一点 $P = (x, y)$ 作为基点，阶数为 q ，随机选取 $x \in Z_q^*$ ，计算 $Q = x \cdot P$ 是容易的，但已知 P 和 Q ，计算 x 是非常困难的，这就是椭圆曲线离散对数问题。

2.3.2 椭圆曲线和 ElGamal 相结合

ElGamal [21] 是基于有限域上离散对数问题的公钥密码算法，可以将 ElGamal 直接平移到椭圆曲线群上，形成基于椭圆曲线的 ElGamal 公钥密码算法。

3 位置隐私保护方案

本文提出基于椭圆曲线的 ElGamal 型位置隐私保护方案 (LPP-ECEG, location privacy-preserving scheme based on elliptic curve ElGamal)。方案主要包括 4 个阶段：初始化过程、次用户加密感知报告、可信第三方解密和混淆感知报告、融合中心解密感知报告。下文中的符号

说明见表 1。

表 1 符号说明
Table 1 Notation description

符号	含义
p	大于 3 的素数
F_p	素数域
E/F_p	有限域 F_p 上的椭圆曲线
G	椭圆曲线点集
P	E/F_p 的一个基点
q	基点 P 的阶数
s_1	TPA 的私钥
s_2	FC 的私钥
PK	系统公钥
P_j	R_j^i 编码到椭圆曲线上的点
Ecpm	椭圆曲线点乘运算
Ecpa	椭圆曲线点加运算
Expp	指数模 p 运算
Inv	模逆运算
Mulp	模 p 乘法运算
l_{EC}	ECC 密钥长度
l_{EG}	ElGamal 密钥长度
γ	感知报告的长度

3.1 初始化过程

首先可信第三方选取一个大素数 p ，确定椭圆曲线上的四元组 $\{F_p, E/F_p, G, P\}$ ， P 是 E/F_p 上的一个基点，阶数为 q ；接着可信第三方随机选取私钥 $s_1 \in Z_q^*$ 在本地秘密保存，融合中心随机选取私钥 $s_2 \in Z_q^*$ 并计算 $PK_2 = s_2 \cdot P$ ，然后融合中心发送 PK_2 给可信第三方，可信第三方计算公钥 $PK = s_1 \cdot P + PK_2$ ；最后可信第三方公开系统公钥 $\{F_p, E/F_p, G, P, PK\}$ 。

3.2 次用户加密感知报告

次用户 SU_j 的感知报告 R_j^i 需经过编码 [22] 嵌入椭圆曲线 E/F_p 上一点 P_j 。每个次用户随机选取 $\kappa_j \in Z_q^*$ ，分别计算 $C_j^1 = \kappa_j \cdot P$ 和 $C_j^2 = P_j + \kappa_j \cdot PK$ ，生成加密后的感知报告对 (C_j^1, C_j^2) 。下面给出次用户加密感知报告的算法。

算法 1 次用户加密感知报告

输入 系统公钥 $\{F_p, E/F_p, G, P, PK\}$ 、 R_j^i 编

码到 E/F_p 上的点 $P_j = \langle X_j, Y_j \rangle$

输出 加密后的感知报告对 (C_j^1, C_j^2)

```

1) for(j=1; j<=n; j++)
    随机选取  $\kappa_j \in Z_q^*$ 
    计算  $C_j^1 \leftarrow \kappa_j \cdot P$ 
    计算  $C_j^2 \leftarrow P_j + \kappa_j \cdot PK$ 
end for
2) return  $(C_j^1, C_j^2)$ 

```

3.3 可信第三方解密和混淆感知报告

可信第三方拥有私钥 s_1 。可信第三方收到加密后的感知报告对 (C_j^1, C_j^2) 后，依次计算 $\bar{C}_j^1 = s_1 \cdot C_j^1$ 和 $\bar{C}_j^2 \leftarrow C_j^2 - \bar{C}_j^1$ ，生成第一次解密后的感知报告对 $(C_j^1, \bar{C}_j^2)$ ，然后进行混淆。可信第三方为每个次用户随机选取各自的随机数 $\kappa'_j \in Z_q^*$ ，分别计算 $D_j^1 = C_j^1 + \kappa'_j \cdot P$ 和 $D_j^2 = \bar{C}_j^2 + \kappa'_j(PK - s_1 \cdot P)$ ，生成混淆后的感知报告对 (D_j^1, D_j^2) 。下面给出可信第三方解密和混淆感知报告的算法。

算法 2 可信第三方解密和混淆感知报告

输入 可信第三方的私钥 s_1 、次用户 SU_j 加密后的感知报告对 (C_j^1, C_j^2)

输出 可信第三方混淆后的感知报告对 (D_j^1, D_j^2)

```

1) for(j=1; j<=n; j++)
     $\bar{C}_j^1 \leftarrow s_1 \cdot C_j^1$ 
     $\bar{C}_j^2 \leftarrow C_j^2 - \bar{C}_j^1$ 
end for
2) 随机选取  $\kappa'_j \in Z_q^*$ 
3) for(j=1; j<=n; j++)
     $D_j^1 \leftarrow C_j^1 + \kappa'_j \cdot P$ 
end for
4) for(j=1; j<=n; j++)
     $D_j^2 \leftarrow \bar{C}_j^2 + \kappa'_j(PK - s_1 \cdot P)$ 
end for
5) return  $(D_j^1, D_j^2)$ 

```

3.4 融合中心解密感知报告

融合中心拥有私钥 s_2 。融合中心收到混淆后的感知报告对 (D_j^1, D_j^2) 后，依次计算 $\hat{D}_j^1 = s_2 \cdot D_j^1$ 和 $P'_j = D_j^2 - \hat{D}_j^1$ 。 $P'_j = (X'_j, Y'_j)$ 经过译码^[21]后转换

为 $R_j^{i'}$ 。融合中心融合分析 $R_j^{i'}$ ($j=1, 2, \dots, n$)，获得频谱感知结果。下面给出融合中心解密感知报告的算法。

算法 3 融合中心解密感知报告

输入 融合中心的私钥 s_2 、可信第三方混淆后的感知报告对 (D_j^1, D_j^2)

输出 融合中心解密后的 $P'_j = (X'_j, Y'_j)$

```

1) for(j=1; j<=n; j++)
     $\hat{D}_j^1 \leftarrow s_2 \cdot D_j^1$ 
     $P'_j \leftarrow D_j^2 - \hat{D}_j^1$ 
end for
2) return  $P'_j = (X'_j, Y'_j)$ 

```

4 方案评估

4.1 有效性分析

不考虑融合算法以及编码和译码产生的影响时，本文可以证明 LPP-ECEG 方案确保了融合结果的有效性。换言之，就是要证明 P_j 和 P'_j 之间的关系，接下来进行如下推导证明。

(1) 加密阶段

$$C_j^1 = \kappa_j \cdot P \quad (4)$$

$$C_j^2 = P_j + \kappa_j \cdot PK' \quad (5)$$

(2) 可信第三方解密和混淆阶段

$$D_j^1 = C_j^1 + \kappa'_j \cdot P \quad (6)$$

$$D_j^2 = C_j^2 - s_1 \cdot C_j^1 + \kappa'_j(PK - s_1 \cdot P) \quad (7)$$

(3) 融合中心解密阶段

$$P'_j = D_j^2 - s_2 \cdot D_j^1 \quad (8)$$

并且 $PK = s_1 \cdot P + s_2 \cdot P$ ，所以 $P_j = P'_j$ ，确保了融合结果的有效性。同时融合中心并不知道此关系，从而防止了半可信融合中心的攻击，4.2 节会对此进行分析。

此外，恶意次用户可能会提交虚假的感知报告，那么融合中心经过解密后获得的也是虚假的感知报告。文献[23]中指出，错误的感知报告所占比重小于总数一半的情况下，融合结果不受其影响。2.2 节假设恶意次用户的数量在总数一半之内，因此在这种情况下，能确保融合结果的有效性。

4.2 安全性分析

本节分析 LPP-ECEG 方案可以抵抗来自外部人员、内部次用户以及半可信融合中心的攻击。

由于编码后的感知报告 P_j 经过加密被隐藏到项 C_j^2 ，其中 $C_j^2 = P_j + \kappa_j \cdot PK$ ，而且系统公钥 $\{F_p, E/F_p, G, P, PK\}$ 是公开的。所以外部人员获得内部次用户感知报告最直接的方法是通过窃听获得加密感知报告对 (C_j^1, C_j^2) ，然后计算以上公式。但求得 P_j ，需要解决椭圆曲线离散对数问题，而椭圆曲线离散对数问题是一个极其困难的问题。因此，外部人员很难获得内部次用户的感知报告，从而无法获取内部次用户的位置信息。

内部次用户 SU_i 获得其他次用户的感知报告也主要是通过窃听获得加密感知报告对 $(C_j^1, C_j^2)_{j \neq i}$ 。结合上面的分析，内部次用户 SU_i 同样无法获取其他次用户的位置信息。

融合中心收到的是经过混淆后的 $D_j^1 = C_j^1 + \kappa_j' \cdot P$ 和 $D_j^2 = \bar{C}_j^2 + \kappa_j'(PK - s_1 \cdot P)$ 。没有进行混淆之前，融合中心可以窃取 (C_j^1, C_j^2) ，同时融合中心拥有可信第三方发送的 $(C_j^1, \bar{C}_j^2)$ ，因此通过比较 C_j^1 项，融合中心可以知道其解密后的感知报告属于哪个次用户。经过混淆后，融合中心需要解出式 $D_j^1 = C_j^1 + \kappa_j' \cdot P$ ，即需要解决更深层次的椭圆曲线离散对数问题，因此无法判断它解密的感知报告隶属于哪个次用户。

综上所述，LPP-ECEG 方案很好地保护了次用户的位置隐私。

4.3 性能分析

4.1 节证明了次用户无论提交正确或者虚假的感知报告，融合中心最终都会得出有效的融合结果。由于网络故障问题，部分次用户可能提交感知报告失败。在这种情况下，LPP-ECEG 方案还能保证融合中心得出最终的融合结果。在 LPP-ECEG 方案中，融合结果的得出取决于融合中心是否可以解密收到的感知报告。因为解密感知报告的两个私钥是由可信第三方基于椭圆曲线群生成的，并和融合中心各自保存。且所有经过公钥加密的感知报告，可信第三方和融合中心都根据这两个私钥依次解密，感知报告数量的多少并不影响解密，融合中心还能得出最终的频谱感

知结果，所以 LPP-ECEG 方案支持容错机制。

同理，当多个次用户同时加入或者退出协作频谱感知过程时，并不影响可信第三方和融合中心解密感知报告，融合中心还能进行融合，即 LPP-ECEG 方案支持动态机制。表 2 是 LPP-ECEG 方案与文献[15]方案和 PPSRA 方案的对比。

表 2 3 种方案对比
Table 2 Comparisons of three schemes

方案	位置隐私	容错机制	动态机制
PPSRA	✓	×	×
文献[15]	×	✓	✓
LPP-ECEG	✓	✓	✓

4.4 开销分析

本节分析 LPP-ECEG 方案的计算、通信和存储开销，并和其他方案进行对比。

4.4.1 计算开销

在感知报告加密阶段，每个次用户需要执行 2 次椭圆曲线点乘运算、1 次椭圆曲线点加运算，所以， n 个次用户的总计算开销为 $n(2E_{cpm} + E_{cpa})$ 。

在可信第三方解密和混淆感知报告阶段，对于每份加密的感知报告，可信第三方需要执行 4 次椭圆曲线点乘运算、4 次椭圆曲线点加运算。所以，对 n 份加密后的感知报告，可信第三方的总计算开销为 $4n(E_{cpm} + E_{cpa})$ 。

在融合中心解密感知报告阶段，对于混淆后的感知报告，融合中心需要执行 1 次椭圆曲线点乘运算、1 次椭圆曲线点加运算。所以，对 n 份解密 1 次后的感知报告，融合中心总的计算开销为 $n(E_{cpm} + E_{cpa})$ 。

根据文献[24]，不同密钥长度下的椭圆曲线点乘和点加运算时间如表 3 所示。假设有 10 个次用户参与协作频谱感知，所有次用户、可信第三方以及融合中心分别的计算开销如图 2 所示。可信第三方执行主要的计算操作。由于可信第三方是系统引入的具有强大计算能力的实体，因此计算开销在其能力允许范围内。次用户通常是一些移动设备，计算能力较弱，由图 2 可以看出，次用户承担少量的计算操作。融合中心不仅要参与位置隐私保护方案，还要融合感知报告，为了避免其负担过重，本文考虑尽量减少融合中心的计

算开销。由图2可知,融合中心承担的计算开销最小。因此,LPP-ECEG方案在计算开销方面是可行的。表4给出了LPP-ECEG方案和其他方案的计算开销对比。LPP-ECEG方案的不足在于,引入可信第三方产生了一些额外系统开销,因此下一步工作是考虑轻量级的位置隐私保护方案。

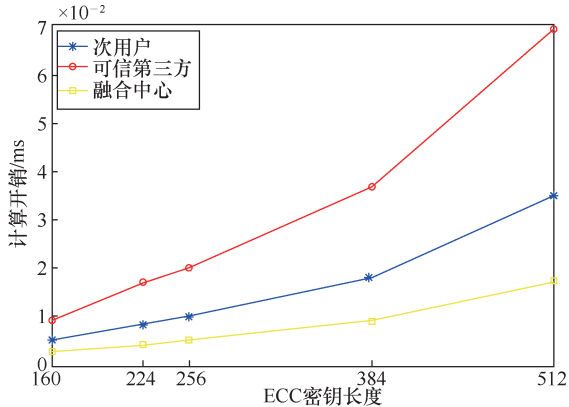


图2 不同实体的计算开销对比

Figure 2 Comparisons of computation cost for each entity

表3 不同密钥长度下两种密码学运算的运行时间
Table 3 Running time of two cryptographic operations under different key lengths

密钥长度/bit	椭圆曲线点加运算/ms	椭圆曲线点乘运算/ms
160	0.056	2.388
224	0.072	4.131
256	0.074	4.822
384	0.112	9.054
512	0.155	17.112

4.4.2 通信开销

加密感知报告后,每个次用户需要发送 (C_j^1, C_j^2) 给可信第三方,所以 n 个次用户产生的总通信开销为 $n(2 \cdot 2 \cdot l_{EC})$ 。第一次解密感知报告后,可信第三方需要发送 (D_j^1, D_j^2) 给融合中心,所以 n 个 (D_j^1, D_j^2) 产生的总通信开销为

$n(2 \cdot 2 \cdot l_{EC})$ 。最终LPP-ECEG方案的总通信开销为 $8 \cdot n \cdot l_{EC}$ 。如果运用点压缩^[25]的方法,那么总通信开销将减小至 $2(l_{EC} + 1) \cdot n \cdot 2$ 。表5给出了LPP-ECEG方案和其他方案的通信开销对比。结合表6给出的密钥长度,LPP-ECEG方案在通信开销方面具有明显的优势。当方案应用在高延迟的广域网中,较低的通信开销是其中比较关键的因素^[26]。

表5 3个方案的通信开销对比
Table 5 Communication cost comparisons of three schemes

方案	通信开销
PPSRA	$n \cdot l_{EG}$
文献[15]方案	$8 \cdot n \cdot l_{EG}$
LPP-ECEG	$4 \cdot n \cdot (l_{EC} + 1)$

表6 不同加密算法的最小安全密钥长度
Table 6 Minimum security key length for different encryption algorithms

加密算法	密钥长度/bit
ElGamal	1 024
ECC	160

说明:PPSRA方案和文献[15]方案的密钥长度是同等级别的,所以本文用 l_{EG} 表示PPSRA的通信开销。

4.4.3 存储开销

表7对比了3个方案的存储开销。根据表6,LPP-ECEG方案的存储开销明显低于PPSRA方案和文献[15]中的方案。

表7 存储开销对比
Table 7 Storage cost comparisons of three schemes

实体	PPSRA	文献[15]	LPP-ECEG
单个次用户	$n \cdot l_{EG} + l_{EG}$	l_{EG}	l_{EG}
融合中心	$n \cdot l_{EG} + l_{EG}$	l_{EG}	l_{EG}

表4 3个方案的计算开销对比
Table 4 Computation cost comparisons of three schemes

实体	PPSRA	文献[15]	LPP-ECEG
次用户	$H + 2\text{Expp} + \text{Mulp}$	$n(2\text{Expp} + \text{Mulp})$	$n(2\text{Ecpm} + \text{Ecpa})$
可信第三方	无此实体	$n(\text{Expp} + \text{Inv} + \text{Mulp})$	$4n(\text{Ecpm} + \text{Ecpa})$
融合中心	$H + n\text{Mulp} + 2\text{Mulp} + 2\text{Expp}2^{r-1}n\text{Expp}$	$n(\text{Expp} + \text{Inv} + \text{Mulp})$	$n(\text{Ecpm} + \text{Ecpa})$

5 结束语

针对协作频谱感知场景下次用户位置隐私保护的问题, 本文提出了一种椭圆曲线和 ElGamal 算法相结合的次用户位置隐私保护方案。次用户通过椭圆曲线上的 ElGamal 公钥密码体制加密原始感知报告后, 发送给可信第三方。可信第三方对加密后感知报告进行第一次解密, 然后混淆第一次解密后的感知报告, 再发送给融合中心。融合中心进行第二次解密操作后得到原始感知报告。安全分析表明, 通过可信第三方对感知报告进行混淆, 融合中心无法将感知报告和其拥有者一一匹配。对于其他攻击者而言, 因为需要解决椭圆曲线离散对数问题, 其很难获得次用户的感知报告。因此, LPP-ECEG 方案很好地保护了次用户的位置隐私。与其他方案对比, LPP-ECEG 方案在通信开销和存储开销具有明显的优势。与此同时, LPP-ECEG 方案具有容错机制和动态机制, 增强了方案的实用性。

参考文献:

- [1] SAMEER S, GHOSH C, DHEKNE R P, et al. Graph theoretic approach to QoS-guaranteed spectrum allocation in cognitive radio networks[C]//2008 IEEE International Performance, Computing and Communication Conference. 2008: 354-359.
- [2] XU T Y, DARWAZEH I. Non-orthogonal narrowband Internet of things: a design for saving bandwidth and doubling the number of connected devices[J]. IEEE Internet of Things Journal, 2018, 5(3): 2120-2129.
- [3] MITOLA J I, MAGUIRE G Q. Cognitive radio: making software radios more personal[J]. IEEE Personal Communications, 1999, 6(4): 13-18.
- [4] 全伟, 毛云龙, 陈庆军, 等. 抗大数据分析的隐私保护: 研究现状与进展[J]. 网络与信息安全学报, 2016, 2(4): 44-55.
TONG W, MAO Y L, CHEN Q J, et al. Survey of big-data-analysis-resistant privacy protection[J]. Chinese Journal of Network and Information Security. 2016, 2(4): 44-55.
- [5] FCC. Spectrum inventory table[EB].
- [6] SESHUKUMAR K, SARAVANAN R, SURAJ M S. Spectrum sensing review in cognitive radio[C]//2013 International Conference on Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System(ICEVENT). 2013: 1-4.
- [7] GUNTER C A, FATEMIETH O, FARHADI A, et al. Using classification to protect the integrity of spectrum measurements in white space networks[C]//NDSS. 2011: 242-251.
- [8] AKYILDIZ I F, LO B F, BALAKRISHNAN R. Cooperative spectrum sensing in cognitive radio networks: a survey[J]. Physical Communication, 2011, 4(1): 40-62.
- [9] 裴庆祺, 李红宁, 赵弘洋, 等. 认知无线网络安全综述[J]. 通信学报, 2013, (1): 144-158.
PEI Q Q, LI H N, ZHAO H Y, et al. Security in cognitive radio networks[J]. Journal on Communications. 2013, (1): 144-158.
- [10] MIN A W, ZHANG X Y, SHIN K G. Detection of small-scale primary users in cognitive radio networks[J]. IEEE Journal on Selected Areas in Communications, 2011, 29(2): 349-361.
- [11] LI H S. Learning the spectrum via collaborative filtering in cognitive radio networks[C]//2010 IEEE Symposium on New Frontiers in Dynamic Spectrum(DySPAN). 2010: 1-12.
- [12] LI S, ZHU H J, GAO Z Y, et al. Location privacy preservation in collaborative spectrum sensing[C]//2012 Proceedings IEEE INFOCOM, 2012:729-737.
- [13] GRISSA M, HAMDADUI B, YAVUZ A A. Location privacy in cognitive radio networks: a survey[J]. IEEE Communications Surveys & Tutorials, 2017, 19(3): 1726-1760.
- [14] WANG W, ZHANG Q. Privacy-preserving collaborative spectrum sensing with multiple service providers[J]. IEEE Transactions on Wireless Communications, 2015, 14(2): 1011-1019.
- [15] CHEN T T, MAO Y L, ZHANG Y, et al. Protecting location information in collaborative sensing of cognitive radio networks[C]//ACM International Conference on Modeling. 2015: 219-226.
- [16] SHENG Z. Privacy, integrity, and incentive-compatibility in computations with untrusted parties[R]. 2004.
- [17] RIFÀ P, HELENA, RIFÀ C. Spectrum sharing models in cognitive radio[C]//International Conference on Cyber-enabled Distributed Computing & Knowledge Discovery. 2011.
- [18] LIU J, ZHANG C, DING H, et al. Policy-based privacy-preserving scheme for primary users in database-driven cognitive radio networks[C]//2016 IEEE Global Communications Conference (GLOBECOM). 2016: 1-6.
- [19] MIN A W, SHIN K G, HU X. Secure cooperative sensing in IEEE 802.22 WRANs using shadow fading correlation[J]. IEEE Transactions on Mobile Computing, 2011, 10(10): 1434-1447.
- [20] PRASANNA Y L, READY E M. A theoretical study of elliptic curve cryptography for location based services[C]//2017 International Conference on Big Data Analytics and Computational Intelligence(ICBDAC). 2017: 404-407.
- [21] SAIKIA M, BORUAH D. Implementation of ElGamal elliptic curve cryptography over prime field using C[C]//International Conference on Information Communication and Embedded Systems(ICICES2014). 2014: 1-7.
- [22] 林淑芬. 基于椭圆曲线的数据加密系统的实现[D]. 厦门: 厦门大学, 2012.
LIN S F. The Implementation of data encryption system based on elliptic curve[D]. Xiamen: Xiamen University, 2012.
- [23] TEGUIG D, SCHEERS B, NIR V L. Data fusion schemes for cooperatives spectrum sensing in cognitive radio net-

works[C]//2012 Military Communications and Information Systems Conference(MCC). 2012: 1-7.

- [24] ZENG Y L, XU L, YANG X, et al. An efficient privacy-preserving protocol for database-driven cognitive radio networks, Ad hoc networks[P]. 2018.

- [25] 苗新亮, 雷波, 刘栋, 等. OpenSSL 中椭圆曲线点的压缩形式研究[J]. 网络安全技术与应用, 2015, (10): 92-93.

MIAO X L, LEI B, LIU D, et al. Study on compression form of elliptic curve points in OpenSSL[J]. Network Security Technology & Application, 2015, (10): 92-93.

- [26] 李欣, 组密钥管理技术研究及其在 IPSec VPN 中的应用[D]. 杭州: 浙江大学, 2006.

LI X. Research of group key management and its application in IPSec VPN[D]. Hangzhou: Zhejiang University, 2006.

[作者简介]



赖慧彬(1995-), 女, 福建漳州人, 福建师范大学硕士生, 主要研究方向为网络与信息安全。



许力(1970-), 男, 福建福州人, 博士, 福建师范大学教授, 主要研究方向为网络与信息安全、无线网络与通信、云计算与物联网。



曾雅丽(1990-), 女, 福建漳州人, 福建师范大学博士生, 主要研究方向为网络与信息安全。



朱瑞(1995-), 女, 福建龙岩人, 福建师范大学硕士生, 主要研究方向为网络与信息安全。