دانشگاه صنعتی شریف
دانشکده علوم ریاضی

پایان‌نامه کارشناسی ارشد
ریاضی کاربردی

محرمانگی تفاضلی محلی و فلان

نگارش

فیروزه ابریشمی

استاد راهنما

جناب آقای دکتر جواد ابراهیمی بروجنی

دی ۱۴۰۴

بسم الله الرحمن الرحیم

به نام خدا

دانشگاه صنعتی شریف

دانشکده علوم ریاضی

پایان‌نامه کارشناسی ارشد

این پایان‌نامه به عنوان تحقق بخشی از شرایط دریافت درجه کارشناسی ارشد است.

عنوان: محرمانگی تفاضلی محلی و فلان

نگارش: فیروزه ابریشمی

کمیته ممتحنین

استاد راهنما: جناب آقای دکتر جواد ابراهیمی بروجنی امضاء:

استاد مشاور: استاد مشاور امضاء:

استاد مدعو: استاد ممتحن امضاء:

تاریخ:

اظهارنامه

(اصالت متن و محتوای پایان‌نامه کارشناسی ارشد)

عنوان پایان‌نامه: محرمانگی تفاضلی محلی و فلان

استاد راهنما: جناب آقای دکتر جواد ابراهیمی **استاد مشاور:** استاد مشاور بروجنی

این‌جانب فیروزه ابریشمی اظهار می‌دارم:

۱. متن و نتایج علمی ارائه شده در این پایان‌نامه اصیل بوده و زیرنظر استادان نام‌برده شده در بالا تهیه شده است.

۲. متن پایان‌نامه به این صورت در هیچ جای دیگری منتشر نشده است.

۳. متن و نتایج مندرج در این پایان‌نامه، حاصل تحقیقات این‌جانب به عنوان دانشجوی کارشناسی ارشد دانشگاه صنعتی شریف است.

۴. کلیه مطالبی که از منابع دیگر در این پایان‌نامه مورد استفاده قرار گرفته، با ذکر مرجع مشخص شده است.

نگارنده: فیروزه ابریشمی

تاریخ:

امضاء:

نتایج تحقیقات مندرج در این پایان‌نامه و دستاوردهای مادی و معنوی ناشی از آن (شامل فرمول‌ها، توابع کتابخانه‌ای، نرم‌افزارها، سخت‌افزارها و مواردی که قابلیت ثبت اختراع دارد) متعلق به دانشگاه صنعتی شریف است. هیچ شخصیت حقیقی یا حقوقی بدون کسب اجازه از دانشگاه صنعتی شریف حق فروش و ادعای مالکیت مادی یا معنوی بر آن یا ثبت اختراع از آن را ندارد. همچنین، کلیه حقوق مربوط به چاپ، تکثیر، نسخه‌برداری، ترجمه، اقتباس و نظائر آن در محیط‌های مختلف اعم از الکترونیکی، مجازی یا فیزیکی برای دانشگاه صنعتی شریف محفوظ است. نقل مطلب با ذکر ماخذ بلامانع است.

استاد راهنما: جناب آقای دکتر جواد ابراهیمی بروجنی

تاریخ:

امضاء:

نگارنده: فیروزه ابریشمی

تاریخ:

امضاء:

سپاس

از استاد عزیزم که با کمک‌ها و راهنمایی‌های بی‌دریغشان، مرا در به سرانجام رساندن این پایان‌نامه یاری داده‌اند، تشکر و قدردانی می‌کنم. همچنین از همکاران عزیزی که با راهنمایی‌های خود در بهبود نگارش این نوشتار سهیم بوده‌اند، صمیمانه سپاسگزارم.

چکیده

کلیدواژه‌ها:

فهرست مطالب

فهرست جداول

فهرست تصاویر

فصل ۱

مقدمه

۱-۱ اهمیت موضوع

۱-۲ ادبیات موضوع

۱-۳ اهداف پژوهش

۱-۴ ساختار پایان‌نامه

فصل ۲

پیش‌نیازها

۲-۱ محرمانگی تفاضلی متمرکز (CDP)

مفهوم محرمانگی تفاضلی یا به اختصار ε-DP، اولین بار توسط دورک و همکاران [؟] معرفی شد و به سرعت به استاندارد طلایی برای حفظ حریم خصوصی در تحلیل داده‌ها تبدیل گشت. این چارچوب، یک تعریف ریاضی قوی از حریم خصوصی ارائه می‌دهد که مبتنی بر پنهان‌سازی حضور یا عدم حضور یک فرد خاص در مجموعه داده است.

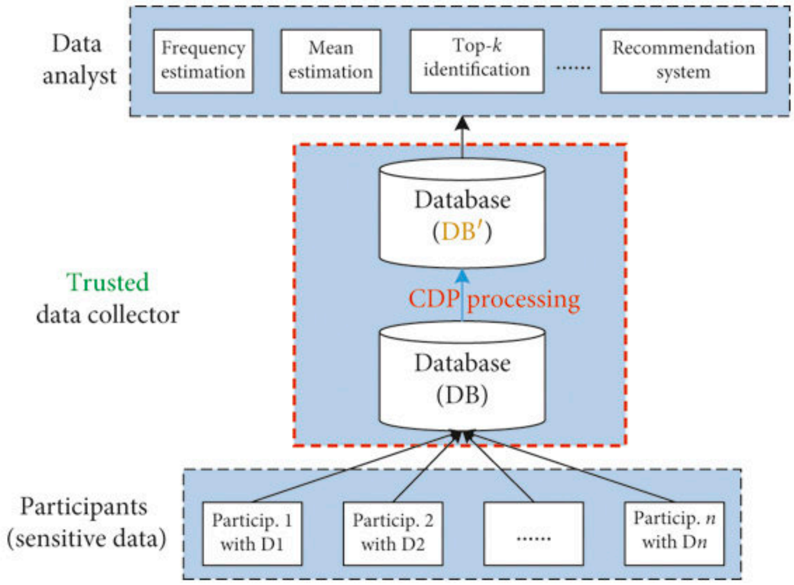
۲-۱-۱ مدل اعتماد و تعریف رسمی

در مدل متمرکز[1]، فرض بر این است که یک متصدی مورد اعتماد[2] وجود دارد. تمام افراد داده‌های خام و حساس خود را در اختیار این متصدی قرار می‌دهند (شکل ۲-۱ را ببینید). متصدی، مجموعه داده‌ی کامل $\mathcal{D}$را در اختیار دارد. وظیفه‌ی متصدی این است که با اجرای یک مکانیزم تصادفی[3] $\mathcal{M}$ بر روی $\mathcal{D}$، نتایجی (مثلاً پاسخ به یک پرس‌وجو[4]) را به صورت عمومی منتشر کند، به طوری که اطلاعات حساس افراد فاش نشود.

برای تعریف رسمی، ابتدا باید مفهوم «همسایگی» مجموعه داده‌ها را تعریف کنیم.

تعریف ۲-۱ (مجموعه داده‌های همسایه) *دو مجموعه داده‌ی $\mathcal{D}_1$ و $\mathcal{D}_2$ را همسایه[5] می‌گوییم (و با $\mathcal{D}_1 \sim$*

[1] Centralized
[2] Trusted Curator
[3] randomized mechanism
[4] Query
[5] Adjacent



شکل ۲-۱: مدل محرمانگی تفاضلی متمرکز با یک متصدی مورد اعتماد.

$\mathcal{D}_2$ نشان می‌دهیم) *اگر تنها در یک رکورد با یکدیگر تفاوت داشته باشند.* (یعنی $\mathcal{D}_2$ از افزودن یا حذف یک رکورد به $\mathcal{D}_1$ به دست آید).

ایده‌ی اصلی محرمانگی تفاضلی این است که خروجی مکانیزم برای دو مجموعه داده‌ی همسایه باید از نظر آماری «شبیه» باشد، به طوری که مهاجم نتواند تشخیص دهد ورودی واقعی کدام بوده است.

تعریف ۲-۲ (محرمانگی تفاضلی (ε-DP)) *یک مکانیزم تصادفی $\mathcal{M}$، تعریف εــ محرمانگی تفاضلی*[6] *را برآورده می‌سازد، اگر برای هر دو مجموعه داده‌ی همسایه‌ی $\mathcal{D}_1$ و $\mathcal{D}_2$ و برای هر زیرمجموعه $\mathcal{S}$ از خروجی‌های ممکن* ($\mathrm{Range}(\mathcal{M})$)*، داشته باشیم:*

$$\Pr[\mathcal{M}(\mathcal{D}_1) \in \mathcal{S}] \leqslant \exp(\varepsilon) \cdot \Pr[\mathcal{M}(\mathcal{D}_2) \in \mathcal{S}] \qquad (۲-۱)$$

گاهی اوقات، یک تعریف انعطاف‌پذیرتر به نام (ε, δ)-DP نیز استفاده می‌شود که اجازه‌ی یک احتمال شکست کوچک δ را می‌دهد:

$$\Pr[\mathcal{M}(\mathcal{D}_1) \in \mathcal{S}] \leqslant \exp(\varepsilon) \cdot \Pr[\mathcal{M}(\mathcal{D}_2) \in \mathcal{S}] + \delta \qquad (۲-۲)$$

[6] ε-Differential Privacy

۲-۱-۲ مکانیزم‌های پایه در CDP

برای دستیابی به ε-DP، باید به پاسخ دقیق پرس‌وجو «نویز»[۷] اضافه کنیم. میزان نویز به حساسیت[۸] پرس‌وجو بستگی دارد.

تعریف ۲-۳ (حساسیت سراسری) *برای یک تابع f، حساسیت سراسری ℓ_1 $(\Delta_1 f)$ و ℓ_2 $(\Delta_2 f)$ به صورت زیر تعریف می‌شوند:*

$$\Delta_1 f = \max_{\mathcal{D}_1 \sim \mathcal{D}_2} \|f(\mathcal{D}_1) - f(\mathcal{D}_2)\|_1 \tag{۲-۳}$$

$$\Delta_2 f = \max_{\mathcal{D}_1 \sim \mathcal{D}_2} \|f(\mathcal{D}_1) - f(\mathcal{D}_2)\|_2 \tag{۲-۴}$$

سه مکانیزم اساسی برای دستیابی به CDP عبارتند از:

- **مکانیزم لاپلاس**[۹]**:** برای توابع عددی، با افزودن نویز از توزیع لاپلاس متناسب با حساسیت ℓ_1، می‌توان به ε-DP دست یافت:

$$\mathcal{M}(\mathcal{D}) = f(\mathcal{D}) + \mathrm{Lap}\left(\frac{\Delta_1 f}{\varepsilon}\right) \tag{۲-۵}$$

- **مکانیزم گوسی**[۱۰]**:** این مکانیزم اغلب زمانی استفاده می‌شود که حساسیت ℓ_2 تابع کمتر از حساسیت ℓ_1 باشد. در اینجا نویز از توزیع نرمال (گوسی) افزوده می‌شود:

$$\mathcal{M}(\mathcal{D}) = f(\mathcal{D}) + \mathcal{N}\left(0, \sigma^2\right) \tag{۲-۶}$$

که در آن $\sigma \geqslant \sqrt{2\ln(1.25/\delta)} \cdot \frac{\Delta_2 f}{\varepsilon}$ است. برخلاف مکانیزم لاپلاس، این مکانیزم تنها (ε, δ)-DP را (با $\delta > 0$) تضمین می‌کند.

- **مکانیزم نمایی**[۱۱]**:** برای خروجی‌های غیرعددی (دسته‌ای)، از یک «تابع امتیاز» $q(\mathcal{D}, r)$ استفاده می‌شود. این مکانیزم خروجی r را با احتمالی متناسب با امتیاز آن برمی‌گرداند:

$$\Pr[\mathcal{M}(\mathcal{D}) = r] \propto \exp\left(\frac{\varepsilon \cdot q(\mathcal{D}, r)}{2\Delta q}\right) \tag{۲-۷}$$

[7] Noise
[8] Sensitivity
[9] The Laplace Mechanism
[10] The Gaussian Mechanism
[11] The Exponential Mechanism

۲-۱-۳ خواص کلیدی محرمانگی تفاضلی

قدرت چارچوب DP در خواص ترکیبی آن نهفته است:

- **مصونیت در برابر پس‌پردازش**[۱۲]: انجام هرگونه محاسبات بر روی خروجی یک مکانیزم ε-DP (بدون دسترسی مجدد به داده‌های اصلی)، نمی‌تواند سطح محرمانگی را کاهش دهد.
- **ترکیب‌پذیری**[۱۳]: اگر چندین مکانیزم ε-DP را اجرا کنیم، بودجه‌های محرمانگی جمع می‌شوند.
  - *ترکیب‌پذیری پایه‌ای:* اجرای k مکانیزم ε_iDP- منجر به $\sum \varepsilon_i$DP- می‌شود.
  - *ترکیب‌پذیری پیشرفته:* با پذیرش یک δ کوچک، می‌توان نشان داد که بودجه کل با نرخ $\sqrt{k}$ رشد می‌کند (نه k).
- **محرمانگی گروهی**[۱۴]: محرمانگی تفاضلی به طور طبیعی برای گروه‌هایی از افراد نیز صادق است. اگر دو پایگاه داده در k رکورد با هم متفاوت باشند، تضمین محرمانگی به صورت $k\varepsilon$-DP برقرار خواهد بود. این یعنی با افزایش اندازه گروه، تضمین محرمانگی به صورت خطی تضعیف می‌شود.

۲-۱-۴ محدودیت مدل متمرکز

با وجود تمام مزایا، مدل CDP یک نقطه‌ی ضعف اساسی دارد: نیاز به یک متصدی کاملاً مورد اعتماد. در بسیاری از سناریوهای دنیای واقعی (مانند جمع‌آوری داده از گوشی‌های هوشمند)، کاربران به سرور مرکزی اعتماد ندارند. این عدم اعتماد، ما را به سمت مدل جایگزین، یعنی «محرمانگی تفاضلی محلی» سوق می‌دهد.

۲-۲ مبانی نظریه اطلاعات و f-واگرایی‌ها

در بخش‌های قبلی، ما مکانیزم‌های محرمانگی تفاضلی را به عنوان روش‌هایی برای ایجاد «شباهت آماری» بین خروجی‌های دو پایگاه داده‌ی همسایه معرفی کردیم. در این بخش، ما ابزار ریاضیاتی اصلی برای سنجش این «شباهت» یا «فاصله» بین توزیع‌های احتمالی را معرفی می‌کنیم. این ابزار، خانواده‌ی f-واگرایی‌ها[۱۵] است که بسیاری از معیارهای رایج فاصله‌ی آماری را به عنوان حالت‌های خاص خود در بر می‌گیرد.

[12] Post-processing Immunity
[13] Composition
[14] Group Privacy
[15] f-divergences

۲-۲-۱ تعریف fـ واگرایی

مفهوم fـ واگرایی اولین بار توسط سیسر [؟] و به طور همزمان توسط علی و سیلوِی [؟] معرفی شد. این معیار، یک روش عمومی برای اندازه‌گیری تفاوت بین دو توزیع احتمال P و Q (تعریف شده بر روی یک فضای یکسان) ارائه می‌دهد.

تعریف ۲-۴ (fـ واگرایی) *فرض کنید P و Q دو توزیع احتمال باشند به طوری که P نسبت به Q مطلقاً پیوسته[16] باشد. فرض کنید p و q توابع چگالی احتمال (یا توابع جرم احتمال) آن‌ها باشند. برای هر تابع محدب $f : (0,\infty) \to \mathbb{R}$ که $f(1) = 0$ باشد، fـ واگرایی P از Q به صورت زیر تعریف می‌شود:*

$$D_f(P||Q) = \int q(x) f\left(\frac{p(x)}{q(x)}\right) dx \quad (۲-۸)$$

در حالت گسسته، این تعریف به صورت حاصل جمع زیر در می‌آید:

$$D_f(P||Q) = \sum_{x\in\mathcal{X}} q(x) f\left(\frac{p(x)}{q(x)}\right) \quad (۲-۹)$$

تابع f «ژنراتور» (تولیدکننده)ی واگرایی نامیده می‌شود و با انتخاب fهای متفاوت، می‌توان معیارهای فاصله یا واگرایی متفاوتی را به دست آورد. شرط $f(1) = 0$ تضمین می‌کند که اگر دو توزیع یکسان باشند ($P = Q$)، واگرایی آن‌ها صفر خواهد بود.

۲-۲-۲ نمونه‌های مهم fـ واگرایی

بسیاری از معیارهای معروف در آمار و نظریه اطلاعات، حالت‌های خاصی از fـ واگرایی هستند:

- واگرایی کولبک‌ـ لایبلر[17]: این معیار که به آن آنتروپی نسبی[18] نیز گفته می‌شود، با انتخاب تابع $f(t) = t \log t$ به دست می‌آید:

$$D_{KL}(P||Q) = \sum_{x} p(x) \log\left(\frac{p(x)}{q(x)}\right) \quad (۲-۱۰)$$

- فاصله‌ی واریانس کل[19]: فاصله‌ی TV (که اغلب با $\Delta(P,Q)$ یا d_{TV} نشان داده می‌شود) ارتباط نزدیکی با fـ واگرایی دارد و با انتخاب $f(t) = \frac{1}{2}|t-1|$ حاصل می‌شود:

$$d_{TV}(P,Q) = \frac{1}{2} \sum_{x} |p(x) - q(x)| \quad (۲-۱۱)$$

[16] Absolutely Continuous
[17] Kullback-Leibler (KL) Divergence
[18] Relative Entropy
[19] Total Variation (TV) Distance

- واگرایی کای‌ـدو[20]: این معیار آماری با انتخاب $f(t) = (t-۱)^۲$ به دست می‌آید:

$$\chi^۲(P||Q) = \sum_x \frac{(p(x)-q(x))^۲}{q(x)} \quad (۲\text{-}۱۲)$$

- فاصله‌ی هلینجر (مربع)[21]: این فاصله با انتخاب $f(t) = (\sqrt{t}-۱)^۲$ (یا معادل آن $f(t) = \frac{۱}{۲}(\sqrt{t}-۱)^۲$) حاصل می‌شود:

$$H^۲(P,Q) = \sum_x (\sqrt{p(x)} - \sqrt{q(x)})^۲ \quad (۲\text{-}۱۳)$$

۲-۲-۳ ارتباط fـ واگرایی‌ها با یکدیگر

این واگرایی‌ها مستقل از هم نیستند و روابط ریاضی مهمی بین آن‌ها برقرار است. یکی از مشهورترین این روابط، نامساوی پینسکر[22] است که ارتباط بین واگرایی KL و فاصله‌ی واریانس کل را نشان می‌دهد:

$$d_{TV}(P,Q)^۲ \leqslant \frac{۱}{۲} D_{KL}(P||Q) \quad (۲\text{-}۱۴)$$

این نامساوی‌ها در تحلیل‌های حریم خصوصی بسیار کاربردی هستند، زیرا به ما اجازه می‌دهند که با داشتن یک کران (حد) بر روی یک معیار واگرایی، بتوانیم کرانی برای سایر معیارها نیز به دست آوریم.

در فصل بعدی، ما به تفصیل بررسی خواهیم کرد که چگونه تضمین ε-LDP(که در معادله ؟؟ تعریف شد) مستقیماً منجر به ایجاد یک کران بالا بر روی fـ واگرایی‌های مختلف بین توزیع‌های خروجی می‌شود.

۲-۳ مبانی آماری و نظریه اطلاعات

در این بخش، ابزارهای آماری و معیارهای نظریه اطلاعات را که در تحلیل حد پایین خطا و نرخ‌های مینیماکس در این پژوهش مورد استفاده قرار می‌گیرند، معرفی می‌کنیم. این تعاریف عمدتاً بر اساس چارچوب ارائه‌شده در [؟] هستند.

۲-۳-۱ معیارهای فاصله اطلاعاتی

برای دو توزیع احتمال P و Q که روی فضای $\mathcal{X}$ تعریف شده‌اند و نسبت به یک اندازه‌ی پایه μ مطلقاً پیوسته هستند (با توابع چگالی p و q)، معیارهای زیر را تعریف می‌کنیم:

[20] Chi-Squared (χ^2) Divergence
[21] Squared-Hellinger Distance
[22] Pinsker's Inequality

تعریف ۲-۵ (واگرایی کولبک-لایبلر) *واگرایی کولبک-لایبلر (KL) بین دو توزیع P و Q به صورت زیر تعریف می‌شود:*

$$D_{KL}(P||Q) = \int_{\mathcal{X}} p(x) \log \frac{p(x)}{q(x)} d\mu(x) \qquad (۲-۱۵)$$

تعریف ۲-۶ (فاصله‌ی واریانس کل) *فاصله‌ی واریانس کل[۲۳] بین دو توزیع P و Q به صورت زیر تعریف می‌شود:*

$$||P - Q||_{TV} = \sup_{S \in \sigma(\mathcal{X})} |P(S) - Q(S)| = \frac{1}{2} \int_{\mathcal{X}} |p(x) - q(x)| d\mu(x) \qquad (۲-۱۶)$$

تعریف ۲-۷ (اطلاعات متقابل) *اگر X و V دو متغیر تصادفی باشند، اطلاعات متقابل[۲۴] بین آن‌ها به صورت امید ریاضی واگرایی KL بین توزیع شرطی و توزیع حاشیه‌ای تعریف می‌شود:*

$$I(X;V) = D_{KL}(P_{X,V}||P_X \otimes P_V) = \mathbb{E}_V \left[D_{KL}(P_{X|V}||P_X)\right] \qquad (۲-۱۷)$$

۲-۳-۲ ریسک مینیماکس

در نظریه تصمیم آماری، هدف تخمین یک پارامتر $\theta(P)$ از یک توزیع ناشناخته $P \in \mathcal{P}$ است. اگر $\hat{\theta}$ یک تخمین‌گر باشد که تابعی از داده‌های مشاهده شده (مانند $Z_1, \ldots, Z_n$) است، کیفیت آن با استفاده از یک تابع زیان صعودی $\Phi \circ \rho$ سنجیده می‌شود (که ρ یک شبه‌متر روی فضای پارامتر است).

نرخ مینیماکس[۲۵]، کمترین خطای ممکنی است که یک تخمین‌گر در بدترین سناریو (بدترین توزیع P در کلاس $\mathcal{P}$) متحمل می‌شود.

تعریف ۲-۸ (نرخ مینیماکس) *برای یک کلاس از توزیع‌ها $\mathcal{P}$ و پارامتر θ، نرخ مینیماکس $\mathfrak{M}_n$ به صورت زیر تعریف می‌شود:*

$$\mathfrak{M}_n(\theta(\mathcal{P}), \Phi \circ \rho) = \inf_{\hat{\theta}} \sup_{P \in \mathcal{P}} \mathbb{E}_P[\Phi(\rho(\hat{\theta}(Z^n), \theta(P)))] \qquad (۲-۱۸)$$

که در آن اینفیمم روی تمام تخمین‌گرهای ممکن $\hat{\theta}$ گرفته می‌شود.

در حالتی که محدودیت حریم خصوصی تفاضلی محلی با پارامتر α وجود داشته باشد، نرخ مینیماکس خصوصی (αPrivate- Minimax Rate) با در نظر گرفتن اینفیمم روی تمام مکانیزم‌های کانال Q که شرط ε-LDPرا برآورده می‌کنند، تعریف می‌شود [؟].

[23] Total Variation Distance
[24] Mutual Information
[25] Minimax Rate

۴-۲ آزمون فرض آماری و روش تقلیل

برای اثبات حدود پایین نرخ‌های مینیماکس، روش استاندارد این است که مسئله‌ی تخمین پارامتر را به یک مسئله‌ی آزمون فرض[۲۶] تقلیل دهیم. ایده اصلی این است: اگر نتوانیم بین چند مقدار گسسته از پارامتر با دقت بالا تمایز قائل شویم، قطعاً نمی‌توانیم پارامتر را در فضای پیوسته با خطای کم تخمین بزنیم.

۲-۴-۱ آزمون فرض دودویی

ساده‌ترین حالت آزمون فرض، تصمیم‌گیری بین دو توزیع احتمال $P_۰$ و $P_۱$ است. فرض کنید داده‌ی مشاهده شده Z از یکی از این دو توزیع تولید شده است. ما دو فرض داریم:

- فرض صفر ($H_۰$): $Z \sim P_۰$
- فرض مقابل ($H_۱$): $Z \sim P_۱$

یک آزمون (یا تابع تست) $\psi : \mathcal{Z} \to \{۰, ۱\}$ تابعی است که بر اساس داده‌ی مشاهده شده، حدس می‌زند کدام فرض صحیح است. خطای این آزمون به صورت مجموع احتمال خطای نوع اول و دوم تعریف می‌شود:

$$P_{err}(\psi) = \Pr_{H_۰}(\psi(Z) = ۱) + \Pr_{H_۱}(\psi(Z) = ۰) \tag{۲-۱۹}$$

لم نیمن–پیرسون[۲۷] نشان می‌دهد که کمترین خطای ممکن برای هر آزمون دودویی، مستقیماً با فاصله‌ی واریانس کل (d_{TV}) بین دو توزیع ارتباط دارد:

$$\inf_{\psi} P_{err}(\psi) = ۱ - \|P_۰ - P_۱\|_{TV} \tag{۲-۲۰}$$

این رابطه نشان می‌دهد که هرچه دو توزیع $P_۰$ و $P_۱$ به هم شبیه‌تر باشند (فاصله‌ی TV کمتر)، احتمال خطا بیشتر شده و به ۱ (حدس تصادفی) نزدیک‌تر می‌شود. در فضای ε-LDP، نویز اضافه شده باعث کاهش شدید فاصله‌ی TV و در نتیجه افزایش خطای آزمون می‌شود.

۲-۴-۲ تقلیل تخمین به آزمون (روش بسته‌بندی)

برای استفاده از ابزارهای آزمون فرض در مسئله‌ی تخمین نرخ مینیماکس (معادله ۲-۲۶)، از تکنیک گسسته‌سازی فضای پارامتر Θ استفاده می‌کنیم. این روش شامل مراحل زیر است:

[۲۶] Hypothesis Testing
[۲۷] Neyman-Pearson Lemma

۱. **ساخت مجموعه‌ی بسته‌بندی**[28]: مجموعه‌ای متناهی از پارامترها $\mathcal{V} = \{\theta_1, \dots, \theta_M\} \subset \Theta$ را انتخاب می‌کنیم به طوری که از یکدیگر فاصله‌ی معناداری داشته باشند. به طور دقیق‌تر، اگر ρ متریک خطا باشد، برای هر $i \neq j$ باید داشته باشیم $\rho(\theta_i, \theta_j) \geqslant 2\delta$.

۲. **تعریف مسئله‌ی آزمون:** فرض می‌کنیم طبیعت[29] یک اندیس V را به صورت تصادفی و یکنواخت از مجموعه $\{1, \dots, M\}$ انتخاب می‌کند و داده‌ها بر اساس توزیع P_{θ_V} تولید می‌شوند. هدف، یافتن V بر اساس داده‌های مشاهده شده است.

۳. **ارتباط خطاها:** اگر یک تخمین‌گر $\hat{\theta}$ وجود داشته باشد که خطای تخمین آن با احتمال بالا کمتر از δ باشد، می‌توانیم از آن برای حل مسئله‌ی آزمون فرض استفاده کنیم (با انتخاب نزدیک‌ترین θ_i به $\hat{\theta}$). بنابراین، کران پایین روی خطای آزمون فرض، یک کران پایین برای خطای تخمین ایجاد می‌کند:

$$\mathfrak{M}_n(\theta(\mathcal{P})) \geqslant \Phi(\delta) \cdot \inf_{\psi} \Pr(\psi(Z^n) \neq V) \tag{۲-۲۱}$$

۲-۴-۳ نامساوی‌های کران پایین

سه روش اصلی که در [؟] برای اثبات کران‌های پایین استفاده شده‌اند عبارتند از:

قضیه‌ی ۲-۱ (نامساوی لو کم[30]) *این روش برای آزمون بین دو توزیع P_1 و P_2 استفاده می‌شود. کمینه احتمال خطا با استفاده از فاصله‌ی واریانس کل (رابطه ۲-۱۶) کران‌دار می‌شود:*

$$\inf_{\psi} \Pr(\psi(Z^n) \neq V) \geqslant \frac{1}{2}\left(1 - \|P_1^n - P_2^n\|_{TV}\right) \tag{۲-۲۲}$$

این روش زمانی مفید است که مسئله را به تشخیص بین دو حالت ساده تقلیل دهیم.

قضیه‌ی ۲-۲ (نامساوی فانو[31]) *زمانی که پارامتر مورد نظر متعلق به مجموعه‌ای بزرگ‌تر $\mathcal{V}$ باشد (تعداد فرضیه‌ها $|\mathcal{V}| > 2$)، نامساوی فانو کران پایین قوی‌تری ارائه می‌دهد که مبتنی بر اطلاعات متقابل است:*

$$\inf_{\psi} \Pr(\psi(Z^n) \neq V) \geqslant 1 - \frac{I(Z^n; V) + \log 2}{\log |\mathcal{V}|} \tag{۲-۲۳}$$

که در آن V متغیر تصادفی یکنواخت روی مجموعه اندیس‌ها $\mathcal{V}$ است.

[28] Packing Set
[29] Nature

لم ۲-۳ (لم اسود[۳۲]) *این لم مسئله تخمین را به چندین آزمون فرض دودویی مستقل روی مختصات یک ابرمکعب $\{-۱, ۱\}^d$ تبدیل می‌کند. نسخه دقیق‌تر آن که در [؟] استفاده شده است، کران پایین را بر اساس فاصله‌ی واریانس کل توزیع‌های مخلوط حاشیه‌ای بیان می‌کند:*

$$\mathfrak{M}_n(\theta(\mathcal{P})) \geqslant \delta \sum_{j=۱}^{d} \left[۱ - \|M_{+j}^n - M_{-j}^n\|_{TV} \right] \qquad (۲\text{-}۲۴)$$

که در آن M_{+j}^n و M_{-j}^n توزیع‌های حاشیه‌ای مخلوط روی مقادیر ۱+ و ۱- در بُعد j_ام هستند.

۲-۵ ریسک مینیماکس و روش‌های کران پایین

در بخش‌های پیشین، ابزارهای سنجش فاصله بین توزیع‌ها را معرفی کردیم. در این بخش، به معرفی چارچوب آماری می‌پردازیم که در آن از این ابزارها برای تحلیل حدود پایین خطا در حضور محدودیت‌های حریم خصوصی استفاده می‌شود. تعاریف و قضایای این بخش عمدتاً بر اساس چارچوب ارائه‌شده در [؟] هستند.

۲-۵-۱ اطلاعات متقابل

یکی دیگر از مفاهیم کلیدی نظریه اطلاعات که ارتباط تنگاتنگی با واگرایی KL دارد، اطلاعات متقابل است.

تعریف ۲-۹ (اطلاعات متقابل) *اگر X و V دو متغیر تصادفی باشند، اطلاعات متقابل[۳۳] بین آن‌ها به صورت امید ریاضی واگراییKL بین توزیع شرطی و توزیع حاشیه‌ای تعریف می‌شود:*

$$I(X;V) = D_{KL}(P_{X,V}||P_X \otimes P_V) = \mathbb{E}_V \left[D_{KL}(P_{X|V}||P_X) \right] \qquad (۲\text{-}۲۵)$$

این معیار در نامساوی فانو (که در ادامه می‌آید) نقش کلیدی ایفا می‌کند.

۲-۵-۲ ریسک مینیماکس

در نظریه تصمیم آماری، هدف تخمین یک پارامتر $\theta(P)$ از یک توزیع ناشناخته $P \in \mathcal{P}$ است. اگر $\hat{\theta}$ یک تخمین‌گر باشد که تابعی از داده‌های مشاهده شده (مانند $Z_۱, \ldots, Z_n$) است، کیفیت آن با استفاده از یک تابع زیان صعودی $\Phi \circ \rho$ سنجیده می‌شود (که ρ یک شبه‌متر روی فضای پارامتر است).

[33] Mutual Information

نرخ مینیماکس[۳۴]، کمترین خطای ممکنی است که یک تخمین‌گر در بدترین سناریو (بدترین توزیع P در کلاس $\mathcal{P}$) متحمل می‌شود.

تعریف ۲-۱۰ (نرخ مینیماکس) *برای یک کلاس از توزیع‌ها $\mathcal{P}$ و پارامتر θ، نرخ مینیماکس $\mathfrak{M}_n$ به صورت زیر تعریف می‌شود:*

$$\mathfrak{M}_n(\theta(\mathcal{P}), \Phi \circ \rho) = \inf_{\hat{\theta}} \sup_{P \in \mathcal{P}} \mathbb{E}_P[\Phi(\rho(\hat{\theta}(Z^n), \theta(P)))] \quad (۲-۲۶)$$

که در آن اینفیمم روی تمام تخمین‌گرهای ممکن $\hat{\theta}$ گرفته می‌شود.

در حالتی که محدودیت حریم خصوصی تفاضلی محلی با پارامتر α وجود داشته باشد، نرخ مینیماکس خصوصی (αPrivate- Minimax Rate) با در نظر گرفتن اینفیمم روی تمام مکانیزم‌های کانال Q که شرط ε-LDPرا برآورده می‌کنند، تعریف می‌شود [؟].

۲-۵-۳ نامساوی‌های کران پایین

برای اثبات کران‌های پایین روی نرخ مینیماکس، معمولاً مسئله‌ی تخمین به یک مسئله‌ی آزمون فرض[۳۵] چندگانه تقلیل داده می‌شود. در اینجا سه روش اصلی که بر پایه fـ واگرایی‌ها بنا شده‌اند را معرفی می‌کنیم:

قضیه‌ی ۲-۴ (نامساوی لو کم[۳۶]) *این روش برای آزمون بین دو توزیع P_1 و P_2 استفاده می‌شود. کمینه احتمال خطا با استفاده از فاصله‌ی واریانس کل (رابطه ۲-۱۱) کران‌دار می‌شود:*

$$\inf_{\psi} \Pr(\psi(Z^n) \neq V) \geqslant \frac{1}{2}\left(1 - \|P_1^n - P_2^n\|_{TV}\right) \quad (۲-۲۷)$$

این روش زمانی مفید است که مسئله را به تشخیص بین دو حالت ساده تقلیل دهیم.

قضیه‌ی ۲-۵ (نامساوی فانو[۳۷]) *زمانی که پارامتر مورد نظر متعلق به مجموعه‌ای بزرگتر $\mathcal{V}$ باشد (تعداد فرضیه‌ها $|\mathcal{V}| > 2$)، نامساوی فانو کران پایین قوی‌تری ارائه می‌دهد که مبتنی بر اطلاعات متقابل است:*

$$\inf_{\psi} \Pr(\psi(Z^n) \neq V) \geqslant 1 - \frac{I(Z^n; V) + \log 2}{\log |\mathcal{V}|} \quad (۲-۲۸)$$

که در آن V متغیر تصادفی یکنواخت روی مجموعه اندیس‌ها $\mathcal{V}$ است.

[34] Minimax Rate
[35] Hypothesis Testing

لم ۲-۶ (لم اسود[۳۸]) *این لم مسئله تخمین را به چندین آزمون فرض دودویی مستقل روی مختصات یک ابرمکعب $\{-۱,۱\}^d$ تبدیل می‌کند. نسخه دقیق‌تر آن که در [؟] استفاده شده است، کران پایین را بر اساس فاصله‌ی واریانس کل توزیع‌های مخلوط حاشیه‌ای بیان می‌کند:*

$$\mathfrak{M}_n(\theta(\mathcal{P})) \geqslant \delta \sum_{j=۱}^{d} \left[۱ - \|M_{+j}^n - M_{-j}^n\|_{TV} \right] \qquad (۲۹-۲)$$

که در آن M_{+j}^n و M_{-j}^n توزیع‌های حاشیه‌ای مخلوط روی مقادیر ۱+ و ۱- در بُعد jـام هستند.

فصل ۳

محرمانگی تفاضلی محلی

در فصل گذشته، مبانی نظری حریم خصوصی متمرکز (CDP) و ابزارهای آماری لازم برای تحلیل آن را مرور کردیم. در این فصل، به طور اختصاصی به **چارچوب محرمانگی تفاضلی محلی**[1] **(LDP)** می‌پردازیم. این مدل، که امروزه در سیستم‌های توزیع‌شده و جمع‌آوری داده‌های بزرگ‌مقیاس کاربرد فراوان دارد، پارادایم اعتماد را از «سرور مرکزی» به «کاربر نهایی» تغییر می‌دهد.

۳-۱ مقدمه و گذار از مدل متمرکز

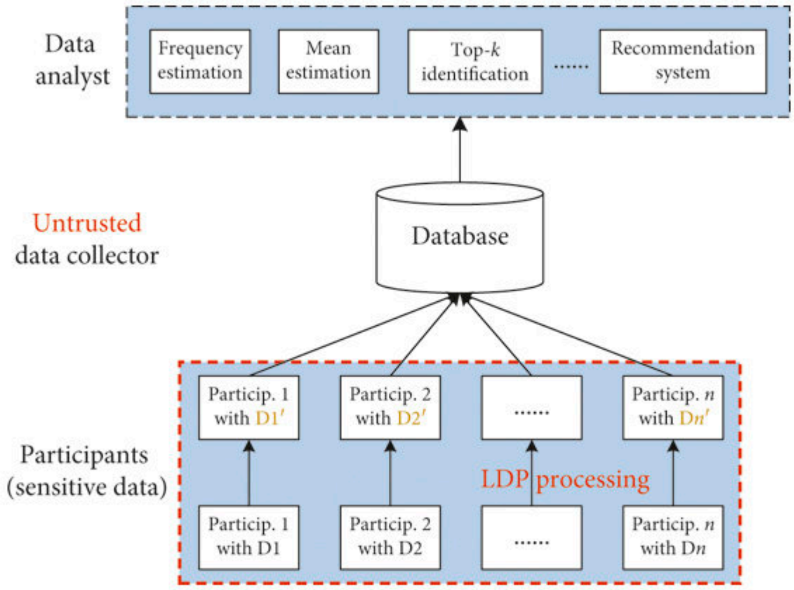
همان‌طور که در بخش ۲-۱ دیدیم، مدل متمرکز نیازمند وجود یک متصدی مورد اعتماد[2] است که به داده‌های خام دسترسی داشته باشد. اگرچه این مدل دقت آماری بالایی را فراهم می‌کند، اما در دنیای واقعی با چالش‌های امنیتی و حقوقی جدی روبروست:

- **نقطه شکست مرکزی**[3]**:** سرور مرکزی هدف جذابی برای مهاجمان است. نشت اطلاعات از سرور (چه بر اثر هک و چه بر اثر خطای انسانی) حریم خصوصی تمام کاربران را به خطر می‌اندازد.
- **عدم اعتماد کاربران:** در بسیاری از کاربردها (مانند جمع‌آوری داده‌های پزشکی یا تاریخچه مرورگر)، کاربران تمایلی ندارند داده‌های حساس خود را حتی به یک سرور «مطمئن» بسپارند.

در پاسخ به این چالش‌ها، مدل محرمانگی تفاضلی محلی مطرح شد. در LDP، فرآیند خصوصی‌سازی (افزودن نویز) به سمت کلاینت (کاربر) منتقل می‌شود. به این معنا که داده‌ها *قبل* از ترک دستگاه کاربر،

[1] Local Differential Privacy (LDP)
[2] Trusted Curator
[3] Single Point of Failure

نویزدار می‌شوند و سرور تنها به داده‌های بی‌نام و نویزدار دسترسی دارد (شکل ۳-۱).



شکل ۳-۱: مدل محرمانگی تفاضلی محلی (LDP). نویز به صورت محلی روی دستگاه کاربر اضافه می‌شود.

این رویکرد توسط شرکت‌های بزرگ فناوری برای جمع‌آوری داده‌های تله‌متری پذیرفته شده است. برای مثال، گوگل از مکانیزم RAPPOR در مرورگر کروم، و اپل و مایکروسافت از روش‌های مشابهی برای جمع‌آوری داده‌های آماری از سیستم‌عامل‌های خود استفاده می‌کنند.

۳-۲ تعاریف رسمی و مدل‌های محاسباتی

در مدل محلی، ما n کاربر داریم که هر کدام یک داده‌ی خصوصی X_i از دامنه $\mathcal{X}$ در اختیار دارند. هر کاربر به طور مستقل یک الگوریتم تصادفی (مکانیزم) را اجرا می‌کند و خروجی Z_i را منتشر می‌کند.

۳-۲-۱ تعریف LDP

هسته‌ی اصلی این مدل، «تصادفی‌ساز محلی» است.

تعریف ۳-۱ (تصادفی‌ساز محلی[۴]) *یک مکانیزم تصادفی $\mathcal{M} : \mathcal{X} \to \mathcal{Z}$ را یک تصادفی‌ساز محلی می‌نامیم که ورودی $x \in \mathcal{X}$ را می‌گیرد و خروجی $z \in \mathcal{Z}$ را بر اساس توزیع احتمال شرطی $Q(z|x)$ تولید می‌کند.*

شرط محرمانگی در اینجا تضمین می‌کند که با مشاهده‌ی خروجی z، تمایز قائل شدن بین هر دو ورودی

اولیه x و x' دشوار باشد. تفاوت کلیدی این تعریف با مدل متمرکز در این است که در CDP ما دو پایگاه داده‌ی همسایه را مقایسه می‌کردیم، اما در اینجا هر دو مقدار ورودی ممکن مقایسه می‌شوند.

تعریف ۳-۲ (αـ محرمانگی تفاضلی محلی) *یک مکانیزم $\mathcal{M}$ دارای αـ محرمانگی تفاضلی محلی (α-ε-LDP) است اگر برای تمام جفت ورودی‌های $x, x' \in \mathcal{X}$ و هر زیرمجموعه از خروجی‌ها $\mathcal{S} \subseteq \mathcal{Z}$ داشته باشیم:*

$$\sup_{S} \frac{\Pr[\mathcal{M}(x) \in \mathcal{S}]}{\Pr[\mathcal{M}(x') \in \mathcal{S}]} \leqslant e^{\alpha} \quad (۳-۱)$$

(نکته: در متون آماری مانند [؟] معمولاً از پارامتر α به جای ε برای نمایش بودجه حریم خصوصی محلی استفاده می‌شود تا تمایز آن با مدل متمرکز مشخص باشد. ما نیز در این فصل و فصول بعدی از این نمادگذاری پیروی می‌کنیم).

این تعریف معادل شرط زیر بر روی واگرایی ماکزیمم (D_∞) بین توزیع‌های شرطی است:

$$\sup_{x, x' \in \mathcal{X}} D_\infty(Q(\cdot|x)||Q(\cdot|x')) \leqslant \alpha \quad (۳-۲)$$

۳-۲-۲ تعمیم‌ها و خواص

علاوه بر تعریف استاندارد α-ε-LDP(معادله ۳-۱)، دو مفهوم دیگر نیز در تحلیل‌های نظری و طراحی مکانیزم‌ها اهمیت دارند: محرمانگی تقریبی و خاصیت ترکیب.

تعریف ۳-۳ ((α, δ)ـ محرمانگی تفاضلی محلی) *یک مکانیزم تصادفی $\mathcal{M}$ دارای محرمانگی تفاضلی محلی تقریبی یا (α, δ)-ε-LDPاست اگر برای هر دو ورودی $x, x' \in \mathcal{X}$ و هر زیرمجموعه خروجی $\mathcal{S} \subseteq \mathcal{Z}$ داشته باشیم:*

$$\Pr[\mathcal{M}(x) \in \mathcal{S}] \leqslant e^{\alpha} \cdot \Pr[\mathcal{M}(x') \in \mathcal{S}] + \delta \quad (۳-۳)$$

این تعریف (که در [؟] نیز بررسی شده است)، اجازه‌ی یک احتمال شکست کوچک δ را می‌دهد. اهمیت نظری این تعریف در آن است که ارتباط مستقیمی با واگرایی E_γ (که در فصل قبل معرفی شد) دارد.

قضیه‌ی ۳-۱ (ترکیب ترتیبی[۵]) *اگر یک کاربر در k مرحله‌ی مختلف در پروتکل‌های $\mathcal{M}_1, \dots, \mathcal{M}_k$ شرکت کند که هر کدام به ترتیب دارای بودجه‌ی حریم خصوصی α_i باشند، آنگاه کل فرآیند دارای محرمانگی تفاضلی محلی با بودجه‌ی $\sum_{i=1}^{k} \alpha_i$ خواهد بود. این خاصیت در تحلیل پروتکل‌های تعاملی (بخش ۳-۲-۳) که در آن خروجی‌های بعدی به خروجی‌های قبلی وابسته هستند، نقش بنیادین دارد.*

۳-۲-۳ پروتکل‌های تعاملی و غیرتعاملی

یکی از جنبه‌های مهم در تحلیل نرخ‌های مینیماکس (که در فصل بعد به آن می‌پردازیم)، نحوه‌ی تعامل کاربران با سرور است. دوچی و همکاران [؟] پروتکل‌های محلی را به دو دسته تقسیم می‌کنند:

۱. **پروتکل‌های غیرتعاملی**[6]: در این حالت، خروجی هر کاربر Z_i تنها به ورودی خودش X_i وابسته است و مستقل از داده‌ها یا خروجی‌های سایر کاربران تولید می‌شود.

$$Z_i = \mathcal{M}_i(X_i) \tag{۳-۴}$$

این مدل ساده‌ترین و رایج‌ترین شکل پیاده‌سازی LDP است.

۲. **پروتکل‌های تعاملی (ترتیبی)**[7]: در این حالت، مکانیزم کاربر i می‌تواند به خروجی‌های منتشر شده توسط کاربران قبلی $(Z_1, \ldots, Z_{i-1})$ وابسته باشد. به عبارت دیگر، کانال ارتباطی Q_i می‌تواند به صورت پویا بر اساس تاریخچه تغییر کند:

$$Z_i \sim Q_i(\cdot | X_i, Z_1, \ldots, Z_{i-1}) \tag{۳-۵}$$

این مدل به الگوریتم‌های تطبیقی اجازه می‌دهد تا دقت تخمین را بهبود بخشند. با این حال، همان‌طور که در فصل بعد خواهیم دید، حتی با وجود تعامل، محدودیت‌های بنیادی f ـ واگرایی همچنان مانع از کاهش چشمگیر نرخ خطا می‌شوند.

۳-۳ مکانیزم‌های پایه در LDP

مکانیزم‌های پایه در مدل محلی با مدل متمرکز متفاوت هستند. دو مورد از رایج‌ترین آن‌ها عبارتند از:

- **پاسخ تصادفی**[8]: پایه‌ای‌ترین مکانیزم در مدل محلی، پاسخ تصادفی است که در اصل توسط وارنر [؟] (حتی پیش از DP) معرفی شد. این مکانیزم اغلب برای پرس‌وجوهای دودویی (مانند «آیا شما ویژگی P را دارید؟») استفاده می‌شود. در این روش، کاربر به صورت زیر عمل می‌کند:

  ۱. یک سکه پرتاب کن.

  ۲. اگر «شیر» آمد، پاسخ حقیقی را بگو.

[6] Non-interactive
[7] Sequential/Interactive
[8] Randomized Response

۳. اگر «خط» آمد، سکه‌ی دومی پرتاب کن و بر اساس نتیجه‌ی آن سکه (شیر = بله، خط = خیر) پاسخ بده.

این روش تضمین می‌کند که هر پاسخی (چه «بله» و چه «خیر») دارای امکان انکارپذیری قابل قبول[9] است. برای مثال، پاسخ «بله» لزوماً به معنای مثبت بودن ویژگی در فرد نیست، چرا که ممکن است در اثر پرتاب سکه‌ی دوم حاصل شده باشد.

- **مکانیزم‌های دامنه بزرگ:** برای داده‌هایی با دامنه‌های بزرگ‌تر (مانند کلمات در یک جستجو یا تخمین فراوانی)، مکانیزم پاسخ تصادفی ساده کارایی ندارد. در این موارد از مکانیزم‌های مبتنی بر کدگذاری یگانی[10] مانند RAPPOR یا OUE استفاده می‌شود.

۳-۴ چالش سودمندی در مدل محلی

بهای عدم اعتماد به سرور، کاهش شدید سودمندی[11] آماری است. از آنجایی که نویز به داده‌ی هر فرد به صورت مستقل اضافه می‌شود، خطای تجمیعی در مدل LDP بسیار بیش‌تر از مدل متمرکز CDP است.

برای رسیدن به سطح دقت مشابه، مدل محلی معمولاً به تعداد کاربران n بسیار بیشتری نیاز دارد. به طور کلی، در حالی که خطای مکانیزم‌های CDP اغلب با $O(1/n)$ کاهش می‌یابد، خطای مکانیزم‌های LDP معمولاً با $O(1/\sqrt{n})$ کاهش می‌یابد. این کاهش در «اندازه نمونه مؤثر» یکی از موضوعات اصلی است که در فصل آینده با استفاده از ابزارهای fــ واگرایی آن را اثبات خواهیم کرد.

۳-۵ مکانیزم‌های پایه در LDP

در این بخش، مکانیزم‌های بنیادین را معرفی می‌کنیم که برای تحقق محرمانگی تفاضلی محلی استفاده می‌شوند. این مکانیزم‌ها بلوک‌های سازنده‌ی پروتکل‌های پیچیده‌تر هستند.

[9] Plausible Deniability
[10] Unary Encoding
[11] Utility

۳-۵-۱ پاسخ تصادفی دودویی (RR)

پایه‌ای‌ترین و کلاسیک‌ترین مکانیزم در مدل محلی، «پاسخ تصادفی»[12] است که توسط وارنر [؟] معرفی شد. فرض کنید دامنه ورودی دودویی باشد ($\mathcal{X} = \{۰, ۱\}$).

مکانیزم $\mathcal{M}_{RR}$ با ورودی $x \in \{۰, ۱\}$، خروجی $z \in \{۰, ۱\}$ را طبق احتمالات زیر تولید می‌کند:

$$\Pr[z = x] = p, \quad \Pr[z \neq x] = ۱ - p \tag{۳-۶}$$

برای اینکه این مکانیزم شرط α-LDP-εرا برآورده کند، طبق تعریف ۳-۲ باید نسبت احتمالات حداکثر e^α باشد:

$$\frac{\Pr[z = ۱|x = ۱]}{\Pr[z = ۱|x = ۰]} = \frac{p}{۱ - p} \leqslant e^\alpha \tag{۳-۷}$$

بنابراین، با انتخاب $p = \frac{e^\alpha}{۱+e^\alpha}$، مکانیزم بهینه α-LDP-εحاصل می‌شود. در این حالت، واریانس تخمین‌گر حاصل از این مکانیزم برابر است با:

$$\mathrm{Var}[\hat{x}] = \frac{e^\alpha}{(e^\alpha - ۱)^۲} \tag{۳-۸}$$

که نشان می‌دهد برای αهای کوچک، واریانس به سرعت افزایش می‌یابد (تقریباً با نرخ $۱/\alpha^۲$).

۳-۵-۲ پاسخ تصادفی تعمیم‌یافته (GRR)

زمانی که دامنه ورودی شامل $k > ۲$ عنصر باشد ($\mathcal{X} = \{۱, \ldots, k\}$)، از نسخه تعمیم‌یافته پاسخ تصادفی[13] استفاده می‌شود [؟]. در این مکانیزم، برای ورودی x:

$$\Pr[\mathcal{M}(x) = z] = \begin{cases} p & \mathrm{if} z = x \\ q & \mathrm{if} z \neq x \end{cases} \tag{۳-۹}$$

از آنجا که مجموع احتمالات باید ۱ باشد، داریم $p + (k - ۱)q = ۱$. برای برقراری شرط α-LDP-ε، باید $\frac{p}{q} \leqslant e^\alpha$ باشد. با حل این دستگاه معادلات، مقادیر بهینه p و q به صورت زیر به دست می‌آیند:

$$p = \frac{e^\alpha}{e^\alpha + k - ۱}, \quad q = \frac{۱}{e^\alpha + k - ۱} \tag{۳-۱۰}$$

این مکانیزم برای دامنه‌های کوچک (k کوچک) بسیار کارآمد است، اما با افزایش k، دقت آن به شدت کاهش می‌یابد زیرا احتمال گزارش پاسخ صحیح (p) به سمت صفر میل می‌کند.

[12] Randomized Response (RR)
[13] Generalized Randomized Response (GRR)

۳-۵-۳ مکانیزم لاپلاس در مدل محلی

برای داده‌های عددی پیوسته یا گسسته (مثلاً $x \in [-۱, ۱]$)، می‌توان از مکانیزم لاپلاس استفاده کرد. اگرچه این مکانیزم در مدل متمرکز بسیار محبوب است، اما در مدل محلی چالش‌برانگیز است. طبق تعریف، حساسیت سراسری در مدل محلی برابر با قطر دامنه است (چون هر دو ورودی x, x' باید تمایزناپذیر باشند). اگر $\mathcal{X} = [-۱, ۱]$ باشد، حساسیت $\Delta = |۱ - (-۱)| = ۲$ است. بنابراین، مکانیزم لاپلاس محلی به صورت زیر تعریف می‌شود:

$$\mathcal{M}_{Lap}(x) = x + \eta, \quad \eta \sim \text{Lap}\left(\frac{۲}{\alpha}\right) \tag{۳-۱۱}$$

نکته مهمی که دوچی و همکاران [؟] به آن اشاره کرده‌اند این است که مکانیزم لاپلاس در مدل محلی، به خصوص برای ابعاد بالا ($d > ۱$)، **زیر-بهینه** (Sub-optimal) است و نرخ خطای آن بیشتر از مکانیزم‌های تخصصی‌تر (مانند نمونه‌برداری هایپرکیوب) است که در تحلیل مینیماکس فصل بعد بررسی خواهیم کرد.

فصل ۴

کارهای پیشین و مرور ادبیات

فصل ۵

نتایج جدید

فصل ۶

نتیجه‌گیری

واژه‌نامه

الف

ابتکاری .... heuristic
ابعاد بالا .... high dimensions
اریب .... bias
آستانه .... threshold
اصل لانه‌ی کبوتری .... pigeonhole principle
ان‌پی-سخت .... NP-Hard
انتقال .... transition

ب

برخط .... online
برنامه‌ریزی خطی .... linear programming
بهینه .... optimum
بیشینه .... maximum

پ

پرت .... outlier
پرسمان .... query
پوشش .... cover
پیچیدگی .... complexity

ت

تجربی .... experimental
تراکم .... density
تقریب .... approximation
تقسیم‌بندی .... partition
توری .... mesh
توزیع‌شده .... distributed

ج

جداپذیر .... separable
جعبه سیاه .... black box
جویبار داده .... data stream

ح

حدی .... extreme
حریصانه .... greedy

خ

خوشه .... cluster
خطی .... linear

د

داده .... data

داده‌کاوی .... data mining

داده‌ی پرت .... outlier data

دوبرابرسازی .... doubling

دودویی .... binary

ر

رأس .... vertex

رسمی .... formal

ز

زیرخطی .... sublinear

س

سرشکن .... amortized

سلسه‌مراتبی .... hierarchichal

ش

شبه کد .... pseudocode

شیء .... object

ص

صدق‌پذیری .... satisfiability

غ

غلبه .... dominate

ف

فاصله .... distance

فضا .... space

ق

قطعی .... deterministic

ک

کارا .... efficient

کاندیدا .... candidate

کمینه .... minimum

م

مجموعه .... set

مجموعه هسته .... coreset

مسطح .... planar

موازی‌سازی .... parallelization

میان‌گیر .... buffer

ن

نابه‌جایی .... inversion

ناوردا .... invariant

نقطه‌ی مرکزی .... center point

نیم‌فضا .... half space

هـ

هزینه‌ی آشوب .... price of anarchy (POA)

ی

یال .... edge

پیوست آ

مطالب تکمیلی

Abstract

We present a standard template for typesetting theses in Persian. The template is based on the XePersian package for the LaTeX typesetting system. This write-up shows a sample usage of this template.

Keywords: Thesis, Typesetting, Template, XePersian

Sharif University of Technology

Department of Mathematics

M.Sc. Thesis

Local Differential Privacy

By:

Firoozeh Abrishami

Supervisor:

Dr. Javad Ebrahimi Boroujeni

January 2026