정 보 보 호 학 회 지
제28권 제2호, 2018. 4

차분 프라이버시 기반 비식별화 기술에 대한 연구

정 강 수*, 박 석**

요 약

차분 프라이버시는 통계 데이터베이스 상에서 수행되는 질의 결과에 의한 개인정보 추론을 방지하기 위한 수학적 모델로써 2006년 Dwork에 의해 처음 소개된 이후로 통계 데이터에 대한 프라이버 보호의 표준으로 자리잡고 있다. 차분 프라이버시는 데이터의 삽입/삭제 또는 변형에 의한 질의 결과의 변화량을 일정 수준 이하로 유지함으로써 정보 노출을 제한하는 개념이다. 이를 구현하기 위해 메커니즘 상의 연구(라플라스 메커니즘, 익스퍼넨셜 메커니즘)와 다양한 데이터 분석 환경(히스토그램, 회귀 분석, 의사 결정 트리, 연관 관계 추론, 클러스터링, 딥러닝 등)에 차분 프라이버시를 적용하는 연구들이 수행되어 왔다. 본 논문에서는 처음 Dwork에 의해 제안되었을 때의 차분 프라이버시 개념에 대한 이해부터 오늘날 애플 및 구글에서 차분 프라이버시가 적용되고 있는 수준에 대한 연구들의 진행 상황과 앞으로의 연구 주제에 대해 소개한다.

Ⅰ. 서 론

다양한 전자, 정보, 통신 기술의 발달에 따른 정보화 시대의 도래는 디지털 데이터의 폭발적인 증가를 가져왔다. 대용량 데이터의 저장 및 분석 기술 발전에 따라 축적된 디지털 데이터는 커다란 경제적 가치를 지닌 자원으로 여겨지고 있으며, 기업이나 조직은 의사 결정에 필요한 지식을 추론해 낼 수 있는 디지털 데이터와 분석 기술 확보에 매진하고 있다. 그러나 개인정보가 포함된 대용량 데이터 분석은 잠재적인 개인정보노출 위험을 야기한다. 선거인명부를 사용한 매사추세츠 주지사의 병원 기록 정보 노출이나 AOL 검색기록을 통한 특정인 식별, 넷플릭스 평점 자료를 통한 이용자 식별 등의 일련의 프라이버시 침해 사건들은 이와 같은 개인정보노출의 위험성을 보여주는 사례들이다. 개인들은 서비스의 혜택을 받기 위해 개인 데이터를 제공하지만 자신이 허락한 수준 이상의 정보가 드러나는 것은 원하지 않으므로 사용자가 원하는 수준의 프라이버시 보호를 제공하는 것은 데이터의 활용을 위해서도 중요한 목표이다.

이 목적을 달성하기 위하여 프라이버시 보호를 위한 많은 모델들과 기술들이 제안되어 왔다. 대표적인 프라이버시 보호 모델 중 하나는 k-익명화로 대표되는 익명화 기술이다. 익명화는 특정 필드의 값을 제거하거나 민감 정보를 지니는 데이터들을 일반화하여 같은 그룹으로 묶음으로써 외부 데이터와의 연결을 방지하고 공격자가 특정 개인을 추론하기 어렵게 만든다. 익명화 기술은 프라이버시 보호를 위해 유효한 기술이나 몇 가지 약점을 지니고 있는데, 첫 번째는 데이터의 과도한 일반화나 삭제를 야기함으로써 유용도를 심각하게 저하시킨다는 점이고, 두 번째는 익명화에도 불구하고 배경지식에 의한 공격에 의해 프라이버시가 노출될 수 있다는 점이다. 예를 들어 3-익명화를 보장하는 의료 데이터는 최소 3명의 사람이 같은 병력과 소득을 얻고 있는 형태로 데이터를 배포하게 된다. 만약 2명이 폐 관련 질병을 지니고 있고 3번째 사람은 간 관련 질병을 지니고 있다는 정보를 공격자가 알고 있다고 가정했을 때 한 명의 의료 정보가 추가로 입력되었을 때 데이터가 배포되지 않았다면 공격자는 4번째 사람이 폐 관련 질병을 앓고 있지 않다는 것을 알 수 있다. 이외에도 통계 데이터를 배포할 때도 공격자가 특정 개인이 유전자 연구에 참여했는지 여부를 두고 추론 공격을 수행한 사례도 있다 [1].

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No. 2018-0-00498, 차분 프라이버시 기반 비식별화 기술 개발)
* 서강대학교 컴퓨터공학과 데이터베이스 연구실 (azure84@naver.com)
** 서강대학교 컴퓨터공학과 데이터베이스 연구실 (spark@sogang.ac.kr)

이처럼 배경지식을 활용한 공격 등으로 인해 의도치 않은 정보가 공개되는 경우 등을 포함하여 데이터를 사용하여 추가적인 정보를 얻는 이상 프라이버시 노출의 위험은 필연적이다. 중요한 지점은, 통계적이고 정량적인 방법으로 사용자가 원하는 수준의 프라이버시 보호를 보장할 수 있는 프라이버시 보호 모델과 기술을 개발하는 것이다.

Ⅱ. 차분 프라이버시

2.1. 차분 프라이버시의 정의

1장에서 이야기한 공격과 방어는 추론에 필요한 보조 정보(auxiliary information)를 전제하고 있다. 이는 공격자가 사용할 정보들을 사전에 정해두고 보호 모델을 만든다는 의미이며, 이 전제가 깨질 경우 프라이버시가 침해될 수 있다. 그러나 공격자가 지닐 수 있는 보조 정보를 모두 가정하는 것은 불가능하므로 이는 프라이버시 침해의 여지가 늘 존재함을 의미한다. 차분 프라이버시는 이러한 보조 정보의 전제로부터 자유롭게 프라이버시 보호 모델을 설정 할 수 있다.

본래 차분 프라이버시는 1970년대와 80년대 암호학 개념에서 영감을 얻었다. 암호학의 개념 중 하나인 시맨틱 시큐리티 (semantic security)는 암호화된 데이터에 대한 접근 없이는 어떤 정보도 추가로 획득하지 못 함을 의미하는데, 이는 공격자가 지닌 데이터에 대한 지식이 질의 이전과 질의 이후에 차이가 없도록 한다는 뜻이다. 그러나 데이터베이스적 관점에서 이 목표는 불가능한 목표이다. 통계 정보를 통해 추가적인 정보를 습득했을 때 질의를 수행한 의미가 발생하기 때문이다. 따라서 프라이버시 보호 모델은 적절한 유용성을 제공하면서도 일정 수준의 프라이버시를 보장할 수 있어야 한다.

차분 프라이버시의 목표는 이 요구사항을 만족시키는데 있다. 즉, 특정 개인의 정보가 삽입되거나 삭제되더라도 질의 결과의 변화량을 일정 수준 이하로 제어하는 것이다. 특정 개인의 정보에 대해 삽입/삭제가 일어나는 경우를 비경계 (unbounded) 변화, 삽입/삭제 대신 특정 사용자의 정보가 변화하는 경우를 경계(bounded) 변화라고 한다. 만약 특정 개인의 정보 변화에 의해 질의 결과가 크게 변화한다면 공격자는 질의 결과의 차이를 보고 특정 사용자의 데이터의 존재 유무와 데이터의 값을 알 수 있게 된다. 반면 질의 결과에 큰 차이가 없다면 공격자의 추론 역시 어려워진다. 차분 프라이버시는 질의 결과의 변화량을 일정 수준 이하로 제한함으로써 프라이버시의 보장 수준과 데이터 유용성을 정량적으로 제어할 수 있다.

정의 1. 차분 프라이버시 (Differential privacy)

임의의 랜덤 함수 A에 대해 레코드 값이 하나만 차이 나는 이웃 데이터베이스 D1과 D2을 입력으로 하는 질의 결과가 $S \in range(A)$ 이고, 아래의 수식을 만족하면 ε-차분 프라이버시를 제공한다고 한다(이 때 ε은 양의 실수이다).

$$Pr[A(D_1) \in S] \leq e^{\varepsilon} \times Pr[A(D_2) \in S]$$

베이지안적 관점에서 차분 프라이버시는 관찰자가 결과값에 접근하여 특정 개인의 값을 추론할 확률이 특정 개인의 참여/불참과 상관없이 유사하며 이는 관찰자의 사전 지식과도 무관하다는 의미로 해석된다.

$$Pr[A(t|D_1)/Pr(t) \in S] \leq e^{\varepsilon} \times Pr[A(t|D_2)/Pr(t) \in S]$$

차분 프라이버시의 중요한 장점 중 하나는 보조 정보와 무관하게 프라이버시와 유용성을 고려한다는 것이다. 즉, 절대적으로 프라이버시만을 고려하는 방법이 아니기에 현실에 적용될 수 있다. 차분 프라이버시에서 프라이버시와 데이터 유용성 수준은 노이즈 삽입 수준에 의해 결정되며, 노이즈의 삽입 수준을 결정하는 것은 차분 프라이버시 패러미터 ε과 함수의 민감도이다.

정의 2. 전역 민감도 (global sensitivity)

차분 프라이버시에서 글로벌 민감도는 임의의 랜덤 함수 A에 대해 레코드 값이 하나만 차이 나는 이웃 데이터베이스 D1과 D2을 입력으로 하는 질의 결과의 차로 결정된다.

$$\Delta f = \max_{D1,D2} ||A(D_1 - A(D_2)||_1$$

수식에서 보이듯 함수의 전역 민감도는 특정 개인의 삽입/삭제에 따른 변화량의 최대값, 즉 최악의 경우를 가정하고 설정된다. 따라서 데이터의 경계가 분명치 않

거나 이상치(outlier)가 큰 경우에는 민감도를 설정하기 어렵거나 지나치게 큰 값이 설정되어 전체 성능을 저하시킬 수 있다. 이를 보완하기 위해 [2]에서는 국지적 민감도(local sensitivity)라는 개념을 제안하였다.

정의 3. 국지적 민감도 (local sensitivity)

차분 프라이버시에서 국지적 민감도는 임의의 랜덤 함수 A에 대해 레코드 값이 하나만 차이 나는 이웃 데이터베이스 D1과 D2을 입력으로 하는 질의 결과가 차로 결정된다. 이 때, 원본 데이터베이스 D1은 사전에 주어진다고 가정한다.

$$\Delta f = \max_{D1} ||A(D_1 - A(D_2)||_1$$

국지적 민감도는 전역 민감도에 비해 작은 경향을 보이는데, 이는 해당 도메인의 모든 가능한 데이터를 대상으로 하는 전역 민감도와 달리 현재 차분 프라이버시 적용 대상인 데이터베이스를 고려하기 때문이다. 이는 데이터에 대한 정보를 노출하는 면이 있으므로, [2]는 이를 극복하기 위해 β-스무딩(smoothing) 알고리즘을 제안하고, 유용성을 향상시킬 수 있는 샘플링 후 집계(sample and aggregate) 알고리즘을 제안하였다.

샘플링 후 집계 알고리즘은 샘플링과 집계 단계로 구성되는데, 샘플링 단계에서 데이터셋 D는 k개의 부분 집합으로 분할되고 각 부분 집합에 대해 함수 f(D)를 수행한다. 샘플링 과정에는 노이즈가 삽입되지 않는다. 이후 집계 단계에서 $f(D_i)$와 $f(D_i)$의 t번째 이웃간의 (t=k/2) 거리 를 나타내는 r(i)를 정한다. 프레임워크는 $g(f(D_i), \cdots, f(D_k))$중 가장 작은 r(i)를 지니는 결과값 $f(D_i)$를 지니는 함수 f를 정의한다. 그리고 β-스무딩이 적용된 노이즈를 함수의 결과에 적용한다. 하나의 샘플 변화는 하나의 부분 집합 D_i에만 영향을 미치므로 함수 g는 작은 국지적 민감도를 지니며 필요한 노이즈 역시 적은 값을 지니게 된다. 또한 각 부분 집합 D_i의 결과도 비교적 정확한 결과를 지니므로 함수 g의 정확도 역시 보증된다.

전역 민감도와 마찬가지로 차분 프라이버시의 정의 역시 너무 엄격하여 유용성을 심각하게 저하시킨다는 지적이 있다. (ε, δ)-차분 프라이버시는 ε - 차분 프라이버시를 보다 완화시켜 유용성을 향상시키고자 한다.

정의 4. (ε, δ)-차분 프라이버시 [2]

임의의 랜덤 함수 A에 대해 레코드 값이 하나만 차이 나는 이웃 데이터베이스 D1과 D2을 입력으로 하는 질의 결과가 S∈range(A) 이고, 아래의 수식을 만족하면 (ε, δ)-차분 프라이버시를 제공한다고 한다(이 때 ε, δ은 양의 실수이다).

$$\Pr[A(D_1) \in S] \le e^{\varepsilon} \times \Pr[A(D_2) \in S] + \delta$$

수식에서 나타난 것처럼 (ε, δ)-차분 프라이버시는 일정 수준(δ만큼의) 오차 허용도를 둠으로써 프라이버시 요구 수준을 완화시키고 유용성을 향상시킨다. (ε, δ)-차분 프라이버시에서 δ가 작을수록 차분 프라이버시의 신뢰도는 증가하고, ε 이 작을수록 더 엄밀한 프라이버시 보호를 나타낸다.

2.2. 차분 프라이버시 메커니즘

2.1 절에서 설명한 차분 프라이버시의 정의를 만족시키기 위한 여러 차분 프라이버시 메커니즘이 제안되었다. 차분 프라이버시 메커니즘 중 가장 기본적인 형태는 라플라스 메커니즘이 있다.

정의 5. 라플라스 메커니즘 (Laplace mechanism)

함수 f(D)를 데이터베이스 D를 사용하는 함수라고 가정할 때, ε - 차분 프라이버시를 만족하는 라플라스 매커니즘은 L(D)=f(D)+Z로 정의된다. 이 때 Z는 평균이 0이고 분산이 b인 라플라스 분포를 통해 결정된다. 라플라스 분포는 다음과 같다.

$$\Pr(z \mid \mu, b) = \frac{1}{2b} e^{-\frac{|x-\mu|}{b}}$$

분포의 분산은 $2b^2$이며 $b=\Delta f/\varepsilon$ 이다. |z|가 커질수록 비례하여 확률은 떨어지며 z의 밀도는 $e^{-\varepsilon|z|/\Delta f}$에 비례한다. 즉, 민감도가 클수록 그리고 ε이 작을수록 보다 큰 노이즈가 삽입될 확률이 증가한다.

라플라스 메커니즘은 실수 데이터를 대상으로 하는 함수에는 적합하나 범주적(categorical) 데이터를 대상으로 하는 함수에는 적용될 수 없다. [3]는 범주적 데이

터를 포함하여 차분 프라이버시를 적용하기 위해 익스퍼넨셜 메커니즘(exponential mechanism)을 제안하였다. 익스퍼넨셜 메커니즘은 입력값 D와 출력값의 범위 T를 설정하고, 입력값과 출력값을 인자로 갖는 스코어(score) 함수 u:(D×T)→R를 사용하여 각 출력값이 결정될 확률을 정한다. 출력값이 질의 목적에 부합할수록 더 높은 스코어를 지니며, 더 높은 스코어를 지닐수록 출력값으로 선택될 확률 역시 올라간다. 스코어 함수의 민감도는 다음과 같이 계산된다.

$$S(f)=\max\forall T,D1,D2|u:(D1\times T)-u:(D2\times T)|$$

스코어 함수를 기준으로 결과값이 선택될 확률은 다음과 같이 계산된다.

$$\Pr[\mathcal{T}(x)=y]=\frac{\exp\left(\frac{\varepsilon}{2S_M(f)}\cdot u(y,f(x))\right)}{\int_{y\in M}\exp\left(\frac{\varepsilon}{2S_M(f)}\cdot u(y,f(x))\right)}$$

익스퍼넨셜 메커니즘은 범용 메커니즘으로 라플라스 메커니즘 역시도 익스퍼넨셜 메커니즘의 형태로 제공할 수 있다. 다만 라플라스 메커니즘은 O(1) 시간 안에 결과값을 출력할 수 있으나 익스퍼넨셜 메커니즘은 O(n)시간이 소요된다. 이 외에도 가우시안 (Gaussian) 메커니즘과 지오메트릭(geometric) 메커니즘[4]이 존재한다. 지오메트릭(Geometric) 메커니즘은 라플라스 매커니즘의 이산 변형(discrete variant)으로써 여기서의 노이즈는 지오메트릭 분포 $\Pr[\Delta=\delta]=\frac{1-\alpha}{1+\alpha}\alpha^{|\delta|}$로 결정된다.

메커니즘 상의 차이 외에도 노이즈를 삽입하는 방식에도 차이가 존재한다. 입력값 교란(Input perturbation)은 가장 쉬운 방식으로, 데이터 자체에 노이즈를 삽입하는 것이다

$$x'=x+z$$

결과값 교란(output distribution)은 함수 f(d)의 결과값에 노이즈를 삽입하는 것으로 노이즈 삽입 수준은 데이터의 입력값에 의해 결정된다.

$$F(x)=f(x)+Z$$

목적 함수 교란(Objective perturbation) [5]은 노이즈를 목적 함수에 삽입하는 경우로, 주어진 알고리즘이 컨벡스 함수(convex fuction) j(g, d)를 수행할 때 노이즈를 삽입하는 것이다

$$F=\text{Arg }\min(j(u,D)+gtZ)$$

2.3. 구성 가능성(Composibility)

데이터베이스에 대한 질의가 거듭될수록 추가적인 정보 노출이 발생하므로 차분 프라이버시에서는 질의를 수행 할 수 있는 한계치를 정하고, 이를 프라이버시 예산(privacy budget)으로 관리한다. 예산은 데이터베이스 자체와는 상관없이 오직 질의의 수와 ε만으로 결정된다. 질의가 여러 번 수행되거나 데이터의 부분 집합에 대해 질의가 수행될 때 차분 프라이버시에서는 다음의 구성 가능성을 제공한다.

정리 1. 순차 구성(Sequential composition)
임의의 함수 A_i가 차분 프라이버시를 만족한다고 할 때, $A_i(D)$의 연속적인 질의에 대해 차분 프라이버시는 $(\sum_i\varepsilon_i)$-차분 프라이버시를 만족한다

정리 2. 병렬 구성(Parallel composition)
임의의 함수 A_i가 차분 프라이버시를 만족한다고 할 때 D_i는 입력값의 도메인 D의 임의의 서로소인 부분 집합들이라고 한다면, $A_i(D)$의 연속적인 질의의 차분 프라이버시는 $(\max(\varepsilon_i))$-차분 프라이버시를 만족한다.

위와 같은 구성 가능성을 제공함으로써 차분 프라이버시는 보다 복잡한 알고리즘을 구성하기 위한 질의 처리 시에도 적용될 수 있다.

2.4. 유틸리티 평가

대부분의 경우 데이터 제공자와 사용자 모두 일방적인 프라이버시 보호보다는 일정 수준의 프라이버시 보호와 데이터 유용성을 보장받길 원하므로, 차분 프라이버시 적용 시 데이터의 사이즈나 신뢰도 수준에 따른 노이즈의 확률 분포 수준을 증명해야 할 필요가 있다. 예를 들어 우리가 차분 프라이버시를 만족시키는 분류

기를 만든다면 우리는 해당 분류기의 정확도나 복잡도를 증명해야 한다. 이를 위해 다양한 형태의 평가 척도가 존재하는데, 가장 널리 쓰이는 방법은 (α, β)-usefulness 이다. 이 외에도 relative error, absolute error, kl-divergence, variance of the error, Euclidean distance 등이 사용된다.

2.5. 차분 프라이버시의 취약점

다른 엄격한 접근들과 마찬가지로 차분 프라이버시 접근 역시 몇 가지 필요한 전제가 있다. 차분 프라이버시의 경우 일정 크기 이상의 데이터베이스와 낮은 민감도를 지니는 데이터에 적용되었을 때 적절한 유용성을 보이며 이 조건이 만족되지 않았을 때는 과도한 노이즈 삽입으로 심각한 유용성 저하를 보인다. [6, 7]은 위에서 언급한 유용성 저하에 대한 우려를 제기하며 몇 가지 예를 제시한다. [8]는 크게 4가지로 차분 프라이버시의 한계를 지적하고 있는데, (1) 소규모 데이터에 대해 부정확한 결과를 제공하고, (2) 이상치가 존재하는 데이터는 노이즈가 지나치게 많이 삽입되어 쓸모없는 결과를 생산하며 (3) 사람들은 노이즈 데이터를 실제 데이터로 오인하고 결과를 사용 할 수 있으며 (4) 상관 관계 계산 시 유용성이 없는 데이터를 제공한다는 것이다. 이와 같은 지적에 대해 [9]는 다음과 같은 반론을 제기한다. (1) 소규모 인구에 대해 부정확한 답변을 제공하는 것이 차분 프라이버시의 목적이며 (2) 노이즈가 지나치게 삽입되는 것은 사실이나, 이를 위해 더 나은 통계적 수단을 사용하게 되고 (3) 사용자들에게 노이즈가 삽입된 데이터임을 의식하고 이에 적합한 통계적 수단을 사용하도록 교육해야 하며 (4) 상관 관계와 같은 복잡한 알고리즘에 대해서는 더 나은 차분 프라이버시 알고리즘이 존재할 수 있고, 이에 대한 연구가 앞으로 필요하다.

또다른 취약점은 [10]에서 보여준 부채널 공격(side-channel attack)에 대한 취약점이다. [10]은 타이밍 공격(timing attack), 상태 공격(state attack), 프라이버시 예산 공격(privacy budget attack)의 3가지 종류의 부채널 공격을 제시하고 있다. 즉, 특정 조건을 탐지했을 때 의도적으로 오랜 시간이 걸리는 질의 코드를 짜거나, 전역 변수를 두어 변화량을 본다거나, 예산의 소모량을 본다거나 하는 것이 그것이다. 차분 프라이버시 외의 요소를 통한 부채널 공격에 대한 대응으로는 퍼지 시스템을 사용하는 방법이 있는데, [11]은 부채널 공격 각각의 경우에 대한 대응을 제시하고 있다.

이 외에도 ε에 대해 정확한 기준이 없다는 점, ε이 의미하는 바가 맥락에 따라 크게 변화한다는 점 등이 차분 프라이버시가 현실에 적용되는 것을 방해하는 요소이다. 또한 예산 할당도 어려운 문제이다. 만약 잠재적인 사용자를 예측 가능하고 이를 통한 예산 할당도 가능하다고 하더라도, 사용자들이 질의에 어떻게 예산을 할당할 것인가의 문제도 남아있다. 또 다른 어려운 부분은 [12]에서 보인 바와 같이 각 데이터들이 독립적이지 않다는 것이다. 이 경우 차분 프라이버시는 각 데이터간의 연관성을 고려해야 하며, 이는 더 많은 노이즈를 삽입하는 결과로 이어지게 된다. 위에서 언급한 차분 프라이버시의 취약점에 대한 연구는 앞으로 보다 많은 연구를 필요로 한다.

Ⅲ. 차분 프라이버시의 적용

차분 프라이버시 적용은 데이터 보유자가 일정 수준의 노이즈를 삽입하여 배포하는 비상호적 (non-interactive) 방식과 데이터 보유자와 데이터 요청자가 질의를 통해 상호 작용하는 상호적 (interactive) 방식으로 나뉠 수 있다. 상호적 방식의 경우, 질의자들이 담합하여 차분 프라이버시에서 설정한 이상의 정확도를 지닌 데이터를 얻을 수 있으나, 비상호적 방식의 경우 이런 위험을 해결 할 수 있다.

3.1. 상호적 방식

상호적 방식은 사전에 정해진 프라이버시 예산 한도 내의 질의에 대해 노이즈가 삽입된 결과를 돌려주는 방식이다. [13]에 따르면 k개의 질의에 대해 ($O(\sqrt{k})$의 노이즈로 질의 결과를 제공할 수 있는 프라이빗 메커니즘(private mechanism)은 없는데, 그 이유는 공격자가 일정 수준의 오류 E 내의 결과를 제공하는 익명화 기법들은 최대 4E의 범위 내로 질의의 대상이 되는 데이터를 재구축 할 수 있기 때문이다. 이 공격은 O(nlog2n)개의 질의로 질의 결과들을 재조합하여 데이터베이스를 재구축할 수 있다. 예를 들어, 데이터 집합이 n=5,000개의 레코드로 이루어져 있고 모든 카운팅(counting) 질

의는 최대 50<n/100내의 오류를 제공한다면 최대 200개 이하의 오류를 지닌 데이터베이스 재구축이 가능하다. 이 경우 최대 오류는 200/5,000=4%에 불과하다. 이를 명백한 개인보호 실패 (blatant non-privacy)라고 부르며 이를 방지하기 위하여 상호적 방식의 차분 프라이버시 적용 시에는 프라이버시 예산을 설정해 질의의 수를 제한 할 필요가 있다. [14]는 기존 명백한 개인보호 실패 방식의 비효율적인 면을 예를 보이고, 푸리에 (fourier) 변환을 통한 보다 효율적인 공격을 보였다.

그러나 질의에 대해 사전에 정해진 예산이 정해져 있다는 제약은 데이터베이스 분석의 효율성을 저하시킨다. [15]는 이 문제를 해결하기 위한 메커니즘을 제안했다. 착안점은 사전에 정의된 '질의들의 집합(class of queries)'에 포함된 질의를 사용하여 예산을 절약하는 것이다. [15]의 문제는 이산 데이터가 아닌 경우에는 효율적이지 않다는 것과 오직 사전에 정의된 질의에 대해서만 사용 가능하다는 것이다. [16]의 저자들은 질의를 어려운 (hard) 질의와 쉬운 (easy) 질의로 분류하고 쉬운 질의는 이전에 질의가 이루어졌던 결과를 재활용하여 예산을 절약하고, 어려운 질의에 대해서만 노이즈를 삽입한다. 여기서의 주된 이슈는 어떻게 질의들을 '쉬운' 질의와 '어려운' 질의로 분류하는지에 대한 문제이다. [17]은 이 문제를 프라이빗 멀티플리케이티브 가중치 (private multiplicative weight)라는 메커니즘을 사용하여 해결하였다. [17]에서 메커니즘은 각 라운드 t마다 질의를 사용하여 데이터베이스를 업데이트하고, 그 결과를 이전의 라운드와 비교한다. 결과는 지연 (lazy)이나 갱신 (update)으로 결정되는데, 지연인 경우 이전의 질의 결과를 사용하고 갱신의 경우 업데이트를 수행한다.

상호적 방식의 도전 과제는 다음과 같다. (1) 랜덤 쿼리에 대한 응답 (2) 일정 수준의 유용성을 보장하는 대량의 질의 지원 (3) 효율성 (4) ε-차분 프라이버시의 만족 (5) 질의 다변에 대한 적응성이다. 지금까지 제안된 각 연구들은 이 요구사항들을 부분적으로만 만족시킨다. 또한 적정 수준의 ε과 프라이버시 예산 설정 문제는 여전히 많은 연구가 필요하다.

3.2. 비상호적 방식

차분 프라이버시에서 비상호적 방식은 실제 데이터를 모사한 생성 데이터를 배포하거나 실제 데이터에 노이즈를 삽입하여 교란한 데이터를 배포함으로써 달성된다.

3.2.1. 히스토그램(histogram) 생성

히스토그램 생성은 비상호적 방식으로 데이터를 배포할 때의 가장 기본적인 방법이다. 그러나 히스토그램을 통한 질의는 노이즈의 총 생성량이 속성의 조합에 비례하여 증가하므로 전체 레코드의 수가 속성의 조합의 수에 비해 작을 때 질의의 유용성이 크게 저하된다. 만약 각 각 속성의 조합이 아닌, 경계(marginal) 마다 노이즈를 삽입할 경우, 적정한 수준의 노이즈를 삽입할 수 있으나 이 경우 경계간의 비일관성이 발생하는 문제가 있다. [18]은 이를 해결하기 위해 모든 low order 경계에 대해 푸리에 변환을 적용해 적은 오류를 발생시키는 기법을 제안한다. [19]는 익스퍼넨셜 메커니즘 기반의 샘플링에 기반한 푸리에 변환을 사용한 노이즈 삽입을 개선하였다. [20]은 히스토그램의 일관성 제약에 대해 지적하고 이를 해결하여 전체 히스토그램의 정확도를 올리기 위한 후처리 (post-processing)를 고려하였다.

히스토그램 생성을 위한 또 다른 방법은 선형 조합을 사용하는 것이다. 만약 4개의 셀이 있고 노이즈의 분산을 V라고 할 때 각각의 셀의 값에 차분 프라이버시를 적용한다면 합계의 분산은 4V이다. 그러나 합산된 결과에 노이즈를 섞는다면 분산은 V이다. 서로 겹쳐진 영역의 경우, 3개의 셀에 노이즈를 섞는 것보다 하나의 총합에 노이즈를 섞은 뒤 합계에 속하지 않은 한 셀의 노이즈만큼을 빼는 쪽이 더 적은 분산으로 합계를 구할 수 있다. 즉, 서로 다른 노이즈 카운팅 질의의 선형 조합으로 에러를 최소화 할 수 있다. [21]에서 선형 조합은 매트릭스의 계수(coefficient)로 저장되고, 매트릭스 메커니즘으로 계산된다. 제안하는 기법에서는 질의들의 워크로드 W를 일종의 질의 프록시로 사용함으로써 데이터베이스에 대한 접근 없이 질의에 대한 전략을 짤 수 있었다. 이는 모든 타입에 대한 질의에 대해 유용성을 최대화 할 수는 없지만, 질의 전략에 해당하는 질의들은 유용성은 최적화 할 수 있다. 그러나 최적의 전략을 계산하는데 소요되는 계산 비용은 존재하며, 이 경우 복잡도는 $O(n^8)$이다. 이는 비효율적이므로 [22]는 프라이버시 버짓 ε을 각 질의마다 배정하고, 특이값 분해

(singular value decomposition)를 사용하여 탐색 공간을 감소시킴으로써 계산 비용을 $O(n^4)$로 줄이는 효율적인 구현을 제안하였다.

3.2.2. 파티셔닝(Partitioning)

파티셔닝의 경우, 히스토그램과 마찬가지로 전체 영역을 하위 영역으로 분할하여 노이즈를 삽입한다. 다만 각 셀의 크기가 고정되어 있지 않으므로 최적의 세부 분할(subdivision)을 찾는 것이 파티셔닝을 통한 노이즈 삽입에서 중요한 문제이다. 일반적으로 트리 기반의 파티셔닝이 차분 프라이버시 적용에 유용하다고 알려져 있다. 트리 기반의 파티셔닝의 경우, 영역은 서로 겹칠 수도 있으며, 하위 레벨로 내려갈수록 더 정확한 값이 노출되므로 더 많은 양의 노이즈를 삽입해야 한다. [23]에서 제안된 것처럼 질의를 포함하는 영역이 일부만 걸친 경우는 해당 영역의 비례로 계산된다. [24]은 범위(range) 질의를 위한 공간 데이터 인덱싱(spatial data indexing)을 위해 차분 프라이버시를 적용한다. 여기서는 데이터 의존적(data-dependent)인 경우와 데이터 독립적(data-independent)인 경우의 두 가지의 경우로 나뉘어 각각의 경우에 적합한 트리 구조를 사용하였다. [25]은 DP-tree를 제안하였다. 이는 적응적인(adaptive) 프라이버시 예산 할당과 일관성 강제(consistency enforcement)를 제공하는 트리 구조이다. 이 작업은 [24]에 비해 질의 정확도를 향상시켰다.

Ⅳ. 다양한 형태의 차분 프라이버시 응용

4장에서는 데이터 마이닝 및 기계학습, 경로(trajectory) 데이터를 비롯한 위치 데이터, SNS에서 사용되는 그래프 형태의 데이터 등 다양한 형태의 데이터에 차분 프라이버시를 적용한 연구에 대해 살펴본다.

4.1. 데이터 마이닝과 기계 학습

4.1.1. 선형 회귀

선형 회귀는 T를 예측하기 위해 wTx값을 모델링하는 기법이다. W는 트레이닝 과정동안 최적화되는 웨이트로써 각 피쳐들과 대응하며 square loss를 최소화하는 값으로 계산된다. [26]은 바운디드 샘플 스페이스와 차분 프라이버시 메커니즘을 제안한다. 메커니즘은 타일러 급수를 사용하고 low-order 근사를 통해 근사치를 찾고 각 텀들의 계수에 노이즈를 더한다. 계수의 민감도는 계산하기 쉽고 원본 데이터에 비해 적은 값을 지니므로 적은 양의 노이즈로 차분 프라이버시를 보장할 수 있다.

4.1.2. 빈발 아이템 집합 마이닝(frquent itemset mining)

최소 지지도 이상을 갖는 아이템들의 집합을 빈발 아이템 집합이라 하며, 빈발 아이템 집합을 사용하여 연관관계를 찾거나 k개의 최다 빈발 아이템 집합을 찾는 것을 빈발 아이템 집합 마이닝이라 한다. [27]은 순차 패턴 마이닝에서 아이템 집합의 prefix 정보를 유지하면서 상위 k개의 부분 아이템 집합을 찾는 기법에 차분 프라이버시를 적용하였다. 제안 기법은 prefix tree를 사용하는 기존의 차분 프라이버시 기법이 ε을 균등하게 분배했던 것과 달리 마르코프 모델을 생성한 뒤 생성된 마르코프 모델에 기반하여 ε을 분배하며 prefix tree를 생성하고 노이즈를 삽입한다. [28]는 빈발 아이템 집합 마이닝의 유용성을 감소시키지 않으면서 차분 프라이버시를 만족하는 알고리즘을 제안하였는데, 각 트랜잭션(tranjaction)의 크기가 특정 임계값보다 작아질 때까지 아이템들을 제거하는 과정에 차분 프라이버시를 적용하여 노이즈를 삽입하였다.

4.1.3. 의사 결정 트리(Decision tree learning)

의사 결정 트리는 샘플 스페이스를 파티셔닝한 후, 각 파티션에 라벨을 할당한다. 의사 결정 트리 분류기는 트리 생성과 프루닝 단계로 나뉜다. 모든 데이터들이 루트로 들어가고, 반복적으로 파티션을 나누면서 지니 인덱스(Gini index)나 인포메이션 게인(information gain) 등의 평가 척도에 따라 분할과 종료 조건을 결정한다. 파티셔닝 프로세스가 종료되면 모든 파티션들은 일정 숫자를 충족할 때까지 불필요한 파티션을 삭제하거나 통합하는 절차를 거친다. [29]은 차분 의사 결정 트리 메커니즘을 제안했다. [29]에서는 N 의사 결정 트리를 만들고 이를 앙상블 시켜 분류기를 만든다. [30]는 또다른 방식을 제안한다. 모든 피쳐들은 범주적 데이터라 가

정하고, 파티션 단계에서 익스퍼넨셜 메커니즘을 사용하여 하위 노드를 선택한다. 매 라운드마다 파티션은 사전에 정한 단계까지 도달하거나 충분한 샘플 개수만큼을 생성할 때까지 파티션을 반복하여 트리를 구성한다.

4.1.4. 클러스터링(Clustring)

클러스터링은 대표적인 비감독 학습이다. 즉, 데이터 집합의 특징을 찾는 알고리즘으로 높은 수준의 정보를 그대로 배포하는 것은 정보 노출을 가져오므로 차분 프라이버시 적용이 필요하다.

[1]은 k-means 클러스터링 알고리즘에 샘플링 후 집계 메커니즘을 적용하였다. 이 메커니즘은 'well-seperated'를 전제하는데, 이는 적은 수의 샘플로도 클러스터가 잘 평가됨을 의미한다. 이는 샘플링 후 집계 메커니즘의 기본요구사항이다. 제안 메커니즘은 랜덤하게 많은 서브셋으로 학습 데이터를 분할한다. 그리고 smooth sensitivity 프레임워크를 사용해서 각 dense region의 차분 프라이버시가 적용된 결과를 만들어낸다.

4.1.5. Robust statistics estimator

[31]에서는 robust statistical estimator를 제안하였다. Robust estimator는 적은 수의 샘플이 변경된다면 변하지 않는 특성을 지닌다. [32]는 이에 기반하여 프로포즈-테스트-릴리즈 프레임워크(propose-test-release framework)를 제안하였다. 이 프레임워크는 전체 공간을 작은 큐브로 분할한 후, 각 데이터 집합의 통계를 계산한다. 만약 숫자가 크면 통계는 안정적이고 여기에 라플라스 노이즈를 삽입해 데이터를 보호한다. 만약 숫자가 적으면 메커니즘은 실패한다. 만약 샘플의 숫자가 무한하다면 프레임워크는 데이터 보호를 적용하지 않은 모델과 점진적으로 동일하다.

[33]은 M-estimator를 위한 차분 프라이버시 메커니즘을 제안한다. Robust estimator와는 달리 m-estimator의 정의는 해당 estimater가 함수에 의존적이다. [33]은 먼저 샘플 스페이스를 노이즈를 적용하지 않고 다수의 작은 큐브로 분할한다. 이후 라플라스 노이즈를 큐브의 샘플들의 카운트에 더한다. 그리고 밀도 함수를 각 큐브마다 구한다. 노이즈가 삽입된 밀도 함수는 노이즈가 삽입된 타겟 함수를 이끌어내고 최종적으로 노이즈가 삽입된 최소값 Θ를 구할 수 있다.

4.2. 위치 패턴 마이닝

4.2.1. 위치 데이터

차분 프라이버시의 다양한 적용 분야 중 하나는 위치 패턴 마이닝이다. 위치 패턴 마이닝 에서 가장 큰 문제는 데이터 집합에 포함된 사용자의 위치가 마이닝의 결과로 노출되는 것이다. 집의 위치는 어디인가? 늦은밤 사용자가 집에 방문했는가? 사용자가 특정 시간 t에 집에 방문했는가? 사용자가 집 근처에 방문했는가? 등의 질의가 그 예이다. 차분 프라이버시가 적용된 공간 데이터 보호 기법은 주로 셀 단위의 위치들에 대한 사용자의 수(count) 값을 보호하는 기법인데, 이 연구들에서의 유용성(utility)은 범위에 대한 카운트 질의(range count query) Q에 대해, 질의 영역에 포함되는 각 셀들에 있는 사용자의 수를 합한 값과 노이즈와의 차이로 평가된다.

[34]의 연구는 사용자들로부터 수집된 위치 정보를 이용해서 특정 위치에 머물렀던 사용자들의 수를 구할 때의 노이즈 삽입 문제를 다룬다. 저자들은 모든 관심위치를 전부 고려할 때 민감도가 지나치게 커지는 문제가 있기에 기존의 차분 프라이버시 메커니즘은 위치 데이터에 적용하기 적합하지 않다고 주장한다. 이 문제를 해결하기 위하여 저자들은 전체 데이터를 차분 프라이버시가 적용된 국지적 쿼드트리를 사용하여 보다 작은 국지적 문제들로 분할하여 같은 차분 프라이버시 레벨에 대해 더 나은 정확도를 제공하도록 한다.

[24]의 연구는 공간 데이터에 대한 트리 구조 기반 인덱싱 구성에 차분 프라이버시를 적용하였다. 저자들은 데이터 반영 여부에 따라 쿼드트리와 kd-트리(또는 힐버트 R-트리)의 2가지 트리 구조를 사용하였다. 쿼드트리의 경우 데이터 분포와 무관하게 전체 영역을 4분할 하고 각 노드의 카운트 값에 노이즈를 삽입하고, 노이즈가 삽입된 카운트 값이 특정 임계값보다 큰 값을 가지면 해당 노드를 재귀적으로 4분할한다. kd-트리나 힐버트 R-트리는 데이터 분포를 고려하여 분할을 수행하므로 데이터 분포 자체도 보호 대상이 된다.

[35]의 연구는 앞선 연구들과는 달리 그리드 셀에 기반한 인덱싱을 수행하였다. 그리드 셀에 차분 프라이버시가 적용되기 어려웠던 이유로는 균등한 그리드 크기

를 정하기 어렵기 때문이었다. [35]에서는 uniform grid method(UG)와 adaptive grid approach(AG)를 제안하였다. UG 기법에서는 각 셀이 동일한 크기를 지니지만, AG 기법에서는 각 셀의 크기가 데이터 분포에 따라 다르다. UG 기법에서는 전체 오류를 가장 작아지도록 하는 셀의 크기를 구하며, AG 기법에서는 데이터가 밀집한 지역에는 작은 크기를 갖는 셀을, 희소한 지역에 대해서는 큰 크기를 갖는 셀을 할당한다. 각 셀에 대한 민감도는 1이며, 전체 그리드 셀들에 대해서도 민감도가 1이 된다. 따라서, 트리 구조보다 민감도가 낮아지는 효과를 얻을 수 있으며 높은 유용성을 보장한다.

[36]의 연구는 새로운 방식의 위치 분할 방법을 제안하였다. 트리 구조의 민감도는 트리의 높이 h이고, 이는 그리드 셀보다 많은 노이즈가 삽입되는 단점이 있다. [36]은 트리의 민감도를 임계값 이하로 낮추어 유용성을 향상시켰다. 저자들은 쿼드트리에서 한 노드 카운트 값이 특정 임계값 보다 큰 경우 해당 노드를 분할 할 때 노드 카운트 값이 임계값보다 매우 큰 경우, 두 이웃 데이터베이스가 같은 트리를 만들 확률의 비가 지수적으로 감소하게 된다는 점을 발견하였다. 이에 착안하여 각 노드 카운트 값에 바이어스 값을 더해 임계값보다 항상 큰 값으로 변환하고, 이 바이어스된 카운트 값에 노이즈를 더해 트리를 구성함으로써 민감도를 낮추는데 성공하였다.

4.2.2. 경로 데이터(trajectory data)

경로 데이터에 차분 프라이버시를 적용하는 연구는 경로의 합성 데이터 생성과 연속적으로 데이터를 배포하는 연구로 분류된다. [38]은 약한 형태의 차분 프라이버시를 만족시키기 위해 샘플링과 보간법 전략(sampling and interpolation strategies)을 개발하였다. 그러나 위 연구들은 실제 경로에 대해서는 효율적인 노이즈 삽입이 안된다는 단점이 있다. [39]의 연구는 실제 경로 데이터 에 대해 차분 프라이버시를 적용할 때, 마르코프 모델에서 이동 객체의 속도를 반영하기 어려워 전이 확률(transition probability)을 제대로 구하기 어렵다는 점을 극복하기 위해, 계층적 참조 시스템(hierarchical reference system, HRS)를 이용한다. 1개의 reference는 1개의 prefix tree를 나타내고, 각 reference의 prefix tree는 다른 크기의 셀을 갖는다. 크기가 큰 셀을 지닌 reference가 더 빠른 속도로 표시된 이동 경로를 표현하므로 한 원본 경로는 여러 개의 reference system들의 조합으로 표현이 가능하다. [39]에서 차분 프라이버시는 각 prefix tree의 노드 카운트 값에 적용된다. 각 노드의 민감도는 1이고, 이웃 데이터베이스 는 한 경로만 다르므로 전체 민감도는 경로의 길이가 된다.

실시간으로 데이터를 배포해야하는 스트림 환경에서의 경로 보호 기법은 경로 데이터의 합성과는 다른 프라이버시 보호 목표를 갖는다. 우선, 경로 데이터 합성에서는 경로 전체의 보호를 목표로 한다. 이는 배포하는 원본 경로의 크기가 미리 정해져 있으므로 가능하다. 한편, 스트림 환경에서는 시간이 지날수록 경로의 길이가 무한대가 되므로 모든 타임 스탬프 마다 차분 프라이버시를 적용하기 어렵다. Dwork은 [40]에서 연속적으로 배포하는 데이터에 대해 보호하고자 하는 대상을 2가지 관점으로 정의했다. (1) 이벤트 레벨의 보호(Event-level privacy): 각 타임 스탬프에서의 차분 프라이버시 만족 (2) 사용자 레벨의 보호(User-level privacy): 전체 타임 스탬프 에 대한 차분 프라이버시 만족이 그것이다. 사용자 레벨의 보호를 보장하는 메커니즘이 가장 이상적이라고 할 수 있으나 이는 어려운 일이다. [41]의 연구에서 밝혀낸 바와 같이 4개의 위치 정보만을 가지고 약 95% 정도의 정확도로 백오십만 명의 사람들을 식별하는 것이 가능하므로 경로는 유일하게 구분되는 특성을 갖고, 프라이버시를 보호하는 것 역시 어렵다. [42]는 위와 같은 사용자 레벨의 보호가 달성하기 어려운 점을 극복하기 위해 이벤트 레벨의 보호와 사용자 레벨의 보호의 중간 단계인 W-event privacy를 정의하였다. 이 정의는 스트림 환경에서 임의의 W개의 타임 스탬프를 포함하는 윈도우 내에서는 차분 프라이버시가 보장되어야 함을 의미한다. 타임스탬프마다 εi만큼의 프라이버시 예산이 할당되어 있다면, 이벤트 레벨의 보호는 각 타임스탬프마다 εi -차분 프라이버시를 만족하며, W-event level privacy에서는 W개의 연속적인 타임 스탬프에 대해 WεI -차분 프라이버시를 보장한다. [43]은 W-privacy 기법의 문제점을 지적하였다. 첫째는 한 사용자의 이동 경로가 체류 시간을 고려할 때 윈도우 내에서 희소하다는 점이고 둘째는 고정된 윈도우의 크기 W가 개인화된 프라이버시를 보호하지 못한다는 점이다. 저자들은 l-trajectory privacy를 제안

하였는데, 이는 한 사용자의 방문 장소 1개를 포함하는 타임스탬프 구간 내의 카운트 값은 ε-차분 프라이버시를 만족한다는 것이다. 한편, 기존의 스트림 환경에서의 경로 보호를 위한 차분 프라이버시 기법들은 로드 네트워크라는 특수한 환경에 대한 시간적 연관성을 고려하지 않았다. [44]의 연구는 이러한 문제점을 지적하였다. 이 논문의 저자들은 데이터에 의존적인 상황에서 배포자가 ε-차분 프라이버시를 만족시켰다고 예상했던 데이터가 실제로는 더 큰 프라이버시 노출을 발생시킬 수 있으며, 공격자는 로드 네트워크의 시간적 연관성을 이용해서 이를 악용할 수 있음을 보였다.

4.3. 소셜 네트워크 그래프 데이터

페이스북, 트위터 등의 온라인 소셜 네트워크가 인기를 얻으면서 소셜 네트워크 그래프 데이터를 활용한 데이터 분석 역시 중요하게 평가되고 있다. 소셜 네트워크 데이터는 사용자간의 관계를 파악하여 마케팅 캠페인에서 얼마나 상품 정보가 빠르게 퍼져나가는지, 또는 유행병의 전파가 어떻게 이루어졌는지를 파악하는데 사용될 수 있다. 그러나 이 정보들은 개인과 밀접한 관련을 맺고 있기에 차분 프라이버시를 적용한다. 소셜 네트워크 그래프 데이터에서의 프라이버시는 크게 간선 프라이버시와 노드 프라이버시가 존재하는데 간선 프라이버시는 하나의 간선의 삽입/삭제에 의한 변화의 차이를 대상으로 하며, 노드 프라이버시는 하나의 노드의 삽입/삭제에 의한 변화를 보호하는데 목표를 두고 있다. 이에 더하여 방향성 그래프에서 임의의 아웃 링크(out link)를 더하거나 뺀 그래프와의 차이를 공격자가 파악 하지 못하도록 하는 경우에는 아웃링크 차분 프라이버시를 만족한다고 한다. 아웃 링크 프라이버시는 노드 프라이버시보다 약하지만 k-간선 프라이버시와 유사하게 k-아웃 링크 프라이버시를 제공한다. [45]에서는 triangle counting, degree distribution과 centrality에 대해 out-link privacy의 민감도를 정의하고 노드/간선 프라이버시와 비교하였다. Triangle counting의 경우 민감도는 1이다. 아웃 링크를 제거하거나 추가하여도 영향을 받는 노드는 오직 1개이기 때문이다. Degree distribution의 경우도 하나의 값에만 영향을 끼치기 때문에 민감도는 1이므로 간선 프라이버시보다 적은 노이즈가 삽입된다. Centrality의 경우 중요한 사용자를 찾을 때 사용하는 합성 네트워크인 popularity graph를 정의하고 이를 생성하는 알고리즘을 제안하였다. 노드 프라이버시와 간선 프라이버시에서 각각의 경우의 민감도는 아래의 표 1과 같다.

〔표 1〕 노드 프라이버시와 간선 프라이버시의 민감도

	Node Privacy	Edge Privacy
# of edges	x	1
# of triangles	nC2	n-2
Degree distribution	2x+1	4
# of distance	x	X
Max cuts	x	1
Max degree	x	1

그래프 노드의 개수: n, 특정 노드의 최대 degree 값: x

[46]에서는 처음으로 frequent 그래프 패턴 마이닝 알고리즘에 차분 프라이버시를 적용시켰다. [46]의 연구에서는 Partial Order Full 그래프를 정의하였는데 이 그래프에서는 그래프 패턴을 노드 프라이버시로 정의하고 Sub-neighbor, Super-backward neighbor, Super-forward neighbor의 3가지 neighborhood를 간선 프라이버시로 정의하였다. POF 그래프에는 output space에서 MH-based random walk를 용이하게 하기 위해 마르코프 체인의 상태 공간(state space)을 사용하였다.

그래프 데이터에 대한 질의에는 언급한 간선과 노드 프라이버시 외에도 서브그래프에 대한 질의도 존재한다. 주로 사용되는 서브 그래프패턴들은 triangles, k-triangles 그리고 k-stars가 있다. [47]에서는 adversarial privacy를 정의하였는데 Adversarial privacy란 공격자의 사전지식을 제한하여 weaker adversary로부터 차분 프라이버시를 보장하도록 하는 것이다. 또한 낮은 국지적 민감도를 가지는 stable한 조인 질의를 정의하여 동일한 프라이버시를 보장하면서 적은 노이즈를 추가하는 방법을 제안하였다. 하지만 공격자의 사전지식에 대한 가정으로 인해 차분 프라이버시의 정의를 훼손하고 정확도를 저하시키는 부분이 존재한다.

Ⅴ. No free lunch in data privacy

차분 프라이버의 기본 전제 중 하나는 데이터 집합이 서로 독립적인 레코드들로 구성되었다는 것이다. 그러나 실제 세계에서의 데이터들은 서로 연관성을 지니는 경우가 빈번하며, 이러한 경우에 대해 고전적인 차분 프라이버시의 전제를 적용하는 것은 기대한 수준의 정보 유용성과 프라이버시 보호를 제공할 수 없다. [12]는 차분 프라이버시 적용 시 데이터 생성에 대한 지식 없이도 적정 수준의 노이즈를 삽입할 수 있다는 차분 프라이버시의 전제의 취약성을 보이고 적정 수준의 유용성을 보장하기 위해서는 노이즈 삽입 시 데이터 생성 알고리즘을 고려해야 함을 보였다. 예를 들어 공격자가 특정 사용자 A의 건강상태를 파악하는 상황을 가정하자. 공격자는 소셜 네트워크 등을 통해 사용자 A의 주변관계를 이미 파악했고, 사용자 A는 다른 9명의 가족들과 한 집에서 생활한다는 정보도 확보했다. 위와 같은 상황에 대하여 고전적인 차분 프라이버시는 Lap(1／ε) 만큼의 노이즈를 질의(e.g. 얼마나 많은 사람들이 독감에 걸렸는가?)의 결과에 섞어 노이즈가 삽입된 결과를 생성한다. 만약 공격자가 사용자 A의 관계를 파악할 수 없다면(independent data), 차분 프라이버시를 충족시켰다 할 수 있다. 그러나 가정처럼 위의 10명이 모두 한 집에 살고 있는 가족관계(strong correlation)라면, 질의 결과의 변화량은 0 혹은 10일 가능성이 매우 높을 것이다. 즉 관계를 맺고 있는 사람들 중 한 사람의 건강 변화는 나머지 9명의 건강에 대한 변화를 유발하며 (correlated/dependent) 이는 질의의 민감도에 큰 영향을 미쳐 공격자가 특정인을 추론할 수 있는 가능성을 높인다. 이러한 환경에서 10명이 서로 독립적인 경우와 동일한 수준의 프라이버시를 보장하려면 Lap(1／ε) 이상의 노이즈를 질의 결과에 삽입해야 하지만, 이 때 얼마만큼의 노이즈를 삽입해야 하는지 결정하는 것은 매우 어려운 일이다. 너무 많은 노이즈의 삽입은 노이즈가 데이터의 유용성을 크게 저하시키는 문제점이 발생하며, 너무 적은 노이즈 삽입은 적절한 수준의 데이터 보호를 이룰 수 없기 때문이다. 이처럼 기존의 차분 프라이버시의 전제로는 적절한 수준의 프라이버시 요구사항을 충족시킬 수 없는, 데이터의 의존성을 고려한 경우에 대한 연구들이 진행되고 있다. 이 연구는 크게 다음의 2가지로 분류할 수 있다.

(1) pufferfish와 그 변형 (2) 그 외의 데이터간 연관성을 고려한 연구

5.1. Pufferfish와 그 변형

[48]은 데이터간의 관계성 문제를 해당 분야의 도메인 전문가를 통해 해결하고자 했다. 이를 위해 Puffer fish라는 프레임워크를 제안하고 도메인 전문가가 추가적인 데이터간의 관계를 입력하면 이를 바탕으로 해당 데이터에 대해 조정된 프라이버시 정의를 생성해주는 방식이다. 이와 같이 연관된 데이터를 고려할 때 베이지안 네트워크를 사용하는데, x와 r이 random variable이고 x가 민감 데이터, r이 질의에 대한 데이터베이스의 결과라 할 때, 오직 Pr (x|r)≡Pr (x)인 경우에만 주어진 결과 r에 대해 민감 데이터 x가 완전히 보호되었다고 말할 수 있다. 그러나 데이터 분포를 임의로 결정할 수가 없기 때문에 완전히 보호된 (x, r)의 쌍이 존재할 수 없으므로 연관된 데이터의 경우 차분 프라이버시에서 요구하는 수준의 데이터 프라이버시를 보장하는 대신 그보다 적은 수준의 데이터 프라이버시만 보장함으로써 데이터의 유용성을 향상시키는 방향의 연구들이 수행되었다.

[49]은 puffer fish의 변형으로, 추가적인 necessary secret과 제약을 특정하고 이를 기반으로 정책을 만들어 노이즈 삽입에 적용한다. [49]의 연구는 Pufferfish와 비슷한 프라이버시 성능을 보이면서도 더욱 좋은 유용성을 보이는 기법이다. [50, 51] 역시 pufferfish의 변형으로 각 튜플의 속성을 베이지안 네트워크의 형태로 만들어 유용성을 향상시킨 연구이다. 그러나 위의 pufferfish의 변형에 대한 연구들은 pufferfish의 일반적인 교란 메커니즘을 제안한 것이 아니라 특정 케이스에 대한 적용에 그치고 있다.

5.2. 그 외의 데이터간 연관성을 고려한 질의

데이터의 연관성을 고려한 연구는 pufferfish의 방식을 따르지 않고 데이터 집합 내의 분포 등을 분석하여 추론하고, 해당하는 수준만큼의 노이즈를 삽입한다. 이는 질의자의 질의 집합이 주어졌을 때, 해당 질의의 결과에 영향을 미치는 레코드만큼 추가적으로 노이즈를 삽입하는 방식이다.

[52]의 연구는 No free lunch in data privacy에서 제

시한 문제점을 pufferfish에 기반하지 않고 해결하고자 한 연구이다. 주어진 질의에 대하여, 특정 레코드 가 빠졌을 때 영향을 받는 레코드들의 수를 연관된 민감도(correlated sensitivity)라 하고 이중 가장 큰 값을 글로벌 민감도로 하여 노이즈 삽입에 적용하였다. 이 방법은 필요한 수준보다 훨씬 더 많은 양의 노이즈를 생성하기 때문에 좋은 데이터 유용성을 보이지 못한다는 단점이 있지만, Pufferfish와는 다르게 어떠한 경우에 대해서도 차분 프라이버시의 요구사항을 충족시키기 때문에, 이후 연관된 데이터 분석을 통한 노이즈 삽입 연구의 기준선으로 사용되고 있다.

[53]의 저자들은 Gowalla 데이터 집합을 관찰하여, 친한 친구일수록 위치 패턴 이 비슷하다는 결과를 얻었으며 이를 토대로 공격자가 높은 확률로 사용자의 위치를 특정화할 수 있다는 것을 보였다. 예를 들어 기존의 독립된 레코드들을 전제 할 때는 특정 사용자 i가 특정 그리드에 존재할 사전확률을 단순히 현재 분포된 전체 사용자의 수를 두고 판단할 수 밖에 없지만, 공격자가 데이터 집합이 서로 의존적이라는 것을 알고 있고, 사용자 i의 친구 관계를 사전에 알고 있다면, 공격자는 가중치 값을 정하여 특정 그리드에 사용자 i가 존재할 확률이 가장 높다는 것을 파악할 수 있게 된다. 이를 방지하기 위해 [53]은 데이터간의 상관 관계를 단순히 상관계수를 통해 정의한 것이 아니라, 확률적인 형태로 모델링하여 엄격한 프라이버시를 보장하는 기법을 제안하였다. 그러나 제안 기법은 논문에서 제시한 추론 공격을 방지할 수 있다는 것을 보였으나, 데이터 사이의 관계에 따른 확률적인 모델링에 따라 그 성능의 편차가 크며 공격자가 해당 모델이 아닌 다른 모델을 사용하게 될 경우 엄격한 차분 프라이버시 요구사항을 만족시킬 수 없다는 단점이 존재한다.

Ⅵ. 차분 프라이버시 응용 사례

지금까지 차분 프라이버시를 현실 세계의 문제 해결에 적용하기 위한 몇 가지 응용들이 제안되었다. PINQ [54]는 다양한 애플리케이션들을 위한 빌딩 블록으로 마이크로 소프트의 LINQ에 차분 프라이버시를 적용시켰다. Airavat [55]는 대용량 데이터의 분산 처리 프레임워크인 하둡에서의 맵리듀스 과정에서 맵퍼와 리듀서 간의 데이터 교환으로 발생할 수 있는 정보 노출을 방지하기 위하여 강제적 접근제어와 차분 프라이버시를 결합시켰다. GUPT[11]는 샘플링 후 집계 메커니즘을 적용하여 더 나은 정확도를 제공하는 차분 프라이버시 프레임워크이다. [56]은 미국 인구 통계청에서 사용하는 지리 데이터에 대해 차분 프라이버시를 적용하였고 [57]은 벨기에의 리테일 스토어의 익명화된 집합 형태의 값을 지니는 데이터-와 mushroom 데이터 집합, AOL 검색 로그 등에 차분 프라이버시를 적용하였다. [58]은 데이터의 특성에 따라 차분 프라이버시 알고리즘간의 오류가 크게 달라진다는 점에 착안해 데이터의 특성에 따라 최적의 알고리즘을 선택할 수 있는 기법을 제안하였다. 데이터의 특성과 특성에 맞는 알고리즘간의 연결은 공개된 정보를 사용하므로 추가적인 프라이버시 예산의 손실이 없다.

Ⅶ. 앞으로의 연구 주제

7.1. 지역 모델(Local model)

차분 프라이버시 적용 모델은 크게 신뢰할 수 있는 서버를 사용하는 중앙 집중형 방식과 데이터 수집 단계에 노이즈가 삽입된 상태로 데이터를 수집하는 지역 모델(Local model)로 구분할 수 있다. 중앙집중형 방식은 신뢰할 수 있는 서버가 모든 데이터를 취합하여 차분 프라이버시를 적용하나, 이는 신뢰할 수 있는 서버를 두어야 한다는 강력한 전제가 필요하다. 반면 지역 모델은 신뢰할 수 있는 서버없이도 데이터 제공자들이 자신의 데이터에 차분 프라이버시를 적용하여 전송하므로 정확한 개별 사용자의 데이터 없이도 전체적인 데이터에 대한 분포를 파악할 수 있다.

중앙 집중형 모델과 지역 모델은 각각 다음과 같은 장 • 단점을 지닌다. 중앙 집중형 모델은 전체 데이터를 취합하여 노이즈 삽입 수준을 결정하므로 데이터 유용성과 프라이버시 보호에 있어 효율적이나, 해당 작업을 처리하는 서버를 신뢰해야 한다는 제약이 존재한다. 지역 모델은 개인의 정보를 직접 수집하지 않으므로 개인의 프라이버시를 원천적으로 보호할 수 있으나, 중앙 집중형 모델에 비해 알고리즘이 복잡하고 데이터 유용성이 크게 저하될 수 있는 문제가 있다. 또한 지역 모델은 중앙 집중형 모델에 비해 많은 데이터가 있어야 일정 수준의 유용성을 보장할 수 있다.

현재 애플과 구글 등, 사용자의 정보 수집에 있어 제약이 따르는 기업들은 지역 모델의 장점에 주목하여 지

역 모델 형태로 차분 프라이버시를 적용하는 연구를 수행 중이다. 애플은 ios10부터 차분 프라이버시를 각 기기별로 적용하여 데이터를 수집하고 있으며 구글은 RAPPOR [59]에 이어 PROCHLO [60], PATE [61]을 통해 지역 모델에 기반한 차분 프라이버시 기법을 소개하고 있다. PROCHLO의 경우, 많은 수의 사용자가 존재하는 애플리케이션의 활동 내역을 수집할 시에 사용자의 프라이버시를 보호하기 위하여 encode, shuffle, alanyze 단계를 거쳐 차분 프라이버시를 적용하고 사후처리(post-processing)을 수행한다. PATE는 머신러닝 시 트레이닝 데이터를 보호하기 위해 차분 프라이버시를 적용한 기법으로 학습을 수행하는 교사(teacher)와 그 결과를 바탕으로 학습을 수행하는 학생(student)의 두 요소를 사용하여 반지도(semi-supervise)학습을 수행한다.

지금까지의 차분 프라이버시 기법은 주로 중앙 집중형 모델을 중심으로 연구가 수행되어 왔으나 지역 모델의 적용이 현실에 더욱 적합한 특징을 지니고 있다. 따라서 지역 모델에 기반한 알고리즘 개발이 필요하다.

7.2. 노이즈 패러미터 결정

차분 프라이버시 개념이 제시된 이후, 노이즈 패러미터 ε의 적정값을 두고 많은 논란이 있어왔다. Dwork이 ε을 사회적인 문제(social problem)으로 취급해야 한다고 주장했음에도 불구하고 최적의 ε을 결정하기 위한 기준이 존재하지 않는다는 사실은 차분 프라이버시가 지닌 가장 큰 취약점 중 하나로 지목되고 있다. [62]의 연구는 패러미터 ε에 의해 설정된 프라이버시 보호 수준이 기존에 공개된 정보를 사용한 추론에 의해 침해될 수 있음을 보이고, 추론을 감안한 패러미터 설정 기법을 제안하였다. [63]는 데이터 샘플의 개수가 N개일 때, 데이터 사용자와 데이터 제공자 모두가 만족할 수 있는 패러미터 결정 기법을 게임 이론에 기반하여 제안하였다. [64]은 경매 기법을 사용하여 주어진 예산과 필요로 하는 정확도에 근거하여 패러미터를 결정하는 기법을 제안하였다. 기존의 연구에서 보여지듯 ε을 결정하는 기법은 최적값을 결정할 수 있는 절대적인 기준은 존재하지 않는다. 그러므로 참여하는 구성원들 모두가 만족할 수 있는(envy-free) 지점을 찾을 수 있는 게임이론 등의 관점을 접목시킨 연구가 필요하다.

Ⅷ. 결 론

데이터 분석에 의한 프라이버시 침해 우려는 통계 분석의 시초부터 존재해왔으며, 디지털 데이터가 폭발적으로 증가하는 오늘날 더욱 심각하고 현실적인 문제로 자리잡았다. 적절한 수준의 프라이버시 보호를 보장함과 동시에 필요한 수준의 데이터 유용성을 제공하고자 하는 다양한 연구들이 수행되어 왔으며, 차분 프라이버시는 이와 같은 노력의 결실 중 하나이다. 차분 프라이버시는 특정 기법이기 전에 배경지식과 무관하게 일정 수준의 정보보호를 제공할 수 있다는 형식저인 접근을 제공하는 개념이며, 이를 현실에 적용하기 위해서는 많은 형태의 기법들이 존재할 수 있다.

우리는 본문에서 현재까지 이루어진 차분 프라이버시 관련 연구들을 개괄하였으며, 앞으로 연구가 필요한 분야의 문제들을 몇 가지 언급하였다. 차분 프라이버시는 Dwork에 의해 처음 제안된 이후로 많은 연구들이 수행되어 왔으나 현실 세계에 적용되기 위해서 해결되어야 할 많은 문제들이 여전히 남아있다. (예를 들어, 차분 프라이버시의 정의가 너무 엄격하진 않은가? 패러미터 ε은 어떻게 정해야 하는가? 프라이버시와 데이터 유용성간의 기회비용은 어떻게 조절할 수 있는가?) 이 문제들은 열린 문제로써 아직 많은 연구들을 필요로 하고 있고, 이 문제들을 해결함으로써 차분 프라이버시의 현실 적용은 더욱 가까워질 것이다.

참 고 문 헌

[1] K. Nissim, S. Raskhodnikova, and A. Smith, “Smooth sensitivity and sampling in private data analysis,” in Proceedings of the 39th Annual ACM Symposium on Theory of Computing, San Diego, CA, 2007, pp. 75-84.

[2] C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor, “Our data, ourselves: privacy via distributed noise generation,” in Proceedings of the 24th Annual International Conference on The Theory and Applications of Cryptographic Techniques, Saint Petersburg, Russia, 2006, pp. 486-503

[3] F. McSherry and K. Talwar, “Mechanism design via differential privacy,” in Proceedings of the

48th Annual IEEE Journal of Computing Science and Engineering, Vol. 7, No. 3, September 2013, pp. 177-186

[4] A. Ghosh, T. Roughgarden, and M. Sundararajan, “Universally utility-maximizing privacy mechanisms,” in Proceedings of the 41st Annual ACM Symposium on Theory of Computing, Bethesda, MD, 2009, pp. 351-360.

[5] Chaudhuri, Kamalika, Claire Monteleoni, and Anand D. Sarwate. "Differentially private empirical risk minimization." Journal of Machine Learning Research 12.Mar (2011): 1069-1109.

[6] R. Sarathy and K. Muralidhar, “Evaluating Laplace Noise Addition to Satisfy Differential Privacy for Numeric Data,” Transactions on Data Privacy, vol. 4, no. 1, pp. 1-17, 2011.

[7] K. Muralidhar and R. Sarathy, “Does Differential Privacy Protect Terry Gross’ Privacy?,” in Privacy in Statistical Databases, vol. 6344, J. Domingo? Ferrer and E. Magkos, Eds. Springer Berlin / Heidelberg, 2011, pp. 200? 209

[8] Bambauer, J. R., Muralidhar, K., & Sarathy, R. (2013). Fool's gold: an illustrated critique of differential privacy.

[9] Frank mcsherry, https://github.com/frankmcsherry/blog/blob/master/posts/2016-02-03.md

[10] A. Haeberlen, B. C. Pierce, and A. Narayan, “Differential privacy under fire,” in Proceedings of the 20th USENIX Conference on Security, San Francisco, CA, 2011

[11] P. Mohan, A. Thakurta, E. Shi, D. Song, and D. Culler, “GUPT: Privacy preserving data analysis made easy,” in Proc. 2012 ACM SIGMOD Int. Conf. Management Data, pp. 349-360.

[12] D. Kifer and A. Machanavajjhala, “No free lunch in data privacy,” in Proceedings of the 2011 international conference on Management of data, 2011, pp. 193-204

[13] Dinur I, Nissim K. Revealing information while preserving privacy. In Proceedings of the Twenty-Second ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems, 2003, 202-210.

[14] C. Dwork and S. Yekhanin, “New efficient attacks on statistical disclosure control mechanisms,” in Proceedings of the 28th Annual Conference on Cryptology: Advances in Cryptology, Santa Barbara, CA, 2008, pp. 469-480.

[15] A. Blum, K. Ligett, and A. Roth, “A learning theory approach to non-interactive database privacy,” in Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, BC, 2008, pp. 609-618

[16] A. Roth and T. Roughgarden, “Interactive privacy via the median mechanism,” in Proceedings of the 42nd ACM symposium on Theory of computing, New York, NY, USA, 2010, pp. 765-774

[17] M. Hardt and G. N. Rothblum, “A multiplicative weights mechanism for privacy-preserving data analysis,” in Proceedings of the IEEE 51st Annual Symposium on Foundations of Computer Science, Las Vegas, NV, 2010, pp. 61-70

[18] B. Barak, K. Chaudhuri, C. Dwork, S. Kale, F. McSherry, and K. Talwar, “Privacy, accuracy, and consistency too: a holistic solution to contingency table release,” in Proceedings of the twenty?sixth ACM SIGMOD?SIGACT? SIGART symposium on Principles of database systems, New York, NY, USA, 2007, pp. 273?282.

[19] G. Acs, C. Castelluccia, and R. Chen, “Differentially private histogram publishing through lossy compression,” in Proceedings of the IEEE 12th International Conference on Data Mining, Brussels, Belgium, 2012.

[20] M. Hay, V. Rastogi, G. Miklau, and D. Suciu, “Boosting the accuracy of differentially private histograms through consistency,” Proceedings of

the VLDB Endowment, vol. 3, no. 1- 2, pp. 1021-1032, 2010.

[21] C. Li, M. Hay, V. Rastogi, G. Miklau, and A. McGregor, “Optimizing linear counting queries under differential privacy,” in Proceedings of the 29th ACM SIGMOD-SIGACTSIGART Symposium on Principles of Database Systems, Indianapolis, IN, 2010, pp. 123-134

[22] C. Li and G. Miklau, “An adaptive mechanism for accurate query answering under differential privacy,” Proceedings of the VLDB Endowment, vol. 5, no. 6, pp. 514-525, 2012

[23] Chen, R., Fung, B. C. M., and Desai, B. C. Differentially private trajectory data publication. CoRR (2011), ?1?1

[24] Cormode, G., Procopiuc, C., Srivastava, D., Shen, E., and Yu, T. Differentially private spatial decompositions. In Proceedings of the 2012 IEEE 28th International Conference on Data Engineering (Washington, DC, USA, 2012), ICDE ’12, IEEE Computer Society, pp. 20-31.

[25] S. Peng, Y. Yang, Z. Zhang, M. Winslett, and Y. Yu, “DPtree: indexing multi-dimensional data under differential privacy,” in Proceedings of the ACM SIGMOD International Conference on Management of Data, Scottsdale, AZ, 2012, pp. 864-864.

[26] Jun Zhang, Zhenjie Zhang, Xiaokui Xiao, Yin Yang, and Marianne Winslett. Functional mechanism: Regression analysis under differential privacy. In International Conference on Very Large Data Bases, pages 1364-1375, 2012

[27] Bonomi, Luca, and Li Xiong. "A two-phase algorithm for mining sequential patterns with differential privacy." Proceedings of the 22nd ACM international conference on Information & Knowledge Management. ACM, 2013.

[28] Li, N., Qardaji, W., Su, D., and Cao, J. Privbasis: frequent itemset mining with differential privacy. Proc. VLDB Endow. 5, 11 (July 2012), 1340–1351

[29] Geetha Jagannathan, Krishnan Pillaipakkamnatt, and Rebecca N. Wright. A practical differentially private random decision tree classifier. In International Conference on Data Mining Workshops, pages 114-121, 2009.

[30] Arik Friedman and Assaf Schuster. Data mining with differential privacy. In International Conference on Knowledge Discovery and Data Mining, pages 493-502, 2010.

[31] Cynthia Dwork and Jing Lei. Differential privacy and robust statistics. In ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems, pages 371-380, 2009.

[32] dam Smith. Efficient, differentially private point estimators. In Computing Research Repository, 2008.

[33] Jing Lei. Differentially private M-estimators. In Advances in Neural Information Processing Systems, pages 361-369, 2011.

[34] HO, S.-S. AND RUAN, S. 2011. Differential privacy for location pattern mining. In Proceedings of the 4th ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS. SPRINGL ’11. ACM, New York, NY, USA, 17–24

[35] W. Qardaji, W. Yang and N. Li, "Differentially private grids for geospatial data," 2013 IEEE 29th International Conference on Data Engineering (ICDE), Brisbane, QLD, pp. 757-768., 2013

[36] Jun Zhang, Xiaokui Xiao, and Xing Xie., ”PrivTree: A Differentially Private Algorithm for Hierarchical Decompositions.”, In Proceedings of the 2016 International Conference on Management of Data (SIGMOD '16). ACM, New York, NY, USA, 155-170., 2016

[37] Rui Chen, Benjamin C.M. Fung, Bipin C. Desai, and Nériah M. Sossou., “Differentially private transit data publication: a case study on the

montreal transportation system.”, In Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining (KDD '12). ACM, New York, NY, USA, 213-221., 2012

[38] D. Shao, K. Jiang, T. Kister, S. Bressan and K.-L. Tan, “Publishing trajectory with differential privacy: A priori vs. a posteriori sampling mechanisms”, In DEXA, pages 357-365, 2013

[39] Xi He, Graham Cormode, Ashwin Machanavajjhala, Cecilia M. Procopiuc, and Divesh Srivastava., “DPT: differentially
private trajectory synthesis using hierarchical reference systems.”, Proc. VLDB Endow. 8, pp. 1154-1165, 2015

[40] Dwork et al., “Differential privacy in new settings”, SODA 2010

[41] Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen, Vincent D. Blondel, “Unique in the crowd: The privacy bounds of human mobility”, Sci. Rep., 3(1376), 2013

[42] Georgios Kellaris, Stavros Papadopoulos, Xiaokui Xiao, and Dimitris Papadias, “Differentially private event sequences over infinite streams.”, Proc. VLDB Endow. 7, 1155-1166, 2014

[43] Y. Cao and M. Yoshikawa, "Differentially Private Real-Time Data Release over Infinite Trajectory Streams," 2015 16th IEEE International Conference on Mobile Data Management, Pittsburgh, PA, pp. 68-73., 2015

[44] Georgios Kellaris, Stavros Papadopoulos, Xiaokui Xiao, and Dimitris Papadias, “Differentially private event sequences over infinite streams.”, Proc. VLDB Endow. 7, 1155-1166, 2014

[45] C. Task and C. Clifton, “A Guide to Differential Privacy Theory in Social Network Analysis,” in 2012 IEEE/ ACM International Conference on Advances in Social Networks Analysis and Mining.

[46] E. Shen and T, Yu, ”Mining Frequent Graph Patterns with Differential Privacy,” in KDD’ 13, August 11-14, 2013, Chicago, Illinois, USA.

[47] V. Rastogi, M. Hay, G. Miklau and D. Suciu, “Relationship Privacy: Output Perturbation for Queries with Joins,” in PODS’ 09, June 29-July 2, 2009, Providence, Rhode Island, USA.

[48] Kifer, Daniel, and Ashwin Machanavajjhala. "Pufferfish: A framework for mathematical privacy definitions." ACM Transactions on Database Systems (TODS) 39.1 (2014): 3

[49] He, Xi, Ashwin Machanavajjhala, and Bolin Ding. "Blowfish privacy: Tuning privacy-utility trade-offs using policies." Proceedings of the 2014 ACM SIGMOD international conference on Management of data. ACM, 2014.

[50] Zhang, Jun, et al. "Privbayes: Private data release via bayesian networks." Proceedings of the 2014 ACM SIGMOD international conference on Management of data. ACM, 2014

[51] Yang, Bin, Issei Sato, and Hiroshi Nakagawa. "Bayesian differential privacy on correlated data." Proceedings of the 2015 ACM SIGMOD International Conference on Management of Data. ACM, 2015

[52] Chen, Rui, et al. "Correlated network data publication via differential privacy." The VLDB Journal 23.4 (2014): 653-676

[53] Liu, Changchang, Supriyo Chakraborty, and Prateek Mittal. "Dependence Makes You Vulnberable: Differential Privacy Under Dependent Tuples." NDSS. 2016

[54] F. D. McSherry, “Privacy integrated queries: an extensible platform for privacy-preserving data analysis,” in Proceedings of the 35th SIGMOD International Conference on Management of Data, Providence, RI, 2009, pp. 19-30.

[55] I. Roy, S. T. V. Setty, A. Kilzer, V. Shmatikov, and E. Witchel, “Airavat: Security and privacy for mapreduce,” in Proc. 7th USENIX Conf. Networked Systems Design and Implementation (NSDI ’10), Berkeley, CA.

[56] Machanavajjhala, A., Kifer, D., Abowd, J. M., Gehrke, J., and Vilhuber, L. Privacy: Theory meets practice on the map. In ICDE'08 (2008), pp. 277 – 286

[57] Li, N., Qardaji, W., Su, D., and Cao, J. Privbasis: frequent itemset mining with differential privacy. Proc. VLDB Endow. 5, 11 (July 2012), 1340 – 1351

[58] Kotsogiannis, I., Hay, M., Machanavajjhala, A., Miklau, G., & Orr, M. (2017, May). DIAS: Differentially Private Interactive Algorithm Selection using Pythia. In Proceedings of the 2017 ACM International Conference on Management of Data (pp. 1679-1682). ACM.

[59] Erlingsson, Ú., Pihur, V., & Korolova, A. (2014, November). Rappor: Randomized aggregatable privacy-preserving ordinal response. In Proceedings of the 2014 ACM SIGSAC conference on computer and communications security (pp. 1054-1067).

[60] Prochlo: Strong Privacy for Analytics in the Crowd

[61] Semi-supervised Knowledge Transfer for Deep Learning from Private Training Data

[62] J. Lee, C. Clifton, "How Much is Enough? Choosing Epsilon for Differential Privacy" Proceedings of the International Conference on Information Security, pp. 325 – 340, 2011.

[63] J. Hsu, et al, "Differential Privacy: An Economic Method for Choosing Epsilon", Proceedings of the 27th IEEE Computer Security Foundations Symposium, pp.1 – 29, 2014.

[64] L. Fleischer, Y. Lyu, C. Science, D. College, "Approximately Optimal Auctions for Selling Privacy when Costs are Correlated with Data" Proceedings of the 13th ACM Conference on Electronic Commerce, pp. 568 – 585, 2012.

〈저자소개〉

정 강 수 (Ksngsoo Jung)
정회원

2007년 8월 : 서강대학교 컴퓨터공학과 졸업
2009년 8월 : 서강대학교 컴퓨터공학과 석사
2017년 2월 : 서강대학교 컴퓨터 공학과 박사
관심분야 : 개인정보보호, 접근제어

박 석 (Seog Park)
정회원

1978년 2월 : 서울대학교 계산통계학과 졸업
1980년 2월 : 한국과학기술원 전산학과 석사
1989년 8월 : 한국과학기술원 전산학과 박사
1983년 9월~현재 : 서강대학교 컴퓨터공학과 교수
관심분야 : 개인정보보호, 접근제어