【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第２区分
【発行日】平成28年8月25日(2016.8.25)

【公開番号】特開2014-98895(P2014-98895A)
【公開日】平成26年5月29日(2014.5.29)
【年通号数】公開・登録公報2014-028
【出願番号】特願2013-216154(P2013-216154)
【国際特許分類】
Ｇ０９Ｃ　1/00　(2006.01)
【ＦＩ】
Ｇ０９Ｃ　1/00　６６０Ｄ
Ｇ０９Ｃ　1/00　６５０Ｚ

【手続補正書】
【提出日】平成28年7月6日(2016.7.6)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
プライベートデータに関する集約統計をセキュアに求めるための方法であって、
クライアントにおいて、データＸ及びＹに別々に第１のランダム化を行って、それぞれランダム化データ
【数１】

$\hat{X}$ 及び $\hat{Y}$

を取得するステップであって、該第１のランダム化は、前記データＸ及びＹのプライバシーを保全し、前記ランダム化はデータＸ及びＹで直接作用し、前記データＸは、第１のデータソースによって生成され、前記データＹは、第２のデータソースによって生成され、前記データＸ及びＹは、分散形式で別々に生成されるものと、
前記クライアントにおいて、前記ランダム化データ
【数２】

$\hat{X}$ 及び $\hat{Y}$

に別々に第２のランダム化を行って、サーバー用のランダム化データ
【数３】

$\tilde{X}$ 及び $\tilde{Y}$

と、前記クライアント用のヘルパー情報
【数４】

$T_{\tilde{X}|\hat{X}}$ 及び $T_{\tilde{Y}|\hat{Y}}$

とをそれぞれ取得するステップであって、ここで、Ｔは経験分布を表し、該第２のランダム化は、前記データＸ及びＹの前記集約統計の前記プライバシーを保全するものと、
前記サーバーにおいて、

【数５】

$$T_{\tilde{X},\tilde{Y}};$$

を求めるステップと、
前記クライアントによって、前記ヘルパー情報
【数６】

$$T_{\tilde{X}|\hat{X}} \text{ 及び } T_{\hat{Y}|\hat{Y}}$$

を
【数７】

$$T_{\tilde{X},\tilde{Y}}$$

に適用して推定された
【数８】

$$\dot{T}_{X,Y}$$

を取得するステップであって、ここで、ＸとＹとの間の「|」及び「，」は、それぞれ条件付き分布及び結合分布を表すものと、
を含む、方法。
【請求項２】
前記ランダム化は、ポストランダム化方法(ＰＲＡＭ)を用いる、請求項１に記載の方法。
【請求項３】
前記第１のランダム化及び前記第２のランダム化は異なるものである、請求項１に記載の方法。
【請求項４】
前記ルパー情報は、前記データＸ及びＹと比較して小さい、請求項１に記載の方法。
【請求項５】
前記データＸ及びＹはランダム系列であり、データ対(Ｘ$_{i}$，Ｙ$_{i}$)は独立同一分布である、請求項１に記載の方法。
【請求項６】
前記ランダム化は、前記データＸ及びＹの差分分散プライバシーを保全する、請求項１に記載の方法。
【請求項７】
前記第２のランダム化は、前記第１のランダム化によって提供される差分プライバシーよりも強い分散プライバシーを提供する、請求項１に記載の方法。