合同会社ジャノム

報道関係者各位

2023年6月30日
合同会社ジャノム
代表社員　日向 理彦

検索匿名化技術「Private Information Retrieval」の高効率実装「EllipticPIR」の特許・商標出願のお知らせ

～サーバに内容を知られることなく検索できる技術の世界初の実用的実装～

ブロックチェーンなどの技術開発およびコンサルティングを行う合同会社ジャノム（東京都墨田区、代表社員：日向 理彦）は、検索匿名化技術である「**Private Information Retrieval (**秘密情報検索**)**」（以下「**PIR**」）に対し、既知の実装では行うことのできなかった**GPU**などを用いた高度な並列化技術を開発し、その特許および商標権（**EllipticPIR**）の出願を行ったことをお知らせします。

Private Information Retrieval (PIR) とは？

PIR はクライアント（検索者）のクエリ（検索）内容をサーバ側に一切知られることなく、サーバ上に存在するデータベース上のデータを検索することのできる暗号技術の総称です。暗号学的に保証されたセキュリティのもとで検索が行われるため、検索内容をサーバ側が解読することは原理的に不可能です。
この技術を利用することでエンドユーザは、サーバ側へのプライバシー漏洩の心配がなく検索を行えるようになります。

既存技術の問題点

既存の PIR 実装ではCPUの単一のコアのみを利用して計算することを前提としており、GPUなどのメニーコア・デバイスを用いて計算処理を分散化することができませんでした。
CPUのマルチコア化やAI技術の発達が後押しするGPU性能の飛躍的な向上がなされた現代においては、多数のコアで分散してワークロードを処理することは必要不可欠な計算手法であり、サーバへ搭載する計算機器を増強することで大規模データを扱えるようにスケーリングできることは非常に大きな強みを発揮します。

特許技術

暗号化アルゴリズムとして楕円曲線エル・ガマル (EC-ElGamal) 暗号を用いることで、非常に高い効率で並列化が行えるアルゴリズムを考案しました。これによりGPUなどのメニーコア・デバイスにおいても効率的に計算ができます。

当社の試験実装によれば、一般家庭向けの安価なGPU (NVIDIA GeForce RTX 3080) 一台でも、従来実装と比べて100倍程度の大きさのデータベースを従来と同程度の実行時間で処理することができました。なお、NVIDIA Teslaなどの産業向けGPUや複数枚のGPUを利用することで、扱うことのできるデータベースサイズや実実行時間は理論的には無制限に向上させることができます。

ユースケース

単純なデータベース・キーを用いた検索であれば、どのようなデータベースでも利用することができ、検索者のプライバシーが重視されるようなユースケースで広く適用可能です。
例えば検索エンジンで行きたいお店の名前を検索すると、検索エンジン側はそのユーザがそのお店に行くことを高い確率で推測できてしまいますが、PIR を用いればそのようなプライバシーの問題は発生しなくなります。
また証券価格を検索した場合、そのユーザがその証券を購入しようとしていることが検索エンジンに知られてしまいますが、これも PIR を用いることで秘匿化が可能です。
当社では様々な企業から PIR のユースケースをヒアリングすることで具体的な PIR に対するニーズを把握してまいります。自社サービスで少しでも有効活用できそうな可能性のある企業様がいらっしゃいましたら、ぜひ当社宛にお問い合わせください。

技術情報（ドキュメント）

本発表に合わせて、技術的な詳細などが掲載されたドキュメント（英語版のみ）を公開いたしました。当社技術に興味のあるご担当者様は、下記のURLから詳細をご覧いただけます。
https://docs.ellipticpir.com/

今後の展開

当社技術をクラウドサービス (SaaS) として利用できる「EllipticPIR Cloud」の提供を行う予定です。
本クラウドサービスを利用することで任意のデータベースを匿名化した状態で提供できるようになり、様々な企業様の検索秘匿化によるエンドユーザへのプライバシー権の向上を目指します。

お問い合わせ先

- 担当：代表社員　日向
- 電子メール：info@janom.co.jp

お問い合わせいただいた企業様には、必要に応じてより詳しい技術資料の開示を行うことが可能です。
お気軽にお問い合わせください。