SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

データ分布情報を用いたレンジクエリに対するボリューム漏洩攻撃
Volume leakage attack against range queries using data distribution information

小谷 俊輔 * 國廣 昇 †
Shunsuke Odani Noboru Kunihiro

キーワード ボリューム漏洩攻撃, レンジクエリ

あらまし

データを外部サーバにアウトソーシングする際，盗聴者からだけでなくサーバ自体からも情報を隠す必要があり，その安全性評価や安全な実装法は重要な研究課題である．典型的な解決策は，暗号化されたデータをサーバに保存し，クライアントは暗号化されたクエリをサーバに送信し，サーバは，その暗号化されたクエリを処理し，クライアントのみが復元可能な応答を生成する方法である．

近年，暗号化データベースに対するレンジクエリの応答ボリュームサイズを観測することにより， データベース全体のデータベースカウントを復元する攻撃 [1, 2, 3] が提案されている．攻撃者は，クエリに対する応答の内部情報は完全に無視して，そのサイズのみに注目し，データベース全体のデータベースカウントの復元を攻撃の目的とする．この攻撃では，固定の窓幅 b に対して，幅 b 以下の全てのレンジクエリに対する応答ボリュームサイズが得られるという仮定のもとで復元を行う．既存研究 [1, 2, 3] では，復元するデータ分布に対する仮定を置かず，どのようなデータ分布に対しても有効な攻撃手法を提案している．しかし，実際のデータベースのデータ分布は，攻撃対象の分野やクエリの種類によって，ある程度の推定が可能であることが多く，分布の情報を用いることにより，高い精度で攻撃に成功する可能性がある．

本発表では，窓幅 b を 2 に固定した上で，対象のデータ分布が事前に得られる仮定のもとで与えられたデータ分布に特化した有効な攻撃を提案する．提案手法では，観測したボリュームサイズをもとに，CSS2021 における我々の発表 [4] で用いたグラフ理論的なアプローチにより，データベースカウントの復元を行う．この攻撃では，観測したボリュームサイズからグラフを構成し，全ての頂点を少なくとも一度通る経路を探索することにより，全てのデータベースカウントを復元している．従来の方式では，計算途中で解候補数が爆発し，正しい解が得られないという問題があったが，データ分布情報を用いて余分な経路を削除することにより，解候補数の爆発を回避している．さらに，実世界のデータベースを対象として， 我々の提案攻撃を実験的に検証し， データベース復元率の評価を行う．

* 筑波大学システム情報工学研究群〒 305-8577 茨城県つくば市天王台 1-1-1.
† 筑波大学システム情報系 〒 305-8577 茨城県つくば市天王台 1-1-1.

参考文献

[1] Z. Gui, O. Johnson and B. Warinschi,“Encrypted databases: New volume attacks against range queries,” in Proc. of ACM CCS2019, pp. 361–378, 2019.

[2] P. Grubbs, M. Lacharité, B. Minaud, and K. G. Paterson,“Pump up the volume: Practical database reconstruction from volume leakage on range queries,” in Proc. of ACM CCS2018, pp. 315–331, 2018.

[3] G. Kellaris, G. Kollios, K. Nissim, and A. O’Neill, “Generic attacks on secure outsourced databases,” in Proc. of ACM CCS2016, pp. 1329–1340, 2016.

[4] 小谷 俊輔, 國廣 昇, “レンジクエリに対するノイズ付きボリューム漏洩攻撃”, 2E4-2, CSS2021.