# 論文審査の結果の要旨

氏名　　トマ　フランシス　ヴァネ

本博士論文では秘匿情報検索法に関して考察をしている．一般の情報検索法ではクライアントは，データを保管しているサーバーにクエリを送付し，クエリに基づくデータを取得する方式である．それに対して，秘匿情報検索法は，クライアントが送付したデータをサーバーに秘匿したままデータの取得を行う方式である．プライバシーを担保したまま，データ取得を行うことができるため，多くの現実の課題に対して適用可能であり，効率的な方式の提案は重要な研究課題である．

本博士論文は 7 章からなる．第一章は序章であり，第二章では必要な諸定義がなされている. 第三章では, SQL-like なクエリに対する秘匿情報検索方式の提案を行っている．第四章では，単一サーバーによる秘匿情報検索プロトコルの提案を行っている．事前計算を導入することにより計算量の削減に成功している．第五章では，サーバー側のパラメタ選択に関して詳細に述べている．サーバー側での事前計算を導入しすることにより効率化をはかっている．第六章では，これまでの議論を全てまとめることにより，効率的な方式の提案を行っている．第七章では，結論および今後の研究課題に関して述べている．

以下，これらの内容の詳細について説明する．

第三章では，SQL-like なクエリに対する秘匿情報検索方式の提案を行っている．ユーザーにより選択された秘密のパターンに適合する field を持つデータベースエントリーを取得するプロトコルの提案を行う. 提案プロトコルは, それほどエントリが多くない SQL データベースで使われる時には十分効率的である．これは，実際の作業環境を考えた場合には，標準的な制約である．このアルゴリズムは，秘匿情報検索の分野で集中的に研究されている Φ-hiding 仮定の困難さに安全性の根拠をおいている．

第四章では，単一サーバーによる秘匿情報検索プロトコルの提案を行う．提案方式の計算量的な安全性は，近似 GCD 問題の困難さに基づいている．この問題は，完全準同型暗号の分野で重点的に研究されている．提案方式は，Goldberg の方式や Beimel らの方式で用いられている 2 次元データベース構成に基づいている．これらの方式は，情報論的な安全性を有しているが, 近似 GCD 問題の困難さに安全性の根拠を置く方式に修正し, 効率の改善に成功している．さらに，事前計算を導入することにより，計算量の削減に成功している．最後に，提案方式の安全性証明を与えている．

第五章では，4 章で提案した方式に対してサーバー側での事前計算を改良した．その結果，十分大きいデータベースに対して，情報論的な仮定に基づく方式の限界を破ることに成功した．計算量的な仮定からアルゴリズムを構成した場合，情報論的な限界を漸近

的に破られることが既存研究により知られており，この結果は，主に理論的な成果と考えることができる．この性能を実現するために，その代償として，クライアント側の計算コストが増加するという問題があった．この問題に対して，安全性を慎重に評価することにより，計算コストの増加を抑えることに成功した．計算コストの増加は，クライアントにとっては，大きな問題ではないことを確認する．クライアント側の計算コストを増加は，クラウドコンピューティングが用いられる状況にとっては，逆の方向の研究とも言える．しかし，秘匿情報検索が用いられる状況では，サーバーの計算コストを増加させることのメリットはない．また，プライバシー中心のシステムは，しばしばビジネスモデルに反することがある．そのため，プライバシーの確保と引き替えにクライアント側の計算量を増加させることは妥当であると判断し，提案方式は十分に意義のあるものであると言える．

第六章では，五章までに得られた方式の結合方式に関して議論する．つまり，これまで提案したプロトコルを用いることにより，複雑な SQL クエリが実行でき，クエリをサーバーに秘匿したまま，クエリの結果を効率的に所得することができる方式の提案を行う．

本論文の第三章，第四章，第五章，第六章は國廣昇との共同研究であるが，論文提出者が主体となり貢献を行っている．そのため，論文提出者の寄与が十分であり，博士（科学）の学位を授与できると認める．

以上 1763 字