学位論文の審査結果の要旨

クラウドコンピューティングが広がる中，ストレージサービスなどにおいて自分のデータの内容を隠して利用したい場合がある。そのための最も有効な手段の一つがデータの暗号化である。しかし，暗号化することによってセキュリティは強化されるが，保存したデータの検索が難しくなる。セキュリティの強い安全なデータの検索手法として，暗号化されたデータを暗号化したまま検索する暗号化検索法の開発が進められている。本論文は，暗号化検索の中でも，XML(Extensible Markup Language)データを対象とした暗号化検索法について述べたもので，全4章で構成されている。第2章及び第3章でXMLデータに対する新たな暗号化検索法を提案し，第4章は結論である。

第2章は「XPathに対応した暗号化検索法」について述べている。本章では，XPathの部分クラスに対応した新たな暗号化検索法として，XMLの構造を隠したまま検索する手法を提案し，実験的にその性能を評価している。XPathはXMLデータの特定の情報を指定するための言語で，広く用いられている。XMLは木構造で表すことができるため，XPathによる検索は，XPathが表す木構造とマッチする部分をXMLデータから探すことになる。従来の暗号化検索法は，木の構造を隠していないため，同じような構造を持つXMLデータから中身を推測されてしまう可能性がある。また，XML全体を暗号化することで構造を隠すこともできるが，検索する場合，すべてを復号化する必要があるため効率が悪い。提案法は，効率的にその構造を隠すことによって，従来よりもセキュリティの高い検索法を実現している。今後の課題としては，より柔軟な検索を実現するため，利用可能なXPathの拡張などがある。

第3章は「XMLキーワード検索に対応した暗号化検索法」について述べている。本章では，キーワードに基づいたXMLの暗号化検索法に対し，新たな手法を提案している。従来から，XMLデータを簡便に検索できる手法として，キーワードを使った検索法が開発されているが，暗号化に対応した手法に関する研究はほとんどない。XMLのキーワード検索では，検索結果としてSLCA(Smallest Lowest Common Ancestor)が広く用いられている。一般に，暗号化されたXMLデータからSLCAを効率的に検索することは難しい。本論文は，ブルームフィルタというデータ構造を利用し，暗号化されたXMLデータにおけるキーワード検索に対し，SLCAを検索するための新たな手法を提案し，実験的にその性能を評価した。提案法は，構造を隠すため安全性が高く，また，必要なデータだけをサーバから取得し，使用するためメモリの節約も可能である。ただし，検索時間に関しては，まだ十分早いとは

言えず今後の課題として残される。

このように，本論文は，XMLデータに対する新たな暗号化検索法を提案するもので，情報セキュリティ分野の今後の発展に大いに貢献することが期待される。さらに，本論文の内容は，2件の原著論文として発表されている。以上，本論文は，博士学位論文に値するものと判断した。

公表主要論文名

・ 中村伸一，山本博章，Bloom Filter を利用した暗号化 SLCA 検索手法の提案，日本データベース学会論文誌，Vol.12，No.2，pp.1-6(2013).
・ 中村伸一，山本博章，XPath を用いた暗号化 XML 文書検索手法の提案，日本データベース学会論文誌，Vol.11，No.2，pp.31-36 (2012).