審 査 の 結 果 の 要 旨

氏　　名　　ファクキアウ　ソムチャート

本論文は題目「Achieving Expressive, Scalable, and Efficiently Revocable Collaborative Data Access Control in Multi-Authority Cloud (マルチオーソリティクラウドにおけるデータアクセス制御の表現性、スケーラビリティ、効率的な失効処理の実現)と称し、近年その重要性を増しているクラウド環境で、属性をベースに効率的にアクセス制御を実現するための属性ベース暗号にアクセスポリシーを組み合わせたアクセス制御方式について研究したものである。

本論文は 6 章よりなる。

第 1 章は、序論であり、本論文の研究背景を述べたものである。すなわち、クラウド環境を前提とすると、ビジネス上重要なデータをクラウドにアウトソースして置くことが必要になり、そのアクセス制御が重要になってくる。アクセス制御の基本は暗号化であり、それによってデータにアクセスする人員を制御するのであるが、多くの人員が関与し、制御のロジックも複雑になってくると、従来型の、アクセスを許す人員にだけ複合鍵を配布するというスキームの運用コストが禁止的になってくる。CP-ABE（暗号化ポリシー付き属性ベース暗号）はその問題を解決するために提案されたが、多人数のデータ所有者が存在するときにスケールしない、書き込み権限の制御ができない、鍵管理のコストが非常に高い、失効管理のコストが非常に高いという欠点が解消されないままになっていたことを述べている。

第 2 章は、本研究に専攻する結果として発表されてきた成果の主なものについて論じている。

第 3 章は、CP-ABE の上記の問題点を解決する新たなスキーム C-CP-ARBE（協調的暗号化ポリシー付き属性ロールベース暗号）を提案する。多人数のデータ所有者の協調を許すスキームであり、さらにアクセス制御として RBAC（ロールベースアクセス制御）に基づきアクセス制御を記述する。ここでは、書き込み権の表現も可能になっている。さらに鍵管理を効率化するために、プロキシにより鍵の集中管理を行う。クラウド上でセキュアに鍵管理を行う。ARBE の鍵は、2 段階で暗号化され、外側の高速な対称鍵暗号システムの利用により、

効率的に管理されるスキームを導入した。これにより鍵管理の効率は劇的に改善された。この効果を証明するために Proof of Concept（PoC）システムを構築して実際の暗号化の効率を測定し、十分な性能が得られたことを確認した。

第 4 章は、属性ロールの管理のうち、CP-ABE で十分な性能を出すことができなかった失効管理の効率化について述べている。プロキシの実装と、プロキシ上で外側の高速な対称鍵暗号システムを保守することにより、非常に効率的に失効管理ができるようになったことを示した。この方式を VL-PRE（Very Light Proxy Re-encryption)と称し、PoC システム上で十分な高速化が達成されたことを確認した。

第 5 章は、C-CP-ARBE のもう一つの重要な機能である暗号化ポリシー管理方式について論じている。中央鍵管理かつプロキシを利用した C-CP-ARBE 上で暗号化ポリシーを管理するために必要な機能を示し、実装した。

第 6 章は以上をまとめて結論とし、さらに将来のこの分野における発展の方向について論じている。

以上要するに、本論文は、クラウド上にアウトソースされたデータのアクセス制御の問題に対して、属性ベース暗号を利用して柔軟なアクセス制御を可能にし、さらに書き込みを含めたアクセス制御ポリシーも併せて制御できるスキームとして C-CP-ARBE を提案し、2 段階鍵管理により、管理コストを十分に低減させ、さらに従来からの属性ベース暗号の問題であった失効管理の運用コスト低減を併せて実現し、十分実用的に利用できるシステムとして完成させたという点で、暗号学の応用を通してセキュリティ工学に寄与するところが少なくない。

よって本論文は博士（工学）の学位請求論文として合格と認められる。