2E-6

鍵失効機能を持つ属性ベース暗号の実装評価

満永　拓邦†　　イスマイル　オマール†　　久野　祐介†　　田所　成久†
近藤　伸明†　　藤木　裕之‡　　五十嵐　寛‡
†株式会社　神戸デジタル・ラボ　　‡金沢工業大学

1　はじめに

近年，脚光を浴びているクラウドコンピューティングは，利用時にプライバシー情報や機密性の高いデータをクラウドサービス提供者に渡して処理を行う場合があり，データの機密性に関するセキュリティ上の問題が普及の妨げの一因となっている．本研究は，多数のユーザが利用するクラウドコンピューティングに適した暗号方式として提案されている属性ベース暗号方式の実装及び性能評価を行う．属性ベース暗号方式とは，データを送信するユーザが，受信するユーザの ID や所属部署など属性情報に関する条件を指定して暗号化及びデータ送信を行い，受信したユーザは秘密鍵内の属性が条件を満たす場合のみ復号できる暗号方式である．各ユーザに対して，各々の公開鍵で暗号化を行う従来の公開鍵方式と比較して，鍵管理の効率がよいとされている．属性ベース暗号方式に鍵失効機能を追加したモデルの実装を行い，秘密鍵に格納する属性数や復号条件の数の変化に対する処理速度の測定を行い，現実的なサービスとして提供が可能かを明らかにする．

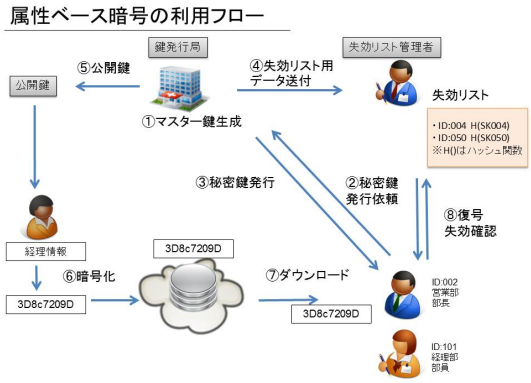
2　関連研究

Sahai, Waters がアクセス制限機能を持つ暗号方式として属性ベース暗号の提案を始めに行った [1]．Goyal らは，より一般的な属性暗号方式を提案した．ユーザの秘密鍵の中に持つアクセス権限をアクセスツリーと呼ばれる木構造を用いて表した [2]．Bethencourt らは，属性ベース暗号方式において，暗号文に復号条件を持たせる方式の提案を行った．Pirretti らは，鍵失効機能を追加した属性ベース暗号方式の提案を行った [3]．

3　提案方式

本研究では，属性ベース暗号方式に失効リストを追加した新方式の研究・実装を行う．利用フローは下図の通りである．

1. （鍵生成局）マスター鍵の公開鍵の作成
2. （各ユーザ）属性に応じた秘密鍵の作成依頼
3. （鍵生成局）身元を確認して個人の秘密鍵を送付
4. （鍵生成局）各ユーザの ID と H（ID）の組み合わせを失効リスト管理者に通知
5. （鍵生成局）公開鍵を公開鍵基盤上に公開
6. （送信者）復号可能な属性条件を指定しデータを暗号化を行い，データベースに格納
7. （受信者）暗号化されたデータを復号・利用（ただし，自分の持つ属性が復号条件を満たす場合のみ復号・利用可能）．また復号時に H（ID）を突合し，秘密鍵が失効していないか確認



4　性能実験

4.1　実験環境

表 1: 実験環境

Client	
OS	CentOS 5.5
CPU	Celeron (1.3G)
Memory	768G

Implementation and Evaluation of Attribute Based Encryption with Revocation Function.
†Takuho Mitsunaga, Ismail Omar, Yusuke Kuno, Naruhisa Tadokoro, Nobuaki Kondo
‡Hiroyuki Fujiki, Yutaka Igarashi
Kobe Digital Lab Inc.(†)
Kanazawa Institute of Technology(‡)

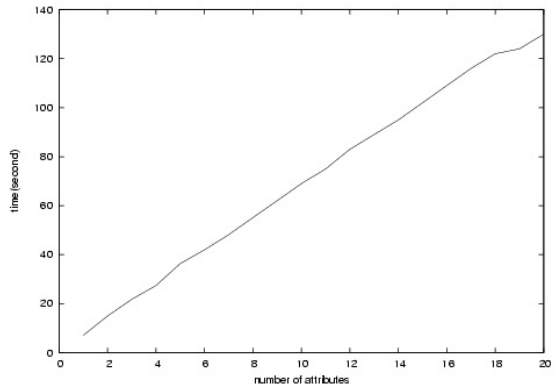


図 1: 属性数による鍵生成時間の変化

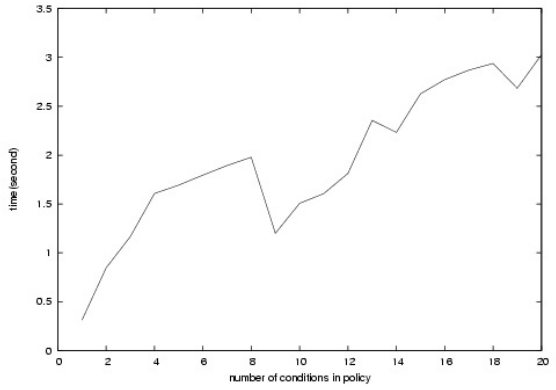


図 2: 条件数による暗号化処理時間の変化

4.2 実験概要

表 1 に示す性能の計算機を用いて，属性ベース暗号方式の鍵生成と暗号化にかかる処理時間の測定を行う．理論的に，鍵生成の計算処理コストは格納する属性の数に依存し，また暗号化の計算処理コストは復号に関する条件に依存する．本研究では，(1) 秘密鍵に格納する属性数の増加による処理時間の変化，(2) 暗号化時の条件の数と処理時間の変化の計測を行う．条件の内容はランダムに選択し，暗号化に使用するデータは 1MB の PDF ファイルを使用する．それぞれ 10 回の測定を行い平均値を処理時間として用いる．

5 実験結果と考察

鍵生成・暗号化の処理時間は上記，図 1 と図 2 の通りである．鍵生成は格納する属性数に，また暗号化は条件数に比例した処理時間が計測された．複雑かつ大規模なサービスでの提供は現状の計算機速度やアルゴリズムでは厳しいと考えられるが，属性数や復号の属性条件数が 10 以下であれば十分に実用可能な処理速度である．

6 まとめ

本稿では，属性ベース暗号の実装を行い，性能評価を行った．鍵生成と暗号化の処理に要する時間は図に示す通りであり，実サービス提供を考えると，ユーザが持つ属性が数種類，暗号化時の条件も数十種類であれば十分に可能であると考えられる．ただし大規模なクラウドサービスを行う事を想定すると，処理速度の向上が必要となる．今後，処理速度を早くするために，より効率的なデータ構造やアルゴリズムの研究を行う．

謝辞

本研究の一部は，経済産業省「平成 22 年度企業・個人の情報セキュリティ対策促進事業（新世代情報セキュリティ研究開発事業）」の委託研究に基づいて行われた．

参考文献

[1] W.Sahai and B.Waters. Fuzzy Identity Based Encryption, 2005. Proceedings of Eurocrypt 2005, volume 3494 of LNCS, pp. 457-473.

[2] A. Sahai V.Goyal, O. Pandey and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data, 2006. Proceedings of the 13th ACM conference on Computer and communications security 2006, pp. 89 - 98.

[3] P. McDaniel M. Pirretti, P. Traynor and B. Waters. Secure Atrribute-Based Systems, 2006. Proceedings of the 13th ACM conference on Computer and communications security 2006, pp. 99-112.