論文 / 著書情報
Article / Book Information

題目(和文)	実用的な属性ベース暗号と属性ベース署名に関する研究
Title(English)	A study on practical attribute-based encryption and signature
著者(和文)	冨田斗威
Author(English)	Toui Tomita
出典(和文)	学位:博士(工学), 学位授与機関:東京工業大学, 報告番号:甲第11759号, 授与年月日:2022年3月26日, 学位の種別:課程博士, 審査員:尾形 わかは,植松 友彦,山田 功,松本 隆太郎,田中 圭介
Citation(English)	Degree:Doctor (Engineering), Conferring organization: Tokyo Institute of Technology, Report number:甲第11759号, Conferred date:2022/3/26, Degree Type:Course doctor, Examiner:,,,,
学位種別(和文)	博士論文
Category(English)	Doctoral Thesis
種別(和文)	審査の要旨
Type(English)	Exam Summary

（博士課程）

論文審査の要旨及び審査員

報告番号	甲第　　号		学位申請者氏名		冨田 斗威	
論文審査 審査員		氏　名	職　名		氏　名	職　名
	主査	尾形わかは	教授	審査員	田中圭介	教授
	審査員	植松友彦	教授			
		山田　功	教授			
		松本隆太郎	准教授			

論文審査の要旨（2000 字程度）

本論文は，「A study on practical attribute-based encryption and signature (実用的な属性ベース暗号と属性ベース署名に関する研究)」と題し，英文 7 章より構成されている．

第 1 章「Introduction (はじめに)」では，まず，クラウドや人工知能などに代表される近年の技術の進歩に伴い，従来の暗号技術では実現できない付加機能を持つ高機能暗号技術の実用化が重要であることを述べた上で，高機能暗号の一種であり本研究の対象である属性ベース暗号と属性ベース署名の説明をしている．次に，既存の属性ベース暗号方式や属性ベース署名方式が効率，安全性，機能性のいずれかの面で欠点を抱えており，そのような欠点のない実用的な属性ベース暗号方式や属性ベース署名方式が欠如していることを課題として設定している．そして，その解決の一環として，本論文では，秘密情報が部分的に漏洩したとしても安全性を達成できる性質である漏洩耐性と CCA2 安全性を兼ね備えた属性ベース暗号方式および，いくつかの望ましい性質を併せ持つ属性ベース署名方式を新たに構築していることを述べている．

第 2 章「Preliminaries (準備)」では，本論文を通じて参照される記法や，属性ベース暗号や属性ベース署名などの暗号プリミティブの定義を概説している．

第 3 章「Leakage-Resilient CCA2-Secure IBE without q-Type Assumptions (q 型仮定を用いない漏洩耐性を持つ CCA2 安全な ID ベース暗号)」では，属性ベース暗号の特殊例の一つである ID ベース暗号に対し，一般に強い仮定とされる q 型仮定に依存せず漏洩耐性と CCA2 安全を証明可能な初めての ID ベース暗号方式を提案している．

第 4 章「Optimal Leakage-Resilient CCA2-Secure IBE (最適な漏洩耐性を持つ CCA2 安全な ID ベース暗号)」では，まず，線形空間によって特徴づけられるある種の言語に対し，暗号方式の安全性の向上に利用可能な quasi-adaptive non-interactive zero-knowledge argument (QA-NIZK)を新たに構成している．そして，新しい QN-NIZK と最適な漏洩耐性を持つ CPA 安全な ID ベース暗号方式と組み合わせることで，最適な漏洩耐性を持つ CCA2 安全な ID ベース暗号方式を構成できることを示している．ここで，秘密情報のサイズと許容される秘密情報の漏洩量との比を漸近的に 1 に近づけることが可能なとき，その暗号方式は最適な漏洩耐性を持つと言う．提案した QA-NIZK の持つ効率性から，提案した ID ベース暗号方式は弱い安全性しか持たない既存方式と暗号文のサイズがほとんど変わらず効率的である．

第 5 章「Leakage-Resilient CCA2-Secure ABE (漏洩耐性を持つ CCA2 安全な属性ベース暗号)」では，まず，4 章で提案した QA-NIZK を，線形写像によって特徴づけられるより広い言語に対して拡張可能であることを示している．また，これを既存の漏洩耐性を持つ CPA 安全な属性ベース暗号方式と組み合わせることで，漏洩耐性を持つ CCA2 安全な属性ベース暗号方式を効率よく構成できることを示している．4 章の結果と同様に，提案方式の効率は弱い安全性の既存方式の効率とほとんど変わらず，また，鍵生成局が持つマスター秘密鍵と各ユーザーが持つ秘密鍵の両方が部分的に漏洩したとしても安全であるという既存方式の利点を引き継いでいる．

第 6 章「Compact Attribute-Based Signature for NC1 Circuits (NC1 回路に対するコンパクトな属性ベース署名)」では，署名ポリシーとして高い表現力を持つ NC1 回路を扱うことが可能な属性ベース署名方式を提案している．提案方式は，署名ポリシーの高い表現力，署名サイズが定数サイズであるというコンパクト性，標準的な計算量的仮定のもとで強い安全性である適応的偽造不可能性を同時に達成している初めての属性ベース署名方式である。

第 7 章「Conclusion (まとめ)」では，本論文の成果を要約するとともに，今後の課題について言及している．

以上を要約すると，本論文は，実用的な属性ベース暗号方式と属性ベース署名方式の構成方法について論じたものである．本論文で提案された手法は属性ベース暗号・属性ベース署名に限らず，実用的な高機能暗号の構築に資するものであり，工学上貢献するところが大きい．よって我々は，本論文が博士(工学)の学位論文として十分価値があるものと認める．