論文 / 著書情報
Article / Book Information

題目(和文)	完全構造保持署名と耐不可逆漏洩署名に関する構成
Title(English)	Constructions for Fully Structure-Preserving Signature and Uninvertible Leakage Resilient Signature
著者(和文)	王 煜宇
Author(English)	Yuyu Wang
出典(和文)	学位:博士(理学), 学位授与機関:東京工業大学, 報告番号:甲第10754号, 授与年月日:2018年3月26日, 学位の種別:課程博士, 審査員:田中 圭介,伊東 利哉,尾形 わかは,渡辺 治,鹿島 亮
Citation(English)	Degree:Doctor (Science), Conferring organization: Tokyo Institute of Technology, Report number:甲第10754号, Conferred date:2018/3/26, 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		王煜宇(Yuyu Wang)	
論文審査 審査員		氏　名	職　名		氏　名	職　名
	主査	田中圭介	教授	審査員	渡辺治	教授
	審査員	伊東利哉	教授			
		尾形わかは	教授			
		鹿島亮	准教授			

論文審査の要旨（2000 字程度）

本論文は「Constructions for Fully Structure-Preserving Signature and Uninvertible Leakage Resilient Signature（完全構造保持署名と耐不可逆漏洩署名に関する構成）」と題し、英文５章よりなる。

電子署名は、紙文書の署名や印鑑と同じように、ある文書が本当に作成者により作られたかどうかを検証できる技術である。署名者は自分だけが知っている秘密鍵を用いて文書に署名をつける。そして、公開された検証鍵を用いて、署名が本物かどうかを検証できる。秘密鍵を持たない不正者が署名を偽造できないことが、電子署名の基本的な安全性、偽造困難性である。電子署名は、様々な暗号プロトコルの構成要素として使われている。そして、検証が必要であるディジタルサービス、例えばスマートカードとディジタルコンタクトに、電子署名は広く応用されている。

本論文では、fully structure-preserving（FSP）署名方式と耐不可逆漏洩署名方式について論じている。FSP 署名方式は、効率が良いモジュラー的なプロトコルを構成するための重要な構成要素である。耐不可逆漏洩署名は、物理的な実装に基づく非常に広範囲なサイドチャネル攻撃に対して安全な署名である。本研究ではまず、FPS 性質より弱い structure-preserving（SP）性質をもつ署名方式から FSP 署名方式へ変換できる一般的な手法を提案している。SP 性質をもつ署名方式は既に広く研究され、具体的な方式も多く存在しているので、本手法により、多くの FSP 署名方式が得られることとなる。以前に提案された FSP 方式とは異なり、本研究で提案する方式の多くは、automorphic という性質を持っている。つまり、署名者が自分の検証鍵に署名することができる。そして、本研究では、はじめての耐不可逆漏洩署名方式を提案している。提案した方式は、敵が秘密鍵を漏洩させることができても、漏洩情報から秘密鍵を完全に計算することができない限り安全性は保たれるという性質を持つ。より詳細には、制限のない任意の不可逆関数を通した秘密鍵の漏洩情報を見ることができる敵に対し、提案方式は偽造不可能性を持つ。さらに、提案した方式は、秘密乱数を使わずに署名することができるため、秘密乱数の漏洩を考える必要がない。

本論文の第 1 章「Introduction」では、本研究の背景、目的および成果の概要を述べている。

第 2 章「Preliminaries」では、本研究の内容を述べるために必要な定義や仮定を説明している。

第 3 章「Generic Constructions of Fully Structure-Preserving Signature」では、FSP 署名方式の定義を説明して、trapdoor 署名方式と auxiliary input 署名方式という二つの新しい構成要素を定義している。どちらも SP 署名方式から作ることができるということを示し、両方の構成要素を組み合わせることにより、SP 署名方式から FSP 署名方式へ変換できる一般的な構成も提案されている。

第 4 章「Signature Resilient to Uninvertible Leakage」では、不可逆漏洩に耐性をもつ署名方式を定義している。そして、耐不可逆漏洩 hard relation という構成要素を定義し、これを point obfuscation with auxiliary input に基づき構成している。この構成要素に加え難読化技術なども用いて、不可逆漏洩に耐性をもつ署名方式を提案している。

第 5 章「Conclusion and Open Problems」では、本研究の成果についてまとめ、今後の研究課題について述べている。

以上をまとめると、本論文は、 FSP署名方式と通常のSP署名方式との今まで知られていなかった関係を示し、FSP署名を構成する一般的な方法を提案している。ここで示された関係は、理論的に精密な議論を行うことによってはじめて得られるものである。さらに、非常に強い安全性を持つ、初めての不可逆関数漏洩に耐性を持つ署名方式を提案している。よって、本論文は博士(理学)の学位論文として十分価値があるものと認める。