論文 / 著書情報
Article / Book Information

題目(和文)	
Title(English)	Multi-Divisible On-Line/Off-Line Cryptography
著者(和文)	山本暖
Author(English)	Dan Yamamoto
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11255号, 授与年月日:2019年9月20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,田中 圭介,笠井 健太
Citation(English)	Degree:Doctor (Engineering), Conferring organization: Tokyo Institute of Technology, Report number:甲第11255号, Conferred date:2019/9/20, 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		山本　暖	
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	笠井　健太	准教授
	審査員	植松　友彦	教授			
		山田　功	教授			
		田中　圭介	教授			

論文審査の要旨（2000 字程度）

本論文は，「Multi-Divisible On-Line/Off-Line Cryptography（多重分割可能オンライン/オフライン暗号方式)」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，IoT（Internet of Things）に代表される環境において，計算量や帯域幅に制限のあるデバイスが，通信の機密性と真正性を効率的に確保することの必要性を述べている．次に，既存のオンライン/オフライン暗号方式がそうした制限付きデバイスの安全性向上に有効であることを示した上で，種々のオンライン/オフライン暗号方式を統一的に議論，構築するための枠組みが欠如していることを課題として設定している．そして，その解決策として「多重分割可能オンライン/オフライン暗号方式」のコンセプトを提案し，当該コンセプトから導出可能な具体的な暗号方式の概要を示している．

第 2 章「Definitions（定義)」では，本論文を通じて参照される記法や暗号プリミティブの定義を概説している．

第 3 章「Framework of Multi-Divisible On-Line/Off-Line Cryptography（多重分割可能オンライン/オフライン暗号方式の枠組み)」では，多重分割可能オンライン/オフライン暗号方式のコンセプトを詳細に論じている．具体的には，計算量の最適化を可能とする incremental processing（暗号化などのアルゴリズムを複数のサブアルゴリズムに分割した上で，それらを異なるフェーズやデバイスで逐次実行可能にする特徴）と，帯域幅の最適化を可能とする incremental sending（分割されたサブアルゴリズムの出力を逐次送信可能とする特徴）を提案している．さらに，これらの特徴を有する方式の具体例として，分割可能オンライン/オフライン KEM（Key Encapsulation Mechanism）および分割可能オンライン/オフラインタグベース KEM を示している．

第 4 章「Multi-Divisible On-Line/Off-Line Encryptions（多重分割可能オンライン/オフライン暗号)」では，incremental processing と incremental sending の両特徴を有する公開鍵暗号を初めて定式化している．また，マルチユーザ環境で想定される脅威を包括する複数の安全性定義を，逐次送信の段数，ユーザ数，ユーザ毎のチャレンジクエリ回数，の 3 つのパラメータを用いて詳細に定義した上で，それら複数の安全性の間に成立する implication / separation の関係を証明し，達成すべき安全性を特定している．さらに，当該安全性を満たす具体的な方式の構成方法を示している．

第 5 章「Incrementally Executable Signcryptions（逐次実行可能署名付暗号)」では，incremental processing の特徴を有する署名付暗号を初めて定式化し，その安全性を機密性と真正性の両面で詳細に定義するとともに，安全な構成方法を示している．

第 6 章「Multi-Divisible On-Line/Off-Line Signcryptions（多重分割可能オンライン/オフライン署名付暗号)」では，逐次実行可能署名付暗号の一般化として，incremental processing と incremental sending を共に有する初めての署名付暗号を定式化し，機密性および真正性の安全性定義を複数定義した上でそれらの関係を明らかにしている．また，最も高い安全性を有する具体的な方式を，分割可能オンライン/オフラインタグベース KEM，分割可能オンライン/オフライン署名，DEM（Data Encapsulation Mechanism）から構成し，クラウドコンピューティング，モバイルコンピューティング，IoT デバイスの三者を用いた実装例における計算量および帯域幅を評価することにより，既存方式に対する優位性を示している．

第 7 章「Conclusion（まとめ)」では，本論文の成果を要約している．

以上を要約すると，本論文は，既存のオンライン/オフライン暗号方式を一般化した多重分割可能オンライン/オフライン暗号方式の提案と共に，その具体例として多重分割可能オンライン/オフライン公開鍵暗号，逐次実行可能署名付暗号，多重分割可能オンライン/オフライン署名付暗号を定式化し，それらの安全性に関する詳細な解析と，実用的な構成方法を示したものであり，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．