

論文審査の要旨および学識確認結果

報告番号	甲 第 号	氏 名	Corena Bossa, Juan Camilo
論文審査担当者：	主査	慶應義塾大学教授	博士(工学) 大槻 知明
	副査	慶應義塾大学教授	工学博士 笹瀬 巖
		慶應義塾大学教授	博士(工学) 寺岡 文男
		慶應義塾大学教授	博士(工学) 重野 寛
(論文審査の要旨)			
Bachelor of Systems and Computer Engineering, Master in Engineering, Juan Camilo Corena Bossa 君提出の学位請求論文は、「Improvements on Aggregation and Security of Encoded Data for Information Transmission, Processing and Reliable Data Storage (情報伝送, 処理, 及び信頼できるデータ保存のための符号化データの集約及び安全性の改善)」と題し, 全6章から構成されている。 近年, ネットワークを流れるトラフィックが急増している。ネットワークのスループットを改善する手法として, 複数の異なるノードからの情報をアナログあるいはデジタルで足し合わせて伝送し, 受信側では, 別途受け取っている一部ノードからの情報を用いて, 全ての情報を取り出すネットワーク符号が注目されている。一般に情報はセキュリティの目的で暗号化される。しかし, 転送される情報を加算するネットワーク符号では, 情報に対する攻撃を検出できないといった問題がある。 また, 近年, クラウドサービスの普及にともない注目されているセキュリティとして, サーバがデータを正しく保管しているかどうかをユーザが確認する問題がある。その際, 通信コストなどから, 全てのデータをダウンロードすることなく確認することが求められる。 本論文では, 情報伝送, 処理, 及び信頼できるデータ保存のための符号化データの集約及び安全性の改善に関する種々の方法を提案している。 第1章は序論であり, ネットワーク符号とその応用例, それに対するセキュリティ問題を説明している。また, 認証者が, サーバが正しくデータを保存しているかを確認できる PDP (Proof of Data Possession) プロトコルの概念を説明している。そして, 本研究の目的と意義を述べている。 第2章では, ネットワーク符号に対し, 不正なパケットを導入するポリューション攻撃を説明し, その影響の低減法を提案している。また, 低減法を分散的に実現する方法も提案している。 第3章では, 再生成符号を用いて符号化されたデータの PDP を取り扱っている。クラウドストレージサービスに見られるように, 認証者はサーバに保存されたデータが正しく保存されているかどうかを, 保存されているデータ全てにはアクセスすることなく確認する必要がある。これに対し, 符号化に用いられた符号語を検査することで実現する手法を提案している。また, 正しく保持されていない場合, どのブロックが失われているかを見つける手法を提案している。 第4章では, まず, ネットワーク符号において, 中継ノードである攻撃者がネットワーク符号化を正しく行わない新たな攻撃であるダイバースチ攻撃を取り扱っている。この攻撃に対し, 送信情報長がパケット長に依存するのではなく, ネットワーク符号のパラメータに依存する特徴を用いた検出法を提案している。また, ネットワーク符号において, ノードが復号できなかったパケットをバッファしない場合に想定される復号可能性攻撃 (Decodability Attack) に対する解決法も提案している。 第5章では, サーバで暗号化されたデータを処理する際に, 暗号化されたデータを復元することなく処理する問題について取り扱っている。これを実現するために, 多項式補間や準同型 (Homomorphic) 暗号化を用いた手法を提案している。 第6章は結論であり, 本論文で得られた結果を総括している。 以上, 本論文の著者は, 情報伝送, 処理, 及び信頼できるデータ保存のための符号化データの集約及び安全性の改善に対し種々の方法を提案し, その有効性を明らかにしており, 工学上, 工業上寄与するところが少なくない。よって, 本論文の著者は博士(工学)の学位を受ける資格があるものと認める。			
学識確認結果	学位請求論文を中心にして関連学術について上記審査会委員で試問を行い, 当該学術に関し広く深い学識を有することを確認した。 また, 語学 (英語) についても十分な学力を有することを確認した。		