様式第８号（第１８条，第３６条関係）

学位論文審査結果の概要

氏　　名	楊 鵬 (Yang Peng)（ヤン ホウ）
学位論文審査委員氏名	委員長　　銭谷　勉
	委　員　　金本　俊幾
	委　員　　丹波　澄雄
	委　員　　阿布　里提
	委　員　　官　　国清
	委　員　　長瀬　智行
論　文　題　目	Research on Signal Processing for a Virtual Optical Encryption System （仮想光暗号化システムの信号処理に関する研究）

審査結果の概要（2,000 字以内）

本学位論文は、深海調査の通信に適用可能な水中通信用仮想光ホログラフィック暗号化（VOHE: Virtual Optical Holographic Encryption）システムについて研究した論文である。光および音響信号に基づいたホログラフィック情報を暗号化する新しい方法を提案している。

提案システムでは、光信号や音響信号などの伝送メディアを、オブジェクト情報を受信機に伝送する干渉縞パターン（IFP: Interference Fringe Pattern）を送信する手段として利用している。光信号は物体情報を暗号化するために使用され、暗号化された信号は音響信号によって伝送される。その後、信号は長距離伝送のために音響チャネルに送信される。この VOHE は、COMSOL Multi Physics シミュレータを用いてシステムを構築している。光暗号化システムにおいて、暗号化および復号化の鍵であるフーリエレンズの伝搬波長（λ）や焦点距離（f）などは安全な通信を構築するための重要なパラメータである。従来の VOHE システムで暗号化された信号は、対称鍵暗号化方式に基づいていた。この方法では、送信者と受信者の 2 人のユーザーにより事前に VOHE システムの鍵（λ, f）が選択され、VOHE システムの鍵を使用してパブリックチャネルを介してシステムの暗号である IFP を送信する。ユーザーはシステムの鍵を定期的に交換できる。ただし、VOHE システムは、鍵交換プロセス中にシステムの鍵を失う可能性がある。この問題を解決し、VOHE のセキュリティを強化するために、Diffie-Hellman（DH）アルゴリズムと Rivest, Shamir and Adleman（RSA）アルゴリズムを複合して用いている。

本研究では、2 つの暗号化システムが導入されている。1 つは拡張 RSA（ERSA）アルゴリズムと呼ばれる RSA アルゴリズムであり、2 つ目は拡張 Diffie-Hellman（EDH）アルゴリズムと呼ばれる DH アルゴリズムである。どちらのシステムも、ERSA アルゴリズムのシステム鍵（λ, f）や EDH アルゴリズムの暗号化ホログラフィック情報などの重要なデータを送信するために、それぞれ複素関数を使用している。

提案された ERSA アルゴリズムと EDH アルゴリズムの効果が拡張ポラード・ロー法を用いて評価されている。その結果、VOHE システムでは、ERSA アルゴリズムと EDH アルゴリズムが、データ送信のセキュリティを強化するためにより適切な方法であることが示されている。また、受信信号の精

度が最小平均二乗誤差（MMSE: Minimum Mean Square Error）を用いて評価されており、VOHE システムをホログラフィック暗号化のみを使用する従来のシステム（フーリエレンズなし）と比較した結果、VOHE システムの精度は従来のシステムよりも優れていることが示されている。

最後に、米国国立標準技術研究所（NIST）の方法を用いて、提案された ERSA および EDH アルゴリズムを評価している。その結果、ERSA アルゴリズムと EDH アルゴリズムの両方が、それぞれ従来の RSA と DH アルゴリズムよりも優れたセキュリティ効果を有することが示されている。

本論文は英語で書かれており全部で 6 章から構成されている。

第 1 章では、暗号システムを考慮した光情報セキュリティの概要と背景を示し、この技術に関する基本的な理論を総括している。

第 2 章では、VOHE システムの暗号化、復号化プロセス、RSA アルゴリズム、および DH アルゴリズムの概要を示し、COMSOL Multi physics を用いた VOHE システムの暗号化および復号化プロセスのシミュレーション、および評価を行っている。

第 3 章では、ERSA 暗号化アルゴリズムの概要を示し、拡張ポラード・ロー法によって提案された ERSA アルゴリズムのセキュリティを評価している。評価プロセスの例により、ERSA 暗号化アルゴリズムがシステム情報（λ, f）（たとえば、λ = 632.8 nm、f = 4.20 mm）を受信機に送信する方法を示している。

第 4 章では、EDH 暗号化アルゴリズムの概要を示し、提案された EDH アルゴリズムのセキュリティを、拡張ポラード・ロー法を使用して評価している。また、送信者と受信者の間で共有鍵を生成する EDH 暗号化アルゴリズムの実行例を示している。

第 5 章では、元のコードと取得したコード間で平均二乗誤差を計算し評価している。 データ送信の乱雑性を NIST のテストスイートを用いて評価し、提案した EDH アルゴリズムと ERSA アルゴリズムの有効性を示した。

第 6 章では結論を示し、課題と将来の展望について述べている。

第 1 回審査会において、予備審査での指摘事項を含めた論文審査および専門分野における口述試験を行った。さらに博士論文公聴会において、論文内容の発表後および質疑応答を行った。本研究は情報セキュリティ分野において有用であり、総合的に判断した結果、論文審査および口述試験において合格と判定する。

学位論文の基礎となる参考論文

（1） Y. Peng, T. Nagase, T. Kanamoto, T. Zeniya and S. You, “A Virtual Optical Holographic Encryption System Using Expanded Diffie-Hellman Algorithm,” IEEE Access, Vol. 9, pp. 22071-22077, 2021.

（2） Y. Peng, T. Nagase, S. You and T. Kanamoto, “A VOHE System for Underwater Communications,” Electronics, Vol. 9, No. 10, 1557, pp. 1-13, 2020.

（3） Y. Peng, T. Nagase and T. Kanamoto, “An Optical Encryption Digital Holographic System Based on RSA Algorithm,” Information: an international Interdisciplinary journal, Vol. 23, No. 2, pp. 139-147, 2020.

（4） Y. Peng and T. Nagase, “Analysis of a Virtual Optical Encryption Holographic System: Decrypted code using the multiple-bit virtual optical encryption holographic system based on the COMSOL Multiphysics,” Proceedings of the 6th IEEE International Conference on Systems and Informatics (ICSAI), pp. 799-803, 2019.