審 査 の 結 果 の 要 旨

氏　　名　　原 田 邦 彦

本論文は、「安全な線形ネットワーク符号化」と題し、５章から構成されている。インターネットを始めとするコンピュータネットワークでは、通信路とその接続点であるコンピュータをそれぞれ枝と点としてモデル化するとき、各点において情報の符号化／復号化を行なうことができる。そのような符号化はネットワーク符号化と呼ばれ、符号化を行なわない場合に比べて、ネットワークを通してより多くの情報を伝送することが可能となる。本論文では、盗聴者がネットワークの幾つかの枝を盗聴する場合でも安全に情報が伝送できるネットワーク符号の構成法を取り扱っており、これらに対して新しい知見を与えている。

第１章「序論」では、ネットワーク符号に対する研究の背景と目的を述べると共に、従来研究に対する本研究の位置付けを与えている。また、本論文の構成を示している。

第２章「ネットワーク符号化」では、従来知られているネットワーク符号に関する重要な知見をまとめている。具体的には、全ての受信点に同じ情報を伝送するマルチキャスト通信に対して、伝送可能な情報量の上限を与える符号化定理、その上限を達成する線形ネットワーク符号の構成方法、その符号化に必要な有限体サイズなどの既知の結果をまとめている。

第３章「盗聴者に対して安全なマルチキャスト通信」では、マルチキャストネットワーク符号化おいて、枝に盗聴者が存在しても安全に情報が伝送可能となるネットワーク符号について論じている。ある閾値以下の本数の枝が盗聴されても、伝送している情報が全くもれないネットワーク符号化法は既に知られているが、従来の符号化法では閾値以上の本数の枝が盗聴されたときに、伝送している情報の一部が完全に盗聴者に漏洩する危険があった。それに対して、本論文では、閾値以上の本数の枝が盗聴されても、盗聴者に対して全情報の曖昧さは減少して行くものの、一部の情報が完全に漏洩することのない強い情報秘匿特性を定義し、その実現法を明らかにしている。具体的には、強い情報秘匿特性を線形符号で実現するためのネットワーク符号構成法を与えると共に、安全でない線形ネットワーク符号を利用して、強い情報秘匿特性を実現するための線形変換法を与えている。その結果、強い情報秘匿特性を実現する場合でも、従来の弱い情報秘匿特性の場合と同じ情報量を、ネットワークを通して伝送可能なことを明らかにしている。さらに、強い情報秘匿特性を持つネットワーク符号を実現するために必要な有限体サイズを評価している。また、直接ネットワーク符号化で利用していないネットワーク内の余剰な枝を利用することにより、さらに多くの情報を安全に伝送可能なことを示し、その伝送可能な情報量を与えている。

第４章「個別情報と共通情報の分離符号化と安全な符号化への応用」では、２つの受信点に共通情報を送ると共に各受信点にそれぞれ個別情報を送る一般の通信問題を取り扱っている。従来知られているネットワーク符号化法では、個別情報と共通情報を分離して符号化できないため、第３章で取り扱ったような情報秘匿特性を実現することができない。本論文では、２つの個別情報と共通情報を伝送するパスをネットワーク上で完全に分離し、かつ伝送可能な情報量の上限を線形ネットワーク符号で実現できることを、具体的な符号構成アルゴリズムを与えることにより証明している。この結果、

２つの個別情報はネットワーク符号化を行なうことなくルーティングだけで伝送でき、共通情報はマルチキャスト通信用のネットワーク符号を利用すれば実現できる。さらに、第３章で示した情報秘匿特性を、２つの個別情報と共通情報にそれぞれ独立に安全性パラメータを設定して適用することが可能となっている。また、必要な有限体サイズも従来方式に比べて小さくなる特長がある。

第５章「結論」では、本論文の成果をまとめると共に、今後の研究課題を示している。

以上を要するに、本論文は、情報理論やグラフ理論などの数理情報学的手法を用いることにより、より安全で性能のよいネットワーク符号の構成法を明らかにしており、その成果は、数理情報学分野、特にネットワーク符号および暗号情報セキュリティ分野における理論研究の進歩に大きく貢献している。よって本論文は博士（情報理工学）の学位請求論文として合格と認められる。