論文審査の結果の要旨

氏名　　川合　豊

本博士論文は大きく 3 部 9 章からなり，第一部は研究の位置づけについて，第二部は様々な拡張された公開鍵暗号技術の安全性の定式化，およびその安全性を達成する具体的方式の設計，第三部は公開鍵暗号とデジタル署名方式における証明不可能性について述べられている． 本研究の目的は様々な公開鍵暗号技術における安全性証明をより厳密なものにすることにある．1976 年に Diffie らによって公開鍵暗号の概念が提唱されて以来，公開鍵暗号やデジタル署名をはじめとする公開鍵暗号技術が提案されており，新しい暗号技術の提案には，その安全性を数学的に証明することが必要不可欠である．暗号方式の安全性証明には帰着技法が広く使われている．これは，暗号方式 S に対する攻撃者 A が存在したと仮定すると，計算量的に困難とされているある特定の問題 P が計算可能となってしまうことを示す証明手法である．この場合，問題 P が計算困難であることから攻撃者 A の存在は否定され，方式 S の安全性が証明される．帰着技法で証明された方式の安全性レベルは，(a) 攻撃者 A の攻撃の種類と程度，(b) 問題 P の困難さ，(c) 証明を行った際のモデル，の 3 点から考察される．(a) はより強い攻撃者に対し安全性が証明できたほうが望ましく，(b) については，より解読が難しいとされている問題を安全性の根拠に置くほうが望ましい．また(c)は，安全性証明を行う際に現実の環境に近い状況を想定したほうが望ましい．しかし，提案されている方式のほとんどは，証明を容易にする目的や，設計者が証明を構成できないなどの理由から，この条件を満たしているとは言えない．また，証明する安全性が高くなればなるほど，また対象とする方式が高機能化すればするほど証明は複雑になっていく．また高機能な方式は安全性の定義自体に改良の余地がある場合も多い．本論文は上記の問題に対し二方面から研究を行った．第二部においては，様々な拡張された公開鍵暗号技術の安全性の定式化は非常に重要な研究であると考え，安全性定義の定式化とその実現方式を示した．具体的には匿名認証方式の一つである Secret Handshake（三，四章）と公開鍵暗号の拡張である代理再暗号化（五章）に対して研究を行った．Secret Handshake とは，グループに所属しているユーザ同士が認証を行い，互いに自らのグループを明かすことなく相手と同じグループに所属しているかを認証する方式である．これに対して，(1)ユーザが複数のグループに所属しているケースを対象とした既存研究の安全性証明の誤りを指摘し，その修正を行った．(2)通常の Secret Handshake はグループに対する匿名性のみを扱うのに対し，ユーザ ID の匿名性を考慮した新たな匿名性を定式化し，それを満たす方式を提案した．代理再暗号化とは，暗号文受信者が復号鍵を渡すことなく他のユーザに暗号文の復号する権利を譲渡することが可能な方式である．これに対して，強い攻撃方法である選択暗号文攻撃

に対して安全な方式をどのように設計すればよいかを分析し，閾値暗号の特性を利用できることを発見した．そして既存研究よりも高い安全性を証明可能な方式を設計した．第三部においては，既存の証明不可能性技法を拡張しいくつかの結果を得た．安全性の定式化や安全性の根拠となる数論仮定によっては安全性証明が不可能である事がある．もし証明不可能であることを示すことができたならば，証明可能な方式設計に有益な情報となる．そこで，メタ帰着技法という証明不可能性技法に着目しその拡張と様々な方式への適用を行った．具体的には，(1)素因数分解問題に基づく方式において，合成数のみを公開鍵とするケースではあるレベル以上の安全性が証明できないこと，離散対数問題に基づく方式において，離散対数問題のみならず Diffie-Hellman 型の数論仮定を用いて安全性証明を行う場合，ある証明方針では証明不可能であること（六章），(2)全てのユーザが全く異なる公開鍵を所持する公開鍵暗号方式は，非常に強い選択暗号文攻撃に対して安全性は証明できないこと，また安全な方式を設計するためには，一部同じパラメータを全てのユーザに共有させる必要があること（七章）を示した．

本論文第三章は，丹野 翔太郎，近藤 崇裕，米山一樹，太田和夫，國廣昇との共同研究，第四章は米山一樹，太田和夫，國廣昇との共同研究，第五章は，花岡悟一郎，國廣昇，松田隆宏，翁健，張鋭，趙運磊との共同研究，第六章は太田和夫との共同研究，第七章は，坂井祐介，太田和夫，國廣昇との共同研究，第八章は花岡悟一郎，太田和夫，國廣昇との共同研究であるが，論文提出者が主体となり貢献を行っており，論文提出者の寄与が十分であると判断する．

したがって，博士（科学）の学位を授与できると認める．

（以上１９９４文字）