研究課題別評価

1. 研究課題名 :情報理論的に安全な秘密鍵共有法

2. 研究者氏名 :水木　敬明

3. 研究の狙い：

秘密鍵を共有したい k 人のプレーヤーがいるとし、プレーヤー間の通信は無制限の計算能力をもつ盗聴者によって盗聴されているとする。このような k 人のプレーヤーが絶対に安全な共通の秘密鍵を共有できるには、どのような条件が必要かについて解明することが、本研究の大きな目的である。例えば、あらかじめプレーヤーにカードをランダムに配布し、そのカードを使って秘密鍵を共有できることが知られている。カードのランダム配布は、プレーヤーにあらかじめ与える入力としての一例であり、極めて単純なモデルのひとつである。カードのランダム配布を用いて秘密鍵を共有するためのプロトコルがいくつか開発されているが、秘密共有に必要な最小なカード配布枚数は見付かっておらず、そのような枚数を見付けることは長年の未解決問題である。本研究では、既存のプロトコルを改良し、より少ない枚数で秘密鍵を共有できるプロトコルを与え、未解決問題のギャップを縮める。また、プレーヤーへの入力として、部分秘密鍵共有グラフというものを定義し、その下でのプロトコルを開発する。さらに、得られた手法を別の問題に応用する。

4. 研究結果：

(1) カードのランダム配布による秘密鍵共有

カードのランダム配布を利用した秘密鍵共有プロトコルとして、変換プロトコルと呼ばれるものが知られている。この変換プロトコルは、カードの配布が入力されると、分割と結合を繰り返すことにより、1 ビットの秘密鍵を複数生成し、秘密鍵共有を実現するものである。変換プロトコルが成功するためのカードの配布枚数に関する十分条件は知られていたが、必要十分条件については知られておらず、未解決問題であった。本研究では、まず、変換プロトコルの改良を行った。改良点は、無駄な分割を無くすことと、鍵集合プロトコルと呼ばれるプロトコルの手法を応用し、特殊な配布枚数の場合にはその手法により分割を行うこと、および結合のときにダミーカードを追加することにより、使用されず無駄になっていたカードを活用したことである。これらの改良により、より少ない枚数でのプロトコルの実行が可能となった。また、この改良変換プロトコルが成功するための必要十分条件を発見した。この結果、長年の未解決問題が解決し、変換プロトコルの潜在的な能力がわかった。

また、階層構造を有するプレーヤーに適した秘密鍵共有を行うプロトコルが成功するための必要十分条件を与えた。階層構造を有する 2 個のグループがあり、各プレーヤーそれぞれが 1 つのグループに属しているとする。Igarashi らは、2000 年に、このような階層構造に適した秘密鍵共有グラフとして、2 レベル木というものを定義し、そのようなグラフを構成するためのプロトコルを与えた。また、そのプロトコルが成功するための必要なカードの枚数に関する十分条件を見付けている。しかし、必要十分条件については知られていなかった。本研究では、この未解決問題に取り組み、必要十分条件を求めることに成功した。

さらに、量子暗号を応用することによってカードの配布を行う手法を提案した。

⑵部分秘密鍵共有グラフからの秘密鍵共有

プレーヤーを点とし、秘密鍵を共有しているプレーヤーの対を辺として得られるグラフを秘密鍵共有グラフと呼ぶ。グラフの辺に対応する秘密鍵のうち、いくつかが盗聴者に知られているとする。このようなグラフを部分秘密鍵共有グラフと呼ぶことにする。部分秘密鍵共有グラフを入力として、プレーヤーで安全に秘密鍵を共有する問題を扱い、そのような秘密鍵共有を実現するプロトコルを与えた。

この問題は、次のような問題のモデル化になっている。プレーヤー対が秘密鍵を共有するとき、それぞれのプレーヤー対で暗号アルゴリズムや物理的状況、あるいは時間的状況が違うため、盗聴者が全てのプレーヤー対の秘密鍵を知っていると仮定することは非現実的である。例えば、あるプレーヤー対が共有した秘密鍵は、暗号アルゴリズムが弱かったため解読されるかもしれないが、別のプレーヤー対の秘密鍵は、強力な暗号アルゴリズムにより作られたため解読てきないかもしれない。したがって、秘密鍵共有グラフの中で、全ての辺に対応する秘密鍵が盗聴者によって知られているとは仮定せず、一部の秘密鍵だけが知られていると仮定することは妥当である。

盗聴者がどのように秘密鍵を知っているかについて、『それぞれの秘密鍵はある確率分布に従い盗聴者に知られている』と『任意のたかだか t 個の秘密鍵が盗聴者に知られている』の2つの場合を考え、それぞれのモデルに対してプロトコルを設計し、理論的限界を求めることに成功した。

⑶電子透かしの安全性指標

上記の秘密鍵共有の研究で得られた手法を応用し、電子透かしの安全性評価に関する研究に取り組んだ。電子透かしは、配布したい電子ファイルに電子透かし情報を埋め込むことにより、不正コピーを防ぐために利用される。個々の電子ファイルにそれぞれ異なった電子透かし情報を埋め込む場合を扱い、本研究では、電子透かしとして埋め込むコードについて、どのようなものが適切なのかを評価する指標を与えた。不正コピーが発見されたとき、そのコピーに埋め込まれた電子透かし情報から犯人が特定できることが望ましいが、一般に、確実に犯人を特定することは不可能であることが示されている。そのため、本研究では、まず、q 人中、少なくとも p 人は犯人であることが言えるとき、そのコードは (p/q)-安全であると定義した。次に、そのようなコードを構築するとともに、コードの長さに関する下界の証明を行い、その理論的限界を示した。

5. 自己評価：

本研究では、情報理論的に安全な暗号の実現の条件に関する基礎的な研究を行った。ひとつのモデルとして、カードのランダム配布による秘密鍵共有問題を扱い、そのような秘密鍵共有を実現できる効率的なプロトコルを開発し、また、必要な配布枚数の下界を理論的に示すことにより、秘密鍵を共有することのできる配布枚数と、できない配布枚数の完全な特徴付けを目指したが、未だ完全な特徴付けには至っていない。今後の展開としては、そのような完全な特徴付けを与えることが挙げられる。それにより、カードのランダム配布が潜在的に持つパワーの完全な解明を目指す。

また、本研究では、部分秘密鍵共有グラフからの秘密鍵共有という問題を扱い、いくつかのモデルを与え、安全な秘密鍵を共有するためのプロトコルを提案した。たかだか t 個の秘密鍵が盗聴者に知られているというモデルにおいては、未解決問題が残されており、今後の課題である。

本研究では、盗聴者に知られている秘密鍵を、確率分布としきい値でモデル化したが、より現実に即したモデルを考案することも、今後の課題である。

今後の展開として、より一般に、個々のプレーヤーへの入力がどのような分布であれば秘密が共有できるのか、あるいは、与えられた入力では共有できないことを示す統一的手法の確立が挙げられる。

6. 研究総括の見解：

コンピュータネットワークがすでに社会基盤となっている現在、この高度情報化社会を安全・安心なものにするために、情報セキュリティや暗号の研究の重要性は益々高まっている。現在使われている暗号方式のほとんどは計算量的に安全なものであり、盗聴者の計算能力によっては、解読されてしまう。それに対し、水木敬明は、情報理論的に安全な暗号について研究し、いくつかのモデルに対してそのような暗号が実現できるための条件を理論的に与えていることは基礎研究として評価できる。ただし、実用化に向けては、少なからず距離があるため、今後はより実社会に適用可能な技術の研究・開発が望まれる。また、当該分野には未解決問題も多く、さらなる研究発展を期待する。

7. 主な論文等：

1. Takaaki Mizuki and Takao Nishizeki, Necessary and Sufficient Numbers of Cards for Sharing Secret Keys on Hierarchical Groups, IEICE Trans. Inf. & Syst., Vol.E85-D, No.2, pp.333-345, 2002.
2. 小泉康一, 水木敬明, 西関隆夫, 量子カード配布, 電子情報通信学会論文誌A, Vol.J86-A, No.4, pp.465-473, 2003.
3. Shingo Orihara, Takaaki Mizuki, and Takao Nishizeki, New Security Index for Digital Fingerprinting and its Bounds, IEICE Trans. Fundamentals, Vol.E86-A, No.5, pp.1156-1163, 2003.
4. Takaaki Mizuki and Takao Nishizeki, Necessary and Sufficient Numbers of Cards for Sharing Secret Keys on Hierarchical Groups, Proc. ISAAC 2001, Lecture Notes in Computer Science, Springer-Verlag, Vol.2223, pp.196-207, 2001.
5. Koichi Koizumi, Takaaki Mizuki, and Takao Nishizeki, Necessary and Sufficient Numbers of Cards for the Transformation Protocol, 2003 Japan-Korea Joint Workshop on Algorithms and Computation, pp.124-137, 2003.