第4回 国際コミュニケーション基金優秀研究賞

本賞は、当財団の助成を受けて調査研究を実施された方の中から、優秀な成果を発表された方を表彰するために設けられました。第4回の受賞者は、審査委員会の審議を経て平成17年11月15日に開催された第63回理事会において、以下の通り決定されました。

「絶対に安全な秘密鍵共有の通信プロトコル」

研究概要：何人かのプレーヤーが通信を用いてカードゲームを行う際、無制限の計算能力をもつ盗聴者に対して、情報理論的に安全な秘密鍵をプレーヤー間で共有したい。プレーヤーにカードをランダムに配布し、そのカードを用いて秘密鍵を共有できることは知られていたが、カードの最少配布枚数を特定することは長年にわたり未解決の問題であった。本研究ではこの難問を解決すると共に、新しいプロトコルを設計し、カードゲームを実行したときに共有できる秘密鍵のビット数を求めることに成功した。

研究代表者：西関 隆夫　東北大学大学院情報科学研究科 教授
共同研究者：水木 敬明　東北大学情報シナジーセンター 助教授

絶対に安全な秘密鍵共有の通信プロトコル

東北大学大学院情報科学研究科 教授
西関 隆夫
東北大学情報シナジーセンター 助教授
水木 敬明

小学校の算数の問題

「整数35を素因数分解しなさい」

に対し、誰でも

$35=5\times7$

と直ちに答えることができます。では7桁の大きな整数2,795,519ならば、いかがでしょうか。2,795,519は2で割り切れないから、2は因子ではない。3でも割り切れないから、3も因子でない。4でも割り切れないので、4も因子でない。5でも割り切れないから、5も因子でない。このように小さい数字から順々に割り切れるかどうか根気よく試していけば、683でやっと割り切れることがわかり、

$2,795,519=683\times4,093$

と素因数分解が求まります。このように計算時間を気にしないならば、どんな大きい整数でも素因数分解を求めることが原理的にはできます。しかし、300桁もの大きい整数になると、スーパーコンピュータで10年間計算しても素因数分解を求めることが(計算量的に)困難になります。

今日、安全に通信するために暗号が用いられていますが、現在利用されている暗号のほとんどは、その安全性の根拠を上に述べた素因数分解の計算量的な困難さ等に依存しており、解読アルゴリズムの発見やコンピュータの高速化などにより、将来にわたり安全であるとは言えません。それに対して、本研究では、絶対に安全な暗号に取り組んでおります。これは、情報理論的に安全な暗号とも呼ばれ、盗聴者がいかなる計算能力・計算資源を持とうとも、安全な暗号のことです。そのような暗号の送受信者AliceとBobは、二人だけが知っていて盗聴者には知られていない秘密の鍵を共有しないといけません。問題はいかにして秘密鍵を絶対に安全に共有するかです。計算量的に安全に秘密鍵を共有する場合とは異なり、絶対的に安全に秘密鍵を共有するためには、あらかじめAliceとBobに何らかの初期情報を与えておく必要があります。そのような初期情報の一例として、トランプのようなカードをAliceとBobにランダムに配布しておくことが考えられます。このため、カードのランダム配布によって秘密鍵を共有する問題が研究されてきましたが、未解決な問題が数多く残されておりました。本研究では、これらの重要な問題に取り組み、それらのいくつかを解決しています。

AliceとBobが秘密鍵を共有したいとしましょう(図1)。しかし盗聴者Eveがいて、スーパーコンピュータを1億台も持っており、無限の計算能力があるとします。そのため上述の初期情報(手品のタネ)が必要です。それがカードのランダム配布です。合計d枚のカードには1からdまでの異なる数字が書かれてあり、よくカードをきってから、Aliceにa枚、Bobにb枚、Eveにe枚配られてあったとします。つまり、盗聴者Eveは既にe枚のカードを盗

聴できているとします。このような状況下で、AliceとBobはある種のトランプゲームを行い、盗聴者Eveに知られないようにして、できるだけ長いビット数の秘密鍵を共有したいわけです。このトランプゲームのルールが「秘密鍵共有の通信プロトコル」です。

図1：新しいプロトコルによる鍵共有の流れ

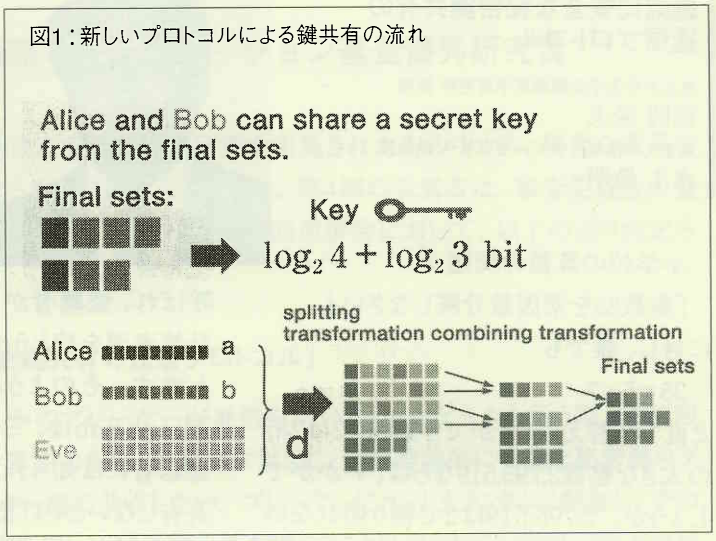
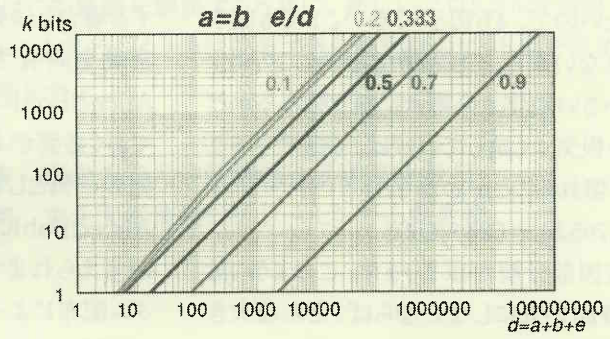


図2：配布枚数dと共有ビット数kの関係



本研究では、AliceとBobにできるだけ長いビット数の秘密鍵を共有させるために、新しいプロトコル(ゲームルール)を設計しました。詳細は省略しますが、AliceとBobは配られたカードを用いて、乱数を利用しながらトランプゲームを行い、盗聴者Eveのカードを含まないカードの山を作っていきます。図1にその流れを図示しました。それらの山からAliceとBobは秘密鍵を共有することができるわけです。

AliceとBobが共有できる秘密鍵のビット数は、むろん配布されたカードの枚数a, b, eに依存しますが、発生させる乱数の値にも依存します。本研究では、最も少ない場合のビット数kを、a, b, eから計算する式を求めることができました。したがって、最悪の場合でも、AliceとBobはkビット以上の秘密鍵を共有できることになります。また、その式が最良であることも示すことができました。ちなみに、a = bの場合には、合計枚数dに対する盗聴者Eveの枚数eの割合e/dをパラメータにすると、dに対してkは図2のようになることがわかりました。

この他にも本研究では、量子暗号を利用したメンタルポーカープロトコルを設計したり、結託攻撃に対する電子透かしの安全性の新しい評価基準を導入し、その安全性の限界を示したりしております。それらの詳細は紙面の都合で省略します。