論文の内容の要旨

論文題目　Bounds and Constructions for Mutually Distrustful Information Theoretically Secure Cryptographic Protocols
(情報論的に安全な暗号プロトコルの理論的考察)

氏名　ナシメント　アンダーソン

幾人かの参加者からの入力に対し、何らかの出力を行う計算を考える。このとき、各々が自分で入力したデータ（と出力）以外の情報を全く得ることができないように計算を実行する方法はあるだろうか。この方法を達成するタスク(Secure function evaluation (以下SFE)と呼ばれる)に関する研究は、現代暗号学における最も重要な課題の一つとなっている。一般に、もしいかなる仮定も用いなければ、SFE を達成することは不可能であることが知られている。しかしながらそれと同時に、その存在を仮定することができれば、安全な分散処理の能力を全て引き出すことができる多くの条件も知られている。例えば、上記の計算への参加者の過半数を信頼することができること、および、ブロードキャスト型の通信路を使用することができる、ということの二つが仮定できるとしよう。この場合、どのような関数に対しても、SFE が達成できることができることが知られている。さらに、もし計算量に対する制限を仮定することができれば、信頼できる参加者は過半数である必要もない。

本論文で考察されるのは、信頼できる参加者が過半数以下であり、かつ、計算量に対する制限も仮定できない状況である。従来、このような状況に対しては、各参加者に（何らかの方法で）予め分配されたなんらかのデータを使うことができる場合に、SFE のタスクを実行できることが示されてきた。Rivest は文献[1]の中で、ある特定のデータが事前に分配されていた場合、SFE を達成するために必要かつ十分な構成要素であるプロトコル、オブリビアストランスファ（OT）およびビットコミットメント（BC）を実装できることを証明した。また、Crepeau と Kilian は、参加者すべてが二元対称通信路によりお互いに通信することが可能であれば、OT と BC を効率的に実装することができるという驚くべき結果を証明した[2]。（ここで「効率的」とは、「高々多項式の通信回数によって」という意味である。）さらに、信頼できるセンターによって分配されたデータを使って、一般的な SFE を達成するプロトコルを非常に効率よく構成する方法が、Beaver によって提案された[3]。これらの結果は、極めて重要な結果であり、現代暗号研究にとって大きな貢献であることは間違いない。しかしながら、同時に、以下のような重大な問題は未整理のままであった。

- このようなシナリオで、二者間あるいは多者間の SFE を安全に行うための、事前に配布されたデータが満たすべき必要十分条件。
- 事前に分配されたデータや雑音のある通信路を資源としてSFEを達成する場合の効率。
- 従来提案された方式の改良の可能性。

本論文は、これらの問題について考察を行ったものである。本論文の構成は以下のようになっている。

第 2 章では、非自明な離散メモリなし通信路によって、コミットメント方式が実装できることを証明する。(従来研究はすべて、二元対称通信路について議論したものであることに注意してほしい。) さらに、雑音のある通信路の最も効率のよいコミットメント方式への利用法を議論し、Shannon 理論における通信路容量に相当する概念、すなわちコミットメント容量の概念を導出する。従来は、雑音のある通信路を使い一つのビットをコミットメントする方法（即ちビットコミットメント）が議論されてきたが、ここでは、大きなメッセージのセットから選んだ一つをコミットメントする、いわばストリングコミットメントが議論される。我々は、このコミットメント容量が、簡便な式で表現できること、さらにはこのコミットメント容量により、一般的な離散メモリなし通信路を完全に特徴付けられることを示す。また、これらの結果は、古典量子通信路の場合に拡張される。

第 3 章では、Rivest による事前に分散されたデータによるコミットメント方式[1]についてその限界を一般的に証明する。これは、文献[4]で提起された問題、即ち、Rivest の提案プロトコルが、その状況において、最も高い効率を達成したものであるかどうかという未解決問題への解答となっている。

第 4 章では、雑音のある通信路について、一般的にどのような雑音（より正確には、その相関）が OT（あるいはそれによって達成される SFE）を実装するための必要十分条件であるかという問題について考察する。これも、文献[2]で提起されて以来の未解決問題であった。我々は、非自明な雑音のある通信路であれば（それがどのようなものであっても)、それを利用することにより OT を達成することができることを証明する。

第 5 章では、もう一つの重要な分散型のプロトコルである紛失多項式評価（obivious polynomial evaluation 以下、OPE）について、事前に分散したデータを使ったシナリオを議論する。OPE を達成するために必要な通信量についてその下限を証明し、実際にその下限を達成できるプロトコル（即ち最適なプロトコル）を提案した。また、この下限についての結果から､OT の実装のために Rivest によって提案されたプロトコルが最適であったことが証明される。

第 6 章では、二者間の SFE を達成するための、相関のあるデータに基づいた一般的なプロトコルを提案する。これは、[3]で提案されているものより、簡便であり効率の意味でも優れたものになっている。続く第 7 章で、これを多者間の状況に拡張する。

参考文献

[1] Ronald L. Rivest, Unconditionally Secure Commitment and Oblivious Transfer Schemes Using Private Channels and a Trusted Initializer, pre-print.

[2] Claude Crépeau, Joe Kilian: Achieving Oblivious Transfer Using Weakened Security Assumptions (Extended Abstract) FOCS 1988: 42-52

[3] Donald Beaver: One-Time Tables for Two-Party Computation. COCOON 1998: 361-370

[4] Carlo Blundo, Barbara Masucci, Douglas R. Stinson, and Ruizhong Wei, Constructions and Bounds for Unconditionally Secure Non-Interactive Commitment Schemes, Designs, Codes, and Cryptography, Vol. 26, pp. 97--110, 2002.