

紛失通信方式の効率化の研究

プロジェクト代表者: 小柴健史 (理工学研究科・准教授)

1 はじめに

大規模コンピュータ通信ネットワークでの情報セキュリティ技術の一つにマルチパーティセキュア計算という概念があり、それは、各パーティの秘密は漏洩させずに各パーティの秘密を引数とする関数値を共有する技術である。更に、そのマルチパーティセキュア計算を実現させる要素技術の一つに紛失通信と呼ばれる暗号プロトコルが存在する。しかしながら紛失通信は他の暗号プロトコル(例えば、デジタル署名方式や公開鍵暗号など)とは異質であることが分かっているだけで究明が十分になされているとはいえない。そこで、効率的な構成方法の可能性も含めて紛失通信に関する理解を深めることが求められている。

2 研究目的

紛失通信には様々な変種が存在するが、(1,2)型紛失通信と呼ばれる方式では、送信者 S が二つの秘密 s_0, s_1 を持っているとし、受信者 R は一方の秘密 s_e だけを受信し他方の秘密 s_{1-e} の情報は一切得ることができない(この性質は送信者のプライバシーと呼ばれる)。さらに、送信者 S は受信者 R がどちらの秘密を得たのかを知ることが出来ない(この性質は受信者のプライバシーと呼ばれる)通信方式である。

一般的な仮定から紛失通信方式を構成することは、困難であると予想されている。本研究では、そのためのアプローチとして以下の二通りの考え方にしたがって研究を行う。(1) 紛失通信方式の間にも比較的単純な(秘密情報が各1ビットの(1,2)型)紛失通信とより難易度のある(秘密情報の長さが各 L ビットの(1,2)型)紛失通信方式があり、その間の帰着可能性については既に知られている。帰着にあたり、単純な方式をどの程度必要とするのか、その下限を見極めること。(2) 一般的な仮定からの構成は困難であると予想されているが、それでも根拠となる仮定を弱めることは安全性の観点から重要であり、既存の仮定を弱めること。

3 研究の進め方

(1), (2)とも数は多くないが既存研究が存在する。それぞれの問題点を究明しそれを克服するような新しい技術を開発することにより改善を行う。(1)においては、 L ビット(1,2)型紛失通信を構成するのに1ビット(1,2)型紛失通信を何回用いなければならないのかを議論している。とくに、毎回の1ビット(1,2)型紛失通信の呼び出しにより必要な情報量が秘密を保ったままどれだけ得られるのかを Shannon エントロピーを用いて議論している。Shannon エントロピーを利用することは常套手段ではあるが Shannon エントロピーは情報量の平均的な性質であり、理論的な限界を導出する道具としてはおのずと限界があることが想像できる。そこで、新しい組み合わせ論的な技法を導入することで、下限を改善することを試みる。(2)を考慮するにあたり、特殊な形の密な落し戸付き一方向性置換を用いることにより紛失通信方式が構成できることが既存技術として知られている。そこで、一方向性置換のどのような性質が本質的に利用されているのかを見極めて、それらの条件の緩和を試みる。また、暗号理論における様々な不可能性が存在しており、その不可能性に抵触しないような限界ぎりぎりまでの緩和が最善であることを念頭におく。

4 研究成果

(1)における従来結果, つまり, 秘密 s_0 と s_1 が1ビットの(1,2)型紛失通信を t 回用いて, 秘密 s_0 と s_1 を L ビット(1,2)型紛失通信を用いたとき, 回数 t の下限に関する従来結果は Micali & Dodis (EUROCRYPT 1999) による $t \geq 2L$ である. まず, 組み合わせ手法として数え上げ論法を活用し, L ビット紛失通信を構成するために必要な1ビット呼び出し回数 t の下限 $t \geq 2L - 1$ を導出した. 続いて, Bush bounds と呼ばれる orthogonal array に関する性質を利用して, $t = 2L - 1$ の不可能性を示し, これにより $t \geq 2L$ の下限を導出した. この結果は, 単なる下限の改善を意味するだけではなく, 紛失通信のある性質に関する分離を導いている. 紛失通信の基本性質として送信者と受信者がプロトコルに従うとき, プロトコルは正常に終了する. この性質は正当性と呼ばれる. 正当性は常に保証される場合 (強正当性) とそうでない場合 (弱正当性) に分けられる. またプライバシーも100%保証される場合 (強プライバシー) と, 非常に小さい割合でのプライバシー漏洩は認める場合 (弱プライバシー) とに分けられる. Crépeau & Savvides (EUROCRYPT 2006) は L ビットの(1,2)型紛失通信を構成するのに1ビットの(1,2)型紛失通信を $t \geq L$ 回呼び出しているが, Crépeau & Savvides のプロトコルは弱正当性かつ弱プライバシー型のプロトコルである. 今回の我々の下界証明での設定は, 強正当性かつ強プライバシーのモデルを採用しているため, この結果は自動的に, 強正当性+強プライバシー型の紛失通信と弱正当性+弱プライバシーとは本質的に異なることを導いている. [発表論文1]

(2)においての従来結果は, 密な落とし戸付き一方向性置換を利用した構成方法が最弱仮定であった (Haitner, TCC 2004) が, これの一般化を行った. 密な落とし戸付き一方向性置換が, 明示的あるいは非明示的に仮定していることとして, (a) 密であること, (b) 落とし戸付き, (c) 一方向性, (d) 長さ保存, (e) 逆像サイズ = 1, の条件がある. これらの条件を一つ一つほぼぎりぎりまで緩和することを行うと同時に, これらの条件はいずれも本質的には無くすることはできなくて, 緩和することしかできないことを導いた. とくに (d)に関して, 紛失通信は仮定無くしては公開鍵暗号あるいは落とし戸付き一方向性関数からはブラックボックス帰着できない (Gertner, Kannan, Malkin, Reingold & Viswanathan, FOCS 2000) という性質があり, (e) に関しては, 落とし戸付き一方向性関数は逆像サイズが指数的に大きいものならば一方向性関数から構成できること (Bellare, Halevi, Sahai & Vadhan, CRYPTO 1998) が既に示されており, このような結果に抵触することを確認した. [発表論文2]

5 発表論文

- [1] Kaoru Kurosawa, Wataru Kishimoto, Takeshi Koshihara, "A Combinatorial Approach to Deriving Lower Bounds for Perfectly Secure Oblivious Transfer Reductions", IEEE Transactions of Information Theory, Vol.54, No.6, pp.2566-2571 (2008)
- [2] Kai Yuen Cheong, Takeshi Koshihara, "Reducing Complexity Assumptions for Oblivious Transfer," 2008年暗号と情報セキュリティシンポジウム, SCIS 2008 (宮崎, 2008.1.23), 2E4-2.