紛失通信の効率化の研究

理工学研究科
小柴健史

紛失通信とは

- 二者間（AとB）のプロトコルで，
  - Aは2つのメッセージを持つが，一方だけしかBに伝えたくない．
  - Bは一つのメッセージは受け取るが，どちらを選択したかをAに伝えたくない．

紛失通信が存在すると

- 多者間で，個人情報を漏らさずに個人情報を入力とする関数評価（セキュア計算）ができる.

- 例えば，
  - AもBも年齢を明かすことなくどちらが年上か知ることができる.

紛失通信の構成は難しい

- 実用的なレベルのよい方法は知られていない.

- そもそも実現できるのか？
  - 構成可能性の限界？

2つの定義

- ビット紛失通信
  - Aの秘密は二つのビット
- 文字列紛失通信
  - Aの秘密は二つのビット列(共に，長さL)

2つの定義の関係

- ビット紛失通信を複数回用いれば，文字列紛失通信が構成可能.
  - では，最低限，何回用いる必要があるのか？

主な結果

- Lビットの文字列紛失通信を構成するのに，情報理論的に，2L回以上のビット紛失通信を用いなければならない.
  - 各紛失通信とも途中でエラーは起きないものとする.
  - 微小のエラーを許す場合には，より効率的に実現できる可能性あり.

参考文献

K. Kurosawa, W. Kishimoto, T. Koshiba:

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)