1. 21世紀初頭の暗号技術

6. 暗号プロトコルの基礎数理

黒澤　馨
茨城大学 工学部 情報工学科
kurosawa@cis.ibaraki.ac.jp

尾形 わかは
東京工業大学 理財工学研究センター
wakaha@craft.titech.ac.jp

日常生活においては簡単に実現できても，通信を介すると途端に難しくなってしまう問題が多く存在する．たとえば，選挙をインターネットを介して実現しようとすると，投票内容をどう秘匿するか（privacy），集計結果の正しさをどうやって検証するか（correctness）などの問題に直面してしまう．このような問題を暗号を利用して解決するプロトコルを，一般に暗号プロトコルという．

本稿では，マルチパーティ・プロトコルと呼ばれる汎用プロトコル，および任意の暗号プロトコルの基本構成要素と考えることができる紛失通信路に関し，最近の研究動向について解説する．また，零知識認証法およびビットコミットメントについても，併せて解説する．

マルチパーティ・プロトコル

以下のような問題を考えよう．$f(x_1, \cdots, x_n)$ を任意の関数とし，n 人の参加者 P_i は，それぞれ入力 x_i を持っている．このとき，x_i を秘密にしたまま，関数値 $y = f(x_1, \cdots, x_n)$ のみを計算したい．

このような計算は，信頼できるセンタ T を仮定すれば，容易に実現できる．まず，各参加者 P_i は x_i を T に送る．次に，T は y を計算し，その値を公開すればよい．これと同じ機能を，センタなしで（各参加者が協力して）実現するための（汎用の）プロトコルを，マルチパーティ・プロトコルという（**図-1**を参照）．

敵がコントロールできる参加者の人数を t としたとき，従来，以下の定理が知られている．

定理 1.1　以下の条件が成り立てば，任意の関数 f に対するマルチパーティ・プロトコルを構成できる．

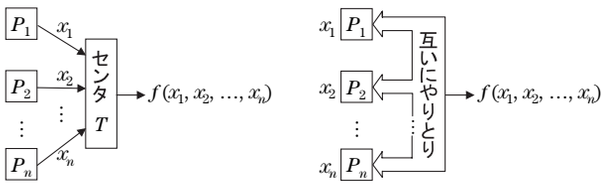
- 任意の2人の参加者間に秘密通信路が存在する場合，$n > 3t + 1$.
- 公開掲示板も利用可能な場合は，$n > 2t + 1$.

Ben-Or らによって示された以上の成果においては，プロトコルを単体で実行することを想定して，安全性が証明されている．しかし，現実には，ある暗号プロトコルを他の暗号プロトコルと組み合わせて実行したり，同一の暗号プロトコルの多くのコピーを同時並行的に実行したりする場合も多い．従来の枠組みでは，このような場合における安全性を証明できない．

この問題を解決すべく，universally composable（UC）security という新しい安全性の枠組みが Canetti によって提案され[1]，最近，活発に研究されている．ある関数 f をサブルーチンとして利用する関数 g の秘密分散計算を考えよう．UC 理論は，まず，各参加者に，関数 f を計算するセンタ F の呼び出しを許すプロトコル ρ^F を考える．ここで，F は，同時並行的に何回呼び出されてもよい．次に，センタ F の機能をシミュレートするプロトコル π を構成し，F を π で置き換えたマルチパーティ・プロトコル ρ^π を考える．このとき，ρ^F，および π が UC security を満たせば，最終プロトコル ρ^π も UC security を満たすことを証明できる．これを，composition theorem という．（なお，ρ^F および ρ^π は，関数 g の秘密計算を実現するプロトコルである）．

ここで UC security は，interactive な distinguisher ともいうべき environment によって定義される．この定義によれば，ある安全なマルチパーティプロトコルをもっと大きなプロトコルのサブプロトコルとしても利用しても，安全性を損なわないことを保証できる．詳細は，文献1）を参照されたい．

では，どのようなプロトコルが UC security を満たすのであろうか．**定理 1.1** は，同様に成り立つ．しかし，ビットコミットメント，零知識証明，コイン投げなどの2者間のプロトコルは，実現できない．一方，これら2者プロトコルも，共有乱数を仮定すると実現できる．



(a) 理想的モデル（センタ T を仮定）　(b) マルチパーティ・プロトコル（センタを仮定しない）

図-1　マルチパーティ・プロトコル

Oblivuous Transfer

Oblivious Transfer（OT, 紛失通信）と呼ばれる2者間のプロトコルを利用すると，汎用的なマルチパーティ・プロトコルを実現できることが知られている．また，オークション，RSA暗号の鍵2者生成，データマイニングなどにも利用されている．このように，OTは，暗号プロトコルにおけるある意味での最小単位と考えることができる．

最も基本的なOTの形式は，1ビットの1-out-of 2 OT（以下，(1,2)-OTと略記）であり，以下のような機能を実現するプロトコルである．アリスは2つの1ビットの秘密m_0, m_1を持っており，ボブは1ビットの秘密bを持っている．プロトコル終了後，ボブはm_bを取得する．しかし，

- ボブは，m_{1-b}についてまったく分からない．
- アリスは，bについてまったく分からない．

kビットの1-out-of n OT（以下，$(1,n)$-OT^{k}と略記）は，(1,2)-OTの自然な拡張として定義される．

文献2）に，OT関係の論文が網羅されているので，参考にされたい．

●計算量理論的仮定の下での実現法

以下のようなOTの一形態を，(1/2,1)-OTと略記することにしよう．ボブは，確率1/2でアリスの秘密mを取得でき，アリスは，ボブがmを取得したのかどうかまったく分からない．Rabinは，素因数分解の困難さに基づく(1/2,1)-OTを示した．これが，計算量理論的仮定の下でのOTの最初の実現法である．

一般に，(1,2)-OT^{k}においては，アリス，ボブのいずれか一方の計算能力は多項式時間に制限されていなければならない．ボブが多項式時間に制限されている方式として，離散対数問題の困難さやRSA暗号の安全性に基づく方式が知られている．一方，無限大の能力を有するボブも不正ができない $(1,n)$-OT^{k}は，準同型性を満たす公開鍵暗号を利用することにより構成できる．

では，一般に，公開鍵暗号を利用すれば，OTは構成できるのであろうか．この問に対し，Gertnerらは，OTと公開鍵暗号は，blackboxの意味で，相互に帰着できない，という否定的な結果を示した．

一方，BeaverおよびIshaiらは，一方向性関数の存在を仮定した場合，(1,2)-OT^{k}をt回利用することにより，(1,2)-OT^{k}をt^c回実現できることを示している（tはセキュリティパラメータ，$c > 1$は任意の定数）．

●OT Reduction

(1/2,1)-OT，(1,2)-OTおよび$(1,n)$-OT^{k}は，計算量的仮定なしに，すべて等価であることが知られている．このようなOT間のreductionの例として，(1,2)-OTを利用して(1,2)-OT^{k}を実現する方法のアイディアを紹介しよう．これは，zigzag関数$f(x_1, \cdots, x_l) = (y_1, \cdots, y_k)$というブール関数を利用し，(1,2)-OTを$l$ ($>k$) 回走らせることにより，(1,2)-OT^{k}を実現する．ここで，zigzag関数は以下のように定義される．

定義 2.1　以下が成り立つとき，ブール関数$f(x_1,\cdots, x_l) = (y_1, \cdots, y_k)$は$I = \{i_1,\cdots,i_t\}$に関しunbiasedであるという．任意の$\alpha \in \{0,1\}^t$，$\beta \in \{0,1\}^k$に対し，

$$\Pr[f(x_1, \cdots, x_l \mid x_{i_1} \cdots x_{i_t} = \alpha) = \beta] = 1/2^k$$

定義 2.2　以下が成り立つとき，ブール関数$f(x_1,\cdots, x_l) = (y_1, \cdots, y_k)$はzigzag関数と呼ばれる．任意の$I \subseteq \{1, \cdots, l\}$に対し，$f$は$I$または$\{1, \cdots, l\} \backslash I$に関しunbiasedである．

この定義より，ボブは，アリスのkビットの秘密m_0, m_1のうちどちらか一方についてはまったく分からない，というプロトコルを構成することができる．また，線形zigzag関数は，intersecting符号という符号の生成行列Gを利用し，

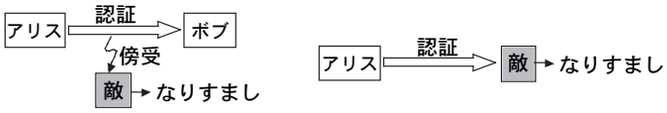
$$(y_1, \cdots, y_k)^T = G \cdot (x_1, \cdots, x_l)^T$$

と実現できる．上記の生成行列Gの代わりにランダムな行列を利用すると，lを小さくできることも知られている．ただし，この場合，(1,2)-OT^{k}に小さな失敗確率を許すことになる．

一方，Dodis and Micaliは，$N \geq n, K \geq k$に対し，$(1,n)$-OT^{k}から$(1, N)$-OT^{K}を実現する際，$(1,n)$-OT^{k}を走らせる回数の下界，およびアリスが必要とするランダムビットのビット数の下界を示している．

零知識認証法

零知識証明とは，証明者が検証者に，ある命題が正しい，ということを，余計な知識は一切もらさずに納得させる方法である[3]．この方法は，暗号プロトコルや個人認証法の構成において非常に有効であり，その概念の導入以来，飛



(a) 受動的攻撃　　(b) 能動的攻撃

図 -2　個人認証における攻撃モデル

躍的な発展を遂げてきた．本章では，個人認証法への応用に絞って解説する（併せて，参考文献4）の13章を参照されたい）．

通信において，自分がある特定の人物であることを相手に納得させる方法を，個人認証法という．アリスの公開鍵が公開されているとしよう．このとき，アリスの公開鍵に対応する秘密鍵を知っていることを示すことが，自分がアリスであることを示す個人認証となる．零知識証明のテクニックを用いてこのような個人認証を実現できることは，Fiat と Shamir によって初めて示された．

個人認証法は，敵がアリスになりすましできないときに，安全であると言われる．なりすましをしようとする敵の攻撃モデルを，以下に示す．

- **受動的攻撃**．アリスが誰か（たとえばボブ）と行っている認証プロトコルの通信内容を傍受できる（**図-2(a)**）．
- **能動的攻撃**．敵自身が検証者となって，アリスと認証プロトコルを走らせることができる（**図-2(b)**）．

明らかに，能動的攻撃のほうが強力な攻撃である．最近では，さらに強い攻撃である同時並行攻撃が考慮されている．

- **同時並行攻撃**．敵は検証者となり，アリスの複数のクローンを相手に，同時並行的に認証プロトコルを走らせることができる．ここで，アリスのクローンはすべて同じ秘密鍵を持つが，それぞれ独立に選ばれた乱数を使用する．

なりすまし不可能性は零知識よりも弱い条件なので，零知識証明よりも効率のよい個人認証法の構成を期待できる．実際，3-move（2者間で3回メッセージをやりとりする）の個人認証法が，Fiat-Shamir（FS）法，Schnorr法，GQ法など，いくつか開発されている．

一般的に，検証者が不正をしないという仮定の下での知識の零知識証明は，受動的攻撃に対し安全な個人認証法となることを示せる．したがって，Schnorr法は離散対数問題が困難という仮定の下で受動的攻撃に対し安全であり，GQ法はRSA暗号の解読が困難という仮定の下で受動的攻撃に対し安全である．

さらに，witness識別不可能性（WI）という性質を満たす知識の対話型証明は，能動的攻撃および同時並行的攻撃に対し安全な個人認証法となることを示せる．したがって，FS法は素因数分解が困難という仮定の下で，能動的攻撃および同時並行的攻撃に対し安全である．

しかし，Schnorr法およびGQ法は，WIという性質を有しない．この問題に対し，離散対数問題のone-more-inversion問題，およびRSA暗号のonemore-inversion問題が定義され，Schnorr法およびGQ法は，これらの問題が困難という仮定の下で，能動的的攻撃および同時並行的攻撃に対し安全であることが証明されている．

Bit Commitment

ビットコミットメント方式とは，以下のような封筒の機能を実現する2者間のプロトコルであり，零知識証明等において重要な役割を演じる[3]．

コミットフェーズ　アリスは，ビット b を封筒に入れる．
デコミットフェーズ　アリスは封筒をあけ，ボブに b の値を見せる．

このとき，以下の2つの条件が成り立たなければならない．

Secrecy　コミットフェーズ終了時において，ボブは b の値が何であるかまったく分からない．
Binding　デコミットフェーズにおいて，アリスは，b 以外の値をボブに見せることはできない．

明らかに，公開鍵暗号方式を利用すれば，ビットコミットメント方式を実現できる．では，この仮定はどこまで弱めることができるのであろうか．この問いに対し，一方向性関数が存在する，という計算量理論的に最も弱い仮定の下で，ビットコミットメント方式を実現できることが知られている[3]．

さらに，trapdoorコミットメント方式，non-malleableコミットメント方式，universally composableコミットメント方式，simulation-sound trapdoorコミットメント方式[5]など，付加的な機能を有するコミットメント方式が開発され，多くの暗号プロトコルに利用されている．

参考文献

1) Canetti, R.: Universally Composable Security: A New Paradigm for Cryptographic Protocols, IEEE Symposium on Foundations of Computer Science, pp.136-145 (2001).
2) http://www.tcs.hut.fi/?helger/crypto/link/protocols/oblivious.html
3) Goldreich, O. : Foundations of Cryptography, Cambridge University Press(2001).
4) 黒澤，尾形: 現代暗号の基礎数理，電子情報通信学会編 (2004).
5) MacKenzie, P.D. and Yang, K.: On Simulation-Sound Trapdoor Commitments, EUROCRYPT 2004, pp.382-400 (2004).

（平成16年9月30日受付）