■1 群（信号・システム）- 3 編（暗号理論）

9 章 暗号プロトコル

（執筆者：阿部正幸）［2009 年 2 月 受領］

■概要■

ある計算タスクに対するプロトコルとは，プレイヤと呼ぶ多項式時間対話チューリングマシン（によって実行されるアルゴリズム）の集合である．暗号プロトコルとは，秘匿性（各マシンの入力や出力の一部が秘密の情報を含む場合にそれらの秘密に関するいかなる情報も攻撃者に漏えいしないこと）や頑健性（攻撃者が各プレイヤの計算を誤った結果に導くことができないこと）などの安全性がディジタル署名，秘密分散，公開鍵暗号，ゼロ知識証明等の暗号技術を用いて実現されているプロトコルの総称である．コイン投げプロトコル，紛失通信プロトコルなどは古くから知られる代表的な暗号プロトコルであり，ほかのより高度な暗号プロトコルの構成部品として利用されることも多い．金持ち比べ，ポーカー，電子現金，電子投票，などの暗号プロトコルはそれ自体を一つのアプリケーションと見ることもできる．

【本編の構成】

本編では，まず攻撃に関する基本的なモデルを紹介し，次に暗号プロトコルでしばしば用いられる基本的な構成要素と一般的な二者間プロトコル，マルチパーティプロトコルについて概説する．その後，正式な安全性概念の一つを提供する大域的構成可能性フレームワークを概説する．

■1 群 - 3 編 - 9 章

9-1 攻撃モデル

（執筆者：阿部正幸）[2009 年 2 月 受領]

攻撃者はプレイヤの外に設けられた１台の対話チューリング機械でモデルされる．攻撃者の計算能力に制限がない場合を情報理論モデル，多項式時間で制限される場合を計算量モデルと呼ぶ．攻撃者はプレイヤを攻撃して，情報を入手したり，プロトコルから逸脱させたりする．攻撃を受けて攻撃者に操られるプレイヤを**不正者**と呼ぶ．攻撃者がどのプレイヤを攻撃できるかは，一般に**アクセス構造**（access structure）を用いて表される．特に閾値構造（threshold access structure）をもつ場合，すなわち n 人のプレイヤのうち最大 t 人まで攻撃できると考える場合が多い．暗号プロトコル安全性解析では，攻撃が成功したことで攻撃者が得る情報や能力によって攻撃を分類する．攻撃者は不正者のビューを継続的に入手することができるが，不正者は攻撃を受けた後もプロトコルから逸脱しない場合を**受動的攻撃**（passive attack）と呼ぶ．一方，攻撃者が不正者を完全に支配し，プロトコルから逸脱することもあり得る場合を**能動的攻撃**（active attack）と呼ぶ．通常，攻撃者は**滞在的**（stationary）であって，いったん攻撃されたプレイヤはプロトコル終了までずっと不正者である．一定時間経過後に不正者に対する攻撃者の支配が解除されるような**機動的**（mobile）な攻撃者を考える場合もある．

攻撃対象のプレイヤが事前に固定されているか否かは暗号プロトコル解析上大きな意味をもつ．攻撃者がどのように攻撃対象を決めるかによって，以下の分類がある．まず，攻撃対象のプレイヤをプロトコル開始以前に（より正確には，攻撃者はプレイヤの ID とセキュリティパラメータのみが決まっている状態で）決定する攻撃者を**静的攻撃者**（static adversary）あるいは**非適応的攻撃者**（non-adaptive adversary）と呼ぶ．プロトコル開始後に共通入力や各プレイヤの通信内容などに応じて攻撃対象のプレイヤを決定する攻撃者を**適応的攻撃者**（adaptive adversary）と呼ぶ．適応的／非適応的の分類は主に安全性解析の都合上設けられたものであり，プロトコルは適応的攻撃者に対して安全であることが望ましい．とはいえ，適応的攻撃者に対する安全性の証明は困難な場合が多い．適応的攻撃者に対して安全となるプロトコルの構成法[1, 6]も提案されているが，非適応的攻撃者に対して安全性が示せる方式に比較して複雑になりがちで，大きなオーバーヘッドを伴う場合が多い．

プレイヤ間の通信には様々な通信路が仮定される．攻撃者がすべての通信を任意に制御できる非同期通信路が最も弱い仮定であるが，高度な暗号プロトコルはより強力な機能を提供する放送型通信路，同期通信路，匿名通信路などの通信路が物理的あるいはほかの低位レベルの暗号プロトコルによって提供されることを前提として構成される．

■1 群 - 3 編 - 9 章

9-2 基本的構成要素

（執筆者：阿部正幸）[2009 年 2 月 受領]

9-2-1 ビットコミットメント

ビットコミットメント（bit commitment）は送信者 S と受信者 R からなる二者間プロトコルであって，送信者 S と受信者 R が以下のコミットフェーズとオープンフェーズからなる手順を実行するものである．コミットフェーズでは，まず，セキュリティパラメータ k と文字列 “commit” が共通入力として両者に与えられ，コミットすべき値 $b \in \{0,1\}$ が送信者 R に与えられる．対話の後，受信者 R は c を出力する．送信者 S はオープンフェーズへの引き継ぎ情報として任意の文字列 ω を出力する．オープンフェーズでは，セキュリティパラメータと文字列 “open” が共通に入力され，S には引き継ぎ情報 ω が与えられる．R には c が与えられる．R は $b' \in \{0,1\}$ または reject を出力する．オープンフェーズにおける受信者 R の出力 c を（値 b' の）コミットメントと呼ぶ．コミットメント c に対して，オープンフェーズで R が b' を出力するとき，「c を（値 b' に）オープンする」という．

ビットコミットメントの安全性は，コミットフェーズ終了時に受信者 R が b の情報を得られないこと（秘匿性（hiding property））及び，オープンフェーズにおいて送信者 S がコミットメント c を 0 と 1 の両方の値にオープンできないこと（拘束性（binding property））の二つの性質によって定義される．これらの条件が確率 1 で成り立つとき，それぞれ完全秘匿（perfectly hiding），完全拘束（perfectly binding）と呼ぶ．完全秘匿かつ完全拘束であるビットコミットメントは存在しないことが知られているが，一方向性関数が存在すれば，いずれか一方の性質が完全で他方が無視できる程度の小さな誤りを許すような構成は可能であることが知られている[19, 20, 21, 18]．

9-2-2 紛失通信

(n,k)-紛失通信（Oblivious Transfer）OT_k^n は，送信者が n 個のメッセージを送信し，そのうち少なくとも k 個のメッセージを受信者が受け取る二者間プロトコルである．OT_k^n の安全性は，受信者がどのメッセージを受信したかをランダムに言い当てる以上に有意な確率で特定できないこと（受信側安全性）及び，受信しなかったメッセージの内容が受信者に対して秘匿される（送信者側安全性）を満たすことである．送信者側安全性は，受信されなかったメッセージが強秘匿（semantically secure）であることを要求しており，紛失通信は公開鍵暗号の存在と等価であることが知られている[12, 14]．

OT_k^n とはやや異なる Rabin-OT と呼ばれる OT がある [22]．Rabin-OT では，送信者は一つのメッセージを送るが，メッセージは確率 1/2 でしか受信者に届かず，届かない場合は受信者はそのメッセージに関する情報を何も得られない．また，送信者はメッセージが受け取られたか否かを知ることができない．Rabin-OT と OT_k^n は相互に帰着可能である[11]．

9-2-3 ゼロ知識対話証明

言語 $L \subset \{0,1\}^*$ に関する対話証明系（Interactive Proof System）とは，証明者 P と検証者 V からなる二者間プロトコルであって，共通入力 x に対して，x が L に属することを P が V に納得させるためのプロトコルである．ゼロ知識対話証明（Zero-knowledge Interactive Proof

System）とは，検証者を納得させる以外に何の知識も漏らさない性質をもつ対話証明系である[17]．

R を多項式時間で認識可能なある 2 値関係とする．$L_R \stackrel{\text{def}}{=} \{x \mid {}^{\exists}w \text{ s.t. } (x,w) \in R\}$ を R で特徴づけられる言語とする．このとき，x に対して $(x,w) \in R$ となる w を x の証拠と呼び，そのような w の集合を $W(x)$ で表す．対話チューリング機械の対 (P,V) において，V が多項式時間限定であって，$x \in L$ に対して，正しい証明者 $P(x)$ と対話した検証者 $V(x)$ は圧倒的な確率で accept を出力する（完全性（completeness）），及び，$x \notin L$ に対して，任意の $P^*(x)$ と対話した検証者 $V(x)$ は圧倒的な確率で reject を出力する（健全性（soundness））の二つの性質が満たされるとき，(P,V) は言語 L の所属に関する対話証明系であるという．

すべての PSPACE 言語に対して対話証明が存在することが知られている[25]．一般的な対話証明系では，証明者 P の計算能力には制限がなく，その強力な計算能力を実際にプロトコル中で使用する場合もある．証明者の計算能力が無制限の場合，すべての PSPACE 言語に対してゼロ知識証明が存在することが知られている[2]．効率的な暗号プロトコルの構成部品としての対話証明では，P が確率的多項式時間で限定され，$|x|$ の多項式で制限された長さの witness $w \in W(x)$ が P への入力として与えられる場合を扱うことが多い．すべての NP 言語に対してこのような外部入力付きの対話証明系が存在する．健全性の定義においても，P^* を確率的多項式時間で限定する場合がある．そのような証明系は**アーギュメント**（Argument）と呼ばれる[4]．

共通入力 x に関して証明者 P と対話証明プロトコルを実行した場合の V の個別入力テープ，ランダムテープ，共通入力テープ，入力通信テープの結合からなる確率変数の族を**ビュー**（View）と呼び，$\mathrm{view}_V^P(x,y)$ と表す．ゼロ知識対話証明系とは，平均的多項式時間チューリング機械 M が存在して，任意の $x \in L, y \in \{0,1\}^{poly(|x|)}$ 及び任意の確率的多項式時間チューリング機械 V^* に対して，M が V^* をブラックボックスとして与えられたとき，$M^{V^*}(x,y)$ と $\mathrm{view}_{V^*}^P(x,y)$ が識別不可能であるような対話証明系である．識別不可能性の程度に応じて完全（perfect）／統計的（statistical）／計算量的（computational）ゼロ知識に区別される．一方向性関数が存在するならば，任意の NP 言語に対して計算量的ゼロ知識証明が存在することが知られている[15]．

9-2-4 秘密分散

$(t+1,n)$-**秘密分散**（Secret Sharing）は，秘密 s をもつディーラーと呼ばれるプレイヤが n 人のプレイヤ $P_1,\ldots,P_n$ に対して**シェア**（share）と呼ばれる値 $s_1,\ldots,s_n$ をそれぞれ配布するプロトコルである．秘密分散プロトコルの安全性は閾値 t によって定まり，どの t 個以下の s_i からも s に関する情報は得られないこと（秘匿性（secrecy）），かつ，どの $t+1$ 個以上 s_i からも s が一意に定まること（復元性（reconstructability））の二つの性質によって定義される．

暗号プロトコルで最もよく利用される Shamir の多項式秘密分散法[24] を説明する．秘密 s を $q > n$ なる $\mathbb{Z}_q$ の元とする．ディーラーは $t(<n)$ 次の多項式 $f(x) \in \mathbb{Z}_q[x]$ をランダムに選ぶ．ただし，$f(0) = s$ となるようにする．プレイヤ P_i が受け取るシェアは $s_i = f(i)$ である．どの t 個のシェアも t 次多項式 $f(x)$ を決定することはできない．すなわち，$f(0) = s$ は $\mathbb{Z}_q$ のどの元でもあり得る．一方，どの $t+1$ 個以上の正しいシェアからも Lagrange の多項式補

完を用いて $f(x)$ を一意に求めることができる．

検証可能秘密分散（Verifiable Secret Sharing）[10]は，ディーラーやプレイヤの能動的な不正に対して頑健性をもつ方式である．秘匿性のためには分散フェーズで不正者が t 以下でなければならず，復元性のためには，$t+1$ 以上の正しいシェアが得られなければならないので，能動的な攻撃者に対しては $t < n/2$ が閾値 t の上限となる．

9-2-5 一般的二者間・マルチパーティプロトコル

計算タスク F に対する**二者間プロトコル**（2-party protocol）は，プレイヤ A, B がそれぞれ秘密の入力 X_a, X_b をもち，互いの入力を秘密にしたまま，協力して $F(X_a, X_b)$ を計算するプロトコルである．Goldreich らは任意の計算タスクに対する二者間プロトコルを OT_1^4 を用いて安全に構成する方法を示した[16]．構成は，まず計算タスク F を GF_2 上の加算 $+$ 及び乗算 $*$ ゲートからなる等価な回路で記述し，入力の各ビット x を $x = x_a + x_b$ のように加法的に分散し，分散された入力に基づいて各ゲートを順次評価して分散された出力を得，各プレイヤがもつ出力ゲートの分散出力値を加算によって再合成して F の出力値を得る，という手順からなる．この基本的な構成は受動的な不正に対してのみ安全である．各ステップごとのプレイヤの出力値が正しいことをゼロ知識証明で証明することで，能動的な不正に対する頑健性を得ることができる．トラップドア一方向性置換が存在すれば，任意の計算タスクに対して頑健な二者間プロトコルが構成可能である．

一方，情報理論モデルにおいては，受動的な不正に対してすら安全な二者間プロトコルが存在しない計算タスクが存在する．例えば，無限の計算能力をもつ攻撃者に対して，論理積 $F(X_a, X_b) = X_a * X_b$ を安全に計算する二者間プロトコルは存在しない．

n 人のプレイヤからなる一般的**マルチパーティープロトコル**（Multi-party Protocol）の場合，入力を分散する段階で各ビットを n 個のシェアに秘密分散することで，計算量モデルにおいて $t < n/2$ の受動的な攻撃者に対して安全な構成法が得られる．能動的な攻撃者に対処するには，検証可能秘密分散とゼロ知識証明を用いて各プレイヤの正しさを検証し，不正者と認定されたプレイヤを排除して計算をやり直すという方針をとる．

情報理論モデルのマルチパーティープロトコルでは紛失通信やゼロ知識証明が使えないため，基本的には検証可能秘密分散のみでプロトコルを構成する[3, 13]．情報理論モデルで $t > n/3$ の場合，安全なプロトコルが存在しない計算タスクが存在する．例えば，ビザンチン合意は $t > n/3$ の不正者に対して解決不可能であることが知られている．すべてのプレイヤが物理的に供給される放送型通信路を利用できる場合，$t < n/2$ の能動的な攻撃に対して情報理論的に安全なプロトコルを構成することができる[23]．

■1 群 - 3 編 - 9 章

9-3 大域的合成可能性

（執筆者：阿部正幸）[2009 年 2 月 受領]

紛失通信のような暗号プロトコルはより高度な暗号プロトコルの構成部品として使用される場合が多々ある．古典的な安全性の定義は，プロトコルが単体で実行される場合の安全性のみを考慮しており，あるプロトコルを別のプロトコルに組み込んで使用したり，複数のプロセスが**同時多発的**（Concurrent）に実行される場合の安全性を考えるうえでは十分とはいえない．複数の同時に実行されているプロトコルが相互に悪影響を及ぼすことは十分考えられる．外部環境から得られる情報をどのように定式化し，安全性の定義でどのように扱うかについて，様々なモデルで様々な提案が行われている．

Canetti による**大域的合成可能性**（Universal Composability）を考慮したプロトコルの安全性定義[5]では，適応的に変化する外部環境（Environment）を対話チューリング機械でモデル化している．外部環境機械 Z は判定機械であり，プレイヤが実際にプロトコル π を実行しているのか，それとも以下に述べる理想状態の計算（ideal process）を行ったのかを識別する 1 ビットの値を出力する．理想状態の計算とは，ファンクショナリティ（Functionality）と呼ばれる，計算タスクを正しく実行するチューリング機械 $\mathcal{F}$ が存在し，各プレイヤから $\mathcal{F}$ への入力が安全な通信路（完全秘匿で相互認証可能な同期通信路）でファンクショナリティに送信され，計算結果が安全な通信路で各プレイヤへ返送される状況を指す．あるプロトコル π に対するどのような攻撃者 $\mathcal{A}$ に対しても，理想状態に対する攻撃者 $\mathcal{S}$ が存在して，任意の環境 Z に対して，プレイヤが π を実行した場合と理想状態の計算が行われた場合において Z の出力分布が計算量的に識別不可能ならば，プロトコル π は理想状態の計算 $\mathcal{F}$ と同等に安全であると考えることができる．そのようなプロトコル π は $\mathcal{F}$ を安全にエミュレートしているという．プロトコル π が上記の意味で $\mathcal{F}$ を安全にエミュレートするとき，π は大域的合成可能性をもつことが示されている．すなわち，プロトコル π は，ほかのプロトコルと組み合わせて使用したときでも $\mathcal{F}$ によって定式化された安全性を損なわないことが保証される．

プレイヤが事前に何も共有情報をもたない，あるいは，過半数のプレイヤが不正者である場合には，大域的合性可能なビットコミットメントや鍵共有を含む多くの有用なプロトコルは実現できないことが知られている[7, 8]．一方，信頼できる共通の乱数がすべてのプレイヤに与えられる CRS モデル（Common Reference String Model）では，大域的合性可能な任意の二者間あるいはマルチパーティプロトコルが構成可能であることが示されている[9]．

■参考文献

1) D. Beaver and S. Haber, “Cryptographic protocols provably secure against dynamic adversaries,” In Advances in Cryptology – Eurocrypt ’92, Springer-Verlag, vol.658 of LNCS, pp.307-323, 1992.
2) M. Ben-Or, O. Goldreich, S. Goldwasser, J. Håstad, J. Kilian, S. Micali, and P. Rogaway, “Everything provable is provable in zero-knowledge,” In S. Goldwasser, editor, Advances in Cryptology — CRYPTO ’88, Springer-Verlag, vol.403 of LNCS, pp.37-56, 1990.
3) M. Ben-Or, S. Goldwasser, and A. Wigderson, “Completeness theorems for non-cyptographic fault-tolerant distributed computation,” In Proceedings of the 20th annual ACM Symposium on the Theory of Computing, pp.1-10, 1988.

4) G. Brassard, D. Chaum, and C. Crépeau, “Minimum disclosure proofs of knowledge,” Journal of Computer and System Sciences, vol.37, no.2, 1988.
5) R. Canetti, “Universally composable security: A new paradigm for cryptographic protocols,” In Proceedings of the 42nd IEEE Annual Symposium on Foundations of Computer Science, pp.136-145, 2001.
6) R. Canetti, R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, “Adaptive security for threshold cryptosystems,” In M. Wiener, editor, Advances in Cryptology — CRYPTO ’99, Springer-Verlag, vol.1666 of LNCS, pp.98-115, 1999.
7) Ran Canetti and Marc Fischlin, “Universally composable commitments,” In Joe Kilian, editor, Advances in Cryptology — CRYPTO ’01, Springer-Verlag, vol.2139 of LNCS, pp.19-40, 2001.
8) Ran Canetti, Eyal Kushilevitz, and Yehuda Lindell, “On the limitations of universally composable two-party computation without set-up assumptions,” In Eli Biham, editor, Advances in Cryptology — EUROCRYPT ’03, Springer-Verlag, vol.2656 of LNCS, pp.68-86, 2003.
9) Ran Canetti, Yehuda Lindell, Rafail Ostrovsky, and Amit Sahai, “Universally composable two-party and multi-party secure computation,” In Proceedings of the 34th annual ACM Symposium on Theory of Computing, ACM, pp.494-503, 2002.
10) B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch, “Verifiable secret sharing and achieving simultaneity in the presence of faults, In Proceedings of the 26th IEEE Annual Symposium on Foundations of Computer Science, pp.383-395, 1985.
11) C. Crépeau, “Correct and Private Reductions Among Oblibious Transfers,” PhD thesis, Massachusetts Institute of Technology, 1990.
12) S. Even, O. Goldreich, and A. Lempel, “A randomized protocol for signing contracts,” Communications of the ACM, vol.28, no.6, pp.637-647, 1985.
13) R. Gennaro, M. Rabin, and T. Rabin, “Simplified VSS and fast-track multiparty computations with applications to threshold cryptography,” In 17th ACM Symposium on Principles of Distributed Computing, 1998.
14) Yael Gertner, Sampath Kannan, Tal Malkin, Omer Reingold, and Mahesh Viswanathan, “The relationship between public key encryption and oblivious transfer,” In Proceedings of the 41st IEEE Annual Symposium on Foundations of Computer Science, pp.325-335, 2000.
15) O. Goldreich, S. Micali, and A. Wigderson, “Proofs that yield nothing but their validity and a methodology of cryptographic protocol design,” In Proceedings of the 27th IEEE Annual Symposium on Foundations of Computer Science, pp.174-187, 1986.
16) O. Goldreich, S. Micali, and A. Wigderson, “How to play any mental game or a completeness theorem for protocols with honest majority,” In Proceedings of the 19th annual ACM Symposium on the Theory of Computing, New York City, pp.218-229, 1987.
17) S. Goldwasser, S. Micali, and C. Rackoff, “The knowledge complexity of interactive proof-systems,” SIAM Journal on Computing, vol.18, no.1, vol.186-208, Feb. 1989.
18) Iftach Haitner and Omer Reingold, “Statistically-hiding commitment from any one-way function,” In Proceedings of the 39th Annual ACM Symposium on Theory of Computing, San Diego, California, USA, June 11-13, 2007, ACM, pp.1-10, 2007.
19) R. Impagliazzo, L. Levin, and M. Luby, “Pseudo random generation from one-way functions,” In Proceedings of the 21st annual ACM Symposium on the Theory of Computing, pp.12-24, 1989.
20) M. Naor, “Bit commitment using pseudo-randomness,” In G. Brassard, editor, Advances in Cryptology — CRYPTO ’89, Springer-Verlag, vol.435 of LNCS, pp.128-136, 1990.
21) M. Naor, R. Ostrovsky, S. Venkatesan, and M. Yung, “Perfect zero-knowledge arguments for NP using any one-way permutation,” Journal of Cryptology, vol.11, no.2, pp.87-108, 1998.
22) M.O. Rabin, “How to exchange secrets by oblivious transfer,” Technical report, Harbard University,

Technical Memo, TR-81, 1981.
23) T. Rabin and M. Ben-Or, “Verifiable secret sharing and multiparty protocols with honest majority,” In Proceedings of the 21st annual ACM Symposium on the Theory of Computing, pp.73-85, 1989.
24) A. Shamir, “How to share a secret,” Communications of the ACM, vol.22, pp.612-613, 1979.
25) A. Shamir, “IP=PSPACE,” Journal of the ACM, vol.39, pp.869-877, 1992.