解　説

ゼロ知識証明モデルと計算量理論†

静谷啓樹††　伊東利哉†††　桜井幸一††††

1. はじめに

証明の検証の効率は計算量理論の中心的課題の一つである．証明の正しさが多項式時間で検証できる問題のクラスNPは，これまでにさまざまな観点から研究が行われてきている．これに対し，最近 Goldwasser, Micali, Rackoff[20] により，効率よく検証できる証明として新しい概念—対話証明—が提案された．

対話証明とは，証明者が入力が与えられた条件を満足することの証明を，質疑応答を繰り返すことにより検証者に示すものである．このとき，証明者と検証者は共にコイン投げを行い，その結果に基づく確率的挙動が許される．対話証明で証明可能な問題のクラスを IP で表す．従来の NP は，証明者がその証明を検証者に送り，検証者はその正当性を検証するという意味で IP の特別な場合とみなすことができる．これまで NP に含まれ（そうも）ないが IP には含まれる問題が数多く見つかっている．

さらに Goldwasser, Micali, Rackoff は，対話証明においていかなる知識が証明者から検証者に伝わるかという視点からゼロ知識という概念を定義した．対話証明がゼロ知識であるとは，検証者がその対話証明において入力が与えられた条件を満足するということ以外何も知識を得ないことをいう．今日までゼロ知識対話証明をもつ手に負えそうもない（検証者自身では解くことのできない）問題が数多く知られている．

本解説では，対話証明とゼロ知識の性質をいくつかの異なるモデルに関して計算量理論の立場から論じる．まず 2. で対話証明とゼロ知識性の定義を与え，それらの主な性質について論じる．3. では証明者から検証者への一方向の通信で，対話を行わずに証明を行うゼロ知識非対話証明の定義とその具体例を紹介する．また 4. では証明者が複数である多証明者ゼロ知識対話証明について解説する．多証明者ゼロ知識対話証明では証明可能な問題の範囲が広がるのみならず，計算量的仮定に依存せずにゼロ知識対話証明が構成可能となることが示される．

2. 対話証明とゼロ知識性

本章では，言語に対する対話証明とそのゼロ知識性に対する定義及び現在までの研究成果について述べるとともに，以後の議論に必要ないくつかの計算量のクラスを定義する．

2.1 対話証明

無限の計算能力（計算時間，記憶領域に制限のない）をもつ確率的 Turing 機械 P は証明者を表し，確率的多項式 Turing 機械 V は検証者を表すものとする．P, V はそれぞれコイン投げが許されており，P（あるいは V）の計算は共通入力 x，そのコイン投げ及びそれまでの V（あるいは P）からのメッセージに基づいて行われる．また P と V の対話は対話用テープを介して行われるものとする．このような Turing 機械の組 (P, V) を対話プロトコルという．このとき，対話プロトコル (P, V) が言語 L に対して対話証明であるとは，直観的には—(完全性) ある証明者 P と任意の $x \in L$ に対して，V は（ほぼ）確率1で x を受理し，(健全性) 任意の P^* と任意の $x \notin L$ に対して，V は（ほぼ）確率0で x を受理する—ことをいう．

次のような例を考える．合成数の集合をCOMPとする．$x \in$COMP の場合，P は（無限の計算能力によって）$a|x$ 及び $1<a<x$ となる a を V に

† Zero-Knowledge Proofs and Complexity Theory by Hiroki SHIZUYA (Tohoku University, Department of Electrical Communications), Toshiya ITOH (Tokyo Institute of Technology, Department of Information Processing) and Kouichi SAKURAI (Mitsubishi Electric Corporation, Computer & Information Systems Laboratory).

†† 東北大学工学部通信工学科
††† 東京工業大学大学院総合理工学研究科物理情報工学専攻
†††† 三菱電機(株)情報電子研究所マルチメディア開発部

送り，V は $a|x$ 及び $1<a<x$ であるときのみ x を受理する．一方，$x\notin$COMP の場合，P はどのように振る舞っても，$a|x$ 及び $1<a<x$ となるような a は存在しないので V は x を受理することはない．さらに次のような例を考える．グラフの組 (G,H) が同型であるとは，G の節点を適当に入れ換えることで H と一致させることができることをいい，$G\simeq H$ と記す．明らかに $G\simeq H$ かつ $H\simeq I$ ならば $G\simeq I$ である．ここで同型でないグラフの組の集合を GNI とする．$(G_0,G_1)\in$ GNI の場合，V は $s_i\in\{0,1\}$ を無作為に選び，G_{s_i} の節点を適当に入れ換えたものを H_i とし P に送る．P は（無限の計算能力によって）$H_i\simeq G_{j_i}$ を求め j_i を V に送る．P, V はこれを k 回繰り返し，V はすべての i $(1\leq i\leq k)$ に対して $s_i=j_i$ であるときのみ (G_0,G_1) を受理する．一方，$(G_0,G_1)\notin$GNI（すなわち $G_0\simeq G_1$）の場合，P はどのように振る舞っても $H_i\simeq G_0$ 及び $H_i\simeq G_1$ であるので V は高々確率 2^{-k} で (G_0,G_1) を受理する．

定義 2.1[20]：対話プロトコル (P,V) が言語 L に対する対話証明であるとは，

完全性：$\exists P\forall k>0\exists N\forall n>N\forall x[x\in L\wedge|x|=n]$
$\Pr\{(P,V)\text{ が }x\text{ を受理}\}>1-|x|^{-k}$

健全性：$\forall P^*\forall k>0\exists N\forall n>N\forall x[x\notin L\wedge|x|=n]$
$\Pr\{(P^*,V)\text{ が }x\text{ を受理}\}<|x|^{-k}$

を満たすことをいう．ただし，確率は P と V の無作為なコイン投げを全空間とする．

ここで V から P 及びそれに続く P から V へのやりとりを1ラウンドと呼ぶことにする．また，一般に多項式ラウンドからなる対話証明をもつ言語のクラスを IP で表し，特に定数ラウンドの場合は IP [const] で表すこととする．

Goldwasser, Micali, Rackoff[20] が対話証明の概念を発表したのと時期を同じくして，これとよく似た対話形式の証明方式が Babai[2] によって提案された．これは Arthur-Merlin ゲーム[2]と呼ばれ，V から P への通信内容が V の無作為なコイン投げの結果そのものである* という点を除いて対話証明と同様に定義される．

* 先に示した GNI に関するプロトコルは Arthur-Merlin ゲームではないが，3.2 で示すハミルトン閉路に関するプロトコルは Arthur-Merlin ゲームとなっている．

一般に多項式ラウンドからなる Arthur-Merlin ゲームをもつ言語のクラスを AM [poly] で表し，特に定数ラウンドの場合は AM と表すこととする．

2.2 ゼロ知識性

共通入力 $x\in L$ に対して，対話証明における P と V の対話を再構成する確率的多項式時間 Turing 機械 M を考える．基本的には，M のこのような出力系列と，P, V の実際の通信系列が識別不可能であるとき，これをゼロ知識と呼び，ゼロ知識である対話証明をゼロ知識対話証明[20]と呼ぶ．ただし，その識別不可能性の度合によって完全（perfect）ゼロ知識[22]，統計的（statistical）ゼロ知識[13]，計算量的（computational）ゼロ知識[20),22]に分類される．これらを定義するために，まず完全識別不可能性，統計的識別不可能性，計算量的識別不可能性という概念を定義する．

定義 2.2[20),22]：L を言語，$\{U(x)\}$, $\{V(x)\}$ を確率変数の族とする．このとき，$\forall x\in L$ $\Pr(x,U,V)=0$ となるならば，$\{U(x)\}$ と $\{V(x)\}$ は L に関して完全に識別不可能であるという．ただし，$\Pr(x,U,V)$ は

$$\Pr(x,U,V)=\sum_{\alpha\in\Sigma^*}|\Pr\{U(x)=\alpha\}-\Pr\{V(x)=\alpha\}|$$

で定義されるものとする．

定義 2.3[13),20]：L を言語とする．このとき，

$$\forall k>0\exists N\forall n>N\forall x[x\in L\wedge|x|=n]\ \Pr(x,U,V)<|x|^{-k}$$

となるならば，$\{U(x)\}$ と $\{V(x)\}$ は L に関して統計的に識別不可能であるという．

定義 2.4[20),22]：L を言語とする．また，$\{U(x)\}$, $\{V(x)\}$ を多項式長限定の確率変数（ある多項式で規定される長さの文字列 s にのみに生起確率が割り当てられている確率変数）の族とする．このとき，

$$\forall k>0\exists N\forall n>N\forall x[x\in L\wedge|x|>n]\forall C=\{C_n\}\ |P(U,C_{|x|},x)-P(V,C_{|x|},x)|<|x|^{-k}$$

となるならば，$\{U(x)\}$ と $\{V(x)\}$ は L に関して計算量的に識別不可能であるという．ただし，$C=\{C_n\}$ はすべての多項式サイズ論理回路の族とし，$P(U,C_{|x|},x)$, $P(V,C_{|x|},x)$ は，それぞれ $U(x)$, $V(x)$ に従って分布する文字列 s を論理回路 $C_{|x|}$ に入力したときに論理回路が1を出力す

る確率を表すものとする.

直観的には一完全に識別不可能: $\{U(x)\}$ と $\{V(x)\}$ が完全に一致すること; 統計的に識別不可能: $\{U(x)\}$ と $\{V(x)\}$ がほとんど一致すること; 計算量的に識別不可能: $\{U(x)\}$ と $\{V(x)\}$ が異なっているとしても, 実行可能なアルゴリズム (多項式サイズ論理回路) ではその相違を検出できないこと一を意味する.

このとき, 完全ゼロ知識 (統計的ゼロ知識及び計算量的ゼロ知識) 対話証明は次のように定義される.

定義 2.5[20]: L を言語とし, (P, V) を言語 L に対する対話証明とする. このとき, ある確率的多項式時間 Turing 機械 M が存在し, すべての $x \in L$ とすべての検証者 V^* に対して, $\{\langle P, V^*\rangle(x)\}$ と $\{M^{V^*}(x)\}$ が L に関して完全に (統計的に, 計算量的に) 識別不可能であるとき, (P, V) を完全 (統計的, 計算量的) ゼロ知識対話証明であるという. ただし, $\{\langle P, V^*\rangle(x)\}$ は P と V^* の対話において V^* が知ることのできるすべての系列* からなる確率変数の族, $\{M^{V^*}(x)\}$ は V^* をブラックボックス** として用いる Turing 機械 M^{V^*} の出力系列に対応する確率変数の族である.

完全ゼロ知識 (統計的ゼロ知識, 計算量的ゼロ知識) 対話証明をもつ言語のクラスを PZK (SZK, CZK) で表す. このとき明らかに PZK⊆SZK⊆CZK⊆IP である. また ZKIP=PZK∪SZK∪CZK に属する言語を, 単にゼロ知識対話証明をもつ言語と言うこととする.

2.3 対話証明をもつ言語のクラス

定義から明らかに NP⊆IP が成り立つが, これに対し, Goldreich, Micali, Wigderson[22] は, NP に含まれ(そうも)ない言語であるグラフ非同型問題 (GNI) が IP に含まれることを示した. IP の上限に関しては早くから IP⊆PSPACE*** が知られていたが, 最近 Shamir[31] によって PSPACE⊆AM [poly] が証明され, 対話証明をもつ言語の上限が明らかにされた.

2.4 ゼロ知識対話証明をもつ言語のクラス

Fortnow[13] は $L \in$SZK ならば $\bar{L} \in$AM であることを証明した (ただし $\bar{L}$ は L の補集合). この結果により, NP 完全な言語 L は (多項式時間階層が第2層までつぶれないかぎり) 統計的ゼロ知識対話証明をもちそうもないことが明らかになった. 一方, Brassard, Chaum, Crépeau[3] は NP 完全な言語に対する完全ゼロ知識のプロトコルを示しているが, これは Goldwasser, Micali, Rackoff[20] による対話証明とは異なるモデル* に関するものであり, Fortnow の結果はあてはまらない. 混乱を避ける目的で, Brassard, Chaum, Crépeau[3] のモデルは対話疑似証明 (argument) と呼ばれている.

さらに Aiello, Håstad[1] は SZK⊆AM を示し, これより PZK⊆SZK⊆AM∩co-AM という包含関係が明らかになった. このほか, Tompa, Woll[32] は, ランダム自己帰着性[32]をもつ言語は, ある緩い条件を満たせばすべて PZK に属することを証明している.

Goldreich, Micali, Wigderson[22] は, 安全な確率的暗号化関数が存在するという仮定のもとで, NP⊆CZK を示した (**3.2** 参照). これは基本的には, 対話証明において, 証明者から検証者へのメッセージに確率的暗号化関数を施すことでゼロ知識性を実現している.

一方, Ben-Or, Goldreich, Goldwasser, Håstad, Kilian, Micali, Rogaway[5] は, やはり安全な確率的暗号化関数が存在するという仮定のもとで IP⊆CZK を証明した. 証明の方針は Goldreich, Micali, Wigderson[22] とほぼ同じであるが, 積極的に Goldwasser, Sipser[23] の結果 (IP=AM[poly]) を用いることにより, IP に属する任意の言語に対して Arthur-Merlin ゲームをまず構成し, 証明者から検証者へのメッセージに確率的暗号化関数を施すことでゼロ知識性を実現している. これにより対話証明をもつ言語は, 確率的暗号化関数を用いることで, すべて (計算量的) ゼロ知識で証明することが可能となる.

2.5 絶対完全性及び絶対健全性

対話証明の絶対完全性 (perfect completeness) とは, 厳密に確率1で完全性が満たされる一正しい入力は必ず受理される一ことであり, 絶対健全性 (perfect soundness) とは, 厳密に確率1で健全性が満たされる一正しくない入力は決して受理さ

---

* 実際には共通入力, V^* のコイン投げ, P と V^* の対話.

** V^* の構造 (プログラム) に一切依存せずに, 入力を与えて V^* からその出力を受け取るような行為.

*** $x \in L$ を判定するのに, 高々 $|x|$ の多項式のメモリ量で計算が終了するような言語 L のクラス.

* 対話証明における健全性が計算量的仮定に基づいているため, 証明者 P は確率的多項式時間 Turing 機械に制限される.

れない一ことである．絶対完全性を満たす完全ゼロ知識（統計的ゼロ知識，計算量的ゼロ知識）対話証明をもつ言語を PZK^{pc} (SZK^{pc}, CZK^{pc})，絶対健全性を満たす完全ゼロ知識（統計的ゼロ知識，計算量的ゼロ知識）対話証明をもつ言語を PZK_{ps} (SZK_{ps}, CZK_{ps})，両方を満足するときは PZK_{ps}^{pc} (SZK_{ps}^{pc}, CZK_{ps}^{pc}) と表すことにする．また IP^{pc}, AM^{pc} なども同様の意味とする．

Zachos, Fürer[33] は $AM^{pc}=AM$ であることを示したが，さらに Goldreich, Mansour, Sipser[21] により，AM [poly]^{pc}=AM[poly] となることが示された．すなわち，絶対完全性の条件を課しても AM[poly] というクラスは不変である．ところが Goldreich, Mansour, Sipser[21] は同時に AM [poly]$_{ps}$=NP を証明し，絶対健全性が大きな制約となることを明らかにした．一方，Oren[29]は，$PZK_{ps}=SZK_{ps}=CZK_{ps}=RP$ を証明し，絶対健全性を満たすゼロ知識対話証明をもつ言語は自明なもの（検証者が証明者との対話なしに検証できる言語）しかありえないことを示した．さらに Itoh, Sakurai, Shizuya[25] は，$PZK_{ps}^{pc}=SZK_{ps}^{pc}=CZK_{ps}^{pc}=RP$ を証明し，Oren の結果が絶対完全性の追加条件に対して不変であることを示した．

このほか，Oren[29] は，証明者（検証者）がコイン投げを行わない場合には，BPP (RP)* に属する言語に対してのみゼロ知識対話証明が存在することを証明し，ゼロ知識対話証明において証明者と検証者の（独立な）コイン投げが必須であることを示した．

2.6 知識の対話証明

2.1 で示した対話証明は言語の所属問題に関するものであったが，これに対し Feige, Fiat, Shamir[14] 及び Tompa, Woll[32] は知識の対話証明を定義した．ここで言語の所属問題に関する対話証明モデルと大きく異なる点は，知識の対話証明モデルにおいては，証明者は共通入力 x に関する特別な知識 w をもつことを除いて証明者と検証者は共に確率的多項式時間 Turing 機械に制限されている** ことである．

多項式時間判定可能な関係を $R=\{(x,w)\}$ とする．このとき知識の対話証明は以下のように定義される．

定義 2.6：関係 R に対して確率的多項式時間 Turing 機械の組 (P, V) が知識の対話証明であるとは，

完全性：$\exists P \forall k>0 \exists N$
$\forall n>N \forall (x,w)$ $[(x,w)\in R \wedge |x|=n]$
$\Pr\{(P(w), V)$ が x を受理$\} > 1-|x|^{-k}$

健全性：$\forall l>0 \exists E \forall P^*$
$\forall k>0 \exists N \forall n>N \forall x[|x|=n] \forall w^*$
$\forall r_{p^*}$
$[\Pr\{(P^*(w^*), V)$ が x を受理$\} > |x|^{-l} \Rightarrow$
$\Pr\{(x, E(P^*(w^*, r_{p^*}), x))\in R\}$
$> 1-|x|^{-k}]$

を満たすことをいう．ただし，r_{p^*} は P^* の無作為なコイン投げ，E は P^* をブラックボックスとして用いる確率的多項式時間 Turing 機械とする．また確率は V と E の無作為なコイン投げを全空間とする．

一方，ゼロ知識性に関しては言語の所属問題の場合とほぼ同様に定義される．このようなモデルに対し，Feige, Fiat, Shamir[14] は効率的なゼロ知識個人認証方式を，また Tompa, Woll[32] はランダム自己帰着性をもつ関係はある緩い条件を満たせば，すべて知識の完全ゼロ知識対話証明をもつことを示している．

3. ゼロ知識非対話証明

本章では，ゼロ知識非対話証明に関する概要と現在までの研究成果について述べる．

3.1 研究の流れ

Oren[29] 及び Goldreich, Krawczyk[17] は，証明者と検証者のやりとりを3回以下（定数ラウンドの Arthur-Merlin ゲーム）に制限した場合には，BPP に属する言語に対してのみゼロ知識対話証明が存在することを証明し，ゼロ知識対話証明において対話（検証者の証明者に対する秘密のコイン投げ）が不可欠であることを示した．これに対し，Blum, Feldman, Micali[7] は，証明者と検証者が共通の乱数系列（コイン投げ）をもつというモデルにおいて，（非自明な問題に対する）ゼロ知識非対話証明を提案した．

ゼロ知識非対話証明は，直観的には，乱数系列 σ（以下参照系列と呼ぶ）を共有する証明者 P と検証者 V において，言語 L と P, V への共通入

☆ コイン投げを用いて多項式時間で $x\in L$ が判定できるような言語 L のクラス．

☆☆ これは先に示した対話疑似証明とは必ずしも同一の概念でないことに注意．

力 x に対し，P が V に "$x\in L$" であることの証明を対話を行わずに一方的に送りつけ，この際 V は "$x\in L$" 以外の情報を一切得ることがないというものである．

ゼロ知識非対話証明は一参照系列を共有する単一証明者と単一検証者における（1）単一定理に対するもの；（2）複数定理に対するもの；参照系列を共有する複数証明者と複数検証者における（3）単一定理に対するもの；（4）複数定理に対するもの一に分類される．Blum, Feldman, Micali[7] 及び De Santis, Micali, Persiano[11] は，数論上の仮定のもとで，NP に属するすべての言語が，単一証明者に関して単一定理ゼロ知識非対話証明をもつことを示した．一方，Blum, De Santis, Micali, Persiano[4] は，数論上の仮定のもとで，NP に属するすべての言語が，単一証明者に関して複数定理ゼロ知識非対話証明をもつことを示した．

また，De Santis, Micali, Persiano[12] は，証明者と検証者の間で参照系列を共有する際に若干の対話（予備通信）を許し，定理を証明する際には一切対話を行わないようなモデルを提案し，数論上の仮定より一般的な仮定（一方向性関数が存在する）のもとで，NP に属するすべての言語が，単一証明者に関して単一定理ゼロ知識（予備通信）非対話証明をもつことを示した．さらに，Kilian, Micali, Ostrovsky[26] は，De Santis, Micali, Persiano[12] より強い仮定（oblivious transfer プロトコルが存在する）のもとで，NP に属するすべての言語が，単一証明者に関して複数定理ゼロ知識（予備通信）非対話証明をもつことを示した．

以上の結果は，すべて単一証明者によるものか，または予備通信を必要とするため，認証方式などへの応用には適当でない．これに対し最近，Feige, Lapidot, Shamir[15] は，一般的な仮定（落し戸付一方向性置換が存在する）のもとで，NP に属するすべての言語が複数証明者に関して複数定理ゼロ知識非対話証明* をもつことを示した．

ゼロ知識非対話証明の応用としては，適応的選択平文攻撃に対して安全な署名方式[8] 及び適応的選択暗号文攻撃に対して安全な公開鍵暗号化方式[28] が知られているが，詳細については太田，藤岡[30] による本解説 2 を参照されたい．

* 一つの参照系列を共有する複数の証明者（及び検証者）が対話をせずに複数の定理をゼロ知識で証明可能．

3.2 NP に属する問題に対するゼロ知識非対話証明プロトコル

本節では，Feige, Lapidot, Shamir[15] によるゼロ知識非対話証明の概略について述べる．また本節を通じ，関係 $R=\{(x,w)\}$ ただし $|w|\leq \mathrm{poly}(|x|)$ は多項式時間判定可能とする．また，任意の x に対し集合 $w(x)$ を $w(x)=\{w|(x,w)\in R\}$，関係 R に対し言語 L_R を $L_R=\{x|\exists w(x,w)\in R\}$ と定義する．

定義 3.1[15]：確率的多項式時間 Turing 機械の組 (P,V) が関係 R に対する非対話証明であるとは，

完全性：$\exists P\forall k>0\exists N\forall n>N$
$\forall(x,w)\ [(x,w)\in R\wedge|x|=n]$
$\Pr\{V$ が $\langle x,\sigma,P(x,w,\sigma)\rangle$ を受理$\}>1-|x|^{-k}$

健全性：$\forall P^*\forall k>0\exists N\forall n>N$
$\forall x[x\notin L_R\wedge|x|=n]\forall w'$
$\Pr\{V$ が $\langle x,\sigma,P^*(x,w',\sigma)\rangle$ を受理$\}<|x|^{-k}$

を満たすことをいう．ただし，確率は参照系列 σ 及び P，V の無作為なコイン投げを全空間とする．

定義 3.2[15]：関係 R に対する非対話証明 (P,V) が単一定理ゼロ知識であるとは，ある確率的多項式時間 Turing 機械 M が存在し，任意の $(x,w)\in R$ 及びすべての多項式サイズ論理回路の族 D に対して，二つの確率分布の族 $\{(x,\sigma,P(x,w,\sigma))\}$ と $\{M(x)\}$ が多項式時間識別不可能となることである．ただし，確率は参照信号 σ 及び P，V のコイン投げを全空間とする．

定義 3.3[15]：関係 R に対する非対話証明 (P,V) が複数定理ゼロ知識であるとは，ある確率的多項式時間 Turing 機械 M が存在し，任意の多項式 t，任意の t 個の組 $(x_i,w_i)\in R(1\leq i\leq t)$ 及びすべての多項式サイズ論理回路の族 D に対して，二つの確率分布の族 $\mathcal{P}$ と $\mathcal{M}$

$$\mathcal{P}=\{(\sigma,x_1,P(x_1,w_1,\sigma),\ x_2,P(x_2,w_2,\sigma),\cdots,x_t,P(x_t,w_t,\sigma))\}$$
$$\mathcal{M}=\{M(x_1,x_2,\cdots,x_t)\}$$

が多項式時間識別不可能なことである．

以下，NP に属するすべての言語が複数証明者に関して複数定理ゼロ知識非対話証明をもつことを，

1. ハミルトン閉路 (NP 完全) に対するゼロ知識対話証明;

2. ハミルトン閉路 (NP 完全) に対する単一定理ゼロ知識 (予備通信) 非対話証明;

3. ハミルトン閉路 (NP 完全) に対する単一定理ゼロ知識非対話証明;

4. ハミルトン閉路 (NP 完全) に対する複数証明者に関する複数定理ゼロ知識非対話証明;

の順で述べる.

まずはじめに, ハミルトン閉路 (NP 完全) に対するゼロ知識対話証明[22]を示す. ただし, グラフ G の節点数を n, 安全な確率的暗号化関数 E は公知とする.

(P, V) への共通入力: G

以下のステップを n 回繰り返す.

1. P は S_n (n 次対称群) から無作為に置換 π を選び, G を π により置換し $\tilde{G}$ を生成する. ここで $\tilde{G}$ の隣接行列* を $B=(b_{ij})$ とするとき, P は $\beta=E(\pi)$ 及び行列 $D=(\delta_{ij})=(E(b_{ij}))$ を計算し V に送る.

2. V は無作為に $e\in\{0,1\}$ を選び P に送る.

3. $e=0$ のとき, P は β と $D=(\delta_{ij})$ を復号化して V に送る. $e=1$ のとき, P は $\tilde{G}$ のハミルトン閉路となっているようなすべての枝 (i,j) について δ_{ij} を復号し V に送る.

4. P から送られたものが β, D の正しい復号化になっていなかったり ($e=0$), ハミルトン閉路になっていないとき ($e=1$) には, V は対話を中止し G を受理しない. もし, 以上のステップを n 回繰り返すことができたなら V は G を受理する.

次にこれを単一定理ゼロ知識 (予備通信) 非対話証明に変形する. グラフ G の隣接行列を $A=(a_{ij})$ とする. また, $H=(h_{ij})$ を n 節点からなる適当なハミルトン閉路の隣接行列とし, $C=(c_{ij})$ を H の落し戸付一方向性置換に基づく確率的暗号化[18),19)]とする.

予備通信:

1. P は $H_i(1\leq i\leq n)$ を生成し, $C_i=E(H_i)$ $(1\leq i\leq n)$ を V に送る.

2. V は $b_i\in_R\{0,1\}$ $(1\leq i\leq n)$ を P に送る.

非対話証明:

1. $b_i=0$: P は C_i のすべての要素を復号し V に送る. V は $C_i=E(H_i)$ となることを確認する.

2. $b_i=1$: P は $\pi_i(H_i)$ が G のハミルトン閉路となるような置換 π_i と $\pi_i(C_i)$ の中で G の枝に対応しないすべての要素を復号し V に送る. V はそれらがすべて G の枝に対応しないことを確認する.

ここで上記のプロトコルを, 任意の参照系列 σ に対する単一定理ゼロ知識非対話証明に変換する.

グラフ G を n 節点からなるハミルトングラフとし, 参照系列 σ は長さ $2n^8\log n^3$ の 2 値系列とする. ここで σ を n^3 個のブロック $B_i(1\leq i\leq n^3)$ に分割し, 各ブロック B_i は各要素が $2n\log n^3$ ビットの $n^2\times n^2$ 行列とする. このとき, 証明者 P は落し戸情報を用いて, 参照系列 $\sigma\in_R\{0,1\}^{2n^8\log n^3}$ から非常に高い確率で n 節点からなるハミルトン閉路 H を見つけることができる. したがって, 上記のプロトコルの非対話証明 step 2 を実行することにより, ハミルトン閉路に対する単一定理ゼロ知識非対話証明が構成される.

さらに Feige, Lapidot, Shamir[15)] は, 一方向性関数が存在するという仮定のもとで, 計算量的に安全な疑似乱数生成器[24)]を用いて, 単一証明者に関する単一定理ゼロ知識非対話証明を複数証明者に関する複数定理ゼロ知識非対話証明に変換する方法を示している.

4. 多証明者ゼロ知識対話証明

本章では, 多証明者ゼロ知識対話証明* の概要と現在までの研究成果について述べる.

4.1 研究の流れ

3.2 においてすでに述べたように, Goldreich, Micali, Wigderson[22)] は, 暗号学的仮定 (安全な確率的暗号化関数が存在する) のもとで, NP に属するすべての言語が計算量的ゼロ知識対話証明をもつことを示している. これに対し Fortnow[13)] は, NP に属するすべての言語が統計的ゼロ知識対話証明をもつことは (恐らく) ありえないことを明らかにしている.

* グラフ G に対して, 接点の組 (i,j) に枝が存在すれば 1, 存在しなければ 0 として生成される行列.

* 前章で述べたゼロ知識非対話証明における複数証明者とは, 複数の証明者が "異なる" 定理を証明することを意味するが, ここで述べる多証明者とは, 複数の証明者が "同一の" 定理を互いに協力して単一の検証者に証明することを意味する.

一般的に，計算量的ゼロ知識対話証明はある計算量的仮定（たとえば，安全な確率的暗号化関数が存在するなど）のもとで，そのゼロ知識性が保証されているため，もしその仮定を破るような効率的なアルゴリズムが発見されれば，認証者 V はそのアルゴリズムを用いて証明者 P から有益な情報を入手することができる．一方，統計的ゼロ知識対話証明は，いかなる計算量的仮定にも依存せずに構成されるため，検証者 V はいかなる方法を用いても証明者Pから有益な情報を一切入手することはできない．したがって，完全ゼロ知識対話証明は計算量的ゼロ知識対話証明と異なり，無条件に安全であると考えることができる．

そこで，Ben-Or, Goldwasser, Kilian, Wigderson[9]は，より広い言語のクラスに対して完全ゼロ知識対話証明を構成するために，新しい対話証明モデルとして，多証明者対話証明を提案しそのモデルのもとで—(1)NP に属するすべての言語は，2証明者2ラウンド完全ゼロ知識対話証明をもつ；(2) 2証明者多項式ラウンド対話証明をもつすべての言語は，2証明者多項式ラウンド完全ゼロ知識対話証明をもつ；(3)任意の $l \geq 2$ に対し，l 証明者多項式ラウンド対話証明をもつすべての言語は，2証明者多項式ラウンド対話証明をもつ；(4) 2証明者多項式ラウンド対話証明をもつすべての言語は，絶対完全性を満たす2証明者多項式ラウンド対話証明をもつ—ことを示した．また，Fortnow, Rompel, Sipser[16]は，多項式証明者多項式ラウンド対話証明をもつすべての言語は，2証明者多項式ラウンド対話証明をもつことを示し，さらに，Babai, Fortnow, Lund[6]は，NEXP に属するすべての言語は，2証明者多項式ラウンド対話証明をもつことを示した．

多証明者ゼロ知識対話証明の応用としては，Ben-Or, Goldwasser, Kilian, Wigderson[10]により，効率的な個人認証方式が知られているが，詳細については，太田，藤岡[30]による本解説2を参照されたい．

4.2 計算量的仮定に基づかない多証明者ゼロ知識対話証明プロトコル

以下本節においては，Ben-Or, Goldwasser, Kilian, Wigderson[9]により提案された多証明者対話証明の概略について述べる．

計算量的に制限のない l 個の確率的 Turing 機械の組 $P_1, P_2, \cdots, P_l$ は証明者を表し，確率的多項式時間 Turing 機械 V は検証者を表すものとする．ここで，すべての P_i は共通の乱数テープをもつものとする．さらに，各 P_i は V との専用の対話用テープをもち，また P_j $(j \neq i)$ と V との対話の内容は一切知ることができないものとする．このような $(P_1, P_2, \cdots, P_l; V)$ を l 証明者対話プロトコルと呼ぶ．

定義 4.1[9]：言語 L に対し，l 証明者対話証明プロトコル $(P_1, P_2, \cdots, P_l; V)$ が対話証明であるとは，

完全性：$\exists P_i \forall k>0 \exists N \forall n>N \forall x[x \in L \wedge |x| = n]$
$\Pr\{(P_1, \cdots, P_l; V) \text{ が } x \text{ を受理}\} > 1 - |x|^{-k}$

健全性：$\forall P_i^* \forall k>0 \exists N \forall n>N \forall x[x \notin L \wedge |x| = n]$
$\Pr\{(P_1^*, \cdots, P_l^*; V) \text{ が } x \text{ を受理}\} < |x|^{-k}$

を満たすことをいう．ただし，確率は $P_1, P_2, \cdots, P_l$ 及びVの無作為なコイン投げを全空間とする．

定義 4.2[9]：対話証明 $(P_1, P_2, \cdots, P_l V)$ が完全ゼロ知識であるとは，確率的多項式時間 Turing 機械 M が存在し，任意の $x \in L$ すべての検証者 V^* に対し，

$$\sum_{\alpha \in \{0,1\}^*} |\Pr\{M^{V^*}(x) = \alpha\} - \Pr\{\langle P_1, P_2, \cdots, P_l; V\rangle(x) = \alpha\}| = 0$$

が成り立つことである．ただし，$M^{V^*}(\cdot)$ は Turing 機械 M が V^* をブラックボックスとして用いることを表し，また $\langle P_1, P_2, \cdots, P_l; V\rangle(\cdot)$ は $P_1, P_2, \cdots, P_l$ と V との間の対話を表すものとする．

以下このモデルのもとで，NP に属するすべての言語が2証明者完全ゼロ知識対話証明をもつことを示す．

3.2 で示したハミルトン閉路問題 (NP 完全) に対する計算量的ゼロ知識対話証明において，そのゼロ知識性の本質は，計算量的に安全な確率的暗号化関数が存在することであった．そこで，2証明者対話証明において，次のような情報理論的（無条件に）に安全な確率的暗号化関数[9]を構成する．

置換 σ_0, $\sigma_1 : \{0,1,2\} \to \{0,1,2\}$ を
$\sigma_0(i) = i$;

$\sigma_1(i) \equiv 2i \pmod 3$,

と定義する．このとき，$m = m_1 m_2 \cdots m_t \in \{0,1\}^t$ に対して，$(P_1, P_2; V)$ は以下の手順を実行する．

—m_k の暗号化手順—

1. V は無作為に $c_k \in \{0,1\}$ を選び P_1 に送る．
2. P_1 は $E(c_k, m_k) = \sigma_{c_k}(r_k) + m_k \pmod 3$ を計算し V に送る．ただし，r_k は P_1 と P_2 が共有する乱数テープの k 番目のセグメントとする．

—m_k の復号化手順—

1. V は k を P_2 に送る．
2. P_2 は r_k を V に送る．
3. V は $\sigma_{c_k}(r_k)$ を求め，$E(c_k, m_k) - \sigma_{c_k}(r_k) \pmod 3$ により m_k を得る．

この手順が，情報理論的に安全な（したがって無限の計算能力をもつ Turing 機械 V に対しても安全な）確率的暗号化関数となっていることは明らかであろう．

よって，NP に属するすべての言語は2証明者完全ゼロ知識対話証明をもつことになる．さらに1証明者ゼロ知識対話証明の場合と異なり，この2証明者（完全）ゼロ知識対話証明の場合は，プロトコルを並列に実行してもその（完全）ゼロ知識性は保たれるので，したがって NP に属するすべての言葉は2証明者2ラウンド完全ゼロ知識対話証明をもつことが示される．

5. おわりに

対話証明とゼロ知識性に関して計算量理論の立場から解説した．Goldwasser, Micali, Rackoff が（ゼロ知識）対話証明の概念を提案して10年足らずであるが，多くの性質が明らかになってきた．すでに知られていた計算量理論の手法で解決された問題もあるが，多くの結果は新しく開発された手法に基づいている．こうしたなかで Lund, Fortnow, Karloff, Nisan[27] に示唆され，Shamir によって最終的に証明された "IP=PSPACE" という結果は，従来から知られていた PSPACE というクラスの新たな一面を浮き彫りにしている．

対話証明とゼロ知識性に関する研究も一段落した感もあるが，いま暫くはさまざまなモデルに対して，計算量理論の立場からの研究が続けられるだろう．

参考文献

1) Aiello, W. and Håstad, J.: Statistical Zero-Knowledge Languages Can Be Recognized in Two Rounds, FOCS '87, pp. 439-448.
2) Babai, L.: Trading Group Theory for Randomness, STOC '85, pp. 421-429.
3) Brassard, G., Crépeau, C. and Chaum, D.: Minimum Disclosure Proofs of Knowledge, JCSS, Vol. 37, No. 2, pp. 156-189 (1988).
4) Blum, M., De Santis, A., Micali, S. and Persiano, G.: Non-Interactive Zero Knowledge, MIT/LCS/TM-430 (1990).
5) Ben-Or, M., Goldreich, O., Goldwasser, S., Håstad, J., Kilian, J., Micali, S. and Rogaway, P.: Everything Provable is Provable in Zero-Knowledge, LNCS 403, Crypto '88, pp. 37-56.
6) Babai, L., Fortnow, L. and Lund, C.: Non-Deterministic Exponential Time Has Two-Prover Interactive Protocols, FOCS '90, pp. 16-25.
7) Blum, M., Feldman, P. and Micali, S.: Non-Interactive Zero-Knowledge and Their Applications, STOC '88, pp. 103-112.
8) Bellare, M. and Goldwasser, S.: New Paradigms for Digital Signatures and Message Authentication Based on Non-Interactive Zero Knowledge Proofs, LNCS 435, Crypto '89, pp. 194-211.
9) Ben-Or, M., Goldwasser, S., Kilian, J. and Wigderson, A.: Multi-Prover Interactive Proofs: How to Remove Intractability Assumption STOC '88, pp. 113-131.
10) Ben-Or, M., Goldwasser, S., Kilian, J. and Wigderson, A.: Efficient Identification Schemes Using Two Prover Interactive Proofs, LNCS 435, Crypto '89, pp. 498-525.
11) De Santis, A., Micali, S. and Persiano, G.: Non-Interactive Zero-Knowledge Proof Systems, LNCS 293, Crypto '87, pp. 52-72.
12) De Santis, A., Micali, S. and Persiano, G.: Non-Interactive Zero-Knowledge with Preprocessing, LNCS 403, Crypto '88, pp. 269-282.
13) Fortnow, L.: The Complexity of Perfect Zero-Knowledge, STOC '87, pp. 204-209.
14) Fiege, U., Fiat, A. and Shamir, A.: Zero-Knowledge Proofs of Identity, STOC '88, pp. 210-217.
15) Feige, U., Lapidot, D. and Shamir, A.: Multiple Non-Interactive Zero Knowledge Proofs Based on a Single Random String, FOCS '90, pp. 308-317.
16) Fortnow, L., Rompel, J. and Sipser, M.: On the Power of Multi-Prover Interactive Protocols, Structures '88, pp. 156-161.
17) Goldreich, O. and Krawczyk, H.: On the Composition of Zero-Knowledge Proof Systems, ICALP '90, pp. 268-282.
18) Goldreich, O. and Levin, L.: A Hard-Core Pre-

dicate for All Oneway Functions, STOC '89, pp. 25-32.
19) Goldwasser, S. and Micali, S.: Probabilistic Encription, JCSS, Vol. 28, No. 2, pp. 270-299 (1984).
20) Goldwasser, S., Micali, S. and Rackoff, C.: The Knowledge Complexity of Interactive Proof Systems, SIAM J. of Comput., Vol. 18, No. 1, pp. 186-208 (1989).
21) Goldreich, O., Mansour, Y. and Sipser, M.: Interactive Proof Systems: Provers That Never Fail and Random Selection, FOCS '87, pp. 449-461.
22) Goldreich, O., Micali, S. and Wigderson, A.: Proofs that Yield Nothing But Their Validity and a Methodology of Cryptographic Protocol Design, FOCS '86, pp. 174-187.
23) Goldwasser, S. and Sipser, M.: Private Coins versus Public Coins in Interactive Proof Systems, STOC '86, pp. 59-68.
24) Impagliazzo, R., Levin, L. and Luby, M.: Pseudo-Random Generation from Oneway Functions, STOC '89, pp. 12-24.
25) Itoh, T., Sakurai, K. and Shizuya, H.: Hierarchical Classification for Interactive Proof Systems, ISEC 90-23, pp. 11-18 (1990).
26) Kilian, J., Micali, S. and Ostrovsky, R.: Minimum Resource Zero-Knowledge Proofs, FOCS '89, pp. 474-479.
27) Lund, C., Fortnow, L., Karloff, H. and Nisan, N.: Algebraic Methods for Interactive Proof Systems, FOCS '90, pp. 2-10.
28) Naor, M. and Yung, M.: Public-Key Cryptosystems Provably Secure against Chosen Ciphertext Attacks, STOC '90, pp. 427-437.
29) Oren, Y.: On the Cunning Power of Cheating Verifiers: Some Observations About Zero Knowledge Proofs, FOCS '87, pp. 462-471.
30) 太田和夫，藤岡 淳：ゼロ知識証明の応用，本小特集号.
31) Shamir, A.: IP=PSPACE, FOCS '90, pp. 11-15.
32) Tompa, M. and Woll, H.: Random Self-Reducibility and Zero Knowledge Interactive Proofs of Possession of Information, FOCS '87, pp. 472-482.
33) Zachos, S. and Fuerer, M.: Probabilistic Quantifiers vs. Distrustful Adversaries, TR 15, Brooklyn College of CUNY (1985).

(平成3年3月22日受付)

静谷 啓樹（正会員）

1981年東北大学工学部通信工学科卒業．1987年同大学院工学研究科博士課程修了．工学博士．同年東北大学情報処理教育センター・助手．1990年より東北大学工学部通信工学科助手．現在，モントリオール大学理学部情報科学科の招聘助教授としてモントリオールに滞在中．暗号理論，構造的計算量理論に興味をもつ．ACM, IACR, IEEE, IEICE, SITA各会員．

伊東 利哉（正会員）

昭和34年生．昭和57年東京工業大学工学部電気・電子工学科卒業．昭和59年同大学院理工学研究科修士課程修了．工学博士．昭和60年東京工業大学工学部電気・電子工学科助手．平成2年同大学院総合理工学研究科講師．現在に至る．有限体演算，情報セキュリティ，ゼロ知識対話型証明，計算量理論などに興味をもつ．電子情報通信学会会員．

桜井 幸一（正会員）

昭和38年生．昭和61年九州大学理学部数学科卒業．昭和63年同大学院工学研究科修士課程修了．同年三菱電機(株)入社．情報電子研究所勤務．以来，暗号と情報セキュリティの研究・開発に従事．現在の主要テーマは，計算量理論に基づく安全性と代数多様体に付随した暗号系，電子情報通信学会，日本数学会各会員．