NP 問題と概零知識証明

NP problem and almost zero knowledge proof

内藤 章子　(指導教員: 金子 晃)

1　はじめに

NP 問題と対話型零知識証明に関する既存の結果を概観し，新しい実用的な対話型零知識証明 (知識の証明) の例を提案する．また，零知識証明の概念を少し緩めた概零知識証明というクラスを新たに提案し，その応用を論ずる．

例として，“ RSA 暗号のモデュラス $n = pq$ の素因数分解を入手したアリスが，ボブにそれを売りつける” という, NP 問題の例に対して，なるべく火急すみやかにアリスがボブに対して自分の知識を証明し，商談に付かせるという問題設定を考える．

2　NP 問題と対話型零知識証明

NP 問題は，正確には，非決定的 Turing 機械により多項式時間で解ける問題と定義される．そのうち特に，他のすべての NP 問題がその問題を解くことに多項式時間で帰着できるようなものは，NP 完全と呼ばれる．NP 完全な問題はいくつか知られているが，NP 完全ではないことが分かっている NP 問題というものは知られていない．大方の予想は P $\neq$ NP である．

零知識証明 (知識の証明) とは，P (prover) が持っている秘密の知識を，V (verifier) に対して，その知識に関する情報を 1 ビットも漏らさずに，知識の所有だけを証明する方法を言う．通常は対話型，すなわち P と V の間で複数回のメッセージの交換を行うものを指し，ZKIP と略称する．対話型証明 IP は，いわゆる言語に対する証明が普通で,prover P と verifier V の間でメッセージのやりとりをし，与えられた文字列 x が形式言語 $L \subset \{0,1\}^*$ に属するか, つまり, $x \in L$ の証明をするしくみである．その要点は

完全性　$x \in L$ のとき P が V に証明を受理させられる確率は，無視できる誤差を除き 1 に等しい．

健全性　$x \notin L$ のとき, どんな prover P* に対しても P* が V に証明を受理させる確率は，無視できる大きさである．

の二つである．

零知識性とは, 証明によって P から V に渡されるのが証明の真偽だけで，それ以外は 1 ビットの情報も渡らないことである．ビューの同一性について，確率分布として，完全，統計的，計算量的，零知識に区別される．

対話型証明 IP は，P に無限の計算量を持たせているが，暗号プロトコルで実際に用いるときには現実的ではない．よって本講演では，最も基本的な場合，すなわち，V も P も多項式時間の計算能力しか無く，P が持っている知識はある NP 問題の答であり，答の所有の事実を数回の対話 (交互のメッセージ伝達) により V に納得させる，そして，零知識性も証明の成功も計算量上確率的に妥当となる，いわゆる計算量的対話型零知識証明のみを取り扱う．

以下，今までに知られている主な零知識証明を NP か NP 完全かの関連に着目して分類してみる．

証明対象	安全性の根拠	文献
3 SAT (NP 完全)	平方剰余仮説 (NP)	BC87
3 彩色 (NP 完全)	1 方向性函数の存在	GMW89
Hamilton 閉路 (NP 完全)	グラフ同型 (NP)	GMW89
グラフ同型 (NP)	グラフ同型 (NP)	GMW89
平方剰余 (NP)	素因数分解 (NP)	GMR85
平方非剰余 (NP)	素因数分解 (NP)	GMR85
離散対数 (NP)	離散対数 (NP)	Kizaki

3　既知の対話型零知識証明の例

(1) **3-SAT**　命題論理式の充足可能性を判定する問題 (Cook-Levin '71).
一般に，k-SAT の $k = 2$ のときは P だが $k \geq 3$ は NP 完全となる．

(2) **グラフの 3 彩色**　与えられたグラフ G を 3 色 (以下 R, G, B とする) で塗り分けられるかどうかを証明する問題.
毎回新しい置換 π を用いて繰り返されるので，1 方向性函数 f の安全性の仮定の下で零知識性を持つ．

(3) **Hamilton 閉路**　与えられたグラフ G に Hamilton 閉路，すなわち，すべての頂点を一度ずつ通る閉路が存在するかどうかを判定する問題.
零知識性は明らかで，NP でしかない．

(4) **グラフ同型**　位数 n が大きな二つのグラフ G_0, G_1 の同型 φ を P が知っていることを証明する問題.
零知識性は，得た同型の知識は，事後に自分でシミュレートでき，もとのグラフの間の同型写像の知識に付け加えられるものは何も無いことから示される．

(5) **合成数を法とする平方剰余の判定**　$n = pq$, 及び x が与えられたとき，$y^2 = x$ となる x が存在するかどうかを判定する問題.
零知識性は明らか．グラフ同型問題の NP 完全性は未解決である．

4　RSA 暗号のモデュラス n の素因数分解に対する対話型零知識証明

RSA 暗号のモデュラス n の素因数分解の知識に対する対話型の知識の零知識証明を直接行うアルゴリズムを考えてみる．$n = pq$, p, q は素数で，そのビット長 $|p|$, $|q|$ は n のビット長 $|n|$ の半分であるとする．P はこの素因数分解を知っているとし，それを V に証明したいものとする．

まず，プリミティブなプロトタイプとして，次を考える：

RSA の基数 n の素因数分解に対する対話型証明 $-$ 1

(1) V は $e, x \in \boldsymbol{Z}_n^*$ を, e は $|n|/2$ ビットの素数となるようにランダムに選び，(e, x^e) を P に送る．

(2) P は e に対して秘密鍵 d を計算し，復号計算により $x = (x^e)^d$ を返す．

(3) V は P から送られた x が自分のものと一致すれば accept し，不一致なら reject する．

RSA 暗号の通常の作り方と同じという仮定から，$(p-1)/2$, $(q-1)/2$ は $|n|/2-1$ ビットなので，e に対する

仮定により e は LCM$(p-1,q-1)$ と互いに素となり，RSA 暗号の復号が可能となる．よって，もし正しい x が返されれば，P は素因数分解を知っていると認められる．秘密鍵 d を求めることは n の素因数分解と同値であることは既に May により知られているので，証明の正当性は RSA 問題に依拠することが分かる．

このアルゴリズムの零知識性は，V が P から得たデータが何も無いことからほとんど明らかである．健全性が RSA 仮説に依拠していることは明らかだが，P が知識を持っていることの証明も同様に RSA 仮説に依拠している．

ただし，このアルゴリズムは，V が，自分では $x=\sqrt[e]{y}$ を知らないような y を選んで P に送ると，V は P から x を入手でき，証明 $x^e=y$ より多くのものを得ることができるため，honest でない verifier に対して，情報を漏らしている．よって零知識にはなっていない．これを防ぐため，OAEP と同様の工夫を用いてみる．

RSA の基数 n の素因数分解に対する対話型証明 − 2

(1) P は k ビットの乱数 r を選んで V に送る．
(2) V は $e, x \in \boldsymbol{Z}_n^*$ を, e は $|n|/2$ ビットの素数となるようにランダムに選び，$|n|-k$ ビットのメッセージ m を選んでビット列 $x=m||r$ を作り，(e,x^e) を P に送る．
(3) P は e に対して秘密鍵 d を計算し，復号計算により $x=(x^e)^d$ を得る．x の下位 k ビットが自分の送った r と異なれば，V が不正を働いたものとみなし，証明を中断する．等しければ m を V に送り返す．
(3) V は P から送られた m が自分のものと一致すれば accept し，不一致なら reject する．

RSA 関数に対して下位の数ビットはハードコアであることが知られているので，今回は V は自分が e 乗根を知らない y に対して P にその e 乗根 x を計算させる方法が無く，V のビューはシミュレータにすべて再現することができ，零知識証明であることが保証される．

このアルゴリズムの難点は，V が生成する素数 e のサイズが大きく，従って冪乗の計算も重いことである．e が LCM$(p-1,q-1)$ と共通因子を持つことが無視できない確率で起こり，もし，それに対して e 乗根の一つを送れば，V に n の素因数分解の手がかりを与えてしまう．しかし，そのような e を P が拒否すれば，やはり V に LCM$(p-1,q-1)$ の，従って p,q の情報を漏らしてしまう．

5 NP 問題の概零知識証明

無視できる確率で，あるいは，大勢に影響の無い数ビットの情報漏れを許すような証明というものを考えてみる．

定義 アルゴリズムが概零知識証明であるとは，証明の間に秘密情報に関するいくつかのビットが漏れるが，その知識を用いても多項式時間では秘密情報全体を復元することはできないことを言う．また，アルゴリズムが確率的零知識証明であるとは，証明の間に秘密情報に関するいくつかのビットが漏れる確率が無視できる大きさであることすなわち，秘密情報のサイズを n とするとき，任意の k について，$O(1/n^k)$ であることを言う．

例として，RSA の基数 n の素因数分解に対して，若干の情報漏れを許した 3 ラウンドだが計算量の少ない零知識証明が得られることを示す．

RSA の基数 n の素因数分解に対する概零知識証明

(1) P は $1 \le e \le n-1$ を LCM$(p-1,q-1)$ と互いに素となるようにランダムに選び，それとは独立に k ビットの乱数 r も選んで (e,r) を V に送る．
(2) V は $|n|-k$ ビットのメッセージ m をランダムに選び，$x=m||r$ を作り, $c=x^e$ を P に返す．
(3) P は $de \equiv 1 \mod \text{LCM}(p-1,q-1)$ となる d を計算し，$x=c^d$ を復号して, 後半の k ビットが自分の送った r と一致することを確かめたら, 残りの $|n|-k$ ビットを m として V に返す．
(4) V は P から送られた m が自分の送ったものと一致することを確認する．

RSA 仮説が正しければ，P は n の素因数分解を知らない限り，m を求めることができないので，その仮定の下でこれが証明となることは前節と同様である．しかし，P は V に LCM$(p-1,q-1)$ と互いに素な数 e を一つ教えているので，完全な零知識証明とはなっていない．ここで漏れた情報は，素因数分解を求める手がかりとして，ほとんど役に立たないことは，もしそうでなければ RSA 暗号が成り立たないことから直感的には明らかである．

定義 概零知識証明の概零知識性は，このプロトコルで漏れるビットを与えられたシミュレータが，verifier と対話して，実際の証明と同じビューを作り出せることとする．

概零知識証明に対する extractor K は，通常のものと同じでよい．上の例の場合には，K は前節と同様，RSA 仮説の下で P とのやりとりから，$x^e \mapsto x$ を得て，RSA 仮説により, n の素因数分解を入手できることになる．

以上により，上の簡単な例が， RSA 仮説の下で概零知識的な知識の対話証明となっていることが分かるが，これは火急の場合に十分実用的なプロトコルであると思われる．

6 まとめと今後の課題

対話型零知識証明について，よく知られた結果を概観し，RSA 暗号のモデュラス n の素因数分解に対する知識の対話型零知識証明の例を与えた．また計算量を減らして効率化するため，安全性を損なわない程度で，ビット漏れを許容する概零知識証明というものを考えてみた．

ここでとりあげたのは，RSA 暗号の n の素因数分解に対する知識の証明であるが，その言語版である，

$$L=\{n;\ \exists p,q \ \text{ s.t. } |p|=|q|=|n|/2,\ p,q \text{ は素数で } n=pq\}$$

に対する対話型零知識証明も考えてみたい．