DEIM Forum 2009 D4-5

非公開データベース間の情報共有における機密性向上の検証

隅　　崇佳† 村本　俊介† 上土井陽子† 若林　真一†

† 広島市立大学大学院 情報科学研究科
E-mail: †t.sumi@lcl.ce.hiroshima-cu.ac.jp

あらまし 近年，膨大な情報を扱うようになり様々な情報がデータベース化されている．データベース化された情報を共有する際に，データベースの機密性を確保する必要がある．そこで，我々はR.Agrawal らの手法を元に可換性のある暗号を用いてデータベース間の情報共有を行う手法を提案した．本稿では，さらに，提案手法の機密性と従来手法の機密性の差異を明確にすることを目標とする．具体的には，機密性の差異を測る方法として多項式時間帰着を用いることで，従来手法の機密性を破ることよりも，提案手法の機密性を破ることが困難である可能性があることを証明する．

キーワード 多項式時間帰着，Decisional Diffie-Hellman 問題，機密性，情報共有

An Improvement of Security for Information Sharing across Private Databases

Takayoshi SUMI†, Syunsuke MURAMOTO†, Yoko KAMIDOI†, and Shin'ichi WAKABAYASHI†

† Graduate School of Information Sciences, Hiroshima City University
E-mail: †t.sumi@lcl.ce.hiroshima-cu.ac.jp

Abstract In recent years, more attention is focused on sharing information in a distributed system consisting of peers, each of which has a private database. It is important to protect private databases when multiple parties share information on the databases. Then, we proposed an information sharing protocol with a commutative cryptosystem based on Agrawal et al. In this paper, we make difference clear between security of the proposal protocol and one of Agrawals'. More specfically, we show that it may be more difficult to break security of the proposal protocol than breaking one of Agrawal's protocol, by applying polynomial-time reduction technique.

Key words polynomial-time reduction, dicisional Diffie-Hellman problem, security, information sharing

1. ま え が き

複数の機関が各々のデータベース上のデータを情報共有する際，それぞれのデータベースのデータが他の機関にすべて明らかになることがこれまでは仮定されていた．これは必要以上に情報を明らかにしたくない非公開データベースにおいて好ましくないため，機密性の観点から質問の回答と無関係な情報が明らかにならないような方法で非公開データベースを共有する要求が高まってきた．文献 [1] では，機関 S と R の二者間において情報共有を行う場合に，可換性のある暗号を用いる手法が提案されている．そこで，我々は文献 [1] に基づき，可換性のある暗号を用いて情報共有を行う新たな intersection プロトコルを提案した [5].

しかし，文献 [5] では，従来プロトコル [1] の機密性と提案プロトコルの機密性の違いを明確にしていなかった．従来プロトコルの機密性は離散対数問題に基づく Decisional Diffie-Hellman(DDH) 問題の困難さを基準として確保されている．そこで，従来プロトコルと提案プロトコルの機密性の差異を明確にするため，DDH 問題，特定の暗号化関数を適用した従来プロトコルの機密性問題，提案プロトコルの機密性問題の困難さについての比較を検討する．さらに，従来手法と同じ暗号法を用いたときに提案手法の機密性が向上する可能性があることを多項式時間帰着を用いて検証する．

2. 機密性について

まず，本稿で扱う機密性について説明する．我々が扱った従来プロトコルや提案プロトコルは情報共有を行う機関のふるまいとして以下のモデルを仮定している．

honest-but-curious

プロトコルに参加する機関は忠実にプロトコルに従う．しかし，プロトコル実行中に受け取ったメッセージや行った計算を全て記録して，後に付加情報を得ることを目的として記録を解析するかもしれない．

本稿での機密性とは，プロトコルから得た情報を用いて相手が独自に持つデータを明らかにできないことを保障する意味で用いる．また，機密性が破られるとは，相手機関が明らかにすることを許していない情報の一部をプロトコルで得た情報から知ることを意味している．よって，プロトコルに参加するある機関が故意に偽データを含ませたデータベースを情報共有して相手機関の情報を得たり，第三者によるデータの改ざんなどでの情報漏えいなどは機密性を破ることの対象としない．

3. 離散対数問題と Diffie-Hellman 問題

離散対数問題とは，g, y, p が与えられたとき $y = g^a \bmod p$ となる a を求める問題である．g を巡回群 G の原始元，p を十分に大きな素数とする．離散対数問題は素数 p が十分に大きいとき現在のコンピュータでは解くことが難しいとされている問題である．

Diffie-Hellman(DH) 問題は離散対数問題解決の困難性に基づいており，DH 鍵配送方式の安全性に関係する問題である [2][7]．DH 問題には Computational Diffie-Hellman(CDH 問題) と Decisional Diffie-Hellman(DDH 問題) と呼ばれる問題があるが，本稿では，CDH 問題を簡単に述べた後，主に本研究で扱う DDH 問題について述べる．

3.1 CDH 問題

CDH 問題は G を素数位数 p の巡回群，g を G の原始元，a, b をランダム値とする．このとき，(G, p, g, g^a, g^b) が与えられたときに，g^{ab} を求める問題のことである．そして，CDH 問題を解く効率的なアルゴリズムが存在しないという仮定のことを，CDH 仮定と呼ぶ．

暗号に使われているほとんどの群においては，CDH 問題と DL(離散対数) 問題は計算理論の意味において等価だと信じられている．

3.2 DDH 問題

G を素数位数 p の巡回群，g を G の生成元，x, y をランダム値とする．このとき，(G, p, g, g^a, g^b) が与えられたときに g^{ab} の部分情報（部分ビット）を求める問題を DDH 問題と呼ぶ．この DDH 問題は，識別可能という表現を使って言い換えると次のようになる．G を素数位数 p の巡回群，g を G の原始元，a, b, c をランダム値とする．このとき，$(G, p, g, g^a, g^b, g^{ab})$ と (G, p, g, g^a, g^b, g^c) を識別する問題である．また，DDH 問題を効率的に解くアルゴリズムが存在しないという仮定を DDH 仮定と呼ぶ．

DDH 問題は図 1 に示すような判定問題と表すことができる．図 1 に示した DDH 問題，特定の暗号化関数を適用した従来プロトコルの機密性問題と提案プロトコルの機密性問題の困難さの比較を互いに多項式時間帰着できるかどうかという観点から検討する．

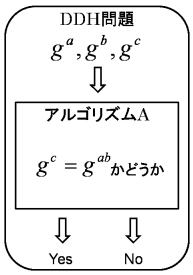

図 1　DDH 問題

次節で従来プロトコルとその機密性問題を説明する．

4. 従来プロトコルとその機密性に関する問題

本節では，まず，従来プロトコルとその機密性を確保するために適用可能な暗号化関数について説明する．次に，従来プロトコルの機密性に関する問題を述べた後，DDH 問題とある暗号化関数を用いたプロトコルの機密性に関する問題を互いに多項式時間帰着させることよって問題の困難さを測る．

4.1 従来プロトコル

Agrawal らの提案したプロトコル [1] を以下に示す．

1　機関 S と R はそれぞれが持つ集合 V_s, V_r をハッシュ関数 h により変換する．変換した集合をそれぞれ $X_s = h(V_s)$，$X_r = h(V_r)$ とする．機関 S と R は領域 $KeyF$ からランダムに鍵 e_s, e_r を選ぶ．

2　機関 S と R はハッシュ関数により変換された集合を選んだ鍵で暗号化する．暗号化後の集合をそれぞれ $Y_s = f_{es}(X_s), Y_r = f_{er}(Xr)$ とする．

3　機関 R は集合 Y_r の要素を辞書式順に並べ換えた列を機関 S に送る．

4　(a) 機関 S は集合 Y_s の要素を辞書式順に並び換えた列を機関 R に送る．
(b) 機関 S は集合 Y_r に含まれるすべての要素 y を鍵 e_s で暗号化する．暗号化後の集合を $Z_r = f_{es}(Y_r)$ とする．それから機関 R に集合 Y_r に含まれる全ての要素 y に関しペア $< y, f_{es}(y) >$ を送り返す．

5　機関 R はステップ 4 の (a) で機関 S から得た集合 Y_s を鍵 e_r で暗号化し集合 $Z_s = f_{er}(Y_s)$ を作成する．また集合 V_r に含まれる要素 v に対してステップ 4(b) で得たペア $< y, f_{es}(y) >=< f_{er}(h(v)), f_{es}(f_{er}(h(v))) >$ からペア $< v, f_{es}(f_{er}(h(v))) >$ を得る．

6　機関 R はステップ 4 で送られてきた暗号化集合 Z_r とステップ 5 で作成した暗号化集合 Z_s から集合 $Z_s \cap Z_r$ を求める．求めた集合 $Z_s \cap Z_r = f_{es}(f_{er}(h(V_s \cap V_r)))$ に属する暗号文とペアになっている集合 V_r に属する要素の集合が $V_s \cap V_r$ となる．

4.2 従来プロトコルに用いられる暗号

従来プロトコルには満たすべき暗号化特性が 4 つある．鍵の定義域を $KeyF$，暗号化した値の定義域を $DomF$ とする．$a \in {}_rb$ は“ b からランダムに選ばれた a ”ということを意味する．

（1） 可換性：全ての $e, e' \in KeyF$ に対して
$$f_e.f'_e = f'_e.f_e \text{ が成り立つ.}$$
（2） 各 f_e に対して暗号化前と後の関係は全単射.
（3） 鍵 e を用い暗号化された情報は鍵 e が与えられると多項式時間内に復号が可能.
（4） indistinguishability：$< x, f_e(x), y, f_e(y) >$ の分布は $< x, f_e(x), y, z >$ の分布と計算的に区別がつかない.
$(x, y, z \in {}_rDomF,\ e \in {}_rKeyF)$

上記の 4 つの暗号化特性を満たす暗号として以下の暗号化関数 f を従来プロトコルでは用いている．

$$f_e(x) \equiv x^e \bmod p$$

indistinguishability 特性はある暗号化前後のペアが与えられたとき，次に与えられるペアが同じ鍵で暗号化されたものかどうかを多項式時間内に判定できるアルゴリズムがないということを意味しており，暗号化関数 f を用いる従来プロトコルの機密性がどの程度か決定する指標となっている．本稿ではこの判別問題を indistinguishability 問題と呼ぶ．

4.3 DDH 問題と indistinguishability 問題の帰着関係

暗号化関数 f を適用した indistinguishability 問題と DDH 問題の困難さが等価であることを多項式時間帰着により示す．DDH 問題は (g^a, g^b, g^{ab}) と (g^a, g^b, g^c) を区別する問題であった (以降，巡回群 G，原始元 g，素数 p は省略する)．また，暗号化関数 f を用いる indistinguishability 問題は $< x, f_e(x), y, f_e(y) >$ の分布は $< x, f_e(x), y, z >$ の分布と区別できるかという問題である．この分布 $< x, f_e(x), y, z >$ を鍵の定義域 $KeyF$ から適当な値 d を用いて変換する．

$$< x, x^e, y, z >$$
$$=< g^d, g^{ad}, g^b, g^c >$$

x は g^d，y は g^b，z は g^c，鍵 e は a に対応している．上記のように変換すると，分布 $< g^d, g^{ad}, g^b, g^{ab} >$ と分布 $< g^d, g^{ad}, g^b, g^c >$ の区別ができるかと言い換えることができる．この問題と DDH 問題を比較すると図 2 のようになる．

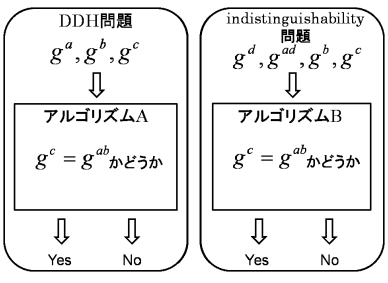

図 2　DDH 問題と indistinguishability 問題の比較

まず，DDH 問題を indistinguishability 問題に帰着させる．図 2 の DDH 問題の入力の g^a と原始元 g を鍵の定義域 $KeyF$ から適当な値 d を用いてそれぞれ g^{ad}, g^d に変換する．すると，変換した 2 つの値と DDH 問題の入力である g^b, g^c を入力とする indistinguishability 問題の出力より，DDH 問題の出力を得ることができる．ここまでで DDH 問題を indistinguishability 問題に帰着できた．

次に，indistinguishability 問題を DDH 問題に帰着できることを示す．indistinguishability 問題の入力である g^c を値 d を用いて g^{cd} に変換する．そして，indistinguishability 問題の入力である g^{ad}, g^bと g^{cd} をそれぞれ DDH 問題の入力である g^a , g^b, g^c として入力することで，DDH 問題の $g^{adb} = g^{cd}$ の判定結果より，indistinguishability 問題の g^c=g^{ab} の判定結果を得ることができる．よって indistinguishability 問題は DDH 問題に帰着可能である．

以上から，DDH 問題と indistinguishability 問題の双方から多項式時間帰着できたことにより，従来プロトコルの機密性を破ることは DDH 問題を解くことと同等の困難さを持つことが証明できる．

5. 提案プロトコルと機密性問題

この節では，提案プロトコル [6] の機密性を確保するために必要な特性を述べる．さらに，提案プロトコルの機密性に関係する問題について述べ，その問題の困難さを DDH 問題，もしくは indistinguishability 問題と互いに帰着可能かどうかを検討する．

5.1 提案プロトコル

提案プロトコルを以下に示す.

1 機関 S と R はそれぞれが持つ集合 V_s, V_r をハッシュ関数 h より変換する．変換後の集合をそれぞれ $X_s = h(V_s)$, $X_r = h(V_r)$ とする．機関 S と R は定義域 $KeyF$ からランダムに鍵 e_s，e_r を選ぶ.
2 機関 S と R はハッシュ化された集合を選んだ鍵で暗号化する．暗号化後の集合をそれぞれ $Y_s = f_{es}(X_s)$, $Y_r = f_{er}(X_r)$ とする.
3 機関 S は集合 Y_s の要素を辞書式順に並び換えた列を機関 R に送る.
4 機関 R は集合 Y_r の要素を辞書式順に並び換えた列を機関 S に送る.
5 機関 S は鍵 e_s を用いて機関 R から送られてきた集合 Y_r を暗号化する．集合 Y_r を暗号化したものを集合 $Z_r = f_{es}(Y_r)$ とする.
6 機関 R は S から送られてきた Y_s を鍵 e_r を用いて暗号化し，辞書式順に並べて機関 S に送り返す．集合 Y_s を暗号化したものを集合 Z_s=$f_{er}(Y_s)$ とする.
7 機関 S は R から送り返された集合 Z_s とステップ 5 で作成した集合 Z_r を比較し，集合 $Z_s \cap Z_r$ を求める.
8 機関 S はステップ 7 で求めた集合 $Z_s \cap Z_r$ を鍵 e_s で復号する．復号すると集合 $W_s = f_{er}^{-1}(Y_s \cap Y_r)$

$= f_{er}(h(V_s \cap V_r))$ を得られる．復号した集合 $f_{er}(h(V_s \cap V_r))$ を機関 R に送る．

9 機関 R は S から送られた集合 W_s を鍵 e_r で復号し，集合 $h(V_s \cap V_r)$ を求め集合 $V_r \cap V_r$ を得る．

従来プロトコルはステップ 4 で暗号化前後のペアが相手機関に明らかになっていた．提案プロトコルでは通信回数が増える代わりに，暗号化前後のペアが明らかにならないように改良した．

5.2 提案プロトコルに必要な暗号化特性

提案プロトコルを機密性を確保し，動作させるために暗号化関数が満たすべき特性を以下に示す．

（1） 可換性：全ての $e, e' \in KeyF$ に対して
$$f_e.f'_e = f'_e.f_e \text{ が成り立つ．}$$
（2） 各 f_e に対して暗号化前と後の関係は全単射．

（3） 鍵 e を用い暗号化された情報は鍵 e が与えられると多項式時間内に復号が可能．

（4） *E-I*(encryption-indistinguishability)
分布 $<(x_1, x_2), (f_e(x_1), f_e(x_2))>$ と分布 $<(x_1, x_2), (z_1, z_2)>$ は計算的に区別がつかない．
$(x_1, x_2, z_1, z_2 \in_r DomF, e \in_r KeyF)$

この特性は入力としてある暗号化前の値の組 (x_1, x_2) が与えられ，それらの暗号化後の値として (z_1, z_2) を選んだとき，x_1 から z_1 の暗号化と x_2 から z_2 の暗号化に用いられた鍵が同じであるかどうかを区別する多項式時間アルゴリズムがないということを意味している．

E-I 特性はプロトコルを改良したことと，従来プロトコルに用いられている暗号

$$f_e(x) \equiv x^e \bmod p$$

を提案プロトコルでも用いることで得られる機密性を決定する指標である．本稿では，この指標を *E-I* 問題と呼ぶ．

5.3 DDH 問題と *E-I* 問題の帰着

E-I 問題は indistinguishability 問題と同様に変換を行うと入力として $g^a, g^b, g^{c_1}, g^{c_2}$ が与えられたとき，$g^{c_1} = g^{ae}$かつ $g^{c_2} = g^{be}$ となる e が存在するかという判定問題に置き換えることができる．上記のように置き換えた $E-I$ 問題と DDH 問題の帰着を考える．

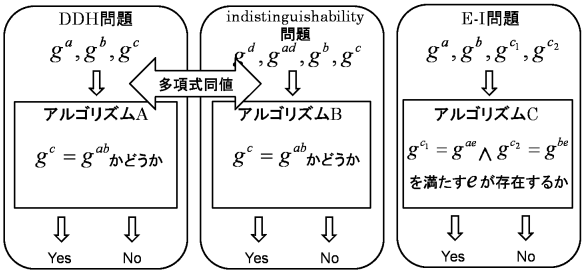

図 3　各種問題の比較

まず，DDH 問題から *E-I* 問題への帰着を考える．鍵の定義域 $KeyF$ から適当な値 f を選び，g^f を作成し，DDH 問題の入力である g^bを g^{bf} と変換する．次に，*E-I* 問題の入力 $< g^A, g^B, g^{C_1}, g^{C_2} >$ に対応するものとして $< g^f, g^a, g^{bf}, g^c >$ を与え，$g^{C_1} = g^{bf} = g^{AE}$かつ $g^{c_2} = g^c = g^{BE}$ となる E が存在するかを判別することで $g^c = g^{ab}$ かどうか判別できれば帰着できたことになる．g^fは g^A, g^aは g^B, g^{bf}は $g^{C_1} = g^{AE}$, g^cは $g^{C_2} = g^{BE}$ にそれぞれ対応している．ここで，出力が yes になるには，入力として $< g^f, g^a, g^{bf}, g^c >$ を与えたとき，$g^{bf} = g^{C1} = g^{AE}$ より E は b になる．また，$g^c = g^{C2} = g^{BE}$ より，g^cは g^{ab} でなければならない．これは *E-I* 問題を利用して DDH 問題を解いたことになり，DDH 問題は *E-I* 問題に帰着できることを意味している．

次に，*E-I* 問題が DDH 問題に帰着可能かどうかを説明する．結論から述べると，*E-I* 問題は DDH 問題にも indistinguishability 問題にも帰着することは難しいと考えられる．帰着するには $g^c = g^{ae}$ もしくは $g^d = g^{be}$ となる e が存在しなければならない．仮に e が存在することが分かると以下のように帰着することができる．*E-I* 問題の入力 $< g^a, g^b, g^{c_1} = g^{ae}, g^{c_2} >$ の g^b, g^{ae}, g^{c_2} を DDH 問題の入力として用いる．ただし，g^{c_2} は a を用いて $g^{c_2 a}$ と変換しておく．$< g^b, g^{ae}, g^{c_2 a} >$ の 3 タプルを入力として DDH 問題を解くと $g^{c_1} = g^{ae}$ かつ $g^c = g^{c_2} = g^{be}$ を満たす e が存在するかどうか判定できる．しかし，$g^c = g^{ae}$ となる e が存在するかどうか判定する問題は DDH 問題よりも困難な問題かもしれない．その場合，*E-I* 問題は DDH 問題に帰着できない可能性がある．

6. 従来プロトコルと提案プロトコルの機密性に関する考察

4.3 節から DDH 問題と indistinguishability 問題が等価であること，5.3 節から，提案プロトコルの *E-I* 問題は DDH 問題に帰着できない可能性があることがわかった．この節では，考察により提案プロトコルと従来プロトコルの機密性の差異を明確にしていく．

E-I 問題を解くには，indisitinguishability 問題を解くことに加えて，$g^{c_1} = g^{ae}$ または $g^{c_2} = g^{be}$ を満たす e が存在するかを判定しなければならない．この問題は indisitinguishability 問題を用いて図 4 のように変換可能である．ここで，indistinguishability 問題は DDH 問題と等価であることから DDH 問題への入力変換を考える．DDH 問題は入力として $< g^a, g^b, g^c >$ が必要であった．よって，変換問題 1 は $< g^a, g^b, g^{c_1} >$

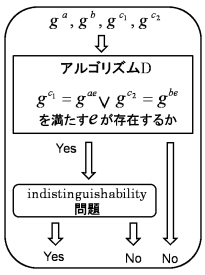

図 4　*E-I* 問題の変換問題 1

を入力とする図 5 のような問題に変換できる．この変換問題 2

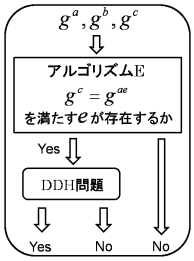

図 5　*E-I* 問題の変換問題 2

は，まず，e が存在するかの判定を行うことと，e が存在する場合に，$e = b$ であるか，そうでないかを判定する三種類の答えを導出する問題と言える．この問題を DDH$^+$ 問題と定義する．DDH$^+$ 問題を図 6 に示す．以上から *E-I* 問題は DDH$^+$ 問題に

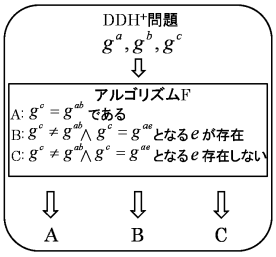

図 6　DDH$^+$ 問題

帰着可能である．DDH$^+$ 問題は DDH 問題の判定が $g^c = g^{ab}$ でない場合，さらに，$g^c = g^{ae}$ となる e が存在するかどうかを判定することを要求する．このことから DDH$^+$ 問題は DDH 問題に比べて困難な問題である可能性がある．

さらに，*E-I* 問題と DDH$^+$ 問題が等価であることを示すため，DDH$^+$ 問題から *E-I* 問題への帰着を考える．まず，定義域 $KeyF$ から適当な値 h を選び，g^h を作成し，DDH$^+$ 問題の入力である g^b を h を用いて g^{bh} へ変換する．次に，DDH$^+$ 問題の入力である $< g^a, g^b, g^c >$ と h をもとに作成した $< g^h, g^a, g^{bh}, g^c >$ を *E-I* 問題の入力 $< g^A, g^B, g^{C1}, g^{C2} >$ に対応するものとして与える．そのとき，$g^{C1} = g^{bh} = g^{AE}$ かつ $g^{C2} = g^c = g^{BE}$ となる E が存在するかどうかを判別することで DDH$^+$ 問題の出力判定をできれば帰着可能となる．また DDH$^+$ 問題は出力パターンが三種類あるのに対して，*E-I* 問題は出力が二種類しかない．よって，三種類の判定を行うため，以下に示すような *E-I* 問題を二回解くことで DDH$^+$ 問題を *E-I* 問題に帰着させる．

E-I 問題への入力として $< g^h, g^a, g^{bh}, g^c >$ を与えるとき，出力が yes の場合に $g^{bh} = g^{C1} = g^{AE}$ となることから $E = b$ となる．その場合，$g^c = g^{BE}$から $g^c = g^{ab}$ とならなければならない．以上から，DDH$^+$ 問題の出力パターン A の $g^c = g^{ab}$ であるかそうでないかの区別が可能である．

また，*E-I* 問題が no と判定すると，$g^c = g^{ae}$ ではないという判定しか行えない．よって，DDH$^+$ 問題の出力パターン B，C の $g^c \neq g^{ab}$のとき $g^c = g^{ae}$ となる e が存在するかどうかを判別するためにもう一度 *E-I* 問題を利用する．二度目の *E-I* 問題では，DDH$^+$ 問題の入力である g^a, g^c から $< g^a, g^a, g^c, g^c >$ を生成し，*E-I* 問題の入力として与える．入力 $< g^a, g^a, g^c, g^c >$ から *E-I* 問題解決アルゴリズム C では $g^c = g^{ae} \wedge g^c = g^{ae}$ を満たす e が存在するかどうかの判定が行われる．この判定は $g^c = g^{ae}$ を満たす e が存在するかどうかを判定することと等しい．つまり，DDH$^+$ 問題の出力パターンが B であるか，C であるかの判定を二度目の *E-I* 問題の yes，no の答えにより判定できることがわかる．よって，*E-I* 問題と DDH$^+$ 問題の双方から帰着可能なことから *E-I* 問題と DDH$^+$ は等価な問題と言える．

DDH 問題は indistinguishability 問題と，DDH$^+$ 問題は *E-I* 問題と等価であることから，*E-I* 問題と indistinguishability 問題の差異は DDH 問題と DDH$^+$ 問題の差異に等しい．以上から，暗号化関数に $f_e(x) \equiv x^e \bmod p$ を用いた提案プロトコルは従来プロトコルの機密性に比べて，機密性向上の可能性がある．

7. おわりに

本稿では，文献 [5] で提案したプロトコルと従来プロトコルの機密性の違いについて述べるため，それぞれのプロトコルの機密性を決定している特性に着目し，多項式時間帰着により，提案プロトコルと従来プロトコルの機密性が等価であるかどうか検証した．その結果，従来プロトコルと提案プロトコルの機密性の差を明確にし，提案プロトコルの機密性は従来プロトコルの機密性より高いものである可能性を述べた．

本稿では，従来プロトコルに用いている暗号と同じ暗号を提案プロトコルで用いることにより，機密性の向上を確認したが，弱い暗号を提案プロトコルに用いて従来プロトコルと同じ機密性を確保することも考えられる．さらに，従来プロトコルで用いている暗号と先に述べた弱い暗号の比較から提案プロトコルの機密性向上を明確にできると思われる．

文　献

[1] R. Agrawal, A. Evfinievski and R. Srikant, " Information sharing across private databases, " Proceedings of the 2003 ACM SIGMOD International Conference on Management of Data (SIGMOD 2003), pp.86-97, 2003.

[2] D. Boneh," The decision Diffie-Hellman problem, "Proceedings of the 3rd International Algorithmic Number Theory Symposium, volume 1423 of Lecture Notes in Computer Sciences, pp.48-63, 1998.

[3] D. R. Stinson, " Cryptography Theory and Practice Third Edition ", Chapman & Hall/CRC, 2006.

[4] B. Schneier," Applied Cryptography, "Second Edition, John Wiley and Sons, 1996.

[5] 隅，村本，上土井，若林，" 複数データベース間における機密性を保持した情報共有の一手法 "，DEWS 2008，2008.

[6] 辻井，岡本，" 暗号のすべて〜ユビキタス社会の暗号技術〜 "，電波新聞社，2002.

[7] N. Zhang and W. Zhao, " Distributed privacy preserving information sharing, " Proceedings of the 31st VLDB Conference, pp.889-900, 2005.