3　情報漏えい対策技術

3 Countermeasures Against Information Leakage

3-1　部分群メンバーシップ問題と情報セキュリティへの応用

3-1 Subgroup Membership Problem and Its Applications to Information Security

山村明弘　齊藤泰一
YAMAMURA Akihiro and SAITO Taiichi

要旨

広く利用されているアルゴリズム問題、平方剰余問題と決定 Diffie-Hellman 問題は、部分群メンバーシップ問題として特徴付けられる。幾つかの暗号理論は、部分群メンバーシップ問題の難解さを仮定することで実現される。部分群メンバーシップ問題を情報セキュリティに適用する：確率暗号、ビットコミットメント、プライベート情報検索。

The widely used algorithmic problems,the quadratic residue problem and the decision Diffie-Hellman problem, are characterized as the subgroup membership problem. Several cryptographic schemes are realized assuming the hardness of the subgroup membership problem.We apply the subgroup membership problem to several information security schemes: a probabilistic encryption, a bit commitment and a private information retrieval.

[キーワード]
部分群メンバーシップ問題，決定 Diffie-Hellman 問題，平方剰余問題，確率的暗号，プライベート情報検索
Subgroup membership problem, Decision diffie-hellman problem, Quadratic residue problem, Probabilistic encryption, Private information retrieva

1　まえがき

オープンなネットワークが高度化し、インターネットは各ビジネス分野においても不可欠なインフラとなりつつある。2005 年 4 月からは e 文書法も施行され文書の電子化は社会のデジタル化を加速させる。情報のデジタル化は利便性を高める一方で、情報漏えいが起きやすくなるといった負の側面も併せ持つ。デジタル情報は簡単に複製することができるし、また、複製のこん跡も残らない。このようなデジタル情報が漏えいして不正に利用されないように、高度ネットワーク社会を構築するためにセキュリティ技術を提供していくことが情報セキュリティ研究者の急務である。暗号・認証技術や暗号プロトコル（セキュアプロトコル）は情報セキュリティにおいて基盤技術であり、これなしでは情報セキュリティは達成できない。攻撃者側は常に攻撃対象の弱い部分をねらうため、学術的に研究が進んでいる暗号技術について攻撃目標とされることは比較的少なかった。しかし、幾つかのハッシュ関数における研究の進展などをかんがみると攻撃者側の能力は常に上昇していると考えるべきである。暗号技術においても現状

に甘んじることなく、安全安心な社会基盤の構築のために研究を進めていくことが必要である。本論文では暗号技術の核心にあるアルゴリズム問題が幾つかの暗号プロトコル（セキュアプロトコル）に適用することを考察する。情報漏えいを含む情報セキュリティに対する一つの取組として紹介する。

2 部分群メンバーシップ問題

有限表示群の部分群メンバーシップ問題は、一般的に決定可能ではないことはよく知られている。Novikov-Boone 定理において、語の問題が決定的でない有限表示群の存在が示されているからである。このことは、幾つかの有限表示群では、語として与えられた元が群の単位元であるかどうか判断するアルゴリズムがないということを意味している。部分群メンバーシップ問題は、組合せ群論の研究では、一般化された語の問題と呼ばれる。一方、語の問題は有限群や有限的生成アーベル群においては、常に決定的である。

しかし、より現実的な計算、つまり確率多項式時間アルゴリズム（又は計算量クラス BPP と等しい）を考える場合、メンバーシップ問題は有限アーベル群の分野においてさえ、自明ではない。数学的オブジェクトを考えるとき、そのオブジェクトは有限データにより表現される。その効率は、数学的命題（述語の計算に匹敵する）や演算関数を決定するといった幾つかのタスクを実行するためのアルゴリズムの漸近的挙動によって測定される。有限表示群のための決定問題の場合は帰納的関数の分野で考える。オートマティック群やワード双曲幾何群のような特定の場合には、語の長さに関する多項式時間で語の問題は解くことができる。有限群の場合は、群の記述は簡単な構造であり、すべての決定問題は可解である。このようなアルゴリズムに関しては、その効率に関心を持つ。アルゴリズムの挙動は群の族のデータ構造のサイズに関係している。

暗号において利用されている幾つかのアルゴリズム問題は部分群メンバーシップ問題として特徴付けられる。素因数分解問題又は離散対数問題のための確率的多項式時間アルゴリズムは存在しないことに注意したい。このため、これらの問題は BPP の計算量クラスには属さない。平方剰余（略して QR）問題と決定 Diffie-Hellman（略して DDH）問題は、暗号技術に多くの応用があり、よく研究が行われている。[17] において、QR と DDH の類似性が論じられている。部分群メンバーシップ問題として暗号学的な難解なアルゴリズム問題を一般化、形式化するためのより形式的な方法を与え、公開鍵暗号で使用される他の暗号に関する問題が同様に部分群メンバーシップ問題として特徴付けられることを示す。暗号に関する問題のこのような統一的手法は著者の知る限り、今までに取り上げられたことはない。

暗号学において広く利用される仮定は、以下の二つのグループ、素因数分解問題（及び QR）に関する仮定と、離散対数問題（及び DDH）に関する仮定に分けられる。前者は、RSA 暗号システム [15] に起因し、後者は Diffie-Hellman 鍵交換プロトコル [6] に起因する。この二つの仮定は、異なるように見えるので、通常別々に論じられている。素因数分解問題と離散対数問題の統一的な観点は、情報セキュリティに必要とされるアルゴリズムの基本的性質に光を当てる。部分群メンバーシップ問題による統一化により、アルゴリズム問題についてより深く理解することができる。部分群メンバーシップ問題を非対称鍵暗号システムなどの暗号スキームに適用するためには、合法的な通信者が効率よく計算できることとトラップドアの存在が必要となる。部分群メンバーシップ問題が一般的に特定のスキームに適用できることを証明できれば、特定の群に関する部分群メンバーシップ問題がそのスキームに適用できる。例として、本論文では、部分群メンバーシップ問題を一般的に RIP システムを構築することにより、すべての部分群メンバーシップ問題が PIR システムを構築するために適用することができることを示す。

与えられた元の部分群のメンバーシップを決定することは、通常、簡単ではない。実際、有限表示群における部分群のメンバーシップ問題は、一般的に決定的ではない。非対称鍵暗号のような暗号スキームにメンバーシップ問題を適

用するためには、合法的な参加者の効率的な計算とトラップドアの存在が必要である。この節では、部分群メンバーシップ問題をトラップドアとともに考察し、暗号学において広く利用されている幾つかの問題は部分群メンバーシップ問題として特徴付けられることを示す。

Gは群であり、Hはその部分群であるとする。メンバーシップ問題は、Gの与えられた元gがHに属するか否かを決定することである。さらに、我々は変数によりインデックスをつけられた有限群の族と計算量の漸近的な挙動を考察する。このような場合、元、部分群、変数によりインデックスをつけられた群を与えられたときのメンバーシップを決定するための計算的問題として、部分群メンバーシップは記述される。計算的問題は効率的なアルゴリズムがない場合は、困難である。この効率性はアルゴリズムの漸近的挙動によって特徴付けられる。

2.1　部分群メンバーシップ仮定

Gのすべての元は、サイズkのバイナリ表現を持つと仮定する。ここで、kはセキュリティパラメータである。トラップドアと呼ばれる特定の情報が提供される場合、メンバーシップはkに関する多項式時間内で決定することができる。トラップドアによりHのGにおける元gのメンバーシップは決定される一方、トラップドアがない場合は1/2よりも十分大きな確率で、メンバーシップを決定することができない。部分群メンバーシップ問題を正式な定義を与える。

kはセキュリティパラメータとする。入力1^kに対して、確率的多項式時間アルゴリズムIGは群Gの記述、Gの部分群Hの記述、GにおけるHの部分群メンバーシップ問題のための多項式時間アルゴリズムを提供するトラップドアを出力する。アルゴリズムIGはインスタンスジェネレータと呼ばれる。Gのすべての元は、長さkのバイナリ列として表現される。Gの演算の計算は、kに関する多項式時間で実行される。

部分群のメンバーシップのための述語はMemによって示される。つまりMemは次のように定義される。

$$Mem(G,H,x)=\begin{cases}1 & \text{if x lies in H}\\ 0 & \text{if x lies in S}\end{cases}$$

ここで、IGは1^kに対し(G, H)を出力する。xはGの元、$S=G\setminus H$である。1^kを入力し、二つの群(G, H)とGの元gを得たときに、kの多項式時間におけるMemを計算することが部分群メンバーシップ問題である。ここで、元gは、コイントス$b\xleftarrow{R}\{0,1\}$に従って、一様にランダムにH又はGから選ばれる。1/2より十分大きい確率でMemを計算する確率的多項式アルゴリズムが存在しない場合、このメンバーシップ問題は難解である。H及びGから一様にランダムに元を選べると仮定する。このことは、暗号スキームへの応用において重要である。

下記事項は自明なことであるが、部分群メンバーシップ問題に基づき、PRIシステムを構築するために有益である。

命題1

Gは群、HはGの部分群とする。Gのすべてのgと、Hのすべてのhに関して、ghがHにある場合、またこの場合に限り、gはHにある。

部分群メンバーシップ仮定Ⅰ

すべての定数cと多項式がkのサイズの回路の族$\{C_k|k\in N\}$に対し、ある整数Kが存在し、すべての$k>K$に対し、

$$\mathrm{Prob}(C_k(G,H,g)=Mem(G,H,g))<\tfrac{1}{2}+\tfrac{1}{k^c}\quad(2.1)$$

が成立する。

この仮定は述語Memを計算するための多項式サイズの回路の族が存在しないことを主張している。次は上記の仮定と同値である。

部分群メンバーシップ仮定Ⅱ

すべての定数cと多項式がkのサイズの回路の族$\{C_k|k\in N\}$に対し、ある整数Kが存在し、すべての$k>K$に対し、

$$\left|P_H-P_S\right|<\tfrac{1}{k^c}|\quad(2.2)$$

が成立する。ここで、確率P_HとP_Sは以下のように定義される。

$$P_H=\mathrm{Prob}_{(G,H)\leftarrow IG(1^k);g\xleftarrow{R}H}(C_k(G,H,g)=1)$$

及び

$$P_S = \mathrm{Prob}_{(G,H)\leftarrow IG(1^k);g\xleftarrow{R}S}(C_k(G,H,g)=1)$$

2.2 具体例

我々は幾つかの部分群メンバーシップ問題を例示する。DDH 問題、QR 問題、高次剰余問題がある。QR 問題が困難であるという仮定（QR 仮定）は、Goldwasser-Micali 暗号システム[8]のセマンティックセキュリティを証明するために利用されていること、また、DDH 問題が困難であるという仮定（DDH 仮定）は、ElGamal 暗号システムのセマンティックセキュリティを証明するために利用されている。これら二つの仮定は、他にも多数、適用されている。上記問題が困難であるという仮定は、対応する暗号システム[10][13][14]のセマンティックセキュリティをそれぞれ証明するために使用されている。

平方剰余問題

p、q は素数とし、$N=pq$ とする。素数 p と q は、平方剰余問題のためのトラップドアであり、一方、N は公開情報である。G をヤコビ記号が 1 である元から成る $(\mathrm{Z}/(N))^*$ の部分群とし、H は G の平方剰余から成り立つ G の部分群とする。つまり、

$$H=\left\{x\in G \middle| x=y^2 \bmod \mathrm{N} \text{ for } y\in(\mathrm{Z}/(\mathrm{N}))^*\right\}$$

である。G の部分群 H の平方剰余問題は与えられた元 g が H に属するか否かを決定することである。p と q の情報が得られる場合は、H の g のメンバーシップを効率的に決定することができる。p と q の情報がない場合は、G のランダムに選ばれた元のメンバーシップを決定する多項式時間アルゴリズムは存在しない。したがって、確率的アルゴリズムとして、QR 問題のインスタンスジェネレータを定義する場合、QR 問題は部分群メンバーシップ問題として考えられる。

決定 Diffie-Hellman 問題

C は位数が素数 p の巡回群であるとする。群 C は有限体の乗法群又は楕円曲線の有理点の群である。g は C の生成元であるとする。決定 Diffie-Hellman 問題は、C 内の元の与えられた四つ組 (g_1, h_1, g_2, h_2) に関して、$h_2=g_2^a$ が成り立つか否かを決定することである。ここで、$1\le a\le p-1$ に関して、$h_1=g_1^a$ である。成り立つ場合は、(g_1, h_1, g_2, h_2) は Diffie-Hellman の四つ組であるという。整数 a は決定 Diffie-Hellman 問題のトラップドア情報である。トラップドア情報 a を得ることにより、効率的に $h_2=g_2^a$ であるか否かを決定することができる。

DDH 問題は、以下のような群に関する、部分群メンバーシップ問題として特徴付けることができる。G は直積 $C\times C$ であるとする。DDH 問題の入力は (x, y), $x, y\in G$ である。つまり $x=(g_1, h_1)$ 及び $y=(g_2, h_2)$。y が、x により生成された G の部分群 $\langle x\rangle$ に属する必要かつ十分条件は (g_1, h_1, g_2, h_2) が Diffie-Hellman の 四つ組であることは明らかである。よって、巡回群 C に関する DDH 問題は群 $H=\langle x\rangle$, $x=(g_1, g_1^a)$ の群 $G=C\times C=\langle g_1\rangle\times\langle g_1\rangle$ における部分群メンバーシップ問題と同値となる。H 内の生成元 x が与えられれば、トラップドア情報がなくても、一様かつランダムに H から元を選ぶことができる。

我々は例を表 1 にまとめる。表はすべてを網羅しているものではない。部分群メンバーシップ問題と同値であるアルゴリズム問題については[17][18]で詳しく述べられているので、参照してほしい。

2.3 確率暗号

Goldwasser と Micali[8]はセマンティックセキュア確率暗号スキームを導入した。その安全性は QR 仮定に基づいている。受動的な攻撃者に漏えいする情報が計算量的に無視できる場合、それは、セマンティックセキュアと呼ばれる。この概念は、Shannon の情報理論的安全性の計算量理論的なものである。この概念は、現代暗号学において、重要である。

部分群メンバーシップ問題を、確率暗号に適用する。決定 Diffie-Hellman 問題に基づく確率暗号に関しては、[16]を参照してほしい。

鍵生成

インスタンスジェネレータと呼ばれる確率的多項式時間アルゴリズム IG に、Bob は 1^k を入力し、群のペア (G, H) と G の部分群 H における部分群メンバーシップ問題に関するトラップドア情報を得る。ここで、k はセキュリティパラメータである。G のすべて元は、長さ k のバイナリ列として表現される。部分群 H の G における

	関連する問題	群 部分群	適用事例
DDH	DLP DH	$C \times C$: 巡回群の直積 $<(g,h)>:(g,h)$	ElGamal により生成された部分群
QR	$FACT(pq)$	$\{x \in \mathrm{Z}_N^* \mid \frac{x}{N}) = 1\}$ $\{x^2 \bmod N \mid x \in \mathrm{Z}_N^*\}$	Goldwasser-Micali[8]
RR	$FACT(pq)$	Z_N^* $\{x^\tau \bmod N \mid x \in \mathrm{Z}_N^*\}$	黒澤-辻井[10]
PSUB	$FACT(p^2q)$	$\{x \mid x = g^m y^N \bmod N \ for$ $m \in \mathrm{Z}/(p), y \in (\mathrm{Z}/((N))^*\}$ $\{y^N \bmod N \mid y \in \mathrm{Z}_N^*\}$	岡本 - 内山 [13] Naccache-Stern[11]
DCR	$FACT(pq)$	$\{x \mid x = g^m y^N \bmod N^2$ $m \in \mathrm{Z}/(N), y \in (\mathrm{Z}/((N^2))^*\}$ $\{y^N \bmod N \mid y \in \mathrm{Z}_N^*\}$	Paillier[14]

図1　部分群メンバーシップ問題

部分群メンバーシップ仮定を想定する。よって、Alice は G と H の両方の元を一様かつランダムに生成することができる。Bob は G と H を公開するが、H の部分群メンバーシップ問題のための トラップドア情報は秘密にする。

暗号化

Alice がメッセージ $M = b_1 b_2 b_3 \cdots n_1$ を暗号化すると仮定する。ここですべての i=1, 2, 3, …, l に対して b_i は{0, 1}に属する。すべての b_i ($1 \le i \le l$) に対し、Alice はランダムに元 r_i を生成する。このとき、もし b_i=1 ならば r_i は H に属し、さもなくば b_i は G/H に属する。このとき群の元の列 ($r_1, r_2, r_3, \ldots, r_l$) が、$M$ に対する暗号文である。暗号化されたメッセージは、直積 $S_1 \times S_2 \times S_3 \times \ldots S_1$ におけるランダムな元であることに注意する。このとき b_i=1 ならば $S_i = H$ であり、さもなくば $S_i = G \backslash H$ である。よってこの暗号は確率的である。

復号

Bob は G の部分群 H における部分群メンバーシップ問題のためのトラップドア情報を知っている。よって、彼は、セキュリティパラメータ k の多項式時間で各元が H に属しているか否かを決定することができる。

安全性

あらゆる攻撃者が同じ長さの二つの暗号文を計算量理論的に識別できない場合、暗号スキームはセマンティックセキュアであるという。これは、あらゆる確率的多項式時間アルゴリズムによって、二つの暗号文 C_1 と C_2 が識別できないということを意味する。よって、上記の暗号がセマンティックセキュアであることの必要かつ十分条件はあらゆる確率多項式時間アルゴリズムが二つの直積 $S_1 \times S_2 \times S_3 \times \ldots S_l$ と $S_1 \times S_2 \times S_3 \times \ldots S_l$ を識別できないということである。このように、G の部分群 H における部分群メンバーシップ仮定の下、この暗号化方法はセマンティックセキュアである。

2.4　ビットコミットメント

部分群メンバーシップ問題の他の応用事例は、ビットコミットメントスキームである。部分群メンバーシップ問題に基づくビットコミットメントについて、簡単に述べる。決定 Diffie-Hellman 問題に基づくビットコミットメントスキームに関しては、[16] を参照してほしい。

鍵生成

Alice はインスタンスジェネレータ IG に 1^k を入力し、群のペア (G, H) と G の部分群 H におけ

る部分群メンバーシップ問題に関するトラップドア情報を得る。ここで、kはセキュリティパラメータである。Gの部分群Hの部分群メンバーシップ仮定を仮定する。AliceはGとHを公表するが、Hの部分群メンバーシップ問題のためのトラップドア情報は秘密にする。

コミットメント

Aliceは(0, 1)内の自分のビットbをコミットする。ビットbに従って、一様かつランダムに元rを生成する。つまりb=1ならばrはHに属し、さもなくばG/Hに属する。

検証

AliceはBobに自分のビットbを伝え、部分群メンバーシップのためのトラップドアを与える。Bobは元rのメンバーシップを検証することができる。

このように、幾つかの部分群メンバーシップ問題をビットコミットメントプロトコル構築のために応用することができる。同様に、ビットコミットメントプロトコルは、コインフリッピングプロトコル構築のために使用できることにも注意する。

3 プライベート情報検索

Chor、Goldreich、Kushilevitz、Sudan[3]らは、リモートデータベースアクセスのためのプライベート情報検索スキーム(PIRスキーム)を紹介した。このスキームを利用すると、情報を漏えいすることなく、自分が選択したデータを、ユーザは検索することができる。彼らのスキームは、情報理論的安全性を実現したが、データベースは複数構築され、管理者はお互いに連絡することが許されない。計算量理論的に安全な情報検索スキームはChorとGilboa[4]によって、導入された。彼らのスキームは、Chor、Goldreich、Kushilevitz、Sudanのモデルと比較すると、情報理論的安全性を犠牲にすることにより、効率的なコミュニケーション方法を実現する。それにもかかわらず、彼らのスキームは擬似乱数生成元の存在を仮定することにより、計算量的安全性を満足する。しかし、彼らのスキームも、複数のデータベースが必要である。KushilevitzとOstrovsky[9]は、一つのデータベースだけで計算量的な安全性を持ったプライベート情報検索スキームを導入した。彼らのスキームは、平方剰余問題の困難性に依存する。より効率的な方法としては、ポリロガリズミック通信複雑度がCachin、Micali、Stadler[2]らによって、実現された。彼らは、Φ仮定と呼ばれる仮定を想定し、ワンラウンド通信を犠牲にし、ポリロガリズミック通信複雑度を得ている。しかし、Φ仮定の厳密な証明や平方剰余仮定や素因数分解問題仮定のような一般的に利用されている仮定は[2]には与えられていない。既存のプライベート情報検索スキームの結果を表2にまとめる。

プライベート情報検索(略してPIR)スキームの一般的なスキームを簡単に説明する。単独のデータベースを持つ計算量的安全性を持つPIRスキームは、二人のプレーヤ、つまりユーザUとデータベース管理者DBのプロトコルである。二人とも確率的多項式時間の計算のみ実行することができる。データベース管理者DBはデータベースを維持管理する。データベースは、バイナリ列$X=x_0x_1x_2\cdots x_{n-1}$である。プロトコルの最終目標は、$U$が、$x_i$の情報を$DB$に漏らすことなく、$X$の$i$番目のビット$x_{i+1}$を得ることである。プロトコルは以下のように実行される。

ステップ1

Uは、自分のランダムテープ(コイントス)を使用して、問い合わせQuery(i)を計算する。このランダムテープは秘密にする。彼は、Query(i)をDBに送る。

ステップ2

DBはQuery(i)を受け取る。彼は入力X、Query(i)、彼のランダムテープに対して多項式時間計算を行い、Answer(Query(i))を得る。彼はAnswer(Query(i))をUに送り返す。

ステップ3

UはAnswer(Query(i))を受け取る。彼はAnswer(Query(i))と自分のプライベート情報(自分のランダムテープ)を使用して多項式時間計算を行い、データベースのi番目のビットx_{i+1}をもたらす。

正当性

すべてのデータベースXとXのi番目のビットのためのすべての問い合わせに関して、Uは最終的にx_{i+1}を得る。

スキーム	ラウンド数	安全性仮定	通信複雑度	DBの個数
Chor, Coldreich, Kushilevitz, Sudan[3]	1	情報理論	$o(n^{1/3})$	≥2
Ambainis[1]	1	情報理論	$o(n^{2k-1})$ for $k(>1)DB$	≥2
Chorと Gilboa[4]	1	擬似数生成元存在	$O(n^c)$ $c>0$	≥2
Kushilevitzと Ostrovsky[9]	1	平方剰余問題仮定	$O(n^c)$ $c>0$	1
Ostrovskyと Shoup[12]	複数	PIRスキームへの帰着		
Cachin, Micali と Stadler[2]	2	Φ仮定	ポリロガリズミック	1
本論文のスキーム[17][18]で導入	1	部分群メンバーシップ仮定（例：DDH仮定）	$O(n^c)$ $c>0$	1

図2　プライベート情報検索スキーム

プライバシー

*DB*は*i*番目のビットのための問い合わせと*j*番目のビットのための問い合わせの識別が多項式時間（確率的）計算によって無視できない確率でできない。形式的には、すべての定数*c*、長さ*n*のすべてのデータベース、二つの$1 \le i, j \le n$すべての多項式サイズの回路の族C_kに対して、ある整数*K*が存在し、すべての$k>K$に対し、

$$\left|\mathrm{Prob}(C_k(\mathrm{Query}(i))=1) - \mathrm{Prob}(C_k(\mathrm{Query}(j))=1)\right| < \sigma \quad (3.1)$$

が成立する。ここで、*k*はプロトコルのセキュリティパラメータであり、$\sigma = \frac{1}{(Max(k,n))^c}$である。

計算量

*DB*と*U*の計算は両方共、データベースのサイズ*n*とセキュリティパラメータ*k*の多項式時間である。

3.1　部分群メンバーシップ問題に基づくPIRスキーム

KushilevitzとOstrovskyのスキーム[9]を変更することにより、部分群メンバーシップ問題はPIRスキームに応用できることを示す。提案されたスキームは、QR仮定に依存しているKushilevitzとOstrovskyのスキームと同じ通信複雑度を持つ。一方、本論文で提案されたPIRスキームの安全性は、部分群メンバーシップ仮定に基づく。したがって、**2.2**におけるどのアルゴリズム問題を基礎にしてもPIRスキームを構築することができる。具体的には、楕円曲線上の有理点群や、DDH仮定に対応する有限体の乗法群を利用することができる。今までに提案されたすべてのPIRスキームは、擬似乱数生成器や素因数分解問題に関連する仮定のどちらかに依存している。著者の知る限り、DDHに基づくPIRスキームはまだ提案されていない。[9]を変更し、部分群メンバーシップ問題に基づくPIRスキームを構築する。

3.2　基本概念

最初に、簡単なモデルを使用して、このスキームの基本概念を説明する。*DB*はデータベース$X=x_0x_1x_2\cdots x_{n-1}$を持ち、*U*は*i*番目のビット

x_{i-1}を知りたいと仮定する。Uは群の元 g_0, g_1, g_2, …g_{i-1}, …g_{n-1}を選択し、$j \neq i-1$のとき g_jはH内にあり、g_{i-1}は$S=G\backslash H$にある。次に、Uは選択した元すべてを DBに送る。DBは群の元 $g=g_0^{x_0} g_1^{x_1} g_2^{x_2}$, …$g_{i-1}^{x_{i-1}}$, …$g_{n-1}^{x_{n-1}}$を計算し、それを$U$に返送する。$G$の部分群 Hにおける部分群メンバーシップ問題が難解である場合、DBは g_0, g_1, g_2, …g_{i-1}, …g_{n-1}のうちどれがSの元か知ることができない。Uはトラップドア情報を知っているので、gがHに属するか否か決定することができる。$x_{i-1}=0$の場合又はこの場合に限り、**命題 1** により、gはHに属する。よってUはi番目のビット x_{i-1}を得ることができる。この簡単なモデルは、部分群メンバーシップ問題の概念を説明しているが、通信複雑度はまだ大きい。この通信複雑度を軽減するために、[9]のトリックが必要である。

3.3 スキーム

部分群メンバーシップ問題を使用して、PIRスキームを説明する。

ステップ 0

ユーザ Uはインスタンスジェネレータ IGに1^kを入力し、二つの群のペア(G, H)とGの部分群 Hにおける部分群メンバーシップ問題のためのトラップドアを得る。ここで、kはセキュリティパラメータであり、Gのすべての元は長さ kのバイナリ列で表現される。Gの部分群 Hにおける部分群メンバーシップ仮定を想定する。群Gは、DBと Uの両者により、共有される。一方、UはHの部分群メンバーシップ問題のためのトラップドア情報を秘密に保持する。DBと U両者の計算は、群 G内で実行される。Xは DBによって保持されるデータベースである。$X=x_0x_1x_2\cdots x_{n-1}$であり、$x_i$は$(0, 1)$に属する。そして$n=t^l$、ここで t, lは正の整数であると仮定する。

ステップ 1

Uは以下の方法で、自分が望むビット x_{i-1}のための、問い合わせ Query$\{$(i)を計算する。ここで、$1 \le i \le n$である。最初に、Uはiの $t-$進展開を計算する。$i=\alpha_0$とする。iの $t-$進展開は$\beta_l \beta_{l-1}\cdots\beta_2\beta_1$とする。ここで、

$$\begin{aligned}
&\alpha_0 = \alpha_1 t + \beta_1 \quad 0 \le \alpha_0 \le t^{l-1} \; and \; 0 \le \beta_1 \le t-1 \\
&\alpha_1 = \alpha_2 t + \beta_2 \quad 0 \le \alpha_1 \le t^{l-2} \; and \; 0 \le \beta_2 \le t-1 \\
&\alpha_2 = \alpha_3 t + \beta_3 \quad 0 \le \alpha_2 \le t^{l-3} \; and \; 0 \le \beta_3 \le t-1 \\
&\qquad\qquad \cdots\cdots \\
&\alpha_{l-2} = \alpha_{l-1} t + \beta_{l-1} \quad 0 \le \alpha_{l-2} \le t-1 \; and \; 0 \le \beta_{l-1} \le t-1 \\
&\qquad\qquad 0 \le \alpha_{l-1} = \beta_l \le t-1 \;\; \alpha_l = 0
\end{aligned} \tag{3.2}$$

である。

各 $u(1 \le u \le l)$に対して、Uは、Hから $t-1$個の元 $g_{(u,0)}$, $g_{(u,1)}$, …, $g_{(u,\beta_u-1)}$, $g_{(u,\beta_u+1)}$, …, $g_{(u,t-1)}$を一様かつランダムに選ぶ。また、$S=G\backslash H$から一様かつランダムに、$S=G\backslash H$から $g_{(u,\beta_u)}$を選ぶ。Uは、Q(u)を以下のように定義する。

$$(g_{(u,0)}, g_{(u,1)}, \ldots, g_{(u,\beta_u-1)}, g_{(u,\beta_u)}, g_{(u,\beta_u+1)}, \ldots g_{(u,t-1)}) \tag{3.3}$$

つまり、Q(u)は群 Gの元の列であり、β_u番目の元は一様かつランダムに $S=G\backslash H$から選ばれ、他の成分は、一様かつランダムに Hから選ばれている。このとき Q(1), Q(2), …, Q(l)は、Xのi番目のビット x_{i+1}のための問い合わせ(Query$\{$(i)により表示される)を構成し、UはQuery(i)を DBに送る。各Q(u)は t個の群 Gの元から成るので、Q(u)は $k \times t \times l$ビットである。よって、Query(i)は $k \times t \times l$ビットから成る。

ステップ 2

Query$\{$(i)を受け取り、DBはオリジナルデータベースから、帰納的に子データベースを構築する。我々は、Xを $t^{l-1} \times t$のバイナリマトリクスとして、みなす。

$$D(0,\lambda) = \begin{pmatrix} x_0 & x_1 & x_2 \; \ldots & x_{t-1} \\ x_t & x_{t+1} & x_{t+2} & x_{2t-1} \\ & & \cdots & \\ x_{t^l-t} & x_{t^l-t+1} & \ldots \; \ldots & x_{t^l-1} \end{pmatrix}$$

ここで、λは$\{0, 1, 2, \ldots, k-1\}^*$における空の列を表す。ターゲットビット$x_{i-1}$は、$D(0, \lambda)$の$(\alpha_1, \beta_1)$成分であることに注意する。($\alpha_1$と$\beta_1$は(3.2)により得られる。)それを Target $D(0, \lambda)$と記す。

我々は帰納的に子データベースを $D(u, s)$と定義する。ここで、$1 \le u \le l$であり、sは$\{0, 1, 2, \ldots, k-1\}^u$に属する。データベース $D(u, s)$、そのターゲットビット Target $D(u, s)$を既に定義したと仮定する。ここで$0 \le u \le l-1$、sは$\{0, 1, 2, \ldots, k-1\}^u$に属する。次に、データベース $D(u+1, s0)$, $D(u+1, s1)$, …, $D(u+1, s(k-1))$を定

義する。

データベース $D(u, s)$ は長さ t^{l-u} のバイナリ列である。$D(u, s)$ を $t^{l-u-1} \times t$ のバイナリマトリクスとしてみなす。

$$D(0,\lambda)=\begin{pmatrix} y_0 & y_1 & y_2 \cdots & y_{t-1} \\ y_t & y_{t+1} & y_{t+2} & y_{2t-1} \\ & & \cdots & \\ y_{t^{l-u}-t} & y_{t^{l-u}-t+1} & \cdots \cdots & y_{t^{l-u}-1} \end{pmatrix}$$

と仮定する。これから、k 個の子データベース $D(u+1, s0), D(u+1, s1), \ldots, D(u+1, s(k-1))$ を構築する。

Q(u) は群 G の t 個の元 $g_{(u,0)}, g_{(u,1)}, \ldots, g_{(u,\beta_u-1)}, g_{(u,\beta_u+1)}, \ldots, g_{(u,t-1)}$ から構成されていることに注意してほしい。((3. 3) に定義されている) 各行 $v=0, 1, 2, \ldots, t^{l-u-1}$ に対して、群の元 g_v を次のように定義する。

$$f_{(v,w)}=\begin{cases} g_{(u,w)} & if \ \ D_{(u,s)(v,w)}=1 \\ 1 & if \ \ D_{(u,s)(v,w)}=0 \end{cases} \qquad (3.4)$$

と設定する。ここで、$D(u, s)(v, w)$ は、$D(u, s)$ の (v, w) 成分を表す。次に、各行 $v=0, 1, 2, \ldots t^{l-u-1}-1$ に対して、

$$f_{D(u,s),v}=\prod_{w=0,1,2,\ldots,t-1} f_{(v,w)} \qquad (3.5)$$

と設定する。群の元 $f_{D(u, s), v}\ (0 \le v \le t^{l-u-1}-1)$ はサイズ k であり、$f_{D(u, s), v}$ は H に属することの必要かつ十分条件は**命題 1** により $D(u, s)(v, \beta_u)=0$ であることに注意する。r 番目の子データベース $D(u+1, sr)\ (0 \le r \le k-1)$ は $g_0(r), g_1(r), \ldots, g_{t^{l-u-1}-1}(r)$ から成る列として定義される。ここで、$g_v(r)$ は、$f_{D(u, s), v}$ の r 番目のビットを示す。よって、以下の行列方程式を得る。

$$\begin{pmatrix} f_{D(u,s),0} \\ f_{D(u,s),1} \\ \cdots \\ f_{D(u,s),t^{l-u-1}-1} \end{pmatrix}=(D(u+1,s0)\ \ D(u+1,s1)\ \ldots\ D(u+1,s(k-1))) \qquad (3.6)$$

ここで、各 $f_{D(u, s), v}$ は行ベクトルであり、各 $D(u+1, sr)$ は列ベクトルである。よって、$D(u+1, sr)$ は長さ t^{l-u-1} のバイナリ列である。それを $t^{l-u-1} \times t$ のバイナリ行列であると考える。よって、すべての r は $\{0, 1, 2, \ldots, k-1\}$ (α_{u+1} と β_{u+1} は (3.2) で得られる) に対して、ターゲットビット (Target $D(u+1, sr)$ により記される) は、$D(u+1, sr)$ の $(\alpha_{u+1}, \beta_{u+1})$ 成分として定義される。

ステップ 3

子データベース構築の最終段階において、DBk^{t-1} 個のデータベース $D(l-1, s)$ を得る (s は $\{0, 1, 2, \ldots, k-1\}^{t-1}$ にある。)。各 $D(l-1, s)$ は、t 個のビットを含むことに注意する。$D(l-1, s)$ を $1 \times t$ マトリクスとして見なしていることに注意する。各 $D(l-1, s)$ に対して、群の元 $A(s)$ を以下のように定義する。最初に、

$$f_{(0,w)}=\begin{cases} g_{(u,w)} & if \ \ D(l-1,s)(0,w)=1 \\ 1 & if \ \ D(l-1,s)(0,w)=0 \end{cases}$$

と定義する。次に、

$$f_{D(l-1,s),0}=\prod_{w=0,1,2,\ldots,t-1} f_{(0,w)}=A(s)$$

と設定する。$\{0, 1, 2, \ldots, k-1\}^{t-1}$ の各 s に対して群の元 $A(s)$ はサイズ k である。よって、群の元 $A(s)$ (s は $\{0, 1, 2, \ldots, k-1\}^{t-1}$ に属する) は、Query (i) に対する Answer (Query (i)) を構成し、DB は Answer (Query (i)) を U に送る。

ステップ 4

U は、$A(s)$ から成る Answer (Query (i)) を受け取る。ここで、s は $\{0, 1, 2, \ldots, k-1\}^{t-1}$ に属する。U は、k, n の多項式時間で、ターゲットビット x_i=Target$(D_{(0, \lambda)})$ を計算することができる。以下の定理が成立する。

定理 2

Target $(D_{(u+1, s0)})$, Target $(D_{(u+1, s1)})$, … Target $(D_{(u+1, s(k-1))})$ が与えられたとき、各 $D_{(u, s)}$ に対して、U は n, k の多項式時間おいて Target $(D_{(u, s)})$ を計算できる。ここで、$0 \le u \le l-2$ であり、s は $\{0, 1, 2, \ldots, k-1\}^{u}$ に属する。

証明については文献[17][18]を参照してほしい。

3.4 プライバシー

提案されたスキームでは、問い合わせQuery (i) は、Q (1), Q (2), …, Q (l) から成り、各Q (u) は、

$$(g_{(u,0)}, g_{(u,1)}, \ldots, g_{(u,\beta_u-1)}, g_{(u,\beta_u)}, g_{(u,\beta_u+1)}, \ldots g_{(u,t-1)})$$

から成る。ここで、成分の一つは $S=G \backslash H$ から一様かつランダムに選ばれ、それ以外は H から一様かつランダムに選ばれる。プライバシーは、下記不等式から保証される。

$$\left|\mathrm{Prob}(C_k(\mathrm{Query}(i))=1)-\mathrm{Prob}(C_k(\mathrm{Query}(j))=1)\right|<\sigma$$

ここで、$\sigma=\frac{1}{(Max(k,n))^c}$ である。提案されたスキームのプライバシーは、部分群メンバーシップ仮定により、保証されることが示される。

3.5 通信複雑度

最初のステップでは、U は

$$\mathrm{Query}(i)=(Q(1),Q(2),\cdots,Q(1))$$

を送る。各Q(u)は群 G の t 個の元から成る。G 内のすべての元は、長さ k のバイナリ列により表されるので、このステージで送られる総ビット数は、$l\times t\times k$ である。2番目のステップでは、DB は、群 G の k^{l-1} 個の元からなる、Answer(Query(i))を送る。よって、このステージで送られる総ビット数は、$k^{l-1}\times k=k^l$ である。その結果、通信複雑度は $ltk+k^l=\ln^{\frac{1}{l}}k+k^l$ である。$k=n^c$ と $l=O\left(\frac{\log n}{\log k}\right)$ を仮定すると、通信複雑度は $O(n^c)$ となることが分かる([17][18]を参照。)。

4 むすび

公開鍵暗号技術の安全性の基礎となるアルゴリズム問題のなかでも頻繁に利用されている QR 問題や DDH 問題が部分群メンバーシップ問題として定式化されることを示し、幾つかの暗号プロトコルはアルゴリズム問題の特殊な性質ではなく、部分群メンバーシップ問題に直接関連していることを、幾つかの例を通してみた。特にプライベート情報検索といった暗号プロトコルに応用できることを示した。このことは DDH 問題を利用した初めてのプライベート情報検索システムの構築につながった。部分群メンバーシップ問題を利用したプライベート情報検索システムについて小さな例が[18]に与えられているので、興味のある読者は参照してほしい。今後は部分群メンバーシップ問題を更に多くの暗号プロトコル(セキュアプロトコル)に活用し、そのことが暗号理論における新しい理論展開を引き起こすことを期待している。

参考文献

1 A.Ambainis, "Upper Bound on the Communication Complexity of Private Information Retrieval, Automata", Languages and Programming, LNCS, Vol.1256, Springer-Verlag, pp.401-407, 1997.

2 C.Cachin, S.Micali, and M.Stadler, "Computationally Private Information Retrieval with Polylogarithmic Communication", Advances in Cryptology, LNCS, Vol.1592, Springer-Verlag, pp.402-414, 1999.

3 B.Chor, O.Goldreich, E.Kushilevitz, and MM.Sudan, "Private Information Retrieval", IEEE Symposium on Foundations of Computer Science, pp.41-50, 1995.

4 B.Chor and MN.Gilboa, "Computationally Private Information Retrieval", ACM Symposium on Theory of Computing, pp.304-313, 1997.

5 R.Cramer and MV.Shoup, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack", Advances in Cryptology, LNCS, Vol.1462, Springer-Verlag, pp.13-25, 1998.

6 W.Diffie and MM.E. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, Vol.22, pp.644-654, 1976.

7 T.ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Transactions on Information Theory, Vol.31, pp.469-472, 1985.

8 S.Goldwasser and MS.Micali, "Probabilistic Encryption", J. Computer and System Science, Vol.28, pp.270-299, 1984.

9 E.Kushilevitz and R.Ostrovsky, "Replication Is not Needed : Single Database, Computationally-private Information Retrieval", IEEE Symposium on Foundations of Computer Science, pp.364-373, 1997.

10 K.Kurosawa and S.Tsujii, "A General Method to Construct Public Key Residue Cryptosystems", Transactions of the IEICE E-73, pp.1068-1072, 1990.
11 D.Naccache and J.Stern, "A New Public-key Cryptosystem", Advances in Cryptology, LNCS, Vol.1233, Springer-Verlag, pp.27-36, 1997.
12 R.Ostrofsky and V.Shoup, "Private Information Storage", ACM Symposium on Theory of Computing, pp.294-303, 1997.
13 T.Okamoto and S.Uchiyama, "A New Public-key Cryptosystem as Secure as Factoring", Advances in Cryptology, LNCS, Vol.1403, Springer-Verlag, pp.308-318, 1998.
14 P.Paillier, "Public-key Cryptosystems Based on Composite Degree Residuosity Classes", Advances in Cryptology, LNCS, Vol.1592, Springer-Verlag, pp.223-238, 1999.
15 R.L.Rivest, A.Shamir, and L.Adlemman, "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM, Vol.21, pp.120-126, 1978.
16 T.Saito, T.Koshiba, and A.Yamamura, "The Decision Diffie-Hellman assumption and the Quadratic Residuosity Assumption", IEICE Transactions on Fundamentals of Electronics (1) E84-A, pp.165-171, 2001.
17 A.Yamamura and T.Saito, "Private Information Retrieval Based on the Subgroup Membership Problem", Information Security and Privacy, LNCS Vol2119. Springer-Verlag, pp.206-220, 2001.
18 A.Yamamura and T.Saito, "Subgroup membership problems and applications to information security", Scientiae Mathematicae Japonicae, Vol.57, pp.25-41, 2003.

山村明弘（やまむらあきひろ）
情報通信部門セキュリティ基盤グループ
プリーダー　Ph. D.
暗号理論、情報セキュリティ

齊藤泰一（さいとうたいいち）
東京電機大学工学部情報通信工学科助教授　博士（工学）
暗号理論