平成２８年度 共同利用研究報告書

平成２８年１２月６日

九州大学 マス・フォア・インダストリ研究所長 殿

所属・職名　　産業技術総合研究所・主任研究員
提案者 氏名（ふりがな）　縫田（ぬいだ）　光司（こうじ）

下記の通り共同研究の報告をいたします.　　記

	※整理番号		20160015	
1.研究計画題目	高機能暗号とプライバシー保護情報分析の基盤数理			
2.種別（○で囲む）	a. 研究集会Ⅰ　b. 研究集会Ⅱ　ⓒ.短期共同研究　d.短期研究員			
3.研究代表者	氏名（ふりがな）	縫田（ぬいだ）　光司（こうじ）		
	所属部局名	産業技術総合研究所　情報技術研究部門	職名	主任研究員
	連絡先			
	e-mail		TEL	
4.研究実施期間	平成 28 年 9 月 5 日（月曜日）～平成 28 年 9 月 8 日（木曜日）			

5.参加者数・参加者リスト（＊別紙「共同利用研究報告書作成上の注意」参照）
(a,b は参加者数のみ記入し, 集会参加者リストを添付. c.の非公開プログラム参加者と d.は参加者リストに記入. c.は公開プログラムを含めた全参加者数を記入し，公開プログラム参加者リストを添付.）

参加者数：　１５　人

参加者リスト（a,b は記入不要，c.は非公開プログラム参加者，d.は共同研究参加者を記入）

氏名（ふりがな）	所属	職名	氏名（ふりがな）	所属	職名
秋山（あきやま） 浩一郎（こういちろう）	東芝研究開発センター	研究主幹	沼田（ぬまた） 泰英（やすひで）	信州大学	准教授
阿部（あべ） 拓郎（たくろう）	九州大学	准教授	野崎（のざき） 隆之（たかゆき）	山口大学	助教
鍛冶（かじ） 静雄（しずお）	山口大学	准教授	前野（まえの） 俊昭（としあき）	名城大学	准教授
栗原（くりはら） 大武（ひろたけ）	北九州工業高等専門学校	准教授			
縫田（ぬいだ） 光司（こうじ）	産業技術総合研究所	主任研究員			

6.本研究で得られた成果の概要

本共同利用研究では、各利用者のプライバシーを保護しながら情報の統合分析処理を実現する暗号技術や、プライバシー保護技術の構成要素となる公開鍵暗号技術、またそれらの構成・安全性解析の基盤となる数学理論について、公開ワークショップとしての講演３件を含む参加者間の情報交換および技術的討論を行った。特に、代数曲面上のセクションという代数的・幾何学的な対象を基盤として構成され、プライバシー保護と情報分析の両立に有益な準同型性と呼ばれる付加機能を持ち、かつ将来的な量子計算機を用いた攻撃にも耐性を有すると期待されるある公開鍵暗号化方式について、数学分野と暗号分野からの参加者間で議論を行い、代数学およびアルゴリズム理論の知見に基づく安全性解析手法の改善、安全性の向上が期待できる方式の改良案、また環論的な視点に基づく同方式の一般化の可能性等、多角的な観点から同方式の実用性を検討した。他にも、プライバシー保護情報分析を実現する暗号技術である秘密計算技術とグラフ理論の関連性や、量子計算機への耐性が期待される符号ベース暗号と呼ばれる技術の基盤となる符号の構成法など、数学の暗号技術への応用に関して両分野の研究者間で集中的な議論を行い、今後の当該技術の研究において有益と期待される新たな知見を得ることができた。

「高機能暗号とプライバシー保護情報分析の基盤数理」
共同利用研究　プログラム

日程　2016 年 9 月 5 日（月）〜9 月 8 日（木）

場所　九州大学産学官連携イノベーションプラザ 3F 研究室 2

プログラム（公開ワークショップ部分）

（＊下記以外の日程・時間帯は非公開の議論を実施）

9 月 5 日（月）

15:00　-　16:30　秋山 浩一郎（（株）東芝 研究開発センター）
代数曲面暗号の狙いと最近の進展について
(Recent developments and the aim of the algebraic surface cryptography)
16:30　-　17:30　講演内容に関する公開議論

9 月 6 日（火）

09:30　-　10:30　縫田 光司（産業技術総合研究所／ JST さきがけ）
秘密計算に関連する研究課題の紹介
(Introduction to Research Topics for Privacy-Preserving Computation)
10:30　-　11:00　講演内容に関する公開議論
13:10　-　14:40　野崎 隆之（山口大学）
噴水符号の基礎と構成
(Fundamentals and Construction of Fountain Codes)
14:40　-　15:40　講演内容に関する公開議論

共同利用研究　報告書
「高機能暗号とプライバシー保護情報分析の基盤数理」

文責：縫田 光司（産業技術総合研究所）

平成 28 年 12 月 6 日

標記の共同利用研究を、2016 年 9 月 5 日（月）から 9 月 8 日（木）までの日程で実施した。本期間中に、公開ワークショップとして下記の講演 3 件（敬称略）を催し、本共同利用研究参加者 8 名に加え、7 名の一般聴講者が出席した。公開ワークショップにおいては、各講演後に 1 時間程度の公開討論の時間を設け、一般聴講者も交えて、講演内容に関する詳しい質疑応答や、その発展研究の可能性に関する技術的な議論を行った。

秋山 浩一郎（（株）東芝 研究開発センター）
代数曲面暗号の狙いと最近の進展について

縫田 光司（産業技術総合研究所／ JST さきがけ）
秘密計算に関連する研究課題の紹介

野崎 隆之（山口大学）
噴水符号の基礎と構成

上記の公開ワークショップ以外の時間帯は、上記各講演の内容に基づく詳細な技術的検討を中心として、本共同利用研究参加者 8 名による非公開の研究討論を行った。以下では、本共同利用研究において行った議論の内容とその成果について題材ごとに概要を述べる。

1　代数曲面暗号と不定方程式暗号

代数曲面暗号は、公開鍵暗号化と呼ばれる暗号技術のうち、ある種の代数曲面のセクションを見つける問題が計算量的に難しい（と期待されている）ことに安全性の基盤を置く構成方法の総称である。公開鍵暗号化方式は、主に暗号化アルゴリズムと復号アルゴリズムよりなる（より正確にはこれに鍵生成アルゴリズムを加えた三つのアルゴリズムよりなる）。暗号化アルゴリ

ズムは、暗号化前の元データおよび公開された暗号化鍵（公開鍵）を入力とし、乱数を用いて、元データに対応する暗号文をランダムに生成する。復号アルゴリズムは、暗号文および秘匿された復号鍵（秘密鍵）を入力とし、暗号化前の元データを出力する。通常は、あるデータを暗号化して得た暗号文を復号すると元のデータに正しく戻ることが要請される。また、安全性の要件として、暗号文および公開鍵が与えられたとき、暗号化前の元データに関する情報を抜き出すことが計算量的に困難であることが求められる（「情報を抜き出す」の厳密な意味はここでは割愛する）。

代数曲面暗号の最もよく知られた構成法として、秋山氏らが国際会議 PKC 2009 で提案した方式 [1] について概略を述べる。この方式では、暗号文は

$$c(x,y,t) = m(x,y,t)s(x,y,t) + X(x,y,t)r(x,y,t)$$

という形の、ある有限体 $\mathbb{F}$ 上の 3 変数多項式 $c(x,y,t)$ である。ここで $m(x,y,t)$ は暗号化したいデータ（平文）に応じて定まる多項式である。多項式 $X(x,y,t)$ は公開鍵であり、代数曲面の定義方程式 $X(x,y,t) = 0$ に相当する。この代数曲面のセクション $(u_x(t), u_y(t), t)$、すなわち $X(u_x(t), u_y(t), t) = 0$ を満たす多項式の組 $(u_x(t), u_y(t))$ が秘密鍵である。多項式 $s(x,y,t)$ および $r(x,y,t)$ は暗号化の際にランダムに選ばれる。復号は以下の要領で行われる。

1. 暗号文 $c(x,y,t)$ にセクション（秘密鍵）を代入する。すると

   $$\begin{aligned} &c(u_x(t), u_y(t), t) \\ &= m(u_x(t), u_y(t), t)s(u_x(t), u_y(t), t) + X(u_x(t), u_y(t), t)r(u_x(t), u_y(t), t) \\ &= m(u_x(t), u_y(t), t)s(u_x(t), u_y(t), t) \end{aligned}$$

   が得られる。ここで最後の等号はセクションの定義に基づく。

2. $c(u_x(t), u_y(t), t)$ を因数分解して $m(u_x(t), u_y(t), t)$ および $s(u_x(t), u_y(t), t)$ を得る。（二つの因数を区別するため、予め多項式 m と s について次数などの性質に違いを持たせておく。詳細は割愛する。）

3. t に関する多項式 $m(u_x(t), u_y(t), t)$ の各係数の情報と、$u_x(t)$ および $u_y(t)$ の形（復号者にとっては既知）を基に、3 変数多項式 $m(x,y,t)$（復号者にとっては未知）の係数に関する連立一次方程式系が得られるので、それを解いて $m(x,y,t)$、さらにはその元となった平文の復元を行う。（この連立方程式系が解ける範囲となるようにパラメータ調整を行う。詳細は割愛する。）

ただし、上記の具体的方式には、暗号文の形の代数的な特徴を利用した攻撃（解読）法が既に指摘されている。例えば、平文多項式 $m(x,y,t)$ を含む暗号文の項 $m(x,y,t)s(x,y,t)$ は、$c(x,y,t)$ および $X(x,y,t)$（どちらも攻撃者にとって既知の情報）で生成されるイデアルの要素であり、このイデアルの

分解を通して $m(x,y,t)$ の（ひいては平文の）情報を抜き出す攻撃法が存在する（Faugere 氏ほか、PKC 2010 [2]）。この方法を含む様々な攻撃法の候補を鑑みた改良版として、秋山氏の講演では下記の改良方式について紹介された（ここでは詳細は割愛し概略のみ述べる）。

- まず、公開パラメータとして異なる素数 p, q を選んでおく。ここで q は p と比べて充分に大きな数としておく。公開鍵 $X(x,y)$ は、多項式環の剰余環 $R := \mathbb{F}_q[t]/(t^n - 1)$ を係数とする 2 変数多項式である（代数曲面の定義方程式、あるいはより一般に不定方程式 $X(x,y) = 0$ と対応付けられる）。秘密鍵 $(u_x(t), u_y(t)) \in R^2$ はこの不定方程式の解（すなわち $X(u_x(t), u_y(t)) = 0$ が成り立つ）のうち、最も小さな係数を持つものとする。ここで $u_x(t)$ や $u_y(t)$ の係数は有限体 $\mathbb{F}_q$ の要素となるが、$\mathbb{F}_q$ を整数の集合 $\{0, 1, \ldots, q-1\}$ と自然に同一視することで係数どうしの大小関係を定めるものとする。

- 平文 $m \in R$ は、各係数が 0 から $p-1$ までの範囲に収まるものとする。これに対応する暗号文は、

$$c(x,y) = m + X(x,y)r(x,y) + pe(x,y) \in R[x,y]$$

  として生成される。ここで $r(x,y)$ および $e(x,y)$ は暗号化ごとにランダムに選ばれる多項式であり、$e(x,y)$ の係数は充分に小さいという条件を課す（$r(x,y)$ にはそうした条件は必要ない）。

- 暗号文 $c(x,y)$ の復号は以下の要領で行われる。

  1. 暗号文に、秘密鍵である $u_x(t)$ および $u_y(t)$ を代入する。すると

$$\begin{aligned} &c(u_x(t), u_y(t)) \\ &= m + X(u_x(t), u_y(t))r(u_x(t), u_y(t)) + pe(u_x(t), u_y(t)) \\ &= m + pe(u_x(t), u_y(t)) \end{aligned}$$

     が得られる。ここで最後の等号は秘密鍵の選び方に基づく。

  2. 多項式 $c(u_x(t), u_y(t))$ の各係数を p で割った余りを計算して、項 $pe(u_x(t), u_y(t))$ を除去することにより平文 m を復元する。ここで注意すべきは、「p で割った余り」の計算は $\mathbb{F}_q$ を整数の集合 $\{0, 1, \ldots, q-1\}$ と考えて行うのであるが、多項式の代入操作 $pe(x,y) \mapsto pe(u_x(t), u_y(t))$ 自体は本来は $\mathbb{F}_q$ を体と考えて行われなければならないという点である。言い換えると、$\mathbb{F}_q$ を整数の集合とみなして多項式の代入操作を行うと考える場合、$pe(u_x(t), u_y(t))$ の計算中に係数の「オーバーフロー」が起こる（現れる係数が q 以上になる）と、後に p で割った余りを計算した際に項 $pe(u_x(t), u_y(t))$ がきれいに除去されてくれず、復号の誤りを引き起こす要因とな

る。この問題を防ぐために、秘密鍵 $(u_x(t), u_y(t))$ および暗号化時に選ぶランダム多項式 $e(x, y)$ には、「項 $pe(u_x(t), u_y(t))$ の計算時にオーバーフローが起こらない程度に充分小さな係数を持つ」という条件を課す必要がある。

例えば、上述したイデアルの分解を用いた攻撃への対処としては、暗号文にランダムな項 $pe(x, y)$ を追加することにより、平文が $c(x, y)$ および $X(x, y)$ で生成されるイデアルの要素とならないようにしている。その他の様々な既知の攻撃法に対処するためには素数の大きさや多項式の次数などの各種パラメータを適切に設定する必要があるが、ここでは詳細は割愛する。

なお、上記方式は以下の通り、プライバシー保護と情報解析の両立に有益な「準同型性」という追加機能を備えている。前述の通り、この方式における暗号文は $c = m + Xr + pe$ という形をしている（簡略化のために変数を省略した）。ここで、こうした暗号文二つを足し算すると、その結果も上記と同様な形となる。ただし m の箇所は二つの平文の和に置き換わり、r および e も同様に別の多項式に置き換わる。これはすなわち、「二つの暗号文を足し算することで、平文の和に対応する暗号文が得られる」、よりくだけた言い方をすると「暗号化状態のままで平文の足し算が可能」ということを意味する。この性質は、上述したプライバシー保護と情報解析の両立と極めて相性の良い性質である。また同様に、暗号文の掛け算を行うことで平文の積に対応する暗号文を得ることも原理的には可能であるが、その際に多項式 r と e の次数が増大することなどから、復号が可能な範囲で暗号文の掛け算を行えるようにするためにはパラメータの慎重な調整が必要となる。

上記の暗号化方式について、講演後の公開討論の時間およびその後の非公開の議論の席上にて、以下に述べるいくつかの観点から上記方式の安全性解析や改良案に関する質問や提案が行われた。

1.1 代入操作と剰余演算の順序交換による攻撃可能性の検討

上記の暗号化方式の復号操作は、まず秘密鍵多項式の代入操作を行い、その後に素数 p による剰余を計算するという順序であるが、その順序を入れ替えて先に p（公開パラメータ）による剰余を計算することで攻撃が可能となるかという疑問が、ある参加者より挙げられた。より詳しくは、前述の通りイデアルの分解を用いた攻撃への対処として暗号文 $c(x, y)$ に項 $pe(x, y)$ を追加してあるが、攻撃者は暗号文を p で割った余りを計算することでこの追加項 $pe(x, y)$ を除去し、残りの項目 $c'(x, y) := m + X'(x, y)r'(x, y)$（$X'$ および r' はそれぞれ X および r を p で割った余りを表す）に関してイデアル分解を用いた攻撃が可能となるのではないか、という疑問である。

講演者の秋山氏および他の参加者で議論した結果得られたこの疑問への回答は主に以下の通りであった。端的に言えば、前述した係数体 $\mathbb{F}_q$ における「オー

バーフロー」現象によりこの攻撃は無効化できるであろう、という内容である。すなわち、暗号文を p で割った余り $c'(x,y)$ は実際には $m + X'(x,y)r'(x,y)$ というきれいな形をしておらず、$X(x,y)r(x,y)$ の項の係数に由来する「オーバーフロー」現象によって係数に多くのずれが生じて上記の形が崩れるものと考えられる。その場合、$c'(x,y)$ と $X'(x,y)$ を基にしたイデアル分解攻撃を行っても平文 m の復元は望み薄である。ただし、公開鍵 $X(x,y)$ およびランダム多項式 $r(x,y)$ の選び方が適切でない場合にはこの攻撃が有効となってしまう可能性も否定しきれないため、本共同利用研究の終了後に念のため上記の点を確認する追加の計算機実験を行う計画となった。

1.2 グレブナー基底を用いた攻撃可能性の検討

上記方式の安全性に関する主な理路の一つは、秘密鍵を知っている正当な復号者はその代入操作によって暗号文の項 $X(x,y)r(x,y)$ を除去可能であるが、秘密鍵を知らない攻撃者にはこの除去操作が不可能と期待されるという点にある。この点に関して、ある参加者から、攻撃者が暗号文 $c(x,y)$ を公開鍵 $X(x,y)$ で「割った余り」を計算でき、しかもそれが $m+pe(x,y)$ と一致するならば、その結果から p で割った余りを計算することで平文を特定できるのではないか、という可能性の指摘がなされた。より詳しくは、一般に 1 変数多項式については割り算の剰余の計算は簡単に行えるが、多変数多項式になると剰余の計算はとたんに複雑な操作となる。しかし、ある種の状況においてはグレブナー基底の理論を用いて剰余計算が可能となる場合があり、本件がそうした場合に該当するだろうか、という疑問である。

この件に関する秋山氏および他の参加者の見解として、前述した係数の「オーバーフロー」の問題および、上記方式では多項式の係数が通常の体ではなく剰余環 $R = \mathbb{F}_q[t]/(t^n - 1)$ であることから、グレブナー基底の理論を直ちに適用することは現実的でないのではないか、という意見が出された。ただ、念のため、本共同利用研究の終了後に改めて上記の点を確認する理論的検討を追加で行う計画となった。

1.3 係数環の変更による効率性や安全性の向上の可能性検討

前述の通り、上記方式では多項式の係数として剰余環 $R = \mathbb{F}_q[t]/(t^n - 1)$ を採用している。ここで、多項式環 $\mathbb{F}_q[t]$ を割るイデアルの生成元として $t^n - 1$ 以外の多項式を採用した場合、出来上がる暗号化方式の効率性や安全性にどのような変化が起こり得るか、という疑問がある参加者より挙げられた。例えば安全性の観点では、イデアルの生成元を変更すると剰余環の環論的な性質（半単純性の有無など）に変化が生じる場合があり、そのことが前節で触れたグレブナー基底の理論の適用可能性など、安全性の強度に影響するだろうか、という疑問である。

この点について、まず秋山氏から、上記方式でイデアルの生成元として t^n-1 を採用している理由の説明が行われた。大まかに言うと、多項式環 $\mathbb{F}_q[t]$ をある多項式（が生成するイデアル）で割るということは、多項式の計算においてある次数を超える単項式が現れたら、その単項式を消去する代わりにその単項式の係数を別の単項式の係数にしかるべき基準で繰り入れる、という操作に相当する。前者の単項式消去により、多項式の次数が有限の範囲に収まることが保証でき、この点は効率性の向上に寄与している。一方、後者の係数の繰り入れは、計算を繰り返すごとに係数の分布が複雑化していくという意味で、安全性の向上に寄与する要因である。ただし、係数の繰り入れが過度に起こると効率性を低下させる要因となり得るため、必要最小限の係数繰り入れを実現するためのパラメータ選択として、多項式 t^n-1 が生成元として採用されている。この多項式の選択は上記方式に限らず、NTRU 暗号など他の暗号化方式でも同様の（あるいは類似の）選択が行われているため、暗号理論の観点からは一定の妥当性があると広く認識されている。

上記を踏まえた上でイデアルの生成元の変更について考えると、素朴な直感としては、生成元の多項式を複雑な多項式にし過ぎると、上述の通り係数の繰り入れに由来する効率性の低下が懸念される。しかしその一方で、イデアルで割った剰余環の構造が変化することで安全性の向上に寄与する可能性も考えられる。ここで着目すべきは、上記方式において様々な攻撃法の候補に対抗するために、素数 q やイデアルの生成元の次数 n といった各種パラメータを充分に大きく選ぶ必要があるという点である。こうしたパラメータを大きく取ると、それだけ効率性にとっては悪影響を及ぼす。もし、生成元の多項式の変更によって上記方式の根本的な安全性が向上すれば、q や n などのパラメータを従来よりも小さく取れる可能性があり、それによる効率性向上の効果が前述した係数繰り入れによる効率性低下を打ち消すほど大きければ、結果として生成元の多項式の変更が暗号化方式の効率性の向上にも繋がる可能性が考えられる。本共同利用研究の参加者間の議論によって、以上のような考察が新たに行われた。ただし、本参加者の知る限りでは上記のような観点での生成元の多項式変更の可能性はこれまでに指摘されておらず、全く新しい視点と考えられるため、この有効性の有無については本共同利用研究の終了後に改めて本格的な検討を行う計画となった。

1.4 本方式の一般化や拡張に向けた新たな定式化の可能性検討

上記の公開鍵暗号化方式は具体的な一方式として提案されたものであるが、数学的観点からその性質を見通し良く理解する一助として、何らかの一般化した枠組みを考えてその特殊例として上記方式を扱えるようにしたい、という提案がある参加者よりなされた。

こうした観点でまず着目された上記方式の特徴が、本方式では二つの異なる素数 p と q について、小さな体 $\mathbb{F}_p$（主に平文に関係する）が大きな体 $\mathbb{F}_q$

（主に暗号文に関係する）の中に埋め込まれた状態で取り扱われている点である。ただし、この埋め込みは体の構造を殆ど保つものの完全に保つわけではない（より詳しくは、$\mathbb{F}_q$ の内部で前述の「オーバーフロー」が起こらない範囲においては両者の構造は整合性を持つ）。このような $\mathbb{F}_p$ と $\mathbb{F}_q$ の関係性を、より一般に二つの体（あるいは環）が「殆ど入れ子になった状態」として上手く定式化できると有益なのではないか、という意見が挙げられた。実際、上記方式以外にも、例えば「完全準同型暗号」と呼ばれるプライバシー保護情報解析の基盤暗号技術のいくつかの方式においても、同様の「殆ど入れ子になった二つの環」が用いられていることから、このような定式化が得られれば暗号分野における応用が期待できる。ただ、具体的にどのような定式化を行えば暗号理論的に役立つかという段階までは議論を詰めることができなかったため、本共同利用研究後の研究課題ということになった。

また別の観点として、上記の暗号化方式について、以下の要領でより一般的な枠組みを与えることができないだろうか、という提案もなされた。

- 暗号化の操作を、平文の集合 M から暗号文の集合 C への（確率的な）関数 $\mathcal{E}\colon M \to C$ として捉える。
- 復号の操作については、まず、C から何らかの補助的な空間 A への関数 $\mathcal{D}\colon C \to A$ を考える。（これは上記の方式では、暗号文にセクションを代入して p で割った余りを取る、という一連の操作に相当する。）その際、合成関数 $\mathcal{D} \circ \mathcal{E}\colon M \to A$ は単射であることを仮定する。そして、暗号文 c の像 $\mathcal{D}(c) \in A$ が平文空間の像 $(\mathcal{D} \circ \mathcal{E})(M) \subset A$ に含まれるならば、何らかの方法で $\mathcal{D}(c)$ の逆像 $m \in M$ を計算することで復号結果の平文 m を得る。
- 暗号化方式の準同型性は、関数 $\mathcal{E}$ および $\mathcal{D}$ が何らかの適切な意味で “morphism” になっていること、として捉える。

こうした統一的な枠組みを導入することで、上記方式の拡張の可能性や他の暗号化方式との関連性の理解向上に役立つのではないかと期待されるものの、具体的に上記方式の拡張などの成果を得るまでには至らなかったため、この点も本共同利用研究後の研究課題ということになった。

2　非可換群上の秘密計算と関連するグラフ構造

秘密計算とは、複数の参加者が各々の入力について何らかの（多変数）関数の値を計算する際、入力を互いに秘密にしたまま通信を介して関数値を計算する暗号技術である。その性質上、各参加者のプライバシー保護と情報の統合分析処理の両立を実現するのに適した暗号技術であり、現代の暗号分野における主要な研究課題の一つとなっている。本共同利用研究の公開ワーク

ショップにおける縫田の講演では、一般の有限（非可換）群上の積演算に関する秘密計算について、既存研究（Desmedt 氏ほか、CRYPTO 2007 [3]；Sun 氏ほか、ASIACRYPT 2008 [4]）の紹介を行った。

問題の設定は以下の通りである。G を群として、n 人の参加者がそれぞれ $g_i \in G$（$i = 1, 2, \ldots, n$）を入力として保持しているものとする。このとき、参加者たちが G の要素を互いに適切に通信し合うことで、以下の条件を達成したい、という問題である。

- 最終的に各参加者は、$h_1 \cdots h_n = g_1 \cdots g_n$ を満たす要素 $h_i \in G$（$i = 1, 2, \ldots, n$）を一つずつ得る。
- あるパラメータ t について、t 人以下の参加者の集団が、通信の過程で得た全ての情報を持ち寄ったとしても、その集団以外の参加者の入力（G の要素 g_j）に関する情報は何も得られない。

上述した既存研究では、これらの要件を満たす参加者間の通信のスケジューリング問題を、ある種の彩色的な性質を持つグラフを構成する問題へと帰着した上で、そうしたグラフの存在性に関するいくつかの定理を与えている。

上記の問題について、講演後の公開討論の時間およびその後の非公開の議論の席上にて、前述の既存研究よりも効率的な解の構成の可能性について議論を行った。例えば、$n = 3$ かつ $t = 1$ の場合、下記のように上記の問題に対するプロトコルを構成できることを確かめた（ここで P_i は i 番目の参加者を表す）。

1. P_2 は、$g_2 = a_1 a_2$ を満たす G の要素 a_1, a_2 の組を一様ランダムに選ぶ。そして、a_1 を P_1 に、a_2 を P_3 に送信する。
2. P_1 は、$g_1 a_1 = b_1 b_2$ を満たす G の要素 b_1, b_2 の組を一様ランダムに選ぶ。そして b_2 を P_2 に送信する。
3. P_3 は、$a_2 g_3 = c_1 c_2$ を満たす G の要素 c_1, c_2 の組を一様ランダムに選ぶ。そして c_1 を P_2 に送信する。
4. P_1 は $h_1 := b_1$ を、P_2 は $h_2 := b_2 c_1$ を、P_3 は $h_3 := c_2$ をそれぞれ得る。

この方式では、以下の計算

$$\begin{aligned} h_1 h_2 h_3 = b_1 \cdot b_2 c_1 \cdot c_2 = b_1 b_2 \cdot c_1 c_2 \\ = g_1 a_1 \cdot a_2 g_3 = g_1 \cdot a_1 a_2 \cdot g_3 = g_1 g_2 g_3 \end{aligned}$$

により、確かに所望の群要素 h_1, h_2, h_3 が得られる。また、安全性については以下のように確かめられる。

- P_1 がプロトコルの最中に受け取る値は、P_2 から受け取る a_1 のみである。ここで a_1 は $g_2 = a_1 a_2$ を満たすようにランダムに選ばれるため、a_2 に関する情報が得られない限りは a_1 から g_2 の情報は何も得られない。

- 同様に、P_3 がプロトコルの最中に受け取る値は、P_2 から受け取る a_2 のみである。ここで a_2 は $g_2 = a_1 a_2$ を満たすようにランダムに選ばれるため、a_1 に関する情報が得られない限りは a_2 から g_2 の情報は何も得られない。

- P_2 がプロトコルの最中に受け取る値は、P_1 から受け取る b_2 と、P_3 から受け取る c_1 である。ここで b_2 は $g_1 a_1 = b_1 b_2$ を満たすようにランダムに選ばれるため、b_1 に関する情報が得られない限りは b_2 から g_1 の情報は何も得られない。同様に、c_1 は $a_2 g_3 = c_1 c_2$ を満たすようにランダムに選ばれるため、c_2 に関する情報が得られない限りは c_1 から g_3 の情報は何も得られない。

このように、比較的小さなパラメータ設定の下ではより効率的なプロトコルの構成が可能であるものの、既存研究で扱っているような一般的なパラメータに関して同様の構成が可能であるかどうかは本共同利用研究の期間中には結論が得られなかったため、今後の研究課題となった。

3　噴水符号とその応用の可能性

噴水符号はデータ符号化技術の一種であるが、有名な通信技術である誤り訂正（線型）符号とは異なる状況下での利用を想定した技術である。

噴水符号では、符号化したいデータ m を、データの（周期的な無限）列 $a_1, a_2, \ldots$ へと変換する。その際、受信者がこれらデータ列 $a_1, a_2, \ldots$ からある個数（例えば t 個）のデータ $a_{i_1}, a_{i_2}, \ldots, a_{i_t}$ を受け取ったとすると（それらのデータは連続しているとは限らないことに注意されたい）、ごく小さな確率を除いて元のデータ m を復元できるようにしたい。通常の誤り訂正符号の設定では、通信は一対一の状況で行われ、特に、通信データの始点と終点が明確であることが多い。一方、噴水符号の設定では、通信データが絶え間なく送信され続けるところに受信者が訪れて、流されているデータを所々拾い集める、といった状況が想定されているようである。日常的な状況で例えるならば、公共施設等で道案内の放送が繰り返し流されているときに、各利用者がどの時点でその場所を訪れて放送を聴き始めるかは予測できない、といった場合が想定状況に近いものと考えられる。野崎氏の講演では、この噴水符号に関して既存研究や最新の研究課題等の紹介が行われた。

噴水符号の構成の基本方針の一つは以下のようなものである。符号を形成するデータ a_i の各々は、元データ m を解とする連立一次方程式系を形成する一つの方程式である。これらの方程式が、m を一意復元するために必要な階数だけ集まれば、m の復号が可能となるという具合である。ここで、受信者が新たに得た方程式がこれまでに得た方程式系と一次独立である（階数が増加する）とは限らないため、データの個数に関するしきい値 t は必要最小

限の階数よりも多めに設定することが求められるが、しきい値を大きくしすぎると効率性の低下を招くため、しきい値の設定を含む符号の設計を慎重に行う必要がある。このような効率的な符号設計について、ブロックデザインのような離散数学的な理論が有効なのではないか、との意見が参加者より出され、野崎氏を含む参加者間で議論したものの、デザイン理論の具体的な応用方法については今後の研究課題となった。

また、実用的な噴水符号においては、上述の連立一次方程式系が単に「解ける」だけでは充分でなく、それが「効率的に解ける」ことが要求される。特に、掃き出し法を用いた汎用的な解法では方程式系のサイズに関し 3 乗程度のオーダーの計算量が必要となるところ、実用的な観点では線形オーダー程度の計算量に収まることが望ましいとのことであり、そうした効率的な復号の条件が符号設計における大きな制約となっている。この点について、復号の計算量のオーダーを抑えつつ、従来よりも広い範囲の符号を扱えるような復号アルゴリズムの候補について、野崎氏を含む参加者間で議論が行われた。

なお、通常の誤り訂正（線型）符号については、McEliece 暗号をはじめ暗号理論への応用例が多く知られている。噴水符号についても同様に、暗号理論への応用が今後見出されることが期待される。

まとめ　本共同利用研究では、準同型性を持つ公開鍵暗号化技術や秘密計算技術といった、プライバシー保護と情報処理の両立に有益な最新の暗号技術について、当該分野を専門とする暗号研究者と、代数学、幾何学、離散数学といった幅広い分野の数学者が一同に会し集中的な議論を行った。これにより、これら技術の実用化やさらなる拡張に向けた数学的課題を洗い出し、いくつかの課題についてはその解決に向けた今後の研究方針を固めるまでに至った。今後は本共同利用研究の成果を基に、上述した研究課題の解決に向けた研究連携をさらに深め、引き続き研究を進めていく計画である。

参考文献

[1] K. Akiyama, Y. Goto, H. Miyake: An Algebraic Surface Cryptosystem. In: PKC 2009, pp.425–442.

[2] J.-C. Faugère, P.-J. Spaenlehauer: Algebraic Cryptanalysis of the PKC'2009 Algebraic Surface Cryptosystem. In: PKC 2010, pp.35–52.

[3] Y. Desmedt, J. Pieprzyk, R. Steinfeld, H. Wang: On Secure Multi-party Computation in Black-Box Groups. In: CRYPTO 2007, pp.591–612.

[4] X. Sun, A. C.-C. Yao, C. Tartary: Graph Design for Secure Multiparty Computation over Non-Abelian Groups. In: ASIACRYPT 2008, pp.37–53.