雑感　「秘密共有法の研究顛末」

西関　隆夫　教授（システム情報科学専攻）

１．はじめに

最終講義を準備するにあたり、Google Scholar で私の論文の引用状況を調べてみたところ、一番たくさん引用されているのは

M. Ito, A. Saito and T. Nishizeki

“Secret sharing scheme realizing general access structure,” Globecom ’87

であり、324 回引用されていました。引用回数が多い 10 件の論文のなかで、他の 9 件の論文は全て「グラフ」を扱っていて、この論文だけが「グラフ」を扱っていません。私にとっては、いわば「余技」で取り組んだ研究の成果が一番引用される結果になってしまいました。25 年前にこの「秘密共有法」の研究を始めた切っ掛けやいきさつをまず最初に話し、次に最近の結果「絶対に安全な秘密共有法」について話します。

２．マトロイド的アクセス構造

研究は学部 4 年生のときから始めているので、かれこれ 42 年間も研究を続けてきたことになります。その大部分は「グラフ」を扱っており、グラフアルゴリズムやグラフ理論を研究してきました。25 年前の 1984 年頃は工学部通信工学科におりましたが、グラフの研究ばかりしていて、通信の何の役に立つのかといつも聞かれて、肩身の狭い思いをしておりました。その 25 年前に考えたことは、グラフ以外にも研究の手を拡げようということでした。どんなテーマがよいかいろいろ考えておりました。1977 年 4 月から 1 年間アメリカのカーネギーメロン大学数学科に客員数学者として滞在していて、ちょうどその時に RSA 公開鍵暗号が発明され、通信や情報の分野で暗号が注目を浴びていました。それまでも回路網理論やグラフ理論など理論的な研究をしていたので、暗号“理論”ならば、何とかなるかなという甘い思いで、暗号の研究を始めようとしていました。でも門外漢にすぐ研究成果が出せる訳もありません。そこで一計をめぐらしました。

その頃、日本で最も活発に暗号の研究をしていたのは日本電気（NEC）の中央研究所でした。当時の NEC には岩垂好裕氏、中村勝洋氏、岡本栄司氏ら、符号理論や暗号理論のそうそうたる専門家が揃っていたし、幸いに 3 人と知り合いでした。ちょうどその時に琉球大学を卒業して修士から私の研究室に入ってきた上原輝昭君がおりました。彼は元気がよく、多少の無理を言ってもへこたれなさそうな頑丈な体を持っていました。多分、彼が修士の２年生の時だったと記憶しておりますが、２年生で修論のネタもなさそうなので、上原君をけしかけて、NEC に夏休み実習、今で言うところのインターンシッ

プに行ってもらい、岡本栄司さんと中村勝洋さんに指導してもらいました。夏休み実習から帰ってきた上原君に NEC で何を勉強してきたのかと尋ねると、

「A. Shamir の(k, n)しきい値法では、秘密情報を n 個に分割し、
n 人の各々に n 個の分割情報を 1 つずつ配布すると、n 人の内の
任意の k 人の分割情報から元の秘密情報が復元できるが、
これではアクセス構造（復元できる人の集合の族）が特殊過ぎる、
何か一般化できないか？」

と岡本さんに言われたので、考えていますが、まだ何も新しいことは得られていませんということであった。そうか、「では、がんばってね」と言っても、何の進展もないし、修士論文の予備審査も迫ってくるしで、手伝う羽目になりました。まず(k, n)しきい値法を見直すことにしました。(k, n)しきい値法は多項式補間で説明されていましたが、本質は行列の基底だということにすぐ気付きました。行列やグラフの概念を一般化、抽象化したものがマトロイドです。幸いマトロイドはグラフの一般化として充分に勉強していたので、

「各人に分割情報を 1 つだけ配布する限り、秘密共有法として
実現できるアクセス構造の必要十分条件は、有限体で表現可能な
基マトロイドであることである」

ことがすぐにわかりました。これと他の結果をまとめて、上原君の修士論文とし、電子通信学会論文誌に

上原，西関，岡本，中村，「マトロイド的アクセス構造を持つ秘密鍵共有法」，
信学論 '86/9，Vol. J69-A，No. 9，pp. 1124-1132

を発表しました。残念なことに、その時は日米セミナー「離散アルゴリズムと複雑度」を開催したこともあり、いろいろ忙しくて、この論文を英語では発表しませんでした。そのこともあり、世界的にはあまり知られることがなく、数多くは引用されませんでした。

3．複数割り当て法

マトロイド的アクセス構造でも秘密を復元できる人数はやはり一定です。もっと一般化したいのですが、どうすればよいかわからなく、放っておきました。そのときに、斎藤明さん（現 日本大学教授）を研究室の助手として迎えました。彼は、当時、東大の情報科学科におられた榎本彦衛先生の指導を受けてグラフ理論で博士号をとられたところでした。彼に修士の学生の伊藤充君を指導してもらうことにしました。何か研究テーマはないかというので、上原君のやり残した一般化の話しをし、どうも難しそうだと言ったのですが、そこは素人集団の恐ろしいところで、未解決問題に果敢に挑戦してくれて、「各人に複素個の分割情報を配付してよいならば、どんなアクセス構造でも実現できる」

ことを証明してくれました。これが「複数割り当て法」であり、最初に述べた国際会議 Globecom の論文です。因みに Globecom は通信分野で最も権威ある国際会議の 1 つであり、1987 年には東京で開催され、その実行委員で研究室の先輩の三木哲也氏（当時 NTT 研究所長、現 電通大理事）に特別セッションへの投稿を強く勧められ、たまたま発表した二編の論文の 1 つです。Globecom に参加したのはこのとき 1 回限りです。

斎藤明さんが Globecom で大変上手に口頭発表してくれたこともあって、発表直後から好評でした。RSA の 3 人 Rivest、Shamir、Adelman の内の何人かが Globecom に参加していて、たくさんの参加者が集まっているところで、我々の論文をべた褒めしてくれたと静谷啓樹先生から聞きました。この論文が切っ掛けとなり、その後、一般的なアクセス構造を有する秘密共有法を扱う論文がたくさん発表されるようになり、情報セキュリティの 1 つの研究分野に発展したと言ってよいでしょう。これらの論文のほとんど全てが、上の我々の論文を引用してくれております。もっとも、その後、アクセス構造をブール式で乗法標準形や加法標準形で表現すると、もっと見通しがよくなることを指摘する論文が国際会議の STOC か FOCS で発表されました。我々の結果をブール代数の言葉で表現すると、単調ブール関数の標準形を独自に求めたということになります。即ち、何の予備知識もなく、組み合せ論として、それを証明したことになります。1 つの教訓は「国際会議では聴衆の興味を引き付けるように上手に講演しないといけない」ということです。

４．絶対に安全な秘密鍵の共有法

1993 年の創設時に情報科学研究科に工学部から移ってからは、水木敬明先生（当時 大学院生）や静谷啓樹先生と協同で「絶対に安全な秘密鍵の共有法」を研究しました。秘密通信をしたい二人、Alice と Bob がいたとき、公開鍵ではなく、二人だけが知っている秘密鍵があれば、二人の間で絶対に安全に秘密通信ができます。問題はどうやって秘密鍵を絶対に安全に共有させるかです。RSA 暗号など通常の暗号では、大きな数の素因数分解を求めるのはスパコンを用いても天文学的時間がかかってしまうということなどに安全性の根拠をおいております。したがって、もし逆に天文学的個数のスパコンを用いることができるならば、暗号が破られてしまい、「絶対に安全である」とは言えません。我々は、どんなにたくさんのスパコンを用いても破れない、「絶対に安全な秘密鍵の共有法」の構築を目途しました。そんな手品みたいなことができるのかと思うでしょう。手品には必ず「タネ」があるように、我々の方法にもタネがあります。それはトランプのようなカードを Alice と Bob に配付することです。そのときに盗聴者 Eve にバレてしまったカードもあるとし、Eve は天文学的個数のスパコンを使えるとします。このような状況下で、できるだけ長いビット長の秘密鍵を絶対に安全に共有するプロトコル（即ちカードゲームのルール）を与え、共有できる秘密鍵のビット長を見積もることに成功しました。これが小泉康一君の博士論文で、

K. Koizumi, T. Mizuki and T. Nishizeki,
"A revised transformation protocol for unconditionally secure
secret key exchange," Theory Comput. Syst., 42, pp. 187-221, 2008

です。まだ発表して間もないこともあり、今のところ他の方にあまり引用されていません。30 年生き延びる成果かどうかは歴史が判断するでしょう。その他にも、オイラー閉路状に秘密鍵を共有するプロトコルや電子透しのような「情報隠れん坊（Information Hiding）」等、いろいろ成果はありますが、省略します。

５．むすび

専門家は難しいと思い込みがちです。単に素人の beginner's luck だっただけかもしれない。しかし、グラフを対象にしてではあるが、論理的思考の訓練を充分に積んでいたことは確かです。そうすれば、零からでも理論を構築できるという一例です。でも、一番重要な役割を果たしたのは、「(k, n)しきい値法を一般化できないか」という岡本栄司さん（現 筑波大学教授）の素朴な直感だったと思います。因みに、岡本さんは東京工業大学大学院で梶谷洋司教授（現 北九州市立大学教授）の指導を受けて「回路理論的グラフ理論の基礎をなす概念について」という博士論文を書いており、私とほとんど同じようなバックグランドの教育を受けた方であり、亀山充隆先生の宇都宮高校のときの同級生でもあります。岡本さんや中村勝洋さん（現 千葉大学教授）と知り合いでなければ、上原君を NEC の夏休み実習に派遣することもなかったでしょう。斎藤明さん（現 日本大学教授）がいなければ、難問に挑戦することもなかったでしょう。また、三木哲也氏の強い勧めがなければ､馴染みのない Globecom で論文を発表することもなかったでしょう。小泉君、水木先生、静谷先生の力がなければ、「絶対に安全な秘密鍵共有法」の研究も進まなかったでしょう。このように人との出会いがとても大事で、大切にしたいものです。