大阪大学 大学院基礎工学研究科 情報数理系専攻計算機科学分野 計算機科学基礎講座（符号・情報セキュリティ研究室）

研究室紹介

藤　原　　融*

Key Words：Error Correcting Code, Decoding, Information Security, Cryptographic Protocol, Database Security

1．はじめに

大阪大学大学院基礎工学研究科情報数理系専攻の計算機科学基礎講座は，柏原敏伸教授が担当されている研究室と藤原が担当している研究室から構成されている．ここでは，藤原が担当する研究室について紹介させていただく．

本研究室では，通信の高信頼化のための重要な技術である誤り訂正符号に関する理論と実用化，及び情報セキュリティに関する研究を行っている．本年度の研究室メンバーは，筆者以外に，石原靖哲講師，吉田真紀助手，唐元生研究員（日本学術振興会外国人特別研究員），大学院生９人，学部学生４人である．

2．研究内容の概要

2.1誤り訂正符号

通信システムを制御するためのコマンド通信やファイル転送では極めて高い信頼性が要求される．また，高速であることも要求される．通信の信頼性向上のための重要な技術の一つが誤り訂正符号である．誤り訂正符号は通信途中で発生する誤りを検出訂正する．

本研究室では，誤り訂正符号の復号法の開発，それに基づく復号器の実現，誤り特性の評価法の研究を行っている．

2.1.1　復号法に関する研究

誤り訂正符号をグラフとして表現したものはトレリスダイアグラム（図１参照）と呼ばれる．

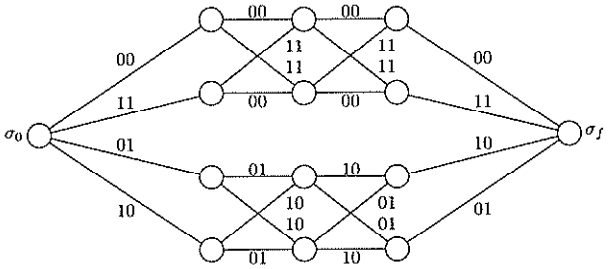
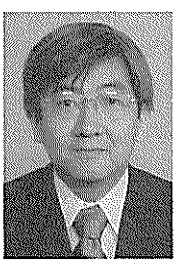


図１　(8, 4)リードマラー符号のトレリス

線形符号の性質に関する研究が進み，1990年代に入って，嵩忠雄教授（現広島市立大学教授）らと共に線形符号の最簡トレリスダイアグラムはきわめて規則的であること，例えば，同一構造の部分グラフに分解できること，を明らかにしてきた．さらに，このようなトレリスダイアグラムの規則性を徹底的に利用することにより復号の複雑さが著しく軽減できる復号法として，再帰的最尤復号法を提案した．これにより，これまで実現が不可能とされていた高信頼，高符号化率の符号の最尤復号器をVLSIチップを用いて実現する道が開かれたといえる．また，衛星通信用の符号の再帰的最尤復号器について，そのVLSI設計・試作を工学研究科白川功教授の研究室と共同で行った．

2.1.2　符号の誤り特性評価法の研究

高速通信を行うためには，要求にあった適切な符号を用いることが重要であり，そのためには符号の性能（誤り特性）を正確に評価することが必要である．



* Toru FUJIWARA
1958年６月18日生
1986年３月大阪大学・大学院・基礎工学研究科・物理系（情報工学）博士後期課程修了
現在，大阪大学・大学院・基礎工学研究科・情報数理系，教授，工学博士，符号理論，情報セキュリティ
TEL　06―6850―6560
FAX　06－6850－6564
E-Mail　fujiwara@ics.es.osaka-u.ac.jp

線形符号の誤り特性は符号の重み分布と密接に関係している．線形符号の重み分布を求める問題は符号理論の初期のころから重要な問題とされてきているが，一部の符号についてしか公式が知られていない．原理的には全ての符号語を生成しその重みを調べればよいのだが実用的な符号では語数が膨大で単純な計算法ではスーパーコンピュータを使っても数万年以上かかる．

本研究室では線形符号のトレリスダイアグラムの構造や記号位置置換に関する不変性を用いて高速な計算方法を開発した．例えば，符号語数が2の64乗の符号について普通のワークステーションでも数日で計算できるようになった．

2.2 情報セキュリティ

20数年前，私が学部4年生として情報セキュリティの研究に入ったときは，DESが標準化され，RSA暗号が提案されて間もない時期であり，情報セキュリティ技術が近い将来民間で重要な技術になるとは思われなかった．

情報セキュリティの研究には，暗号の研究，すなわち，破ることのできない暗号をどのように作るかという研究や，破れない(と信じられている)暗号を使って，不正防止の方式(セキュリティプロトコル)をどのように作るかという研究などがある．本研究室では，主に後者の研究を行なっている．

2.2.1　セキュリティプロトコルの開発

本研究室におけるセキュリティプロトコルの設計事例として，入札やコンテンツの放送型配信のプロトコルなどがある．コンテンツ配信は吉田助手を中心に研究を進めている．このシステムでは，図2に示すように，コンテンツを暗号化して配信する．サービス加入者は復号器(加入者ごとに異なる復号器)を与えられている．加入者が自分の復号器をもとに海賊版復号器を作成した場合に，押収した海賊版復号器から，作成に加担した加入者を特定したり，同型の押収できていない海賊版復号器を使用不可能にしたりする機能があると便利である．もちろん，原理的に実現できることは明らかであるが，できるだけ少ない放送データ量でこれらの機能を実現することが課題である．また，暗号学的な前提をなるべく少なくして実現することも重要である．このような意味で優れた放送型配信のプロトコルの設計を行っている．

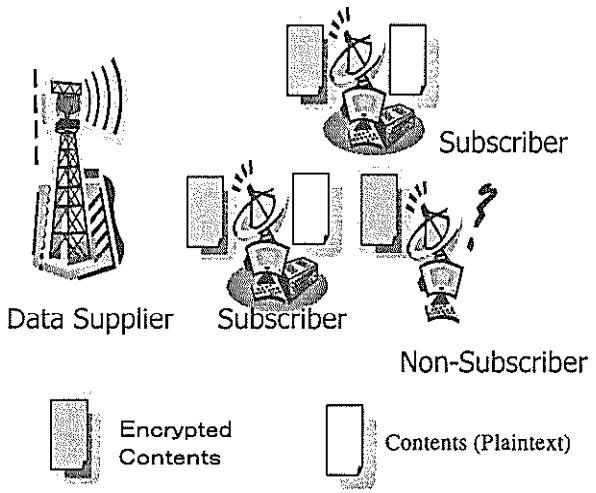


図2　コンテンツ配信システム

2.2.2 プロトコルの安全性検証

コンテンツ配信や入札など，セキュリティプロトコルを考案したとする．考案した方式が本当にうまく働くだろうか(安全だろうか)? 何か設計ミスがあって不正を行う抜け道がないだろうか? このことを論理的(数学的)に証明する方法の研究も行っている．セキュリティの専門家でない人々に利用してもらうためには，安全性を保証することが重要である．

抜け道がないということを示すのは極めて難しい問題である．このことに限らず，一般にできないということを証明するのはきわめて難しい．セキュリティプロトコルの安全性判定の問題は，一般の場合にこれを解くアルゴリズムが存在しないことがわかっている．

本研究室では，適当な条件の下で，与えられた方式の安全性を判定する方法を開発し，いくつかの実用的な方式について，その安全性を判定することができた．

2.2.3　データベースセキュリティに関する研究

石原講師を中心に，データベースセキュリティの研究も行っている．通常，データベースにおいてはアクセス制御により，データの保護を行っている．しかし，様々なデータが存在し，様々な操作を行える環境では，特定のデータへのアクセスや特定の操作を行うことが禁止されていても，関連するデータへのアクセスや別の操作の組み合わせで，保護されたデータを知ることができるかもしれない．このような攻撃を推論攻撃と呼ぶ．本研究室では，推論攻撃の定式化を行い(図3参照)，可能かどうかの判定や推論で得られる情報量等に関する研究を行っている．

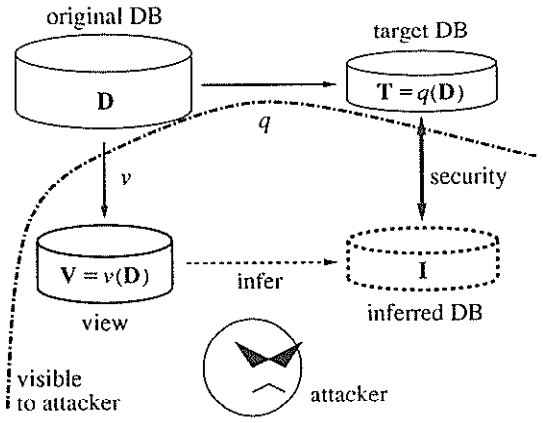


図3　推論攻撃のモデル化

3．おわりに

自然(雑音)を相手にする誤り訂正符号と，人間(悪人)を相手にする情報セキュリティの研究を行っている．セキュリティの研究は理論寄りで行ってきたが，ここ数年，企業との共同研究も行うようになってきた．どこまで効率と安全を達成できるかという理論的限界も重要であるし，現実的な解決策も重要である．今後も，両方から攻めていきたい．