情報通信からセキュリティまで

Communication Technology and Information Security

辻井重男

Abstract

「無能無才にしてこの一筋につながる」というような研究生活にあこがれながら，大学，学会，行政などの雑務に埋没してしまった筆者の悔い多き研究人生の中から拾い上げた幾つかの話題について，昔を今に生かすという視点から反省を込めて記述している．

キーワード：カラーテレビ信号のディジタル化，アイパターン，Y00 量子暗号，多変数多項式公開鍵暗号，情報倫理

1. 昔とったきねづか——団塊の世代よ，研究に復帰しよう——

瀬戸内寂聴さん(83 歳)と作曲家三木　稔さん(75 歳)による新作オペラが，今年 2 月初演された．また，来年米寿を迎える大西巨人さん（86 歳）が大長編小説に挑むという．才能豊かな超人のまねをしようというわけではないが，同じ創造的な仕事でありながら，なぜ，科学者・技術者は，研究は若いうちと決めてしまっているのだろうか．

70 歳近い F 教授から今春，「昨年は学会発表を 9 件やりました．自分が 20 代のころ，年配の人（40 代？）が発表しているのを聴いて哀れを催したのを思い出し，後ろめたい気持ちで」という文面の賀状を頂いた．筆者も今年の 1 月，暗号と情報セキュリティシンポジウムで，同じような気持ちで発表させてもらった．若い人に発表してもらってもよかったのだが，情報セキュリティ大学院大という新しい大学で，筆者が 3 年前に考え出した概念を軸に 4 人の博士課程学生を指導することになり，雑務に追われる中で研究の時間をねん出するには，発表するのが一番と考えたのである．

さて，研究の主軸は若い男性という現状は続くだろうが，今後，少子高齢化に対応して，女性と団塊の世代の活躍を是非期待したい．日本の企業では，有能な研究者も 40 歳くらいで管理職に就き，研究開発から離れてしまい 60 歳で定年というパターンが多い．しかし，昔とったきねづかということもある．若いころより視野も広がり，研究に対する郷愁と情熱を持っている人も多い．

筆者は以前，中大で何人かの社会人博士課程学生を指導したが，その中には，現在，情報セキュリティ大学院大の板倉征男教授，中大研究開発機構山口　浩教授などがいる．板倉は社長業の傍ら DNA による個人識別で，山口はある企業の取締役で多忙な中，電子投票の研究を続け学位を取得した．また，板倉から刺激を受けた O 氏(60 歳)は，ある企業の経営監査本部長の要職にありながら，今年，情報セキュリティ大学院大の博士課程に入学し，数学科卒のキャリアを生かして多変数公開鍵暗号を研究している．創造的な仕事には分野を問わず，年齢制限はないはずである．抽象的概念構築能力は 70 歳前後にピークを迎えるという学説もある．団塊の世代よ，研究に復帰しようではないか．

筆者には語るべき過去も乏しいが，本稿が，昔を今につなげて若い会員はもちろん，広い層に多少でも刺激になればと思い，執筆をお引き受けした次第である．

2. 周波数を 3 倍するだけで放送事業部が・・・

「こんなの特許になりますか？」入社 4 年目の筆者の問いかけに，上役の松島氏は「君，そういうのが特許になるのだよ」と答えた．1961 年，N 社の伝送事業部での会話である．当時，我々は，日本初の白黒テレビ信号のディジタル化の符号器を試作していた．標本化周波数は，切りの良い 10MHz として実験していた．当時のトランジスタは 10MHz では働かず，エサキダイオードを 500 対並べて悪戦苦闘した．どうにか組み上げて，ディジタル化された信号の再生画像を見ると変調積によるし

辻井重男　名誉員　情報セキュリティ大学院大学
E-mail　tsujii@iisec.ac.jp
Shigeo TSUJII, Fellow, Honorary Member (Institute of Information Security, Yokohama-shi, 221-0835 Japan).
電子情報通信学会誌　Vol.89 No.8 pp.698-703 2006 年 8 月

ま模様が画面に出ていて，これを消すのに一苦労した．

その間に，ふと，今，白黒テレビで実験しているが，これがカラーテレビならどうなるかと考えた．カラーテレビの場合，3.58MHz の色搬送波情報を水平同期信号に重畳して伝送している．この 3.58MHz の 3 倍と 10MHz の差，約 700kHz が変調積となって，画面にしま模様が現れるのではないかと想像したのである．当時，まだカラー映像は手に入らなかったから実験もできなかったが，とりあえず，「3.58MHz を 3 倍して，標本化周波数とする」という特許を出願しておいた(1)．

筆者は，その後，1965 年に N 社を辞め，山梨大を経て，1971 年東工大に転じたが，特許出願から 17 年を経た 1978 年，「色彩テレビジョン符号化方式」の発明に対して，井深　大発明協会会長から表彰頂いた．

その後，ある雑誌が特許の特集号で，「特許には 4 種類のタイプがある．その 1 は，早く開発を手がけていれば，だれでも気が付く特許である」として，その典型例に，上記の特許が挙げられていた．編集者に「白黒で実験していて，カラーならと想像したのだから，多少のオリジナリティはあったのだよ」と話したことを覚えている．確かにカラーテレビで実験すれば，だれでも気が付くので，カラーの時代になって，他社は悔しがったそうである．

筆者が驚いたのは，一昨年（2004 年），山梨大の辻井研究室の同窓会でのことである．N 社の放送事業部に永年勤務し，既に退職していた S 君が，たまたま，当日，放送事業部でも同窓会をやり，「放送事業部が今日あるのは，あの特許のお陰だ」という話になったというのである．伝送事業部では余り使われなかった特許だが，放送事業部では，フレームシンクロナイザに使われ，米国にもかなり輸出されたという話を，発明から 40 年たって初めて聞いたからびっくりした．

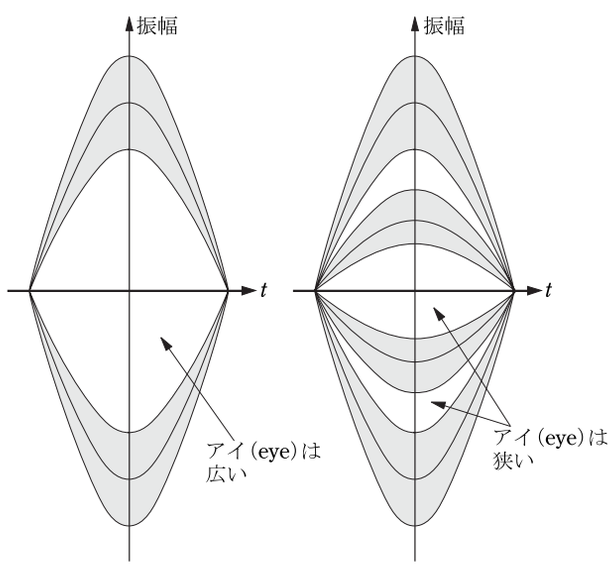
たかが周波数を 3 倍するだけだが，2 倍では標本化定理にもとり，4 倍では帯域の無駄になり，整数倍でなければならないとなれば，ほかに逃げようのない特許になるという次第．その後，別の理由で 4 倍になったようであるが，正に「そういうのが特許になるのだよ」というわけである．ベンチャー企業などから，「せっかく，特許を出しても，大企業に，抜け道を考え出され，金にものをいわせてやられてしまう．」という嘆きを聞く．特許はできるだけ，単純なのが良い．

3．アイパターンと Y00 光通信量子暗号

1963 年から 1965 年までの 2 年間，筆者は N 社で，シンクロスコープのアイパターンをにらんで暮らした．当時，日本経済の高度成長に伴い通信多重化への需要が高まり，ディジタル伝送方式の開発が進められていた．電話の音声信号（アナログ）を 2 値信号に変換して伝送路に送出する．各タイムスロットごとのパルスの有無が情報（信号）となるが，伝送路では，信号は減衰し，また，漏話雑音や熱雑音が発生する．このため，受信側で，信号のピーク値を 1 とするとき，雑音のピーク値が 0.5 より小さければ誤りは起きず，大きければ誤りが起きる．そこで，再生中継器を適当な間隔で伝送路に挿入して，SN 比（信号対雑音比）が 0.5 になる前に雑音を除去してパルスを再生する．再生中継器で 1 か 0 かを判別する際の波形を観測すると，連続するパルスが重なって，図 1 (a)のようなアイパターンが現れる．

平衡対ケーブルのように SN 比の低い伝送路では 1 か 0 かの 2 値伝送でもやむを得ないが，同軸ケーブルのような SN 比の高い伝送路ではパルス振幅を 3，1，－1，－3 のように 4 値にすれば 1 タイムスロット当り 2bit の伝送が可能となるので，その後，多値伝送の研究が活発に展開された．4 値の場合のアイパターンは図 1 (b)のようになる．

さて，時は流れ，昨年（2005 年）の夏，広田教授（玉川大）から，Y00 暗号（図 2）という新しい量子暗号の話を詳しく聞き，そうか，Y00 暗号はアイパターンをうまく利用した方式だったのかと合点した．正当な受信者には，2 値伝送として受信され，盗聴者にとっては多値（1,000 ～ 2,000 値）伝送として受信されるように，送受信者間で鍵を共有するのである．光通信における基本的な雑音はショット雑音である．その量子論的原理は，約 30 年前，グラウバー博士により解明された（2005 年ノーベル物理学賞）．通常の光通信では，ショット雑音に対する SN 比を大きくするために，1 パルス当りの光子数を大きくするが，Y00 暗号では光子数を 1 万から 10 万個というように比較的少なくして，正当な受信者は誤らずに受信でき，盗聴者には真の値と隣接値の判別がつ



(a) 2 値伝送の場合　　(b) 4 値伝送の場合

図 1　アイパターンの説明

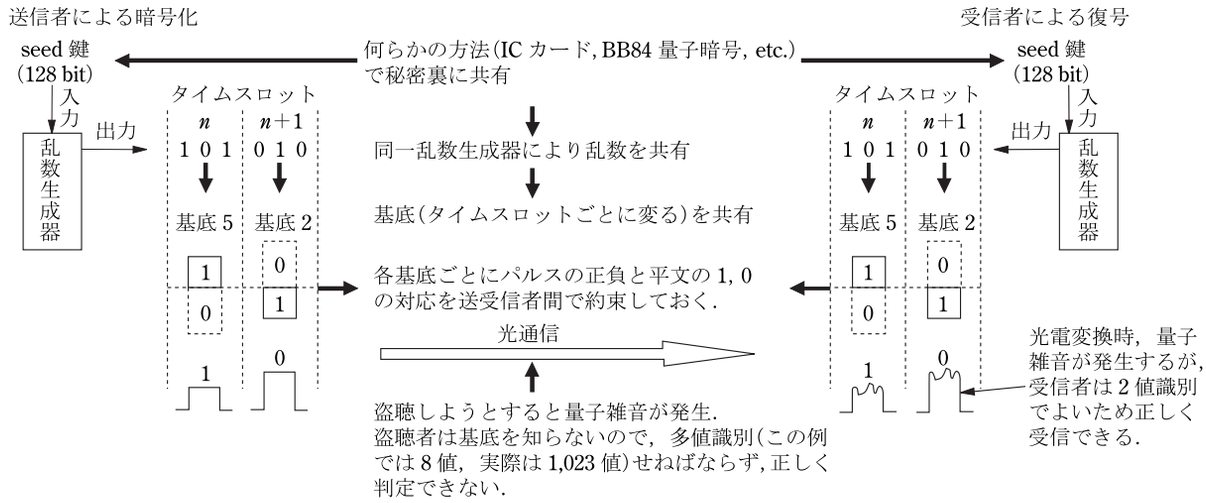
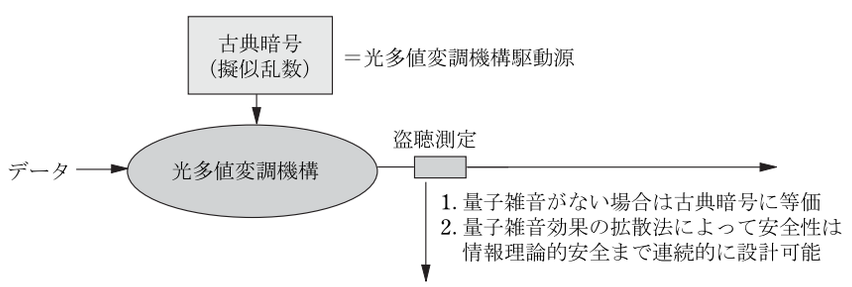


図 2　光通信量子暗号 Y00 方式の概念

国	機関・企業	期間	伝送速度	伝送距離	備考
米国	Northwestern 大	2004	650 Mbit/s	200 km	位相変調, 波長多重
	Telecordia	2005	650 Mbit/s	800 km	位相変調
	Bell 研		設計理論研究		
	陸軍研究所		設計理論研究		
日本	玉川大 日立ハイブリッドネットワーク	2006	2.5 Gbit/s	20 km (200 km準備中)	強度変調 (加入者, 基幹系)
	玉川大 松下電器	2005	1 Gbit/s	40 km	強度変調 (HDTV)

(a)　実証実験状況



(b)　安全性特性

図 3　Y00 光通信量子暗号の実証実験状況と安全性特性

かず誤りが起きるようにシステム設計される.

発明者の Yuen 教授の方式は多値（2,047 値）位相変調方式だが[2),3)]広田教授は，現在，通常の光通信で使用されている強度変調で実現する方式を考案した[4)].

実は，Y00 暗号については話は聞いていたのだが，よく理解できていなかった．しかし，Yuen は，量子情報の分野で数々の顕著な業績を挙げ，米国物理学会 100 周年記念大会では招待講演をするほどの研究者であり，また，MIT の電気工学科を卒業した工学的センスの持ち主である．Y00 暗号は図 3 のように，米国政府系のみでなく，Telecordia などの通信業者も数百 Mbit，800km の伝送実験を[5),6)]，また，ベル研も開発に着手している方式であり, 信頼性は高いとは感じていたのだが，アイパターンを利用するのだと聞いて，これは昔とったきねづかだと納得できたのである.

日本では広田の指導の下に，多値数は 1,023 値で日立ハイブリッド(株)が光通信の幹線系を対象に 2.5Gbit/s, 200km の実験を，また，松下電器産業(株)が 1Gbit/s で HDTV の加入者線による配送実験を進めている.

通常のストリーム暗号では，盗聴者は暗号文を読めるのに対し，Y00 暗号では, 暗号文を取得しようとすると，量子雑音が発生して暗号文が読めなくなり，コピーして解析しようにもコピーするごとに異なる量子雑音が発生するので，解読に役立たない．通常のストリーム暗号では，乱数の精度（真正乱数との差）が問題となるが，Y00 暗号でもそれは問題である．しかし，暗号文が読めない

ということは，等価的には，乱数の精度を向上させていると見ることができる．したがって，その安全性は，多値変調を駆動する乱数生成器と量子雑音効果の組合せで，どこまで乱数性能を上げられるかに依存するが，従来のストリーム暗号より，盗聴者が被る量子雑音効果分だけ強いことは直感的に明らかであろう．情報理論的な意味での安全性証明も完成したようである[7]．

現在の Y00 暗号は，鍵共有を量子的に行うことはできない．他方，1984 年に提案された，BB84 量子暗号は鍵共有が主たる機能であり，共有した鍵による平文の暗号化は，現在，通常の用途に耐える速度には達していない．そこで，BB84 暗号で鍵を共有し Y00 暗号で暗号化するという win-win の関係で，技術開発を進めるのが建設的な提案といえよう[8],[9]．

Y00 暗号は，量子力学，変調方式，暗号理論が三位一体となった方式である．筆者は，昔，アイパターンで苦労し，その後，数論的暗号の研究を進め，また，フォン・ノイマンや朝永振一郎の本で量子力学をかじっていた経験を生かせば，Y00 暗号を着想できる位置にいたともいえる．総合化能力に欠けていたというほかはない．

4．多変数公開鍵暗号の研究

筆者は，1979 年，東工大同級生の高田　稔君から，ホテルのカードキーの安全性の検証を依頼されたのが切っ掛けで暗号研究を始めた．同時に，1976 年から 1978 年にかけて，米国で公開鍵暗号の概念とその具体的方式としての RSA 暗号が発表され，その数学的構造の魅力に取り付かれて，黒澤（現茨城大教授）や趙（現中大教授）を誘って，公開鍵暗号の研究を始めた．そして，RSA 以外の方式はないものかと模索し始めた．

新しい公開鍵暗号は，筆者より早く横浜国大の今井研究室（当時）で研究されていた．筆者は，岸・梶谷の順序解析と呼ぶ回路解析の手法にヒントを得て，順序解法を落とし戸とする多変数多項式型公開鍵方式を 1986 年，本学会論文誌に掲載したが[10]，東京理科大の金子教授らに一部，解読された．その弱点を除くため，核変換と名付ける双有理変換を導入し一般化順序解法として，1989 年に再び本学会論文誌に掲載したが[11]，これはこれまで破られていない．海外での発表も考えたが，雑務に紛れたのと，この程度のことは米国でもやっているのだろうと勝手に想像して，そのまま時が過ぎてしまった．しかし，1993 年，Shamir 博士（RSA 暗号の発明者の 1 人）がやはり順序解法的手法を利用した署名方式を CRYPTO という最もレベルの高い暗号学会で発表しているのを知って[12]，やはり国際会議には出しておくべきだと悔やんだものである．

他方，松本・今井は，エレガントな多変数二次多項式公開鍵暗号系を，1988 年，EUROCRYPT という国際会議で発表した[13]．この MI 方式は，1995 年，Patarin により解読され，その後，Patarin は MI 方式を拡張し，HFE と命名した．その安全性をめぐって，ここ数年，多くの研究が展開されている．

MI 方式は多変数公開鍵暗号の世界的源流となり，現在でも多くの論文に引用されている．多変数多項式系の求解は NP 完全であり，巧妙に落とし戸を埋め込めば，量子コンピュータの出現にも耐えられるので，現在，内外で様々な方式が提案されている．我が国では，笠原・境[14]，秋山らの発表が続いている[15]．

筆者は，これらの多変数公開鍵の強度を高めるため，持駒行列（Piece In Hand Matrix，Soldiers In Hand Matrix）と呼ぶ，素朴な順序解法を除く多くの方式に適用可能なはん用的手法（図 4）を考案し，発表を続けている[16]～[19]．上記の 1989 年版も遅まきながら，英訳して，持駒行列の付録として，e-Print に掲載しておいた[18]．2006 年 5 月にベルギーで開催されたポスト量子暗号国際会議[20]で，J．Ding が，「1980 年代に日本でこのような論文が発表されていた」と紹介してくれた．

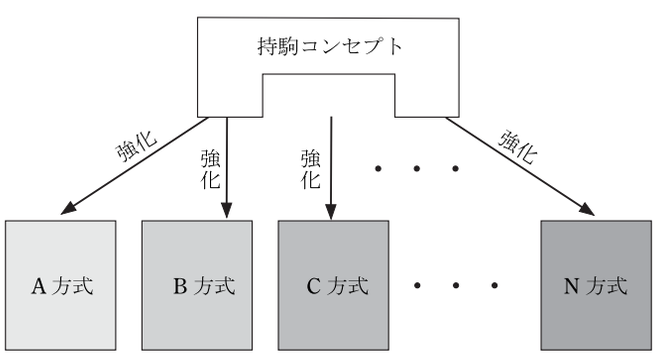


図 4　持駒行列による多変数公開鍵暗号の諸方式に対する安全性向上

5. アナログからディジタル，そして mod.p へ ――縄のイデアと楕円暗号，数学的実在は物理的実在を超えて社会的実在へ――

「君，この精度の抵抗を現場に要求するのかね」N 社に入社して間もないころ，設計値をそのまま書いて，上役に提出したところ，このように注意された．回路理論は，現実にない理想化された R，L，C を想定して構成されている．プラトンの 2 世界モデルに例えれば，回路理論はイデアの世界であり，ある種の虚構である．この虚構は，実際の製品設計には極めて有効であるが，様々な誤差を考慮しなければならない．

筆者は，1970 年ごろからディジタル信号処理（DSP）の研究を始めた．DSP の場合は，製品のばらつきは少ないが，設計値からの誤差があることはもちろんである．アナログ設計にしろ，ディジタル設計にしろ，実数体上の設計では，上のような状況だが，公開鍵暗号で常用される有限体の話になると様子ががらりと変る．

哲学者，西田幾多郎は，「善の研究」において，「物理学者のいう如き世界は，幅なき線，厚さなき平面と同じく，実際に存在するものではない．」と述べている．果たしてそうだろうか．古代ギリシャの哲学者タレスが考えた，縄のイデア，つまり，幅のない線は，例えば，電子マネーの真正性を保証するための楕円暗号として IC カード等に収まり，電子社会に見事に実在している．

円から作られる代数曲線は一般に二次であり，それから設計される暗号の安全性（計算量）は，RSA 暗号と同じく準指数時間である．これに対し，楕円曲線を利用する楕円暗号の安全性は格段に高く指数時間である．

仮に，宇宙の広がりを持った円と，短径は宇宙の直径として，素粒子一個分だけ長径が短径より長い楕円を考えよう．離心率が 10 の－100 乗の楕円を想像するのである．このようにアナログ感覚では十分，円とみなせる楕円からでも，安全性の高い暗号，つまり指数時間計算量の暗号が設計できるのだろうか．そのはずではあるが，筆者は，中大での卒業研究で，離心率 2 分の 1 のいかにも楕円らしい楕円から作られる楕円暗号と，上記の楕円暗号を比較してみた．その結果は，予想どおりで両者に有意差は認められなかった[21]．

近代の科学・技術は，プラトンの 2 世界モデル（イデアの世界と現実の世界）を指導原理として，進んできた．例えば，理想的な電子部品の存在を仮定して，システムを設計し，現実に得られる製品が，設計値に対し可能な限り誤差が小さければ満足するという手順である．

上に述べた例は，このようなアナログ技術時代の 2 世界モデルとも本質的に異なることはもちろん，ディジタル信号処理技術とも違う有限体特有の（数学的には当然ではあるが）不思議な世界である．ゼロとそれに限りなく近い数とでは，数学的にはもちろん，社会的存在として，全く異質なのである．上の例にプラトンの 2 世界モデルの極限を見た思いがする．

ある雑誌で哲学者の加藤尚武教授と対談したとき，東洋には厳密値という概念がないといわれたのが印象に残っているが，イデアの世界が希薄，あるいは概念世界を徹底化しないと言い換えてもよいのではなかろうか．

6. 倫理をベースとする情報セキュリティ総合科学の構築へ向けて

さて，上の話に関連して筆者が言いたいことは，飛躍するようだが，以下のとおりである．プラトンの 2 世界モデルは近ごろ評判が芳しくない．イデアの世界から現実世界を見下す物質的自然観が，近代科学と産業技術を発展させ，その挙句が，地球環境を悪化させ，様々な公害をもたらしたというわけである．木田　元氏は，「プラトンのイデア，中世キリスト教の人格神，近代の理性とつながる 19 世紀までの西洋哲学は，世界でもローカルな思想であり，自分には馴染めなかった．」といっている．20 世紀に入り，西洋の思潮は多元，相対，関係という方向に概念軸を変え，東洋的思考に近づいたようにも思われる．しかし，我々は，それ見たことかと安易にその思潮に乗るべきではないだろう．我々は，明治以来，和魂洋才を唱え，いわゆる近代の超克と正面から向き合わず，これを回避してきたし，それによって苦い経験もした．

これからの IT 社会は，小さな輪の中で，「和をもって貴きとなし，逆らうことなきをむねとす．人皆党有（それぞれに組織を作って，仲良くやろうじゃないか）」で済めばよいが，それほど甘いものではなく，否応なしに冷徹な論理の支配する契約社会へ移行することは避け難い．こうした中で，情報セキュリティガバナンスの確立が叫ばれている．筆者は，今，数学的暗号理論を研究する傍ら，情報セキュリティ大学院大の学長として，林紘一郎副学長（法制度，経済・経営），田中英彦研究科長（計算機科学）等の同僚たちとともに，和魂と洋魂（近代の理念）を統合した情報倫理をベースとし，技術，管理・経営，法制度を連携させ，様々な相克を止揚した情報セキュリティ総合科学を構築し，それを通じて人材を育成したいと考えている．このとき，社会的森羅万象や多様な言説はもちろん，筆者の若いころからの乏しい体験や雑学的読書も多少は役立っているように感じている．

文　　献

（1） 辻井重男，松島孝夫，“色彩テレビジョン符号変調方式，”特許第 488883 号，1967 年 1 月 26 日公示．

（2） G.A. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, “Secure communication using mesoscopic coherent states,” Phys. Rev. Lett., vol.90, no.22, 227901, 2003.

（3） E. Corndorf, C. Liang, G.S. Kanter, P. Kumar, and H.P. Yuen, “Quantum noise randomized data encryption for wavelength-division multiplexed fiber optic network,” Phys.

Rev. A, vol.71, no.6, 062326, 2005.
（4） O. Hirota, M. Sohma, M. Fuse, and K. Kato, “Quantum stream cipher by the Yuen 2000 protocol: design and experiment by an intensity modulation scheme,” Phys. Rev. A, vol.72, no.2, 022335, 2005.
（5） M.S. Goodman, P. Toliver, and T. Banwell, “Transitioning multi-Gb/s optical line encryption to the real world: Technologies and testing,” DARPA Quantum Information Science and Technology (QuIST), Nov. 2003.
（6） P. Kumar, “Practical high-speed implementations of the Alpha Eta (Y-00) protocol,” 光通信量子暗号シンポジウム―Y-00 の展望―, 117-132, pp.1-16, Nov. 2005.
（7） O. Hirota and K. Kurosawa, “An immunity against correlation attack on quantum stream cipher by Yuen 2000 protocol,” Quantum Information Processing (to appear early in 2007).
（8） 辻井重男, “BB84 と Y-00 の研究を win-win で推進しよう,” 光通信量子暗号シンポジウム―Y-00 の展望―, 001-016, pp.1-15, Nov. 2005.
（9） 黒澤 馨, “暗号学から見た Y-00,”光通信量子暗号シンポジウム―Y-00 の展望―, 047-072, pp.1-26, Nov. 2005.
(10) 辻井重男, 黒澤 馨, 伊東利哉, 藤岡 淳, 松本 勉, “非線形連立方程式の順序解法による公開鍵暗号方式,” 信学論(D), vol. J69-D, no.12, pp.1963-1970, Dec. 1986.
(11) 辻井重男, 藤岡 淳, 平山祐介, “順序解法の一般化による公開鍵暗号系,” 信学論(A), vol. J72-A, no.2, pp.390-397, Feb. 1989.
(12) A. Shamir, “Efficient signature schemes based on birational permutations,” Proc. CRYPTO ’93, Lecture Notes in Computer Science, vol.773, pp.1-12, Springer, Aug. 1993.
(13) T. Matsumoto and H. Imai, “Public quadratic polynomial-tuples for efficient signature-verification and message-encryption,” Proc. EUROCRYPT ’88, Lecture Notes in Computer Science, vol.330, pp.419-453, Springer, May 1988.
(14) 笠原正雄, 境 隆一, “新しい公開鍵暗号の原理とその一実現法,” 信学技報, ISEC2000-92, pp.97-104, Nov. 2000.
(15) K. Akiyama and Y. Goto, “An algebraic surface public-key cryptosystem,” 信学技報, ISEC2004-80, pp.13-20, Nov. 2004.
(16) S. Tsujii, “A new structure of primitive public key cryptosystem based on soldiers in hand matrix,” Technical Report TRISE 02-03, Chuo University, July 2003.
(17) S. Tsujii, R. Fujita, and K. Tadaki, “Proposal of MOCHIGOMA (piece in hand) concept for multivariate type public key cryptosystems,” 信学技報, ISEC2004-74, pp.47-54, Sept. 2004.
(18) S. Tsujii, K. Tadaki, and R. Fujita, “Piece in hand concept for enhancing the security of multivariate type public key cryptosystems : public key without containing all the information of secret key,” Cryptology ePrint Archive, Report 2004/366, Dec. 2004. http://eprint.iacr.org/2004/366
(19) S. Tsujii, K. Tadaki, and R. Fujita, “Proposal for piece in hand matrix ver.2 : General concept for enhancing security of multivariate public key cryptosystems,” Cryptology ePrintArchive : Report 2006/051, Feb. 2006. Available at URL : http://eprint.iacr.org/2006/051
(20) S. Tsujii, K. Tadaki, and R. Fujita, “Proposal for piece in hand matr ver.2 : enhancing security of multivariate public key cryptosystems,” PQCrypto 2006, International Workshop on Post-Quantum Cryptography, Leuven, Belgium, May 2006.
(21) 辻井重男, “身分を保証する暗号とその社会的利用,”数学セミナー, no.528, pp.12-15, Sept. 2005.

（平成 18 年 3 月 31 日受付　平成 18 年 4 月 25 日最終受付）

辻井（つじい） 重男（しげお）（名誉員）
昭 33 東工大・電気卒．昭 45 工博．日本電気（株），山梨大，東工大，中大を経て，現在，情報セキュリティ大学院大学長，中大研究開発機構教授，東工大名誉教授．本学会会長，電波監理審議会会長，日本学術会議会員等歴任．本学会論文賞，業績賞，功績賞等各受賞．IEEE Life Fellow，第三千年紀記念賞受賞．日本放送協会「第 55 回放送文化賞」受賞．著書「暗号－ポストモダンの情報セキュリティ」（講談社メチエ選書），「暗号と情報社会」（文藝春秋社），「電子社会のパラダイム」（新世社）等．