3 層公開鍵暗号の提案 ― 秘密鍵に極秘密鍵を内蔵・盗用されない為に

辻井　重男(Shigeo TSUJII, Ph. D.)
東京工業大学　名誉教授、
中央大学研究開発機構　機構教授、SIOTP 理事長

1933 年 9 月 13 日生　1958 年 東京工業大学卒業、
1970 年 工学博士
1979 年　東京工業大学教授、1994 年 中央大学教授、
1996 年　電子情報通信学会　会長
1999 年　中央大学研究開発機構　機構長
2003 年　日本学術会議 会員
2004 年　情報セキュリティ大学院大学初代学長
2004 年　中央大学研究開発機構教授・東京工業大学名誉教授
2007 年　日本ペンクラブ会員
2010 年　（一財）マルチメディア振興センター理事長
2013 年　（一財）放送セキュリティセンター理事長
2017 年　（一社）セキュア IoT プラットフォーム協議会理事長

専門は　情報セキュリティ総合科学　暗号理論等。
瑞宝中綬章、NHK 放送文化賞、C&C 賞、高柳記念賞、
信学会業績賞・功績賞、IEEE 第三千年記 記念賞、発明表彰等受賞

暗号と言うと、文字通り暗いイメージを伴いますがそれは、暗号の役割が「秘密にする」ことだけにあると考えられているからでしょう。暗号が、もっぱら戦争や外交に利用された 20 世紀前半までは、その通りでした。そして、現在、その用途は企業間通信やプライバシィ保護の分野で、益々重要になっています。だが、数千年に及ぶ暗号の歴史の中で、１９７０年代に公開鍵暗号と言う画期的な発明があったことは、余り認識されていません。

公開鍵暗号は、秘匿にも使えますが、大事な役割は本人認証などの真正性保証です。人だけではありません。自動車等の現物をはじめ、やがて 400 億個にも昇ると予想されているモノをネットワークで繋ぐには、それらの本物性を保証しなければなりません。そうでなければ、私達は安心して生活できないでしょう。

ある科学史の本に、公開鍵暗号の発明は、火薬の発明に匹敵すると書かれているそうですが、その通りです。しかし、目に見えて実感できる発明と違い、数学的構造の発明は、説明が難しくて、理解され難いですね。そこを何とか、理解されやすいように説明するのが本文の狙いです。

数千年前から使われてきた暗号は、共通鍵暗号と呼ばれています。例えば、A さん（A 社）と B さん（B 社）は、共通の鍵を持ち、両者だけの秘密を保ちます。20 世紀後半になり、コンピュータとネットワークが普及し始めると、それまで、手書きで本人が書いた文書に間違いないと確認していた手書き署名を、どうするかが問題になりました。そこで、本人だけが持っている鍵で署名するデジタル署名方式として公開鍵暗号が発明されました。

公開鍵暗号は共通鍵暗号と違い、A さんは、A さんだけの秘密鍵 dA を持っています。平文 M を dA 乗できるのは A さんだけです。それを M に戻せる公開鍵 eA は公開します。しかし、eA から秘密鍵 dA を求めることは、A さん以外には出来ません。何故でしょうか？
それは、数の世界を使い分けるからです。我々は、10 進数を使い慣れています。これを 10 を法とする数の世界と呼びます。他方、我々は 1 週間を法として生活していますね。しかし、何日を法として暮らしているのか分からない民族もいるかも知れません。そこを上手く数学的構造として工夫するのが、公開鍵暗号です。例えば、300 桁×300 桁＝600 桁として 600 桁の整数だけを公開鍵として公開し、２つの 300 桁の整数を秘密にします。これ以上の説明は難しいので、この辺にしておきましょう。

繰り返しますが、公開鍵暗号は秘匿より、皆さんが安心して正確出来るための本人・本モノ性保証が大事な役割なので、私は、1980 年頃から、安号と呼びことを提案しています。

公開鍵暗号は、4 千年の歴史を持つ共通鍵暗号鍵暗

3 層公開鍵暗号の提案 ― 秘密鍵に極秘密鍵を内蔵・盗用されない為に

号と異なり、公開鍵の中に秘密鍵を秘密に入れるという 2 重構造になっています。秘密鍵は、文字通り秘密保管せねばなりません。秘密鍵を盗難されれば、生命・財産に関わる場合もあるでしょう。そこで私は、水原弘さんに倣って

「秘密鍵こそ命、我が命」

と永い間、唱えて来ました。しかし、現在の秘密鍵は乱数で、本人・本モノ情報が含まれておりません。秘密鍵を盗難されたら、盗用されることもあるでしょう。そこで、私は、秘密鍵の中に、本人・本モノ情報を含む極秘密鍵を内蔵する 3 層構造の公開鍵暗号を提案しました。送信時、極秘密鍵を所有していることを、それを見せずに、広く納得して貰うために、零知識証明というシステムを利用します。関心のある方は文献（１１）をご覧ください。

下記に、公開鍵暗号の構造を易しく解説しました。
非専門家向け説明のご参考になさって下さい。

公開鍵暗号解説 対話編

公開鍵暗号の歴史―その 1：発明の動機は？

Q：公開鍵暗号って、火薬の発明にも匹敵する程の歴史的発明と言う人もいるけど本当なの？

A：生命・財産にも関わる社会的基盤だから、と言うより、公開鍵暗号の秘密鍵は、生命・財産そのものという状況になってきている。

Q：どういう動機で発明されたの。

A：動機は２つ。1 つは 1977 年頃、米国西海岸で、これからのコンピュータ社会での手書き署名に代る方式の必要性。これは、本人・モノ認証の社会基盤となっている。

もう一つは、1973 年頃イギリスの諜報機関による軍事・外交用に鍵を白昼堂々と送れないかという動機。

Q：そうだったの。大戦中は、鍵を送るのが大変だったのね。

A：第 2 次大戦の日本海軍が使ったパープル(紫)暗号を、アメリカが解読できたのは日本が同じ平文をレッド(赤)暗号で、異なる場所に送っていた（そこにはパープル暗号用の鍵はなかったので)が、レッド暗号は、既に解かれていたので、パープル暗号文も解かれたしまったというようなこともあるからね。

Q: 鍵の安全な配送は、古典暗号と現代暗号に共通の課題ね。さて、公開鍵暗号のもう一つの役目、認証・署名は、正に社会基盤ね。送信者・受信者や何百億とも言われる IoT の真正性保証や、メタバースでの本人確認でも不可欠なのね。それに量子暗号も問題ね。耐量子コンピュータ暗号と云っても、数理暗号と量子暗号の２種類があるのでしょう。

A ： その通り。量子暗号では、認証・署名機能を実現できないから、データ伝送（YOO により）する場合でも、送信者・受信者の本人確認は、公開鍵暗号という数理的手段に頼らざるを得ないのだ。公開鍵暗号に内蔵される秘密鍵は、

「秘密鍵こそ命、我が命」だ。

Q ： 歌の文句のようだけど冗談ではないのね。先生は秘密鍵の中に、本人確認の完全性・健全性を保つ為、マイナンバーや STR・DNA 等を入れる 3 層構造の公開鍵暗号を提案してるわね。

A ： 話が難しくなったな。出来れば、何兆人に 1 人でも同定できる Short Tandem Repeat (STR)というデジタル DNA 情報を秘密鍵に埋め込みたいが、経費と時間を考えると当分は無理だろう。そこで、マイナンバー・乱数を極秘密鍵として秘密鍵に埋め込み、運用時に、盗難された秘密鍵が、悪用されないように、極秘密鍵を所持していることを、送信相手に、零知識証明することを提案しているのだ。

Q：公開鍵暗号はそんなに大事なのに、社会的認知が低いのは困ったものね。宇宙や細胞の話だと何となく分った気になるけど暗号は数学的だから玄関払いになるのね。

A：18 世紀ヨーロッパ最大の数学者、オイラーより少し早く江戸時代の和算家久留島義太が発見していた公式が、これまで広く使われている RSA 公開鍵暗号の基礎になっているのだ。心と頭を開いて少し聴いて欲しいな。

Q：それにしても暗号で使う数の世界って独特ね。

A：そんなことはないよ。我々は 7 を法として暮らしているではないか。これを mod 7 と書いているだけだ。7 は素数だから四則演算が自由にできる。素数 P の場合、整数

(平文 M に対して M^P-1 mod P＝M になるが、合成数 N=PQ の場合は、M ^(P-1)(Q-1)＝1 mod N ,例えば、
N＝10＝2×5 の場合、
M^(P-1)(Q-1) mod10 = M^4 mod10=1 となる。
Q：合成数を法とする場合は、1 階では 10 進数で暮らしているのに，2 階（冪）では 4 進数なのね。2 階の人は、1 階の人が 10 進数で暮らしていると分かるけれど、逆に、1 階の人は、2 階の人が何進数で暮らしているか分からないという訳か。
A：それを上手く使うのが RSA(Rivest-Shamir-Adleman)暗号だ。
公開鍵：N(=pq)，e　　秘密鍵：p、q
　　平文：　m<N　　暗号文：C= m^e　modN
Q ： 公開鍵、N と e を知っていれば、誰でも m を暗号化出来ることはわかったわ。復号はどうするかを知りたいわ。
A: さて、C= m^e　modN　をどうしたら　m に戻せるかな。
Q ： C^d＝1 modN となるような d が見付かるといいわね。
mod P　の場合は　ed＝1　mod P-1 だから、誰でも復号出来てしまうから駄目ね。
A ：そこで、久留島―オイラー関数（P－1)(Q－1）の出番という訳だ。
ed＝1　mod (P－1)(Q－1)　だから。
Q ： 数学というのは、いつどこで役に立つか、分からないものね。
A ： さて、素因数分解ベースの RSA 暗号に続いて、1985 年頃、楕円曲線暗号が提案された。
Q ：　ブロックチェインでは、楕円曲線暗号が認証基盤になっているわね。
A：RSA の場合、鍵長 2024 ビットとすれば、楕円曲線暗号なら鍵長 200 ビット位で済むし、安全性も効率性も楕円曲線暗号は RSA 暗号に優るのだ。
公開鍵暗号の歴史―その 2：耐量子・IoT 環境に向けて
Q ：　発明の順が逆だと良かったけれど、それが歴史の皮肉かな。さて、量子コンピュータの導入が予想より早くなりそうだとも言われているので、そちらに話題を移しましょう。NIST で選定中の数理耐量子コンピュータ暗号は、4 種類あるのでしょう。
A ： 2023 年 5 月現在、NIST の耐量子コンピュータ暗号として標準化が決まっている暗号は、Kyber,Dilithium,FALCOM,SPHINCS+の 4 方式だ。これまで格子（lattice）系、多変数多項式系、誤り訂正符号系、同種写像系の 4 種類などが候補で、効率性の点で格子系が最も人気があったのだが、今後の動きに注目したい。多変数多項式系は、日本発だ。1983 年に、横浜国大の今井研究室（当時）から、MI(松本・今井)暗号が提案され、1985 年、辻井（当時 東工大）が、回路解析の順序解析からヒントを得て、順序解法方式を提案した。欧米で多変数多項式系の研究が始まったのは、1993 年頃、耐量子コンピュータ暗号の必要性が叫ばれるようになってからだ。
Q ： 当時、大阪大学におられた笠原正雄先生達は、符号理論をベースに暗号研究を始められたと伺っているわ。先生は、何故、多変数多項式系を始めたの？
「RSA 暗号の他に何かないかなぁ」という好奇心からだ。
さて、次の誤り訂正符号系は、符号理論の専門家たちが考えたのだろう。最後の同種写像だが、私は、これに大きな期待を抱いているが落選したのは残念だが、今後の研究に期待している。
Q ： どうして？同種写像って、どんな写像ですか。
A ：楕円曲線から楕円曲線への一方向性の写像を同種写像と呼ぶ。この一方向性は、耐量子コンピュータだ。先程も言ったように、これからのブロックチェインなどの分散系システムでは、楕円曲線暗号が基盤となるが将来、量子コンピュータに耐えられなくなったとき、現在、公開している楕円曲線をそのまま活用するためだ。
Q ： 成程。どのような方式が提案されているの？
A ：公開鍵方式が提案された 1980 年前後に、Diffie と Hellman が離散対数問題の困難性に依拠する鍵共有方式を提案した。DH 鍵共有方式と呼ばれている。お互いに相手に秘密を漏らさずに、同じ鍵を共有する巧みな方式だ。これを耐量子化する方式として、同種写像を使った研究が深められることを期待している。
Q ： 先生は玉川大学の廣田先生と一緒に、YOO 量子ストリーム暗号の鍵の種生成に CSIDH を利用する方式、数理暗号と量子暗号を結合する方式を提案してますね

3 層公開鍵暗号の提案 ― 秘密鍵に極秘密鍵を内蔵・盗用されない為に

（文献（10））。

A ： そうだね。YOO は、世界的に普及している AES 共通鍵暗号を,盗聴不可能で(盗聴しようとしても量子ノイズで暗号文自体が変化する)、且つ、真正乱数を鍵にできるように理想化した方式だ。どこにでも使えるわけではないが、今後、5G,6G 環境に向けて、空間光通信への利用が広がるから期待しているよ。最後にもう一つ。秘密鍵が盗まれても使われないようにする為、秘密鍵の中に、マイナンバーやＤＮＡ情報等、本人性を確認できる情報を秘密に埋め込む３階層公開鍵方式を提案している（文献（11））。

この研究は、令和３年度ＳＣＡＴ研究助成の対象として採用され、令和４～５年度に実施されたものです。

参考文献

（1）辻井重男、暗号　講談社学術文庫　２０１２
（2）辻井重男、フェイクとの闘い 暗号学者が見た大戦からコロナ禍まで　コトニ社　２０２０
（3）辻井重男、情報社会・セキュリティ・倫理　電子情報通信学会編　コロナ社　２０１２
（4） 辻井重男・笠原正雄編著、暗号理論と楕円曲線―数学的土壌の上に花開く暗号技術、森北出版 2008
（5） 新人物往来社、太平洋戦争情報戦　１９９８
（6） 吉田一彦　友清理士、暗号事典　研究社 2006
（7） フレッド・B・リクソン、松田和也訳、暗号解読事典　２０１３　創元社
（8） 岡本龍明、現代暗号の誕生と発展　ポスト量子暗号・仮想通貨・新しい暗号　近代科学社、２０１９
（9） 小松啓一郎、 暗号名はマジック―太平洋戦争が起こった本当の理由　KK ベストセラーズ　２００３
(10) 辻井、廣田修、同種写像数理暗号と YOO 量子暗号の結合による耐量子コンピュータ暗号システムの提案、電子情報通信学会　情報セキュリティ研究会 202211 月
(11) 辻井他　究極の本人確認のための 3 層型公開鍵暗号の提案―第 3 報 ―秘密鍵が紛失・盗難されても盗用されないマイナンバー・カード利用、電子情報通信学会 SCIS2020