1. 21世紀初頭の暗号技術

1. 数論アルゴリズムと公開鍵暗号の安全性

岡本 龍明
NTT情報流通プラットフォーム研究所
okamoto@sucaba.isl.ntt.co.jp

内山 成憲
NTT情報流通プラットフォーム研究所
uchiyama@sucaba.isl.ntt.co.jp

公開鍵暗号の誕生

1976年のDiffieとHellmanによる公開鍵暗号の提案は，数千年の歴史を持つ暗号史上，最も革新的な出来事と言えよう．この公開鍵暗号は，いまや情報ネットワーク社会に不可欠のインフラストラクチャとなっている．

暗号にとり最も重要なことは，その安全性であることはいうまでもないであろう．本稿では，公開鍵暗号の安全性の現状について解説する．

現在インターネットなどで用いられている公開鍵暗号のほとんどが，数論（整数論）に基づく方式であり，その安全性はいくつかの数論の問題を解く効率的なアルゴリズムが存在するかどうかに依存している．本稿前半では，そのような数論アルゴリズムの現状を解説する．

一方，数論の問題のような基本的な問題の困難性を仮定することにより，さまざまな攻撃に対する公開鍵暗号の安全性を証明することが可能となる．本稿後半では，そのような安全性の証明手法の現状を解説する．

数論アルゴリズム研究の四半世紀

現在，世界中で最も使われている公開鍵暗号方式は，1977年に，Rivest，ShamirとAdlemanによって提案されたRSA暗号であろう（この3人は，RSA暗号の発明によりコンピュータサイエンス界のノーベル賞とも呼ばれるTuring賞を2003年に受賞している）．RSA暗号の安全性は，素因数分解問題の困難さに基づいている．IT社会とも呼ばれる現代社会における暗号の役割の重要性を考えると，それまで数学の中でも実社会への応用からは最も遠いと考えられてきた数論は，素因数分解問題といった数論の問題に対して効率的なアルゴリズムを見つける研究（数論アルゴリズムの研究）が，直接的に公開鍵暗号の研究と結びついたことにより，突然，現代社会の基盤を支える重要な分野へと変貌してしまったとも言えよう☆1．

ここでは，この四半世紀ほどの間に，過去に見られないほどの目覚ましい発展を遂げた数論アルゴリズム研究の中で，公開鍵暗号との関連から素数判定問題と素因数分解問題について述べる．

●素数判定問題－2000年来の未解決問題と拡張Riemann予想－

与えられた自然数が素数かどうかを効率的に判定することは，公開鍵暗号の鍵生成において不可欠である．素数判定問題とは，1より大きな自然数nが与えられたとき，nが素数かどうかを判定する問題である．この問題は，紀元前300年頃にはすでに知られていたようであるが，入力サイズの確定的多項式時間で解けるかどうかは，2000年以上未解決であった．ところが，2002年8月にAgrawal，KayalとSaxenaによりこの問題は肯定的に解決された．しかし，このアルゴリズムには，すでにいくつかの改良も提案されてはいるが，どれも現時点では実用的なものとは考えられていない．2003年2月にAgrawalらによって提案された改良アルゴリズムの計算量は（高速乗算法などを用いて）入力サイズの$7.5+o(1)$乗のオーダである（ただし，$o(1)$は，入力サイズを十分大きくす

☆1 このような数論の変化について，Fermat予想の解決で有名なWilesは，文献2）の中で以下のように述べている：“... One change in number theory over the last twenty years is that it has become an applied subject. (Perhaps one should say it has gone back to being an applied subject as it was more than two thousand years ago. Public key cryptography has changed the way we look at secrecy and codes...)”

るとき0に近づく）．

素数判定問題に対する効率的な解法を求めようという研究は，1970年代以降に本格化したと考えられる．実際，1976年にはMillerにより，拡張Riemann予想（ERHと略す）☆2と呼ばれる数論の予想を仮定すると，素数判定問題は入力サイズの確定的多項式時間で解けることが示されていたのである．また，この判定法は効率が良く，入力サイズの$4+o(1)$乗のオーダの計算量である．

素数判定問題に限らず，ERHを仮定することにより効率の良いアルゴリズムの存在を示せる数論アルゴリズムの問題は数多くあるが，（そもそも応用など考えず）純粋に数論の問題としての予想が，計算量的な観点からも非常に有用であることは，ある意味で驚くべきことのように思われる．しかし，このことは「良い数学は，有用な応用をも与える（？）」ということを示唆しているのかもしれない．

●素因数分解問題－現代暗号を支える最も重要な数論の問題－

素因数分解問題とは，合成数nが与えられたとき，nの非自明な約数を求める問題である．この問題も古くから知られている計算量的に困難な問題☆3であるが，いまだ効率的なアルゴリズムは知られておらず，RSA暗号に代表される公開鍵暗号の安全性の礎を与えている．現時点で，（漸近的に）最も高速な素因数分解アルゴリズムは数体ふるい法であり，その計算量のオーダは，対象となる合成数をnとすると

$$e(1.9+o(1))(\log n)^{1/3}(\log\log n)^{2/3}$$

となる．これは，nのサイズに対して準指数時間と呼ばれる．現在の計算機の能力の下でどの程度のサイズの合成数を分解することが可能かという問題は，数論の問題として興味深いだけでなく，実際にRSA暗号を用いる上でも最も重要な問題である．RSA社では，さまざまなサイズの大きさのRSA暗号で用いられる合成数の分解コンテストを行っている．現在の世界記録は，2003年12月に，ドイツのボン大学のチームによる数体ふるい法の実装で分解された576ビットの合成数（RSA-576）である．特殊な型の合成数の分解の世界記録は，立教大学，NTT，富士通研究所のチームによる特殊数体ふるい法の実装によるもので，822ビットの合成数である．さて，現在のRSA暗号の公開鍵の推奨サイズは，多くの場合1,024ビットであるが，最近，専用のハードウェアを用いた方法なども提案されており，1,024ビットRSAの安全性については，さらなる詳細な評価が必要と思われる．ShamirとTromerにより提案されたTWIRLと呼ばれる数体ふるい法専用のハードウェアを用いると，1,024ビットのRSA公開鍵は，1年以内に1Mドル（約1億円）で分解できるという見積りもされている．しかし，現時点の技術ではこのハードウェアの実現は難しいという意見もあるようである．

公開鍵暗号の安全性の証明

古来より，暗号の歴史は，作っては破られ，それに対抗して改良を加えるということの繰り返しであった．しかし，1980年以降の現代の暗号理論が目指した目標は，そのような繰り返しを断ち切るための手法を確立すること，つまり安全性を証明する手法を確立することである．

この目標は，ある意味では大成功したが，ある意味ではいまだに達成される見込みすらない．という意味は，公開鍵暗号の安全性は本質的に数論の問題の困難性などの計算量的な仮定に依存しており，そのような計算量的な仮定を前提としない絶対的な安全性を証明することは，いまだに我々にとって絶望的といえるほど解決の糸口が見えない問題である（つまり，有名なP vs NP問題を解くことに相当する問題である）．

そこで，現在の我々が取り得る次善の策が，素因数分解問題のような基本的な問題の困難性だけは仮定して，その仮定の下で公開鍵暗号の安全性を証明するという方法である．つまり，絶対的な安全性の証明は諦めて，相対的な安全性を証明しようという立場である．以下，その現状について解説する（なお，ここでは紙数の制約のため，秘匿のための公開鍵暗号のみについて述べる．同様のことが，ディジタル署名についても知られている）．

●安全性の定義

暗号は攻撃者（盗聴者）に通信内容を隠して送ることを目的とするためどの程度通信内容を隠しているかの度合いが重要である．このとき，いかなる部分的な情報も秘匿できることを強秘匿と呼ぶ．さらに，暗号文から平文の内容を知ることはできないが，暗号文を操作するこ

☆2 ERHは，Riemann予想（RHと略す）と呼ばれる有名な数論の予想の一般化である．RHは，米国のClay研究所により発表された数学における未解決の7つの難問の1つで，100万ドルの懸賞金が提供されている．

☆3 素因数分解の困難さについて，Adlemanは文献1）の中で，数論と化学の間のアナロジーを用いて興味深い考察を行っている．たとえば，$2H_2+O_2\rightarrow 2H_2O$と$p\times q=n$（$p,q$は自然数）という式が見かけだけでなく，本質的に似ているのではないかというものである．酸化反応は速い（やさしい！）が，その逆は，いわゆる「水の電気分解」であり，ポテンシャルエネルギーの差分だけ外部からエネルギーを与えてやる必要があり遅い反応（困難！）となる．これは，まさに“一方向性”とみなせる．文献1）では，数にも“ポテンシャルエネルギー”に相当するものが定義できるかどうかを論じている．

とにより，対応する平文に意図的な変更を加えること（たとえば，平文をビット反転させるなど）などの攻撃があり得る．このようなことが一切できないことを頑強性と呼ぶ．

一方，攻撃者のタイプには単に暗号通信を受信し，それだけから解読を試みる受動的攻撃と，送信者にさまざまな質問をし（暗号文を送り）その回答（その復号結果）をもらうことが許され，そこで得られた情報を利用して目的とする暗号文の解読をするような能動的攻撃（適応的選択暗号文攻撃）がある．

公開鍵暗号に対して求められる安全性は，「適応的選択暗号文攻撃に対して頑強かつ強秘匿」であるが，この安全性は「適応的選択暗号文攻撃に対して強秘匿」であることと等価であることが知られている．

●安全な暗号の具体的構成方法およびその証明手法

安全性の証明ができて実用性に優れた公開鍵暗号の構成法には，大きく2つの方法がある．1つは，暗号の構成に用いる一方向性関数（たとえば，SHA-1などのハッシュ関数）をランダム関数に理想化した上で安全性の証明を行う方法（ランダムオラクルモデルと呼ばれる方法）と，一方向性関数に対して現実的な仮定（関数値が一致するような入力値のペアを見つけるのが難しいなどの仮定）を前提にして安全性を証明する方法である．前者の代表は，1994年にBellareとRogawayにより提案されたOAEP（Optimal Asymmetric Encryption Padding）と呼ばれている方式であり，後者の代表が，1998年にCramerとShoupにより提案されたCramer-Shoup方式である．RSA暗号に基づくRSA-OAEP方式は，RSA関数が一方向性であるという仮定とランダムオラクルモデルの下で「適応的選択暗号文攻撃に対して強秘匿」である．また，Cramer-Shoup方式は，決定Diffie-Hellman仮定という仮定と汎用一方向性ハッシュ関数という仮定の下で「適応的選択暗号文攻撃に対して強秘匿」である．

1999年，藤崎と岡本は，一般の（確率的）暗号関数（トラップドア一方向性関数）を，ランダムオラクルモデルの下で「適応的選択暗号文攻撃に対する強秘匿」である暗号方式に変換する一般的で効率的な方法を示した．彼らの方法は，共通鍵暗号と公開鍵暗号を組み合わせたハイブリッド暗号方式を安全かつ効率的に構成する方法も示している．

一方，2000年に始まったISOにおける公開鍵暗号の標準化活動において，Shoupはハイブリッド暗号方式を構成する標準的な枠組みとして，鍵カプセル化メカニズム（KEM）とデータカプセル化メカニズム（DEM）を作り，それらの安全性の定義とその具体的な構成方法を示した．公開鍵暗号と同様に，KEM, DEMに対して，「適応的選択暗号文攻撃に対する強秘匿」をそれぞれ定義している．KEMの具体的な方式としては，RSA-KEM, PSEC-KEM, ACE-KEMなどが提案されており，いずれも数論的困難性仮定とランダムオラクルモデルの下で「適応的選択暗号文攻撃に対する強秘匿」であることが示されている．これらは近いうちにISO標準となることが見込まれている．

これから

素因数分解など数論の問題の困難性は，現在広く使われている公開鍵暗号の安全性を根本から支えるものであるため，適切な鍵サイズを知る上でもその研究動向に注意していく必要がある．

一方，本稿で紹介したRSA-OAEPやCramer-Shoup方式は，「相対的な」安全性しか証明されていないが，通常「安全性の証明のついた」（provably secure）方式と呼ばれる．実用に供される暗号・認証方式がなんらかのかたちで「安全性の証明のついた」方式であるべきであるという認識が暗号設計者や利用者の間で着実に広まりつつある（常識となりつつある）ことを強調しておきたい．

最後に，将来量子計算機が実現されると，素因数分解問題などが効率よく解かれることが知られているが，その実現にはかなりの年月が必要とされると予想されており（最も楽観的に見積もっても20年以上かかると思われている），公開鍵暗号の当面の安全性には影響しないと考えられている．

参考文献
1）Adleman, L. M.: Time, Space and Randomness, MIT/LCS/TM-131, MIT (1979).
2）Wiles, A.: Twenty Years of Number Theory, Mathematics: Frontiers and Perspectives, AMS, pp.329-342 (2000).

（平成16年9月30日受付）