公開鍵配送方式に代えＩＣカード共通鍵配送方式へ

1S－8

足立　宗三郎
オムロン(株)ソシアールグループ拡業開発室

１、はじめに

公開鍵暗号方式は、鍵をオープンにできる暗号方式としてインターネット上の個人決済関連にも用いられようとしている。

処理効率上、公開鍵で全文を暗号化するのではなく、相手に対し共通鍵を配送する手段として公開鍵を用いることは、実用化されている。

２、公開鍵暗号方式に用いる素数判定の通説。

通説では、必要とする桁数の乱数をランダムに発生させ、その時の乱数ｐを次の式で、素数とならないかプログラムで判定する。

1) $a^{(p-1)} \equiv 1 \pmod{p}$ が成立すること。
ａはｐとは素な整数。
ａは、ｐ－１までの素数：2,3,5,7,11,13,17,19,……ｐ－１までを順次、当てはめて検証するは定説である。

しかし、ｐ－１までの素数列のチェックでなく省略する諸説がある。

2) $a^{(p-1)} \equiv 1 \pmod{p}$ において素数：2,3,5,7,11,13,17,19,……(p-1ではなく)、1000以下の素数でよしとする説。

3) $a^{(p-1)} \equiv 1 \pmod{p}$ においてランダムにとったいくつかのａに付いて、常に成立すれば、ほぼ素数である確率が高いとする説。

３、[仮説]:公開鍵Ｎの素数分解は容易。

公開鍵Ｎの素数分解の通説は、小さな素数から、√Ｎまでの大きな素数へと順次、割ることを繰り返すとある。その時、商をあらかじめ想定することはない。

今回の仮説は、Ｎを素数分解するＰ、Ｑを、Ｙ＝Ｎ／Ｘの曲線上にあるものとして、仮の長方形Ｐｎ×Ｑｎ＋Ｃ＝Ｎとする仮想のＰｎ、Ｑｎをとって、剰余Ｃを、０とする条件を追う。

Ｎの桁数をｋ＋１とする。Ｎの先頭の数値をＡとすると、10のｋ/2乗の面積がＡ個あると想定できる。[ここのｋが、奇数値の場合(ｋ－１)とするが、ｋの表現に含める。]

The crypto key transport system :
from the public key method,
to the symmetric key in IC cards.
Sousaburo Adachi(SGY02446@niftyserve.or.jp)
Omron co.social systems future business dept.

Ｐｎは、10のｋ/2乗を最大とする、10を基準とする「べき乗数」のいくつかでプロットする。

暗号機能としてのＮは、Ｐと、Ｑとの桁数を相当異ならせることが多い。

よって、まづ、偏平な長方形を設定する。

10進数で表現されたＮの数値をそのままに分解する。Ｎの桁数ｋの約1/3ぐらいの10のべき乗、$10^{k/3}$をＰｎとおく。

$10^{k/3}$のＰｎを一辺とする正方形の面積は、当然$10^{2k/3}$となる。この$10^{2k/3}$の面積を持つ正方形タイルの数Ｌは、Ｎの先頭から1/3のＮの数値が、そのままＬとなる。

Ｎの先頭より1/3以降の桁から2/3桁までのＮの数値は、長辺をＰｎとするタイルのかけらであり、その短辺の巾を示している。それをＴｎとする。

Ｎの先頭より2/3桁以降、末尾までのＮ値は、単位１の剰余であり、Ｃとする。

Ｎの面積は、Ｌ×Ｐｎ^2＋Ｐｎ×Ｔｎ＋Ｃで表され、Ｃ＝０の条件が、ただ一つの素数分解条件を与える。

Ｎの数値により、10のべき乗のＰｎによって、Ｌ、Ｔｎ、Ｃが上述のように得られる。

Ｌ×Ｐｎ＋ＴｎをＱｎ（仮のＱとし）と置く。

Ｐｎより下方向への減分をｙｄ、Ｑｎ方向の増分をｘｉとする。

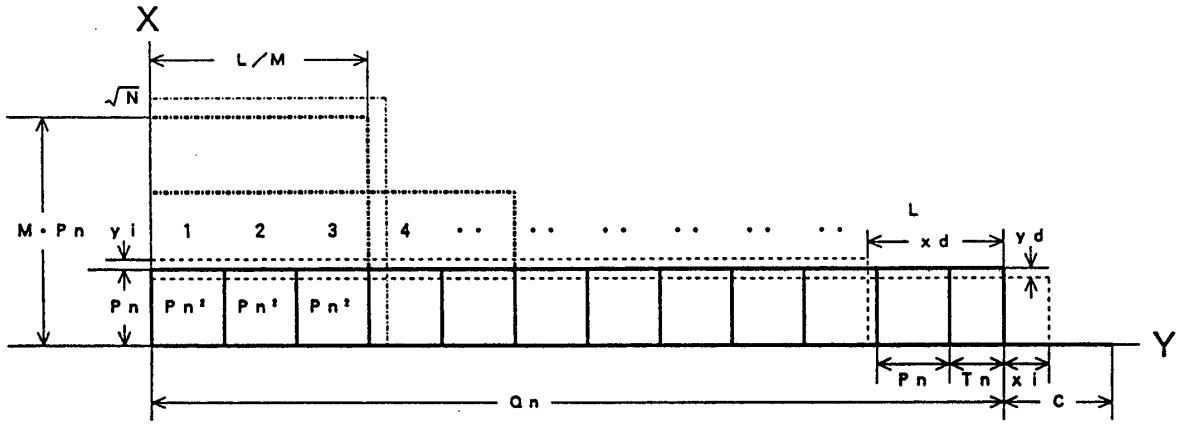
（Ｑｎ×ｙｄ)＋Ｃ＝（Ｐｎ－ｙｄ）×ｘｉ…Ａ　この式が成立するときは、Ｐｎ－ｙｄ＝Ｐが、Ｎの短辺、Ｑｎ＋ｘｉ＝Ｑが、Ｎの長辺であり、その成立が素数分解となる。

もう一つ、Ｐｎ方向の増分をｙｉ、Ｑｎ方向の減分をｘｄとし、

ｙｉ×（Ｑｎ－ｘｄ）＝(Ｐｎ×ｘｄ)＋Ｃ…Ｂ　この式が成立するときは、Ｐｎ＋ｙｉ＝Ｐが求める短辺、Ｑｎ－ｘｄ＝Ｑが求める長辺である。

Ｐ、Ｑの桁数が、接近した桁として想定すれば、$10^{2k/3}$＝Ｐｎ^{2}のタイルをＭ段重ねて、Ｍ×Ｐｎと、Ｌ／Ｍ＋Ｔｎ／Ｍ＝Ｑｎとの長方形とし、ＰｎのＭ倍のＭ×ＰｎをＰｎにして、同様の式が立てられる。

このＭは、Ｎの先頭2～3桁の数値から取り得る各種の長方形を想定し、その短辺対長辺の比、Ｍ：Ｌ／Ｍを、細かくプロットすることも効果的である。



Nが２進数で表現されている場合、ｋはビット数を適用すれば良い。例えば７６８ビットならばｋ/3は２５６であり、Ｐｎは、2^{256}とする。

上式を構成する(Ｐｎ＋ｙｉ)、(Ｐｎ－ｙｄ)あるいは(Ｑｎ＋ｘｉ)、(Ｑｎ－ｘｄ)のいずれにも、前記１項で述べた、$a^{(p-1)} \equiv 1 \pmod{p}$ の素数判定式をプログラム化して通し、選別済みの素数；飛び飛びの数値から、Ｐｎ、Ｑｎを引いてｙｉ、ｙｄ、ｘｉ、ｘｄを得て、それらをＡ、Ｂ両式に適用し、Ｃ＝０のシュミレーション、つまり左辺と右辺がイコールの条件で終了するプログラムとする。

この仮説は、Ｎの数値から、剰余Ｃを許容し、10進数Ｐｎで、Ｙ＝Ｎ／Ｘの曲線をプロットすれば、Ｎの数値Ｌが、おおまかな曲線近辺の基点をさす。その曲線近辺の素数を判定式で抽出し、その比較シュミレーションをおこなうのみである。この抽出、比較アルゴリズムのプログラムは、「乱数から素数を選定する」と同等程度の容易なレベルと考える。公開鍵Ｎは、素数の積の選別と、分解に必要な計算量との比は大きくなく、Ｎの桁数を増やしても、そう強くはならないとの結論に達した。

これらから、金融、流通関係の社会インフラに相当するシステムでは、十年以上の長年継続して使用する基盤システムである。懸念点を提起し、専門家に検証していただけることを期待する。

４、ＩＣカードによる共通鍵配送方式の紹介。

上述の公開鍵暗号方式は、不特定多数の相手に暗号を適用する場合、同一の暗号鍵が配布できるところに特徴があり、共通鍵のように誰にどの鍵を送ったかという鍵管理は、不要にできるという利点を持っている。

それに相当する機能として、ＩＣカードを用い、オリジナルなカード番号、あるいは別の一元的なオリジナルなカード番号を対象とし、配布元が持つ複数の共通暗号鍵で暗号化したもの、つまりＩＣカード番号を暗号化した複数のコードを、個々のＩＣカード特定の共通暗号鍵として、ＩＣカード内に秘匿させる方法を推奨できる。

そのＩＣカードとは、ISO7816-4の規定で、拡張機能として含む共通鍵暗号機能を内蔵したものであって、その規定では、誤ったアクセスには、15回を最大とする設定した回数でロックする機能もある。

配布元は一組の複数の共通暗号鍵を管理するのみで、個々にＩＣカードを配布し、各々のＩＣカード番号所持者と複数の暗号鍵を共有でき、所持者を特定した暗号化メッセージを交信でき、それによって鍵管理を不要にできる。

一度ＩＣカードを配布すると、交信に使用していない暗号鍵で、再度複数の共通鍵をＩＣカードに送り込むこともできる。標準的な共通鍵の鍵種類は、２の64乗あり、これは、およそ一兆の一千万倍以上に相当し、ほかダブル、トリプル共通鍵と称される128ビット、192ビットの共通鍵も開発されているから、鍵種類には困らない。

５、ＩＣカード鍵配送方式の応用

インターネット上でのクライアント間、あるいはサーバとの長文メッセージの暗号化には、このＩＣカード共通鍵配送方式で、無限数列を生成する関数と、その使用桁の最初の位置を暗号化して、メッセージの前後に交信者に送付し、その無限数列を長文メッセージに重畳して送信すれば、交信者と無限数列を共有することによって、ヴァーナム暗号方式と同様、暗号強度は強く、処理は早い、この鍵種類は、整数以上に無限に近い種類を持っていることから、アルゴリズムを公開し共有しても、その暗号の強度は強い。無限数列の関数とは、平方根、立法根であって、その無理数の数列を指し、パソコンと拡張言語で可能である。

参考文献

[情報処理学会H7前期全国大会講演論文集(1)
2S-6:ICｶｰﾄﾞを媒体とした電子ﾃﾞｰﾀｻｰｸﾙ]
[(株)ｼｰﾒﾃﾞｨｱ出版:「ICｶｰﾄﾞ総覧」ｾｷｭﾘﾃｨの章]