第01回

- 講演者 桶屋 勝幸 氏 (日立製作所 システム開発研究所)
  - 題目：RSA暗号のビット長2倍化技術
  - 日時：平成19年5月29日（火）16:30-17:30

n ビットの剰余乗算(\(x*y \mod m\))を行う演算器があったとします。 この演算器を用いて \(2n\) ビットの剰余乗算を実現できるか、 というのが問題です。 ここで法が n ビット以下の整数の積に分解できればCRT(Chinese Remainder Theorem)を用いて簡単に求めることができますが、 法の因数分解がわからない状態でできるか、 というのが上記の設定です。

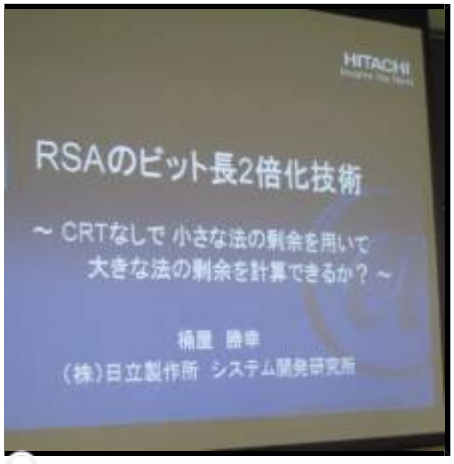
RSA暗号は公開鍵暗号の一つで、その安全性は素因数分解の困難さに由来します RSAの暗号化や復号は、1024ビット相当の大きな整数を法とした剰余乗算を 繰り返し用いて計算されています。 昨今では RSAはICカードのような計算リソースの乏しいコンピュータ上にも実装されています。 上記の剰余乗算は相当に重い計算ですので、コプロセッサなど専用演算器を用いて計算するのが通常です。

ところで RSAを安全に保つビット長はどのように定められているかご存知でしょうか？ このところの素因数分解記録の進展は目覚しいものがあり、より大きなビット長の分解記録の報告がなされています。 もちろん、これらの分解記録よりも大きくとらなければなりませんが、 時間と共に安全性は逓減しますから、マージンも必要となります NIST(米国標準技術局)など各種の標準化団体は年次ごとに安全と見込まれるビット長を公表しています。 たとえばNISTの場合は、2010年までは1024ビット以上のRSAの使用を推奨していますが、 それ以降の年は2048ビット以上を推奨しています。

ここに至って上記の問題が出てくることになります。 コプロセッサなどの専用演算器は、扱えるビット長の上限が定まっています。 1024ビットの剰余乗算を行うために作成した演算器であれば、 1024ビットより大きな数を扱うことはできません。 2010年以降も用いようとした場合、2048ビットの演算が必要ですが、 その演算が実現できない、ということになってしまいます。

この問題を解決するのがビット長2倍化技術です。 歴史的な背景と研究動向、最近の研究結果などをご紹介いたします。

講義資料(PDF) okeya.pdf



.lg-outer.lg-pull-caption-up.lg-thumb-open .lg-sub-html {bottom:80px;}

31 images