L-024

認証手続きを効率化する 3 つ組暗号の改善

Improvement of dual encryption method for efficient authentication

八反地　鉄平†　　佐藤　康臣†　　島　和之†　　大場　充†
Teppei Hattanchi　Yasuomi Sato　Kazuyuki Shima　Mitsuru Ohba

1．はじめに

近年，インターネットの普及により，通信情報の秘匿，通信相手の認証などに公開鍵暗号が使用される機会が増加している．情報の秘匿では送信者と受信者の 2 者間でデータを送受信するのに対し，認証では通信相手に対する存在証明を行う仲介者を含めた 3 者間でデータを送受信することになる．

一般的な公開鍵暗号を使用した認証手続きは最低でも 2 組の鍵対を使用し，手続きが複雑になる．このような 3 者間において，3 つの鍵を 1 組とした暗号を使用することにより認証手続きを効率化する 3 つ組暗号[1][2]が提案されている．

[2]で提案された手法は[1]の脆弱性を改善している．しかし，[1][2]はともに 1 組の鍵を生成する時間が 1024bit の鍵長を仮定すると，通常能力の PC では 10 の 20 乗秒以上かかり，実用的に使用するには問題が多い．

本研究ではフェルマーの小定理を応用した 3 つ組暗号を提案する．認証手続きの状況を想定し，鍵特定時間に加え，解読時間，鍵生成時間，暗号化・復号時間を加えて評価し，[1][2]と比較し，暗号の実用性を改善することを目的とする．

2．オイラーの公式を用いた 3 つ組暗号

p，q を素数とし，X を pq と互いに素な数とするとき，オイラーの φ 関数を用いて(1)が成立する．

$$X^{\phi(pq)} \equiv 1 \pmod{pq} \tag{1}$$

(1)式の両辺に X を掛けると，(2)式が成立する．

$$X^{\phi(pq)+1} \equiv X \pmod{pq} \tag{2}$$

このとき任意の数 k と自然数 a，b，c は以下の式を満たす．

$$k \cdot \phi(pq) + 1 \equiv abc \pmod{\phi(pq)} \tag{3}$$

(3)式を満たす a，b，c を鍵として用いて，以下に暗号化，及び復号方法を示す．

(ⅰ)送信者は鍵 a と法 pq を用いて平文 X を

$$X^a \equiv Y \pmod{pq} \tag{4}$$

で暗号化し，暗号文 Y を仲介者に送信する．

(ⅱ)仲介者は鍵 b と法 pq を用いて Y を

$$Y^b \equiv Z \pmod{pq} \tag{5}$$

でさらに暗号化し，暗号文 Z を受信者に送信する．

(ⅲ)受信者は鍵 c と法 pq を用いて Z を

$$Z^c \equiv ((X^a)^b)^c \equiv X \pmod{pq} \tag{6}$$

で X に復号する．

3. 提案する 3 つ組暗号

p を素数とし，自然数 a と p が互いに素であるとき，(7)式が成立する．

$$a^{p-1} \equiv 1 \pmod{p} \tag{7}$$

このとき，自然数 d，e，f は(8)の式を満たす．

$$p - 1 = d + e + f \tag{8}$$

(8)式を(7)式に代入すると次の式が成立する．

$$a^d \cdot a^e \cdot a^f \equiv 1 \pmod{p} \tag{9}$$

(9)式の積の要素に対して，任意の自然数 m と p を掛けた値で剰余をとったものを K_1，K_2，K_3 とする．

それを(10)，(11)，(12)式に示す．

$$a^d \equiv K_1 \pmod{mp} \tag{10}$$

$$a^e \equiv K_2 \pmod{mp} \tag{11}$$

$$a^f \equiv K_3 \pmod{mp} \tag{12}$$

3 者間での暗号化及び復号を図 1 のように行う．以下に暗号化，及び復号方法を示す．

(ⅰ)送信者は鍵 K_1 と法 p を用いて平文 X を

$$K_1 \cdot X \equiv Y \pmod{p} \tag{13}$$

で暗号化し，暗号文 Y を仲介者に送信する．

(ⅱ)仲介者は鍵 K_2 と法 p を用いて Y を

$$K_2 \cdot Y \equiv Z \pmod{p} \tag{14}$$

でさらに暗号化し，暗号文 Z を受信者に送信する．

(ⅲ)受信者は鍵 K_3 と法 p を用いて Z を

$$K_3 \cdot Z \equiv K_1 \cdot K_2 \cdot K_3 \cdot X \equiv X \pmod{p} \tag{15}$$

で X に復号する

図 1:提案する暗号系を用いた情報の変換

4. 実験

4.1　提案手法する暗号系で用いる m の設定

提案手法において m は任意の数であるが，m の値を大きくすればするほど，鍵長が長くなり強度は強くなる．一方，本実験では他の暗号系と比較することが必要となるため，鍵の探索範囲が RSA 暗号と同等となるような m の値を決め，鍵長の範囲を設定した．以下に法を Nbit，提案手法において使用される a を αbit とし，鍵長の範囲の設定方法を示す．

$$m = \log_2 N / \log_2 \alpha \tag{16}$$

†　広島市立大学大学院情報科学研究科

4.2　攻撃者による解読を想定した実験

認証手続きにおいて図 2 に示す「なりすまし」の状況を想定する．提案法は(16)式の m の値を用いて鍵を生成し，他の暗号系は法の大きさと同等の鍵を生成する．

送信者，仲介者，受信者はすでに鍵と法を入手し，攻撃者は受信者が受信した暗号文と法を入手しているものと仮定する．さらに攻撃プログラムには解読確認のために平文を与えた．比較する暗号系は鍵特定時間においては 12bit から 18bit まで，解読時間は 24bit から 36bit まで，鍵生成時間と暗号化，復号時間は 20bit から 80bit までで提案法(F)，積暗号を用いた 3 つ組暗号(TS)[1]，オイラーの公式を用いた 3 つ組暗号(TR)[2]，RSA 暗号とした．

攻撃プログラムが暗号文を解読するまでの解読時間，送信者鍵を特定するまでの鍵特定時間，それら 2 つと鍵生成時間，暗号化時間と復号時間を求めた．

その結果をもとに鍵特定時間，解読時間，鍵生成時間，暗号化，復号時間の 1024bit の値を予測し，認証における状況で実用的に改善されているかを確認する．

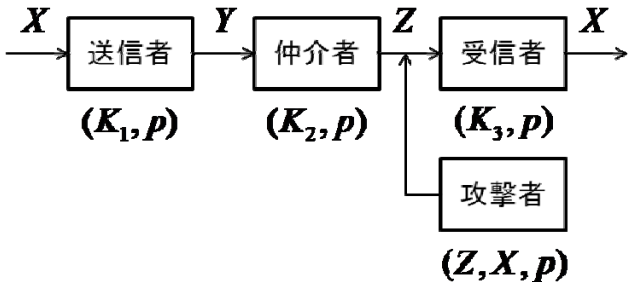

図 2:認証における「なりすまし」の状況

4.3　実験結果

図 3 は提案法と他の暗号系を 1024bit で鍵強度と暗号強度により比較したものである．鍵強度とは鍵生成時間に対する鍵特定時間の比率を表しており，暗号強度とは暗号化時間に対する解読時間の比率を表している．鍵強度を(17)式に，暗号強度を(18)式に示す．

鍵強度＝鍵特定時間/鍵生成時間　(17)

暗号強度＝解読時間/暗号化時間　(18)

ここで鍵特定時間，解読時間，鍵生成時間，暗号化時間は常用対数をとっている．このとき，右上に行くほど認証における暗号系の性能は実用的であると考えられる．

提案する暗号系は他の暗号系と比較して代数的構造が簡単になるので，鍵生成時間，暗号化時間が短くなり，鍵強度，鍵強度が増加し，改善されていることが分かった．

5. 考察

本研究では鍵特定実験を 12bit から 18bit までを行った．実験で用いた a は 2~31 までの自然数を乱数によって選択した．

RSA 暗号では法が 1024bit の暗号が多く使用されており，ここでも 1024bit における実用性を評価した．

このとき，法である p と互いに素であるという条件を満たせばよい a は 2~31 までの自然数とは限らない．

a を大きくすると，a のべき乗計算回数が増え，鍵生成の計算量が増加してしまう．一方，a を小さくすると鍵探索範囲は狭くなり，強度が弱まるが鍵生成の計算量は減少すると考えられる．

さらに，実験では 1024bit における評価をしたが，現在では 2048bit の暗号も使用されて来ている．a を大きくしていくと，a が p より大きな値になれば，a が素因数として p を含むカーマイケル数になる可能性が発生する．

p より大きいカーマイケル数 a を 選択し，a を構成している要素が法に使用されている素数 p であった場合，鍵生成が不可能となる．

a と p が素数であることが保証されれば，上述のような問題は発生しないが，暗号に必要となる素数の個数が増大するために，より大きな p が必要となる．

6. まとめと今後の課題

本研究ではフェルマーの小定理を利用した 3 つ組暗号を提案し，鍵特定時間，解読時間，鍵生成時間，暗号化時間，復号時間を他の暗号系と比較し，1024bit の値を予測した．提案手法は鍵強度，暗号強度がともに他の暗号系より強くなっており，認証における状況で実用的に改善されていることがわかった．今後の課題として，a の値を大きくすることによる計算量と強度の変化の関係の考察，実験が考えられる．

参考文献

[1] 大場充．暗号化方法，データ送信システム，及び鍵セット生成装置．　特開 2005-258188．　2005-09-22.

[2] 六角晃子．オイラーの公式を用いた三つ組み暗号の提案とその評価．広島市立大学卒業論文　2004

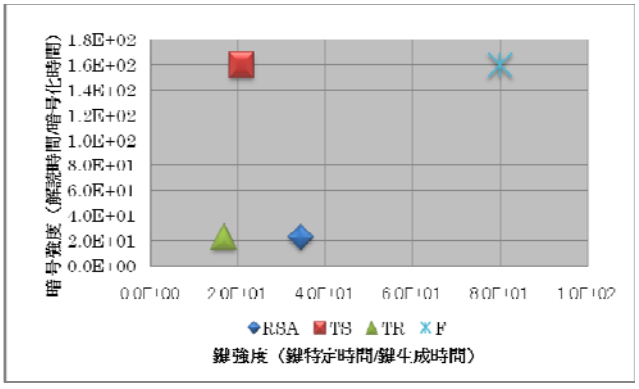

図 3:各暗号系における暗号強度と鍵強度の比較