原理的解読不能な暗号アルゴリズムへのアプローチ

4C－6

五十嵐 育弘

概要

鍵の全件試行以外に有効な解読方法がない暗号文を生成する暗号アルゴリズムを提案する。
そして、このアルゴリズムに、復号化時に復号鍵が正しいかどうかを検知するアルゴリズムを付加する。
このモデルで、原理的に解読不能な暗号文を生成する暗号アルゴリズムへのアプローチを試みる。

1　暗号アルゴリズムの提案

暗号化側が平文を暗号化するにあたり、暗号鍵以外のパラメータを用い、復号化側が、そのパラメータに依存せず、復号鍵だけで平文をえられるようにする。この構造にすることにより、暗号文は暗号化側だけの暗黙のパラメータにも依存して変化することになり、平文、鍵、暗号文の間に相関を見出せなくなる。
この指針に基づき、バーナム暗号を核として、その拡張を施した拡張バーナム暗号（仮称）を考案したので、これを提案する。
概略を下記と図１に示す。

拡張バーナム暗号のアルゴリズムの概略

①. 十分大きな桁数を持つ乱数を暗号化側の暗黙のパラメータとして用いる。
②. ①のパラメータと平文を演算する。
③. ①のパラメータに対して任意の暗号化関数と暗号鍵で暗号化を施す。
④. ②、③の結果データを混合して最終暗号文を生成する。

Consider cipher algorithm of basically impossible decipher, Ikuhiro Igarashi
e-mail:igarashi@iwangc.eec.toshiba.co.jp

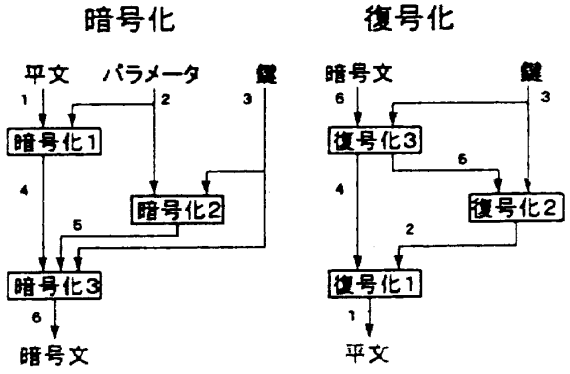

図1　拡張バーナム暗号の暗号構造

拡張バーナム暗号のアルゴリズムのモデル

E1 = f(M, R)　　R　：パラメータ
E2 = k(R, KEY)　　M　：平文
E　= g(E1, E2, KEY)　　KEY：暗号鍵

暗黙のパラメータＲの生成の方法は問わないが、平文の大きさに対し、十分大きなものであること。
パラメータ E1 は、平文Mとパラメータ R に依存する暗号関数 f()で生成される。
f()関数は、以下の逆関数を持つことを要請する。

$$M = f^{-1}(E1, R)$$

パラメータ E2 は、パラメータＲと暗号鍵ＫＥＹに依存する暗号関数 k()で生成される。
k()関数は、以下の逆関数を持つことを要請する。

$$R = k^{-1}(E2, KEY)$$

暗号文Ｅは、選択関数 g()で生成される。
暗号鍵 KEY にしたがって発生する乱数系列をもとに E1 と E2 の情報を混合する。
g()関数は、以下の逆関数を持つことを要請する。

$$(E1, E2) = g^{-1}(E, KEY)$$

選択関数 g( ) の例

暗号鍵に依存して変化する一様乱数系列を用いる。この乱数を以下のように使用する。

今、乱数の値が **39682** だったとすると、

E2 の先頭から **3** バイト目に E1 のデータを **3** バイト挿入し、E2 の先頭から **3＋9** バイト目に E1 のデータを **9** バイト挿入。同様に、**3＋9＋6** バイト目に **6** バイト、**3＋9＋6＋8** バイト目に **8** バイト、**3＋9＋6＋8＋2** バイト目に **2** バイト挿入する。この操作を E1 のデータが空になるまで乱数系列から乱数を取り出して行う。

2　不正鍵検知アルゴリズム

不正鍵での復号化を検知することで、復号化装置を利用した暗号文に対する攻撃を防衛する。

復号化装置が不正鍵を検知すると、復号化装置の内部状態を不可逆的に変化させる。以後、全ての暗号文と鍵の組み合わせに対し、復号した平文にフィルター関数を作用させて、攻撃者に悟られずに擬似的な復号文を出力させる。

復号鍵を一度でも間違うと、以後、復号化装置はただの乱数発生装置になってしまう。

不正鍵検知アルゴリズムの概略

－暗号化－

①. 任意のハッシュ関数を用いて、平文のハッシュ値を求める。

②. ①のハッシュ値と平文の情報を混合させ、拡張平文を作成する。（ハッシュ値の情報を平文に混合させる方法は任意であるが、分離させる方法をもっているものに限る）

③. 拡張平文を暗号化する。

－復号化－

④. 復号化でえられた拡張平文から、平文とハッシュ値を分離させる。

⑤. 拡張平文から分離した平文のハッシュ値を、①と同じハッシュ関数を用いて求める。

⑥. ④と⑤のハッシュ値を比較する。

LSI 回路技術

前記の不正鍵検知アルゴリズムを取り入れた復号化装置をカスタムＬＳＩで実現する。

不正鍵を検知した情報を保持するために、不揮発性メモリである EPROM を利用する。

当該 EPROM は、正しい復号鍵を用いている間は消去状態にあるが、一度でも不正鍵を用いると書き込みが施される。以後、この情報は EPROM に紫外線照射を行わない限り消去不能になる。

復号結果の平文にフィルター関数を作用させるかどうかは、この EPROM が書き込み状態であるかどうかで決定する。

検知アルゴリズムの効果と欠点

効果：鍵の再試行が無意味となるので、１台の復号化装置では、鍵を１回しか試行できない。

鍵の総当たり攻撃以外に有効な解読方法がない暗号アルゴリズムに、不正鍵検知アルゴリズムを組み込んだ暗号アルゴリズムを用いて生成された暗号文は、確率的にしか解読できなくなる。

欠点：鍵を間違ったり、故意に別の鍵を用いて暗号化や復号化をおこなったりすると、復号者の復号化装置が以後正常な機能をしなくなり、復元不能になる。この問題のために、不特定多数者間で、この方式を用いて暗号通信をする場合は、認証局の介在が必須となる。（認証局用の復号装置には不正鍵使用情報を保持する EPROM は組み込まず、ハッシュ値の比較のみを行う機能だけをもたせ、平文の出力は行わないようにする。）

3　まとめ

ハードウエアのセキュリティに依存する形で原理的解読不能性にアプローチを試みた。ソフトウエアだけで実現するのが今後の課題である。

4　参考文献

土居範久，小山謙二：コンピュータセキュリティ，共立出版，1986