2F - 6 可変長鍵暗号システムの提案

富山県立大学大学院工学研究科 野村幸徳

1. はじめに

秘密鍵暗号方式では現在主にブロック暗号が用いられている．しかしブロック暗号は暗号化，復号化に比較的複雑なアルゴリズムを用いるため，今後超高速データ転送が行われるようになると計算時間が問題になると予期されている [1][2][3][4]．

これに対し，ストリーム暗号は暗号化，復号化の計算時間が少なく，高速処理が可能である [1][2][3][4]．ストリーム暗号の研究の中心は，暗号化鍵に用いる疑似乱数列の生成方式の改善である．本研究では，ストリーム暗号の鍵生成方法についての新しい方法を提案する．

2 暗号システム概要

可変長鍵暗号システムとは，平文，暗号文の長さから暗号化鍵，復号化鍵を生成するストリーム暗号システムである．すなわち，鍵のビット長は一定の長さではなく，平文，暗号文の長さに応じて可変となる．以後，可変長鍵暗号システムを $VLK(Variable\ Length\ Key)$ 暗号システムと略して説明する．

• 2.1 疎言語 ($SlenderLanguage$)

疎言語とは本研究において重要な概念である．特定の長さの記号列を 1 つまたはあらかじめ与えられた定数個以下しか作らない鍵生成メカニズムをいう．与えられた定数が k である場合は，そのような鍵生成メカニズムを k-疎言語と呼ぶ．そして与えられた定数が 1 の場合は 1-疎言語となる．

• 2.2 1-疎言語 VLK 暗号システム

1-疎言語を VLK 生成装置として用いる場合の暗号システム概要図は図 1 のようになる．平文及び暗号文の長さから暗号化及び復号化鍵を生成する．暗号化と復号化の手続きでは共通の 1-疎言語を持ち，かつ平文と暗号文の長さは等しいので暗号化と復号化で必然的に同一の鍵が生成される．平文の暗号化，復号化は平文 (暗号文) と鍵が 0 と 1 の 2 記号からなるので，排他的論理和の演算によって実行できる．

暗号化，復号化に用いた鍵は使い捨てであり，一度使用した長さの鍵は二度と使用しない．平文と同じ長さの鍵が 1-疎言語にない場合，1-疎言語の中で平文の長さ以上の鍵の中から未使用で最小の長さの鍵を選択する．

• 2.3 k-疎言語 VLK 暗号システム

2 以上の k に対して k-疎言語を VLK 生成装置として用いる場合の暗号システム概要図は図 2 のようになる．

k-疎言語暗号システムは，可能な k 個の記号列のうち 1 つを選ぶため，平文の特徴を小さな正の整数で表すハッシュ関数を用いる．送信者は k 個の記号列の中から任意に選んだ 1 つを鍵として 1-疎言語と同様の方法で暗号化し，暗号文とハッシュ関数値を受信者に送信する．受信者は暗号文の長さから生成される k 個の記号列すべてについて鍵として復号化し，得られた記号列からハッシュ関数値を求めて，送信されてきたハッシュ関数値と一致したものを平文として出力する．

ハッシュ関数は本来逆関数を求めるのが困難であるが，暗号システムとしての安全性を高めるため，ハッシュ関数値自体を別の暗号方式 ($OneTimePad$ 等) で暗号化する．ハッシュ関数自体の長さは極めて短い (数十ビット程度) ため，従来用いられてきた真性乱数列を鍵とするストリーム暗号 ($OneTimePad$) を用いても鍵配送の問題は生じない．

k-疎言語 VLK 暗号システムの特徴として 1-疎言語 VLK 暗号システムと異なるのは，1-疎言語の場合 1 つの平文に対して 1 つの暗号文が生成されるが，k-疎言語の場合は 1 つの平文に対して k 個の暗号文が生成されるという点である．この特徴により，k-疎言語暗号システムを用いることにより，安全性の向上が期待できる．

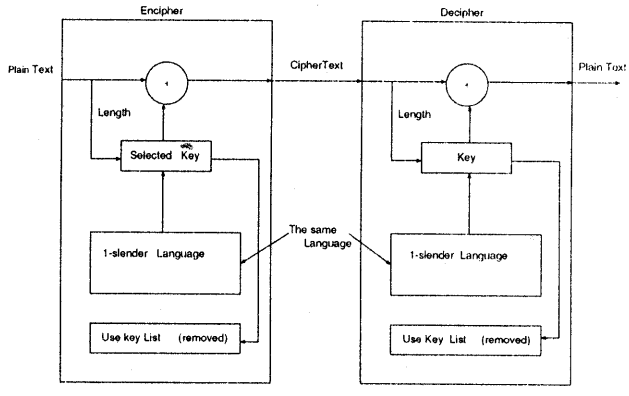

図 1: The simplest VLK cryptosystem

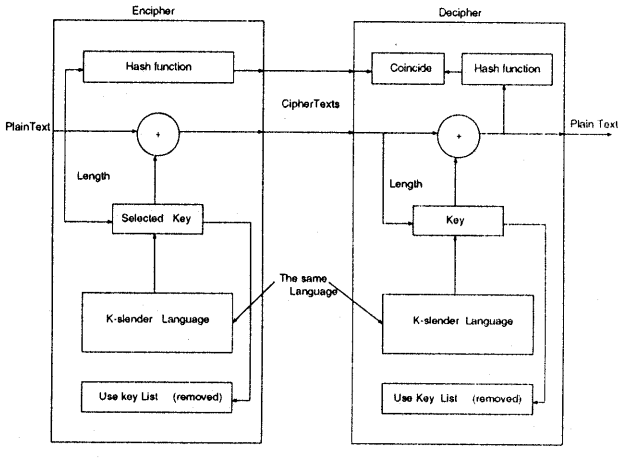

図 2: Type 2 VLK cryptosystem

A proposal of Variable Length Key Stream Cryptosystem
Yukinori Nomura
Department of Electronics & Infomatics, Faculty of Engineering
Toyama Prefectual University ,Kosugi-mati,939-0398 Toyama.Japan

3 鍵生成メカニズム

暗号化及び復号化鍵生成には大きく分けて二つの要素がある．一つはカオス [5] であり，もう一つは並列書き換えシステムである．鍵生成はまず記号書き換え規則の組を数種用意しておく．カオスを生じる離散力学系の時系列データにより，書き換え規則の組を選択して記号列を生成し，暗号化，復号化の鍵とする．具体的説明は以下に記す．

カオス

カオスとは，決定的であるが不規則で予測不可能に見える現象である．一次元の例では漸化式

$$X_{n+1} = f(X_n)$$

と，初期値 X_0 を与えれば，点列 X_n が計算できる．もし，点列 (X_n) が発散でもなく，収束でもなく，ある範囲内でランダムに振る舞う状態になれば，カオスが発生したことになる．上の漸化式を

$$f(x) = ax(1-x)$$

ただし

$$x_n = f(x_{n-1}) \quad 3.56 < a < 4.00$$

のように置き換えると，x の取り方に依存して，計算値がいかなる周期も持たない離散的な分布になる．[5]

本研究ではカオス式における計算値の小数点第 5 位の値を参照し，その値によってあらかじめ用意されている 10 種類の書き換え規則の中からどれを使用するか決定している．

例 1
パラメータ $x = 3.75$　初期値 $a = 0.50$
初期列 $ABCDEFGHIJA$
生成規則 10 種類

カオス式の計算結果の少数点第 5 位の値は，
$f(0) = 0, f(1) = 2, f(2) = 2, f(3) = 9, f(4) = 7 \cdots$
となる．
選択される生成規則は順に
$1 \rightarrow 3 \rightarrow 3 \rightarrow 10 \rightarrow 8 \cdots$ の規則となり生成される記号列は
初期列 $ABCDEFGHIJ$
$Step1$　$AaDEBCFGHIJ$
$Step2$　$EaABDCcFGHIJ$
$Step3$　$BaEDACCcFGHIJ$
$Step4$　$BaEDACCcHFIGJj$
$Step5$　$BeEDACCcHhGJIHj$
⋮
のようになる．
上記の例 1 では $Step1$ において規則 1 により初期列の記号が $A \rightarrow Aa, B \rightarrow D, C \rightarrow E, D \rightarrow B, E \rightarrow C$ と並列に書き換えられていく．この変換を平文と同じ長さになるまで繰り返し，各記号を 0 と 1 の 2 つの記号に変換して暗号化鍵の生成を行う．
この生成規則により生成される記号列の集合はカオス式の初期値とパラメータのどんな組み合わせに対しても，必ず 1-疎言語になる．

• 3.1 周期チェック

暗号化鍵の生成と同時に，その生成された記号列に周期があるかどうかも調べている．生成された記号列について，先頭から 5 文字を 1 つの組とし，5 文字間隔で記号列の最後まで参照する．周期がない場合は参照文字間隔を 1 文字ずつ増加させ，最終的には生成された記号列の半分まで参照を繰り返している．これによって周期が確認されなかった場合のみ，0，1 の記号に変換して暗号化鍵を生成している．

これは生成された記号列に周期がある場合，その記号列から解読される恐れが生じるため，それを未然に防ぐために行っている．

• 3.2 暗号強度

現在の鍵生成メカニズムは，

カオス式の初期値 x : 56 ビット
カオス式のパラメータ a : 56 ビット
変換規則 (記号 10，規則数 10) : 100 ビット

の計 212 ビットで記述されている．

これは 1 億 MIPS(10^{63}) のコンピュータで鍵をすべて探索するには 2.0×10^{42} 年必要である．また，この数値は探索された鍵の参照時間を除いたものである．

4 まとめ

本研究での疎言語という概念とカオス，並列書き換えを用いた VLK 暗号システムは，カオス式のパラメータ a と初期値 x_0，変換規則が解析できなければ，解読されるシステムではない．この 3 つの中で可変なのは変換規則であり，規則数と文字数を増やし，改良すれば現状より優れた暗号システムになると考えている．現在は文字数 40，規則数 20 に増やしたシステムを開発している．
今回の提案でストリーム暗号の疑似乱数生成方法について提案したが，将来の暗号技術の開発において，本研究が参考になりセキュリティ向上につながることを望む．

参考文献

[1] D.R.Stinson 著，櫻井幸一監訳，暗号論の基礎，1996，共立出版

[2] 加藤正隆著，基礎暗号学 1，1989，サイエンス社

[3] 加藤正隆著，基礎暗号学 2，1989，サイエンス社

[4] 松井甲子雄著，コンピュータによる暗号解読法入門，1990，森北出版

[5] 山口昌哉著，カオスとフラクタル 非線型の不思議，1986，講談社