VSC128S(Vector Stream Cipher:128bit S Version)　仕様書

平成16年9月17日

株式会社カオスウェア
梅野健 (chaosken@chaosware.com) [1]

[1]東京都小金井市貫井北町 4-2-1 独立行政法人情報通信研究機構内

1　はじめに

本資料は、平成 16 年 2 月 16 日に仕様公開された独立行政法人情報通信研究機構の多次元ランダムベクトル列発生方法[2]に基づくストリーム暗号方式である鍵長 128bit の Vector Stream Cipher(以下 VSC128 という。)[1] を、より安全性をより向上 (More Secure) する目的で VSC128 の基本変換の前のステップで行われる鍵配置プロセスに対して改良を加えた同じ鍵長 128bit のストリーム暗号 (以下 VSC128S という。Vector Stream Cipher-128bit More Secure Version　の略）の仕様を公開する。

2　VSC128S 公開仕様

本節では、種々の環境で実装され、フレキシブルかつ、暗号処理速度の高速性が示されている VSC(Vector Stream Cipher) ストリーム暗号アーキテクチャの鍵長 128bit 版である VSC128 を、より安全性を高めるため改良した VSC128S の仕様を記述する。VSC128S は、VSC128 と同様に、有限体上のパラメータ付き 2 次置換多項式の変形 Skew Product 変換[3]の巡回的接続[4]をコアとする非線形変換を 8 回繰り返すことによって、ストリームキーを生成する仕組みとなっており、VSC128S の具体的な仕様は下記の通りとなっている。

1. 32bit 長の変数 K_1, K_2, K_3, K_4 に秘密鍵 (32*4=128bit) を格納する。
2. 32bit 長の変数 IV_1, IV_2, IV_3 及び 16bit 長の変数 IV_4, に初期ベクトル (32x3+16=112bit) を格納する。
3. 32bit 長の変数 A,B,C,D に K_1, K_2, K_3, K_4 のそれぞれ上位 2bit を 00 にリセットした値を格納する。
4. 32bit 長の変数 X,Y,Z に IV_1, IV_2, IV_3 のそれぞれ上位 2bit を 00 にリセットした値を格納する。
5. 32bit 長の変数 W に、00, 並びに $K_1, K_2, K_3, K_4, IV_1, IV_2, IV_3$ のそれぞれ上位 2bit を順番に上位桁から並べたものを
　　上位 1bit-16bit とし、IV_4 を下位 16bit とした値を格納する。

[2]日本国特許第 3030341 号, 第 3455748 号, 米国特許 第 6,668,265 号

[3]エルゴード理論において多次元力学系を構成するのに良く用いられる方法である。

[4]この部分が、日本国特許第 3030341 号, 第 3455748 号, 米国特許 第 6,668,265 号のランダムベクトル列発生技術に相当する。

6. 以下の変数変換を行う
   $a = A - (A \bmod 4) + 1$
   $b = B - (B \bmod 4) + 1$
   $c = C - (C \bmod 4) + 1$
   $d = D - (D \bmod 4) + 1$
   $x = X - (X \bmod 4) + 1$
   $y = Y - (Y \bmod 4) + 1$
   $z = Z - (Z \bmod 4) + 1$
   $w = W - (W \bmod 4) + 1$
   $A' = A(2A + y) \bmod 2^{32}$
   $Z' = Z(2Z + a) \bmod 2^{32}$
   $C' = C(2C + z) \bmod 2^{32}$
   $X' = X(2X + c) \bmod 2^{32}$
   $B' = B(2B + x) \bmod 2^{32}$
   $W' = W(2W + b) \bmod 2^{32}$
   $D' = D(2D + w) \bmod 2^{32}$
   $Y' = Y(2Y + d) \bmod 2^{32}$

7. 256bit のビット列 (A',B',C',D',X',Y',Z',W') を左に 5bit 回転させたものを、32bit の８つの変数 (A,B,C,D,X,Y,Z,W) へ代入する。
8. (6),(7) を 8 回繰り返す。
9. 得られた A,B,C,D,X,Y,Z,W のうち、X,Y,Z,W を 128bit 長のストリームキーとし、平文を D1,D2,D3,D4(それぞれ 32bit 長)、暗号文を E1,E2,E3,E4 とすると
   $E1 = D1 \oplus X$
   $E2 = D2 \oplus Y$
   $E3 = D3 \oplus Z$
   $E4 = D4 \oplus W$
   となる。
10. (6),(7),(8) の処理を進め、新たに得たストリームキーで、次につづく平文データの暗号化を行う。

図１は、その VSC128S の本公開仕様アルゴリズムの概要を模式的に示したものである。

3　VSC128S のランダム性評価及び安全性評価

VSC128S のランダム性評価については、誤りを修正された NIST SP800-22 テストによる評価 [2] を行うと、本 VSC128S の基本変換部分のアルゴ

リズムの構造が VSC128 と同じであるため、VSC128 について示された最上位のランダム性 [1] が VSC128S についても保証される。更に、文献 [3] で扱われた様な VSC128 暗号の鍵差分評価、ブロック単位のスライディング攻撃に対しても同様な耐性を持つことが保証される。また、VSC 暗号アーキテクチャで用いられている非線形変換

$$Y = 2 * X^2 + p * X \qquad \mathrm{mod} \quad 2^{32} \tag{1}$$

において、32bit の変数 X の上位 2bit が、$2X^2$ 演算のところで X の下位 16bit との掛け算が 0 となることからくる非鋭敏性をあらかじめ取り除いているため、ラウンド数が 8 回で秘密鍵、初期ベクトルに対する十分な攪拌が行われる。よって、VSC128S は、VSC128 と比較して、鍵配置プロレスの中の上記の秘密鍵及び初期ベクトルの各ブロックの上位ビットの非鋭敏性[5]をあらかじめ取り除くことでより鍵、初期ベクターに対するビット依存性を向上させ、VSC128 と比較して同等もしくはそれ以上の安全性を持つことが、VSC128 の持っている実装速度の高さを失わずに持つことが期待される。これらの VSC128S のより詳細なランダム性評価、安全性評価、及び実装評価については、別の機会に報告する。

4 まとめ

本資料では、128 ビット長ストリーム暗号 VSC128S の仕様を記述した。

参考文献

[1] 梅野健、金成主、長谷川晃朗, "VSC128 仕様書", http://www.chaosware.com/vsc128.pdf

[2] 金成主　梅野健　長谷川晃朗,"NIST のランダム評価テストについて",ISEC2003-87(2003-12),PP.21-27
http://xxx.lanl.gov/PS_cache/nlin/pdf/0401/0401040.pdf

[3] 田中秀和、根本和徳、三木武、佐藤光浩、谷口晴美,"128bitVSC 暗号の安全性評価", Technical Report of IEICE, ISEC(2004-3)
http://www.tech.softbank.co.jp/release/2004/pdf/vsc040406.pdf

[5] 但し、VSC128 の仕様においてもラウンド数 8 回としているので、これらの非鋭敏性が見えないことを確認している。