Digital Chaos and Cryptography

Vector Stream Cipher and Digital Chaotic Public Key Systems

Ken Umeno

National Institute of Informations and Communications Technology, Japan

March 28, 2005

Hasamuddin University, Indonesia

Outline

- Introduction
- Digital Chaos
- Vector Stream Cipher [New Digital Chaotic Cipher]
- New Digital Chaotic Public Key Encryption
- Summary

Key Concepts

- Digital Chaos
- Transform serial video stream into parallel streams
- Developed scalable encryption processors
- FPGA(Xilinx) with 30 execution units
- With adequate data feeds reaches 14.85GBPS(all frames encrypted)
- 64 execution unit chip attains 25GBPS

Markets

- Video security and copyright protection
- Mobile market – Low power, cost, overhead such as wireless lan and cellular phone
- Set-top market
- Corporate
- PC
- New

Comparison with BCM5840

(BCM5842:the world's first single–chip security processor)

Ours (Chaos)	BCM5842 (BROADCOM)
No Limit, Full Scalable. Ex. Scalable up to 40 Gbps in case of VertexII FPGA(xcv1000) Demo on 25Gbps encryption done in June, 2002.	Scalable up to 4.8 Gbps
Vector Stream(Chaos)	AES

14.85 Gbps Real-Time Encryption of HDTV (Demo)

(The first demonstration of realtime encryption of HDTV in the world. Date: April 2003)

Decrypted HDTV(Left) versus Encrypted HDTV(Right)

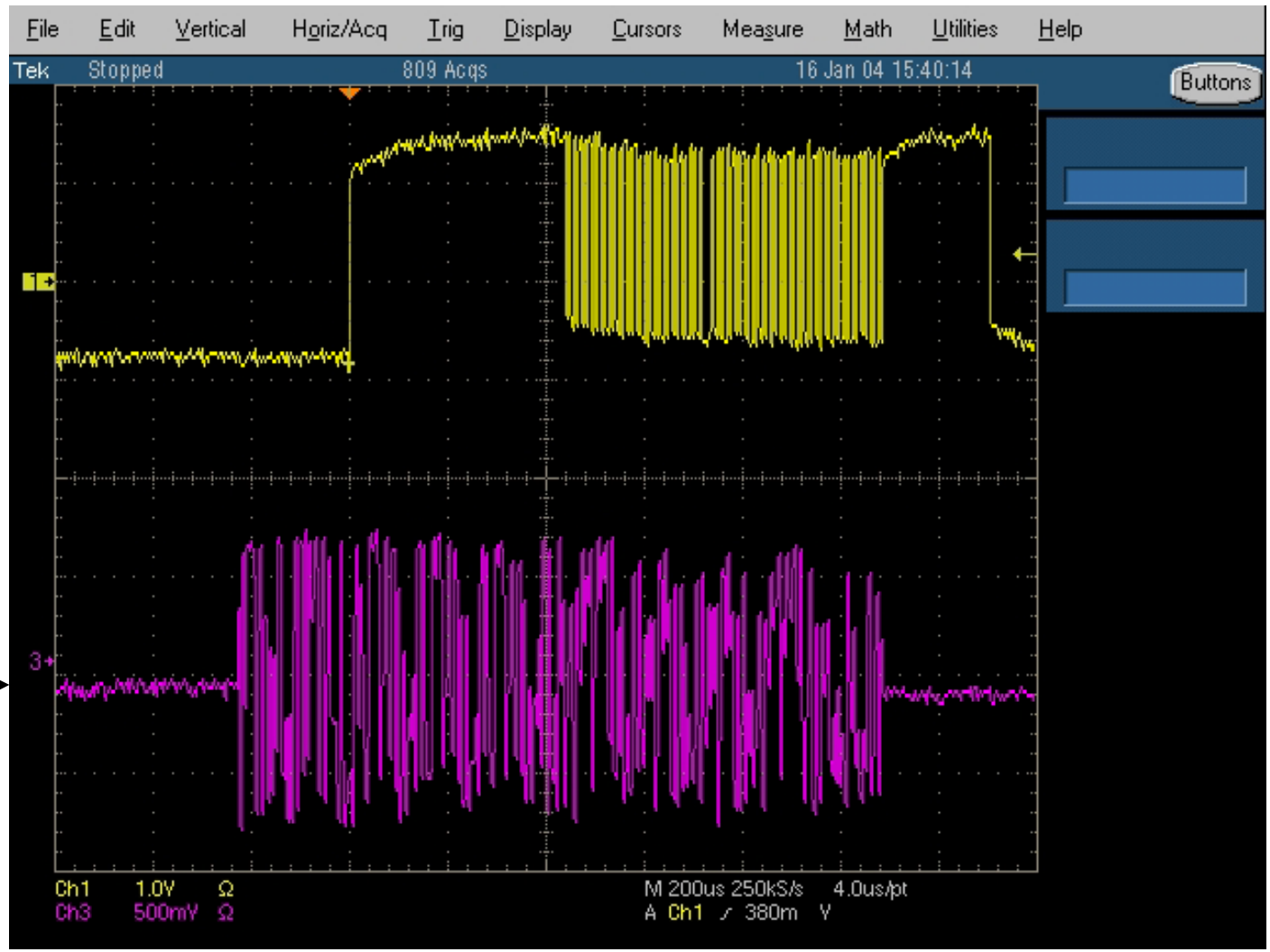
Digital Chaos in a Real World

January, 2004

Digital Chaos Observed in Mobile ChaosCDMA terminal.

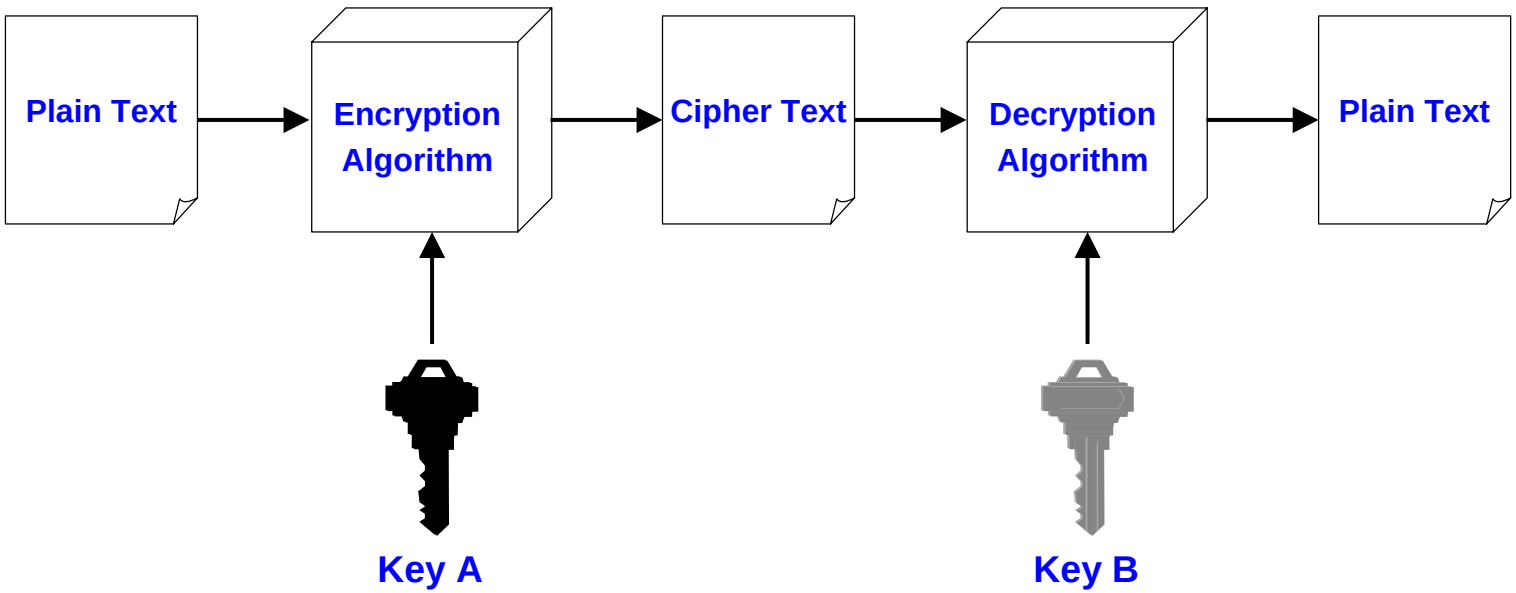
Decoded Signal →

Observed Digital Chaos
（Base band） →



Encryption - Cipher

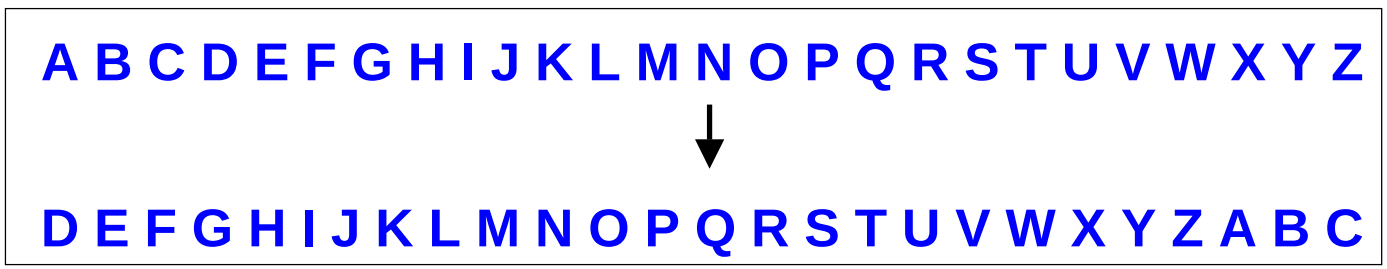
- Cipher is a method for encrypting messaged



- The key which is an input to the algorithm is secret
  - Key is a string of numbers or characters
  - If same key is used for encryption & decryption the algorithm is called symmetric
  - If different keys are used for encryption & decryption the algorithm is called asymmetric

Simple Dynamics – Caesar Cipher

- Caesar Cipher is a method in which each letter in the alphabet is rotated by three letters as shown



- Let us try to encrypt the message
  - Attack at Dawn

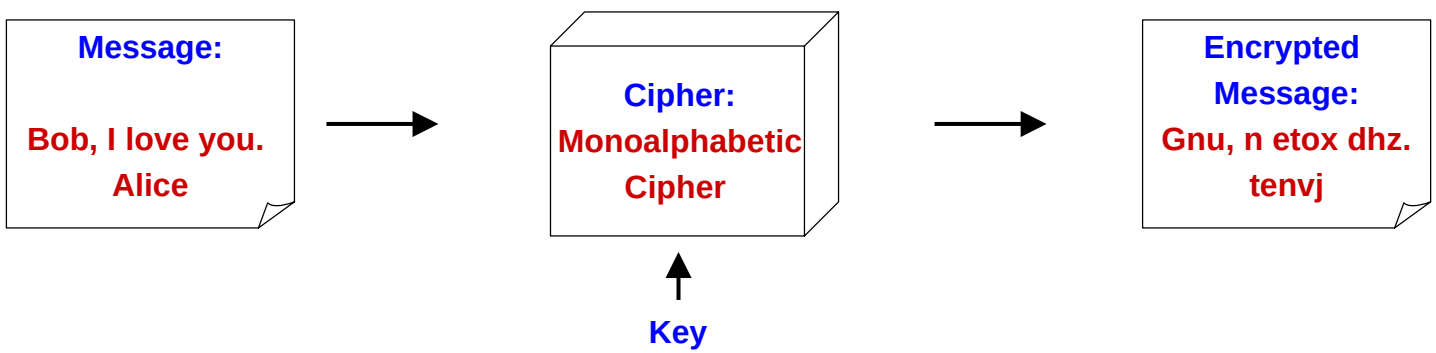
Assignment: Each student will exchange a secret message with his/her closest neighbor about some other person in the class and the neighbor will decipher it.

More Complex Dynamics - Polyalphabetic Cipher

- Developed by Blaise de Vigenere
  - Also called Vigenere cipher
- Uses a sequence of monoalpabetic ciphers in tandem
  - e.g. C_1, C_2, C_2, C_1, C_2

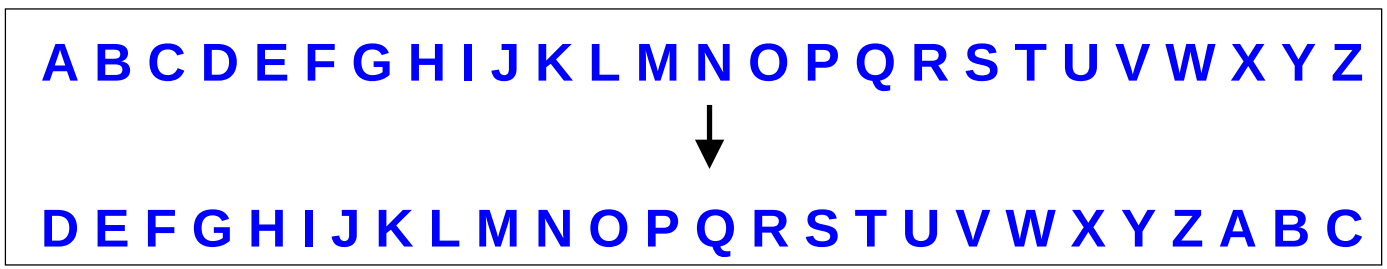
Plain Text	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
	↓
C1(k=6)	F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
C2(k=20)	T U V W X Y Z A B C D E F G H I J K L M N O P Q R S

- Example



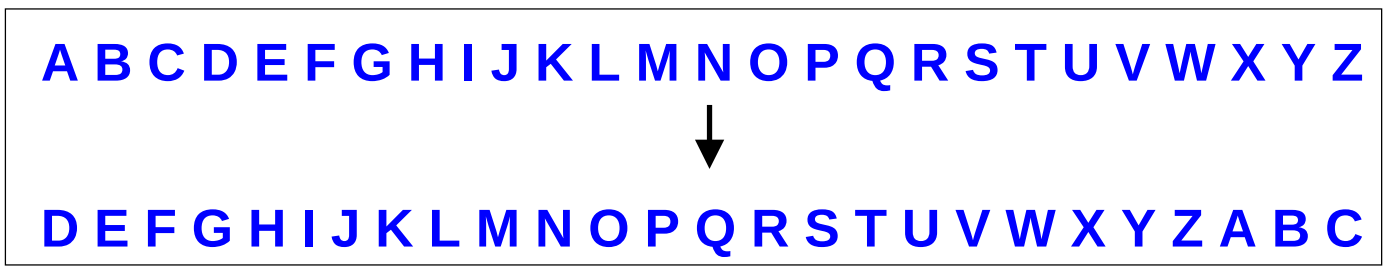
Requirments for Dynamics of Cipher

- Dynamics is reversible.
- Dynamical State => Information Bit
- Uniform Randomization in reversible dynamics.
- "Some Computationally irreversible"
  in reversible dynamics.



Dynamics (Encryption Process) of Cipher

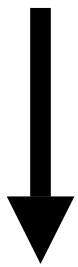
- Dynamics is reversible.
- Dynamical State => Information Bit
- Uniform Randomization in reversible dynamics.
- "Computationally irreversible" in reversible dynamics.



What is Digital Chaos?

A new chaotic dynamics

which is suitable to digital signal processing



Is there unique digital chaos whose analogue counterpart (analogue chaos) does not exist?

Dynamical System over R

$X_{n+1}=F(X_n)$ $X_n \in R$

=>

Dynamical System over Finite Field

$Y_{n+1}=F(Y_n)$ $Y_n \in Z_p$

$Z_p=[0,1,\ldots..,p-1]$

Permutation Polynomial module 2^n

Examples: Prime Primitive in RC6 Cipher

$$Y = X*(2X+1) \mod 2^{32}$$

which is very similar to the chaotic map Y=2X*X-1.

Is there a rigorous relation between a class of permutation Polynomials and Chebyshev Polynomials?

=>Yes!

Example: Y=X*(2X+1) mod 8

0 1 2 3 4 5 6 7

↓ X^2 mod 8

0 1 4 1 0 1 4 1

↓ 2X^2 mod 8

0 2 0 2 0 2 0 2

\+ mod 8

0 1 2 3 4 5 6 7 ← X

0 3 2 5 4 7 6 1 (Permutation!)

Some Computational Irreversibility of $f(x)=x(2x+1) \mod 2^n$

n=32

$$f^{-1}(x)= x+4294967294x^2+8x^3+4294967256x^4+224x^5+4294965952x^6+8448x^7+4294912384x^8+$$
$$366080x^9+4292477952x^{10}+17199104x^{11}+4174573568x^{12}+85201152x^{13}+250497792x^{14}+$$
$$868352000x^{15}+146898944x^{16}+221288576x^{17}+238367392x^{18}+323275808x^{19}+$$
$$270637456x^{20}+198396792x^{21}+239075280x^{22}+234881024x^{23}+385875968x^{24}+208074784x^{25}+$$
$$281857280x^{26}+161061736x^{27}+375809384x^{28}+2147483648x^{29}+2147483648x^{32} \mod 2^{32}$$

Some Computational Irreversibility of $f(x)=x(2x+1) \mod 2^n$

n=64

$$f^{-1}(x)= x+18446744073709551614x^2+8x^3+18446744073709551576x^4+224x^5+18446744073709550272x^6+8448x^7+18446744073709496704x^8+366080x^9+18446744073707062272x^{10}+17199104x^{11}+18446744073589157888x^{12}+852017152x^{13}+18446744067623714816x^{14}+43818024960x^{15}+18446743756028870656x^{16}+2317200261120x^{17}+18446727080907636736x^{18}+125210119372800x^{19}+18445817518826192896x^{20}+6882979133521920x^{21}+18395434592896024576x^{22}+33705682655066560x^{23}+155689514541682524416x^{24}+319425642524101836800x^{25}+288084674822012928000x^{26}+151270994920034867200x^{27}+41727757865739878400x^{28}+6979422766256195200x^{29}+1683173158609643110400x^{30}+81295399535719219200x^{31}+9493391139638607872000x^{32}+1291989410325200896000x^{33}+31413120907199119360000x^{34}+6515414741776455680000x^{35}+538871920833372160000x^{36}+74968828691509809440000x^{37}+1715023129831748403200x^{38}+99731751953239680000x^{39}+1544027136455662720000x^{40}+18222711982480424960000x^{41}+172824756910405632000000x^{42}+11537975954718888928000000x^{43}+148154705835374673920000000x^{44}+4715972497288859520000000x^{45}+132284794804706000320000000x^{46}+901508355403889036800000000x^{47}+3920102000649306112000000000x^{48}+2728055474279677952000000000x^{49}+1055868932637012787200000000x^{50}+373798769071751168000000000x^{51}+163668104586433246400000000x^{52}+11997589407315001344000000000x^{53}+1736588016314632576000000000x^{54}+100886316530991104000000000x^{55}+44675708305153203200000000000x^{56}+4035225261239644160000000000x^{57}+149879755988901068800000000000x^{58}+13335058055282163712000000000000x^{59}+13335058055282163712000000000000x^{60}+9223372036854775808000000000000x^{64} \mod 2^{64}$$

Why Permutation Polynomial is Important?

Main Reason 1.

A permutation polynomial preserves a uniform invariant measure.

Main Theorem(K.U., 2003):

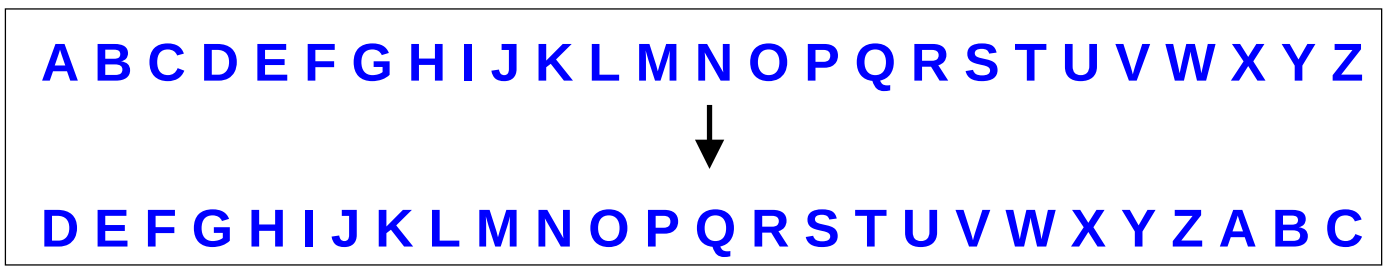
A Chebyshev polynomial of degree p is a permutation polynomial module 2^n

if and only if p is an odd natural number.

5次.txt 3次.txt

Dynamics of Cipher

- Dynamics is reversible.
- Dynamical State => Information Bit
- Uniform Randomization in reversible dynamics.
- "Computationally irreversible" in reversible dynamics.



The fastest stream cipher in the world at 25 Gbps

VECTOR STREAM CIPHER

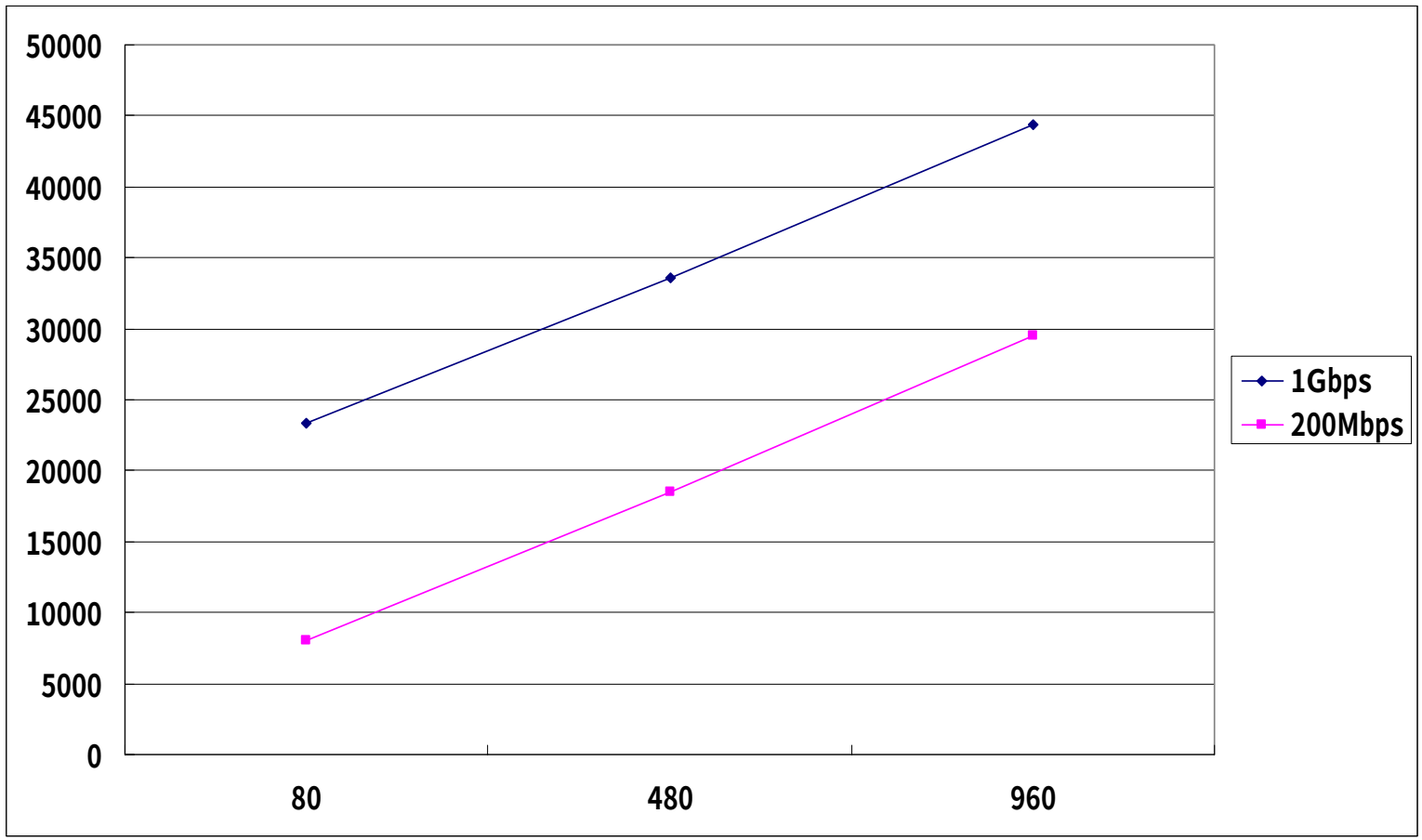
Digital Chaos Dynamics in Cipher

Features of Vector Stream Cipher

- Full Scalable Cipher Chip Architecture
- The fastest encryption speed record (25 Gbps) in the world
- Reconfigurable Chip Implementation
- FIPS140-2, NIST800-22 Randomness Test Passed
- Patented Technology (JP3030341, US Patent Approved)
- 1.4 Gbps LVDS Interface for 1 Gbps Encryption Demo
- Very Low Power LSI Chip Implmentation
  (70MHz for 14.85 Gbps Encryption)

Scalability Features in Encryption

Gate Size



Key Length [bit]

Table : VSC Implementation Result Based on Heron-FPGA Evaluation Board

Type of Algorithm	Encryption Speed	Key Size	Clocks	Gate Size	Implementation Efficiency [Kbps/Gate]
VSC 1024	21.06 Gbps	1024bit	20.57M Hz	156,479	134.6
VSC 512	25.62 Gbps	512bit	50.05M Hz	141,112	181.6
VSC 256	12.88 Gbps	256bit	50.33M Hz	70,703	182.2
VSC 128	7.033 Gbps	128bit	57.05M Hz	36,323	193.5

Permutation Polynomial module 2^n

Examples: Prime Primitive in RC6 Cipher

$$Y = X*(2X+1) \mod 2^{32}$$

which is very similar to the chaotic map Y=2X*X-1.

Example: Y=X*(2X+1) mod 8

0 1 2 3 4 5 6 7

↓ X^2 mod 8

0 1 4 1 0 1 4 1

↓ 2X^2 mod 8

0 2 0 2 0 2 0 2

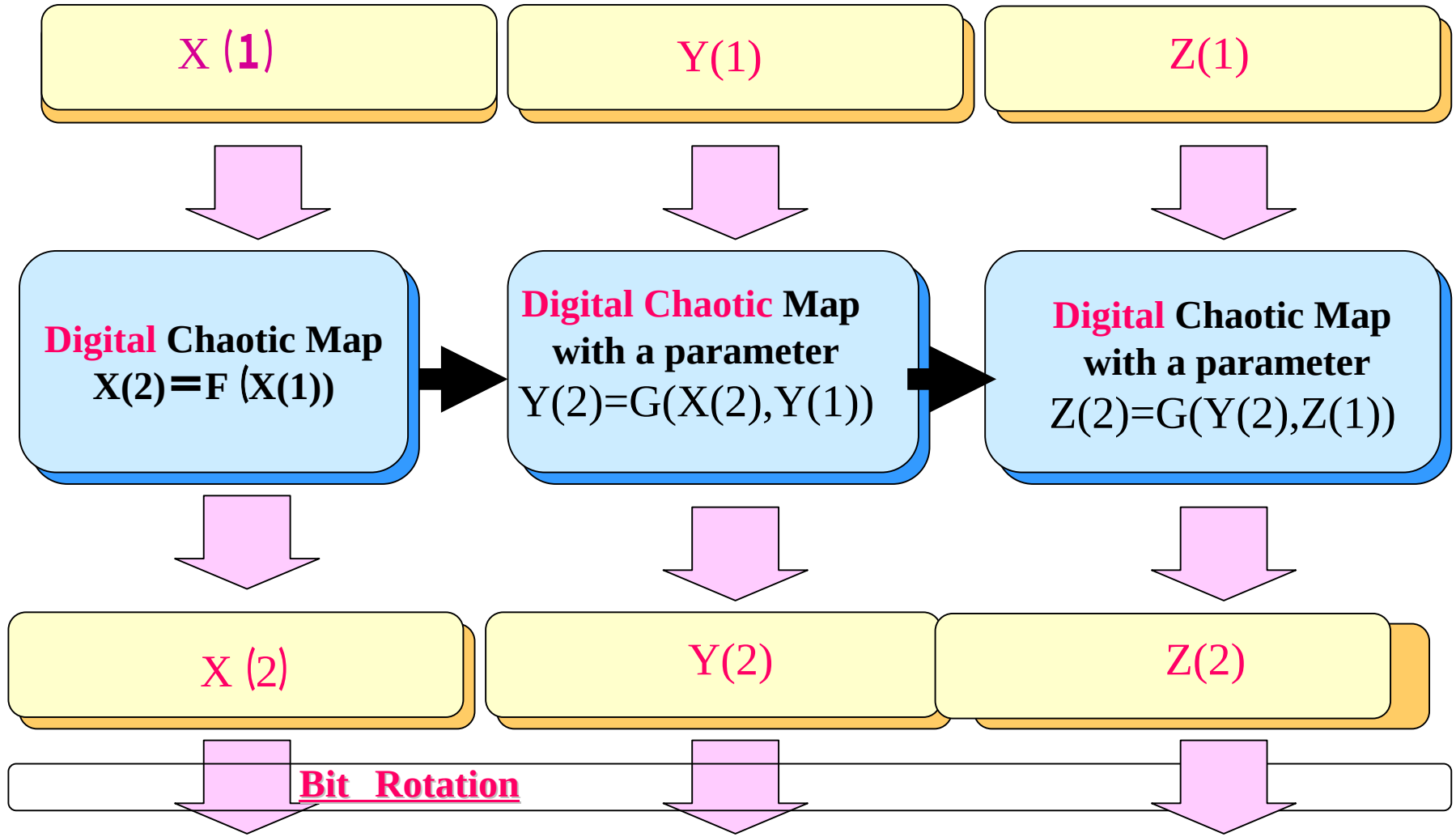
\+ mod 8

0 1 2 3 4 5 6 7 ← X

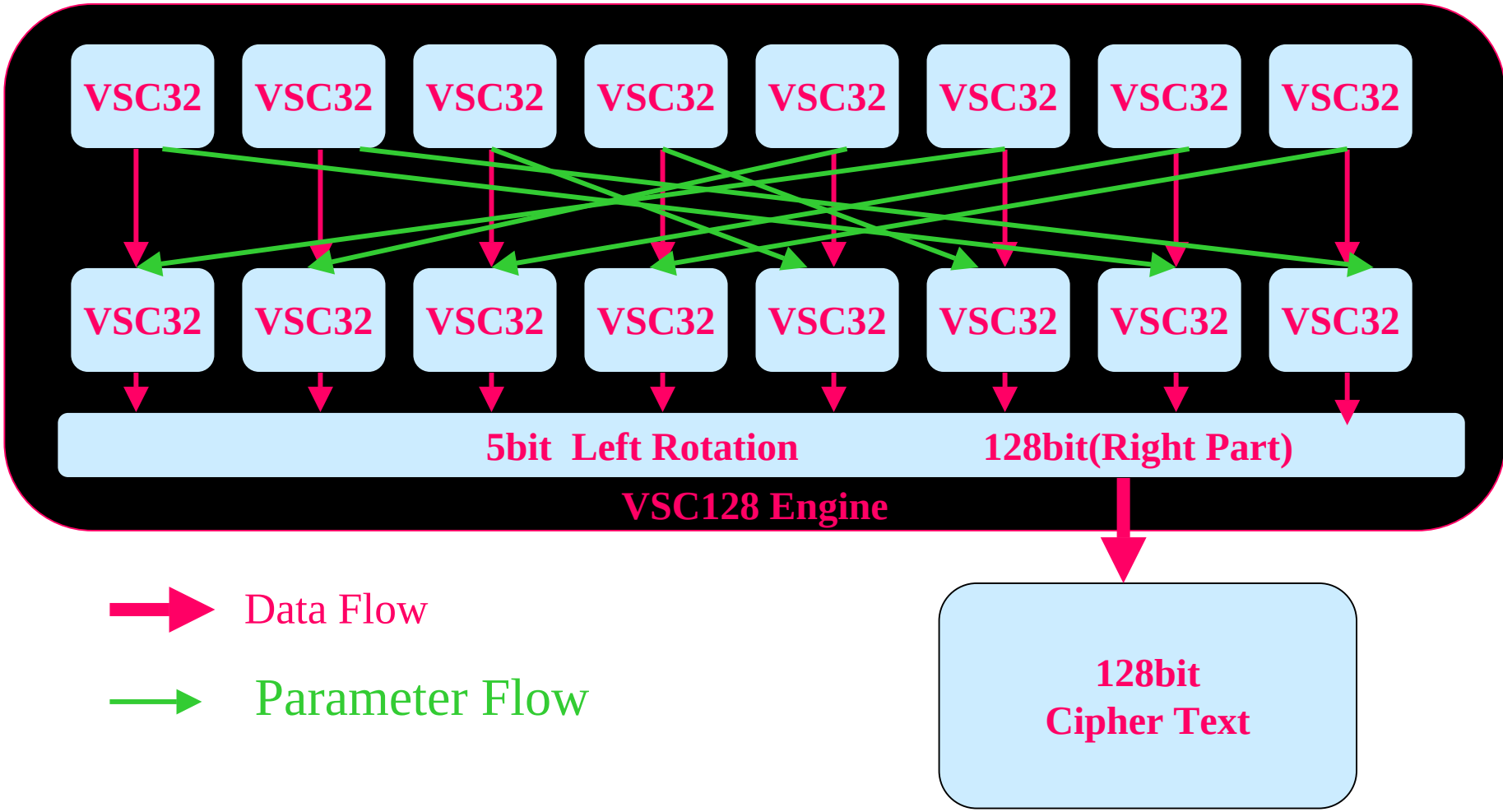
0 3 2 5 4 7 6 1 (Permutation!)

Basic Concept of our chaotic cipher(Ex. 3D Case) using permutation map: $G(x,y)=y(2y+x) \mod 2^n$

vector3d_16.exe



VSC128 Nonlinear Function



Realtime HDTV Encryption:

20bit × 74.25MHz × 10 (Parallel Series)　= 14.85Giga bit/s.

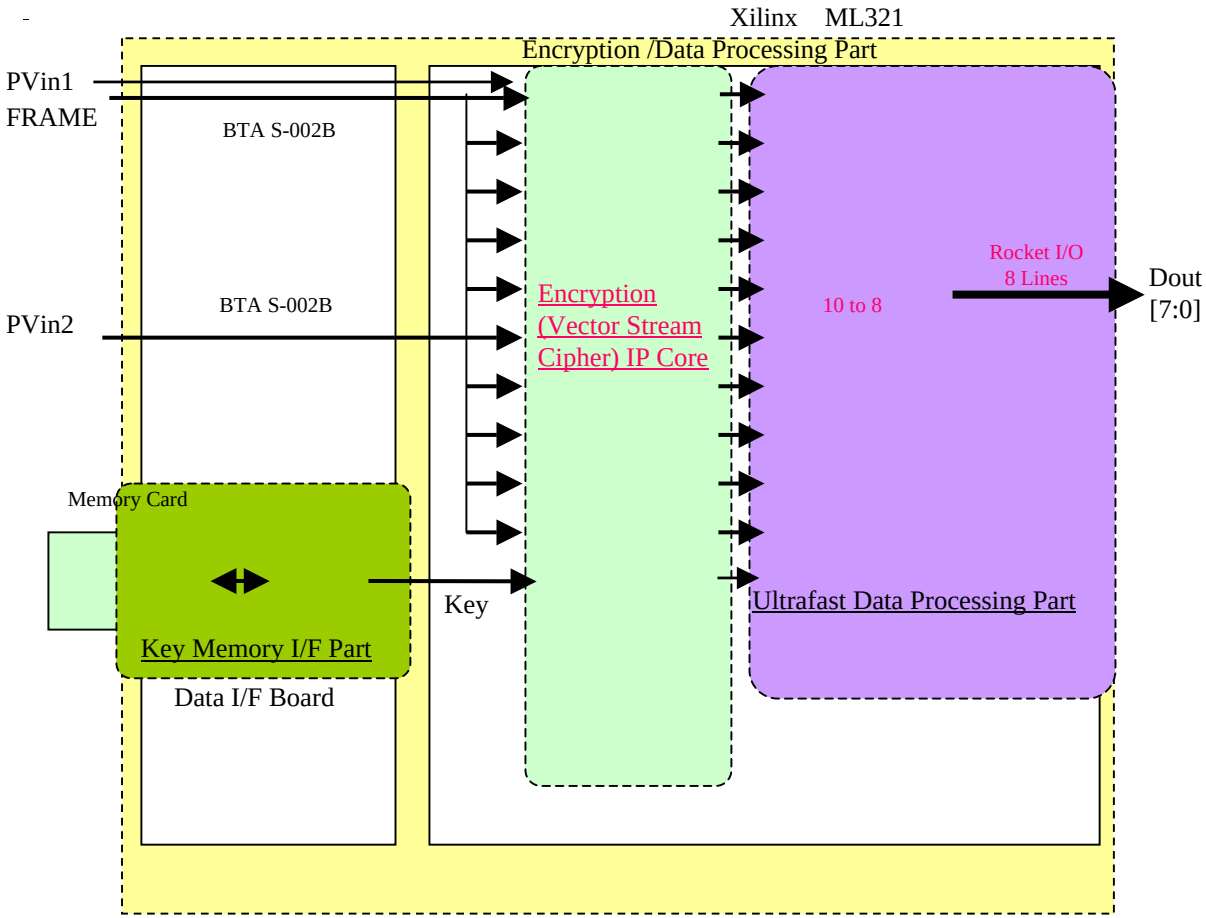


Figure : Schematic Diagram for Encryption/Data Processing Function of HDTV Encryption System.

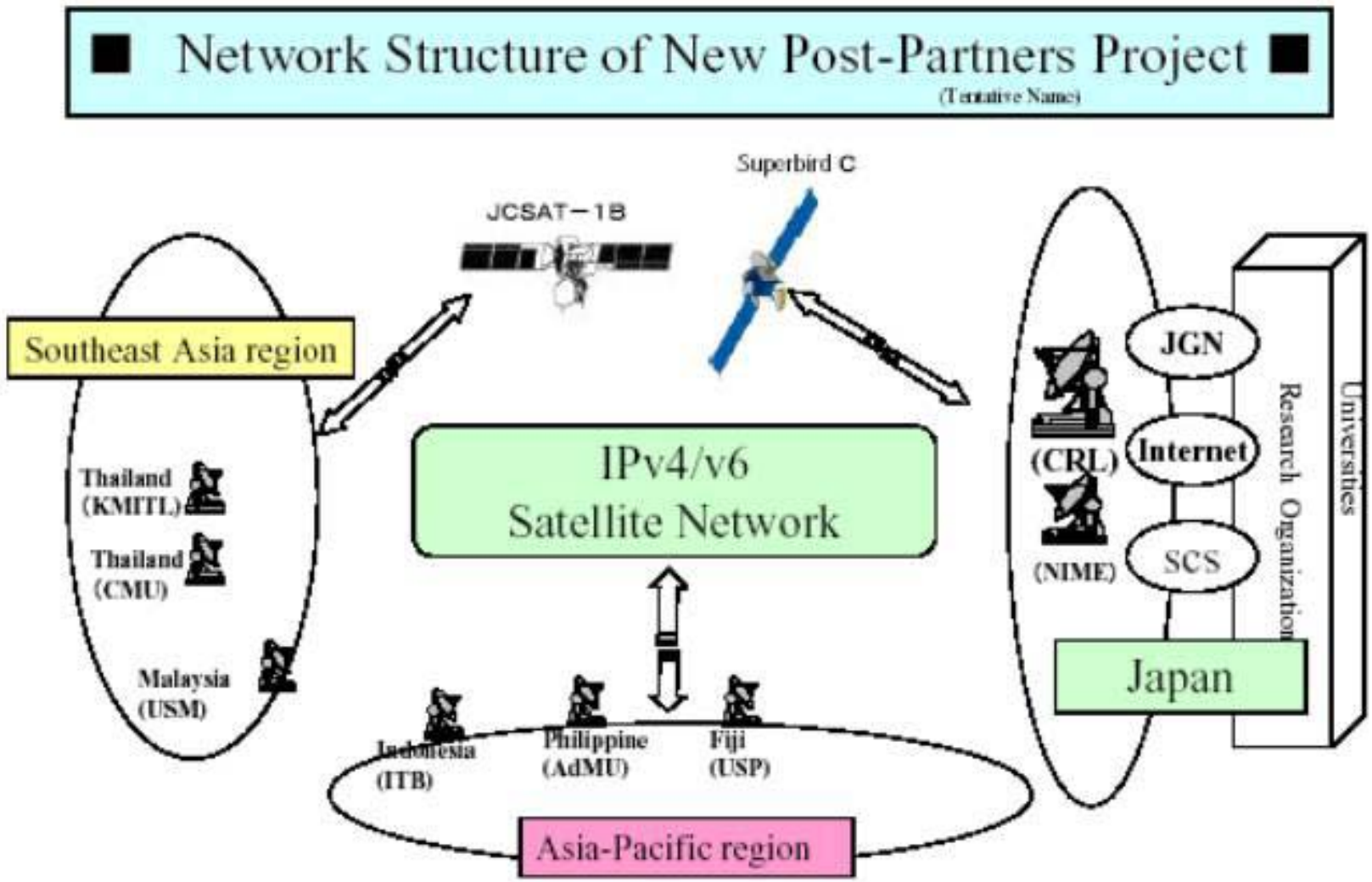
14.85 Gbps Real-Time Encryption of HDTV (Demo)

(The first demonstration of realtime encryptionn of HDTV)

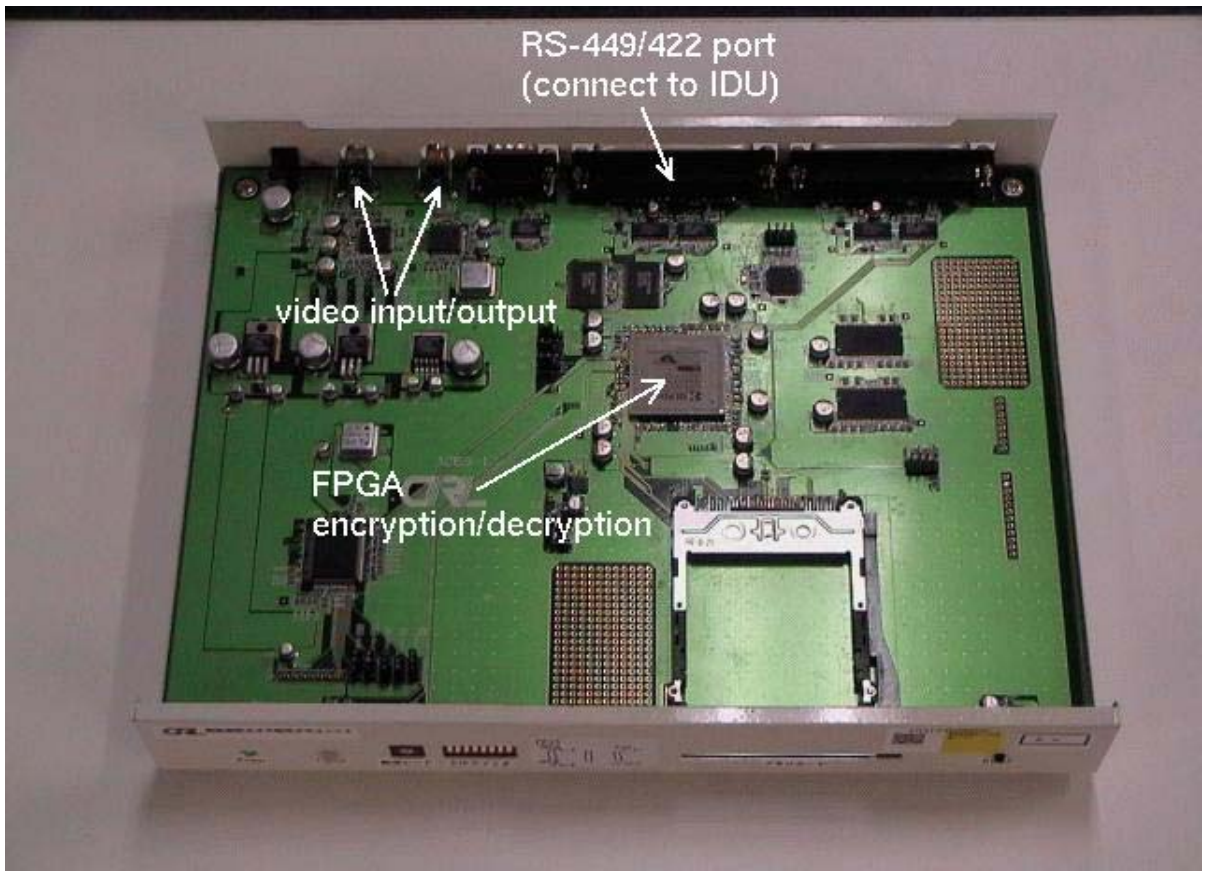
Decrypted HDTV (Left) versus Encrypted HDTV(Right)

New Post-Partners Project

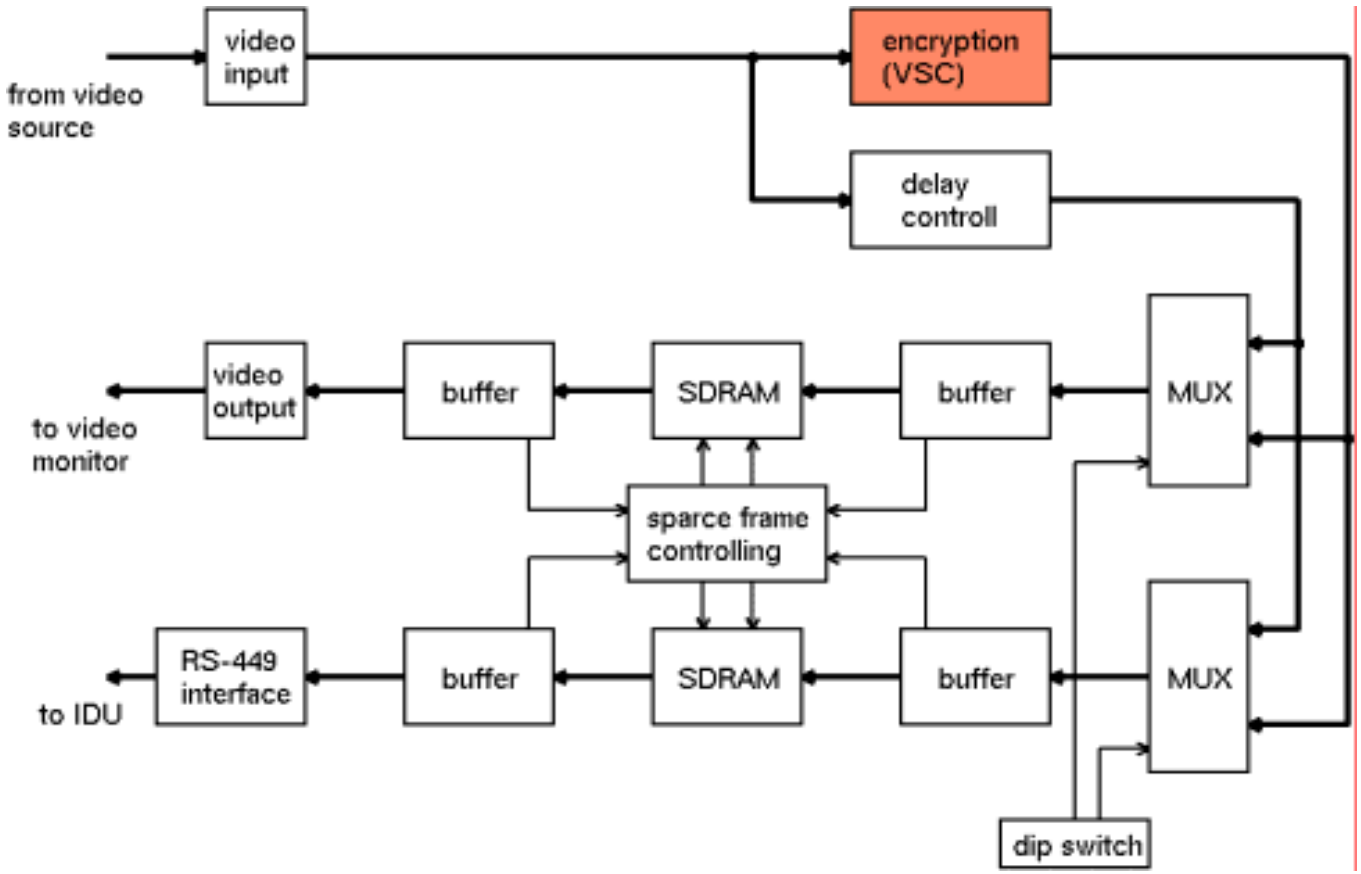
http://www.newpp.net/purpose.html



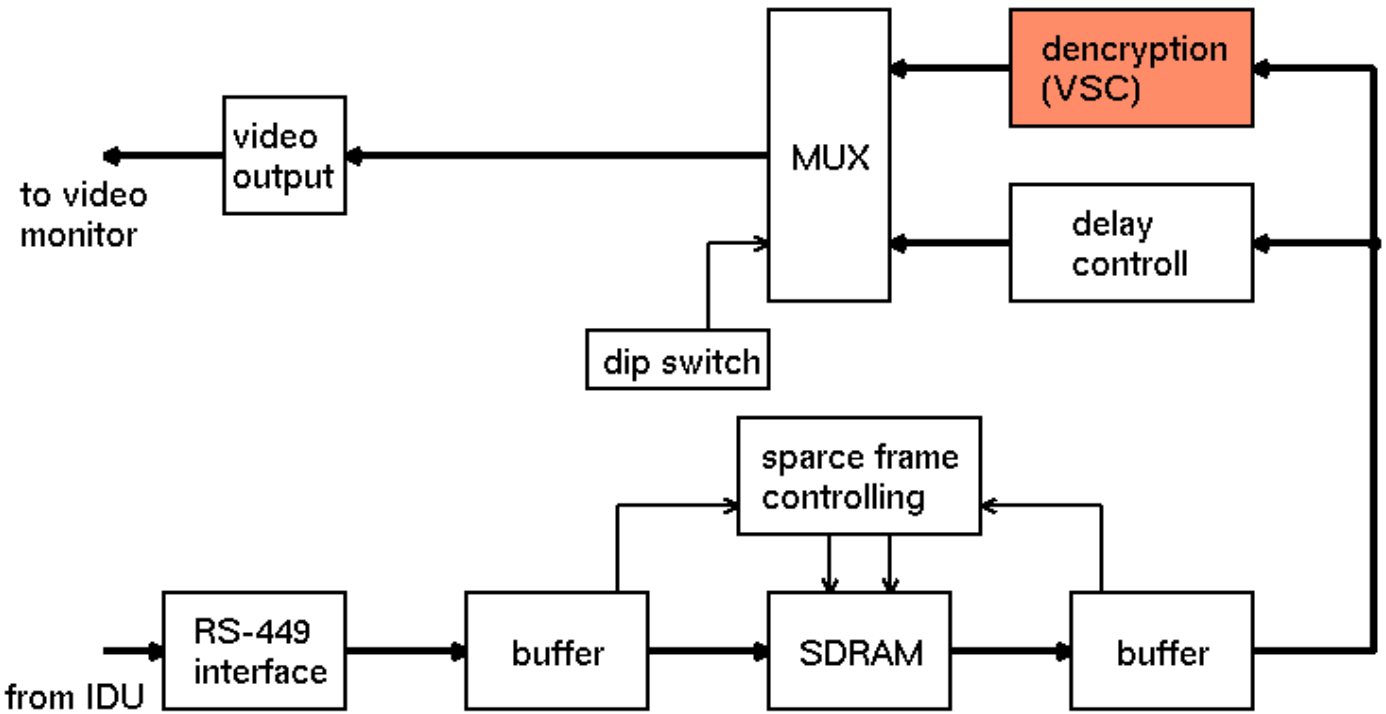
Encryption/Decryption Unit for New PP Satellite Networks (A4 Size)



Block diagram of encryption module (TX)

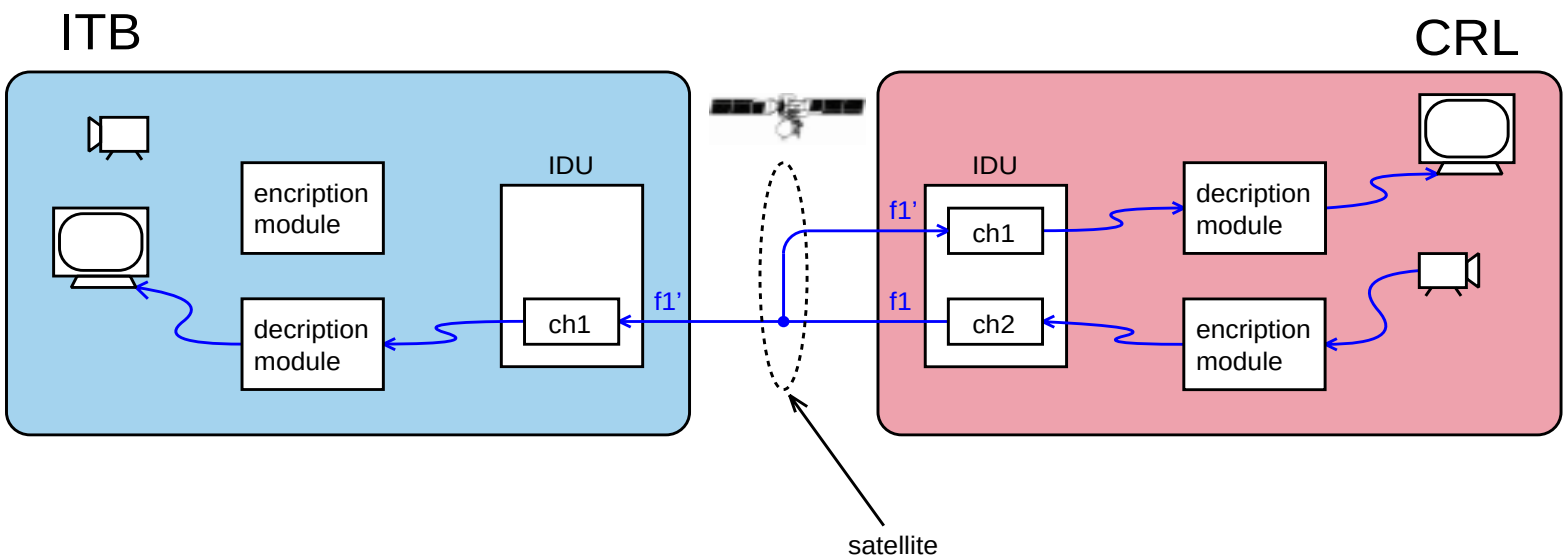


Block diagram of decryption module (RX)



CRL(Japan) -> ITB(Indonesia) and CRL(Japan)

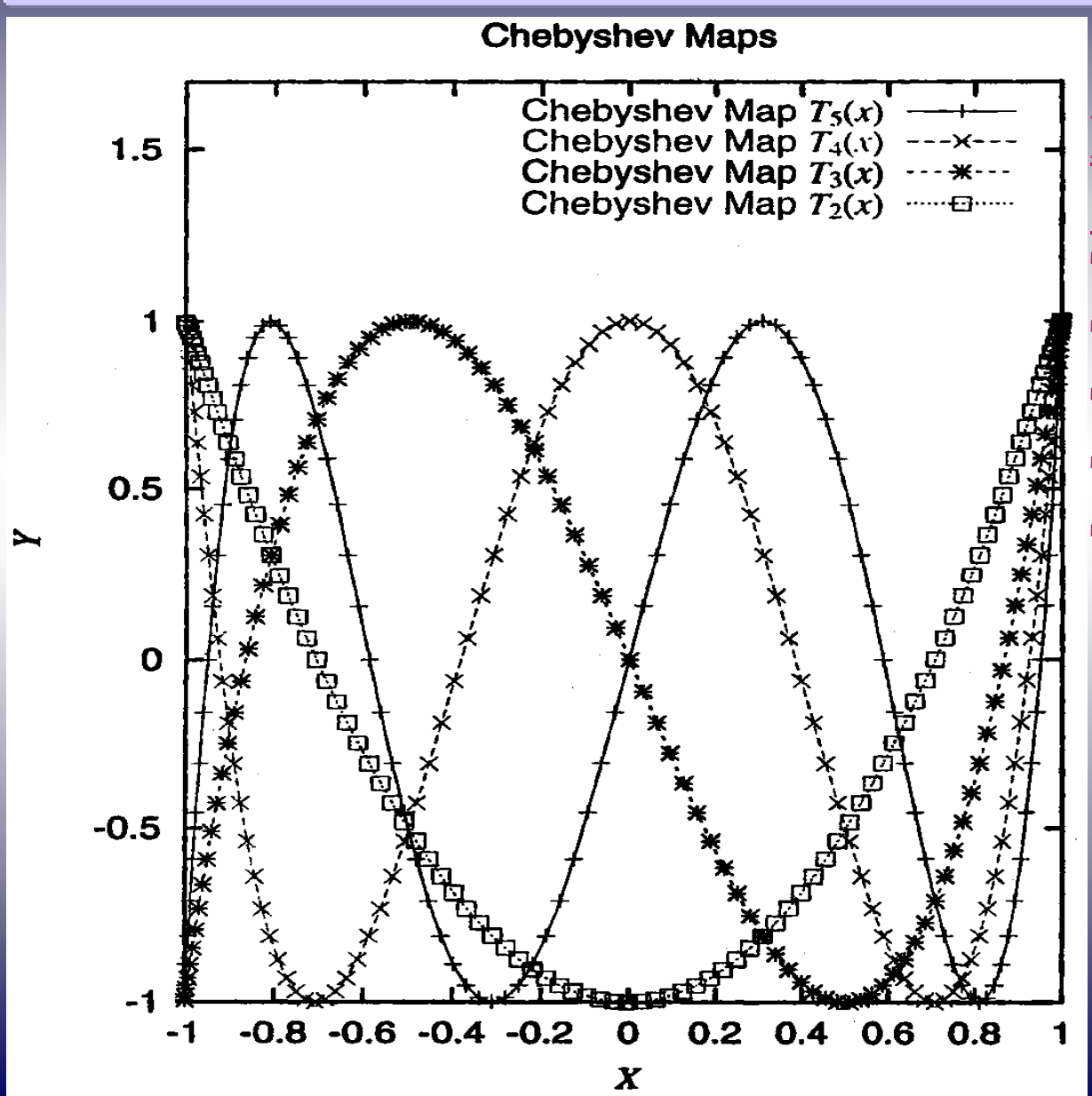
(Encryption of Multicast)



ITB(Indonesia) Recived a decrypted image at CRL(Japan) transmitted by NPPP Satellite Link on Oct.27,2003)

ITB (Indonesia) Recieved an Image partially encrypted transmitted by CRL(Japan) on Oct. 27

Backgrounds: *Chebyshev Polynomials*



Multiplication Formula:

$T(a,\cos\theta)=\cos(a\theta)$

$T(0,x) = 1$

$T(1,x) = x$

$T(2,x) = 2x^2-1$

$T(3,x) = 4x^3-3x$

Chebyshev Polynomials for Communications

(1) Orthogonality:(clear from addition theorems)

(2) Mixing Properties:(Adler and Rivin,1964)

(3) Explicit Ergodic Invariant Measures:

(Ulam-von Neuman,1947;Adler-Rivin,1964)

(4) Commucativity:(clear from definition)

(1) ,(4)→Lebesgue Spectrum bases:

(K.U, 2001)

(2) , (3)→Monte Carlo Computing:(K.U,2000)

(3) ,(2),(1)→Spreading Sequences for CDMA:

(K.U and K. Kitayama, 1999)

***(4)→Public Key Distribution Systems* (K.U, 2001)**

Chebyshev Maps over a Finite Field:

Remark: Commutativity is preserved for Quantized Chebyshev maps

Commutativity

$$T_l \circ T_m(x) = T_m \circ T_l(x) = T_{ml}(x), \tag{1}$$

Examples of Chebyshev polynomials over a finite field GF(7)

$$\begin{aligned} S_3(X) &\equiv T_3(X) \bmod 7 = 4x^3 + 4x, \\ S_4(X) &\equiv \quad T_4(x) \bmod 7 = x^4 + 6x^2 + 1, \cdots. \\ S_p(X) &\equiv T_p(X) \bmod 7 \end{aligned} \tag{2}$$

$$S_l \circ S_m(x) \equiv S_m \circ S_l(x) \equiv S_{ml}(x) \tag{3}$$

where $x \in \mathrm{GF}(n)$.

Example:

T3 3次.txt

T5 5次.txt

Main Theorem(K.U., 2003):

A Chebyshev polynomial of degree p is a permutation polynomial module 2^n

if and only if p is an odd natural number. Asia.ps

Public-Key Distribution System

Table 1:Public-Key Distribution Systems

	Alice	**Bob**
Public Key	X	X
Private Key	p	q
Chaotic Maps over a Finite Field	$T_p(x) \bmod n$	$T_q(x) \bmod n$

Commutativity

$$T_l \circ T_m(x) = T_m \circ T_l(x) = T_{ml}(x), \tag{1}$$

Examples of Chebyshev polynomials over a finite field GF(7)

$$\begin{aligned} S_3(X) &\equiv T_3(X) \bmod 7 = 4x^3 + 4x, \\ S_4(X) &\equiv \quad T_4(x) \bmod 7 = x^4 + 6x^2 + 1, \cdots. \\ S_p(X) &\equiv T_p(X) \bmod 7 \end{aligned} \tag{2}$$

$$S_l \circ S_m(x) \equiv S_m \circ S_l(x) \equiv S_{ml}(x) \tag{3}$$

where $x \in \mathrm{GF}(n)$.

Steps:

1. Alice picks up a random integer p from the integers $2, .., n-1$.
2. At this moment, she has a secret key p but sends

$$Y = T_p(X) \bmod n, \quad \text{for} \quad 1 < X < n \tag{4}$$

to Bob.

3. Bob picks up a random integer q from the integers $2, ...n-1$.
4. Bob sends

$$Y' = T_q(X) \bmod n, \quad \text{for} \quad 1 < X < n \tag{5}$$

to Alice.

5.Now Alice can compute

$$Z \equiv T_p(Y') \equiv T_p \circ T_q(X) \equiv T_{qp}(X) \pmod n. \tag{6}$$

6. Bob can compute

$$Z' \equiv T_q(Y) \equiv T_q \circ T_p(X) \equiv T_{qp}(X) \pmod n. \tag{7}$$

7. Now Bob and Alice have the common key Z:

$$Z = Z' \tag{8}$$

because of the commutativity (3).

Example:

$$n = 2^{200} = 1606938044258990275541962092341162602522202993782792835301376 \tag{9}$$

and $X = 123$.

Alice picks up a private key $p(= 251)$ and sends

$$Y = T_p(X) \bmod n = 1051937263758371990097586384146037381059241137335343438748379 \tag{10}$$

to Bob.

Bob has a private key $q(= 127)$ and sends

$$Y' = T_q(X) \bmod n = 389805704436066900356221107082190652128452589999625926802555 \tag{11}$$

to Alice.

Now Alice can compute

$$Z = T_p(Y') \bmod n = 1209219195210417873778621423700158842142848251849230516156123. \tag{12}$$

On the other hands, Bob can compute

$$Z' = T_q(Y) \bmod n = 1209219195210417873778621423700158842142848251849230516156123. \tag{13}$$

Thus, in this case, Alice and Bob have the 200-bit common

secret key

$$Z = 120921919521041787377862142370015884214284825184923051615612 3. \tag{14}$$

No one but Alice and Bob knows either p or q so anyone else must compute Z from Y and Y' alone.

The security of this public key distribution system relies on the difficulty about the problem ,given $Y \in$ GF(n), of finding an index l of the Chebyshev map $Y = T_l(x)$ over GF(n). Note that for $m < n$),

$$Y = T_m(X) \equiv a_m X^m + (\text{lower order terms in} X) \mod n \tag{15}$$

where,

$$a_m = 2^{m-1} \mod n. \tag{16}$$

An Exponential key exchange as originally proposed by Diffie and Hellman, where an exponential function

$$Y = X^m \mod n \quad \text{for} \quad X \in \text{GF}(n) \tag{17}$$

is used for constructing a one-way function called *the discrete logarithm* over GF(n).

Summary

- New notion of digital chaos and its relation to cryptography is introduced.
- Scalable vector stream cipher is introduced.
- Realtime partial encryption is realized with VSC.
- We show that Chebyshev polynomials of odd degree are permutation polynomial module 2^n.
- Construction of New Public Key Key Exchange.
- Application includes satellite encryption which are directly applicable to secure TV conference,

  e-learning and e-health.