Demonstration of 10Gbps Optical Encryption and Decryption by Using SOAs

Y. J. Jung(1, 4), C. W. Son(1), S. Lee(1),S. K. Gil(2), H. S. Kim(3) and N. K. Park (4)

(September 27, 2007)

Korea Institute of Science and Technology, Korea (1)
Suwon University, Korea (2)
Sejong University, Korea (3)
Seoul National University, Korea (4)

Contents

- Introduction
  - Introduction for XOR based encryption systems
- Study with steady state simulation
  - Steady state simulation method.
    - Shooting method, Picard method
  - Simulation results of cross gain modulation characteristics of SOAs
  - Operation principles of single XOR gate utilizing cross gain modulation in SOAs
- Study with dynamic simulation
  - Dynamic simulation method
    - Transfer matrix method
  - Simulation results of encryption and decryption system.
- Experiment
  - Experimental setup for encryption and decryption system
  - Experimental results of encryption and decryption system
- Conclusion

What is XOR encryption?

- Converting *Plaintext* to *Ciphertext* with XOR Encryption
  - The *plaintext* we will start with is the term "FAQ".
    - ASCII representation of the *plaintext*: FAQ
    - Binary representation of the *plaintext*: 01110000 01100101 1000000
  - We will XOR the first character of this *plaintext* into *ciphertext* using a "V" as the *key*:
    - ASCII representation of the *key*: V
    - Binary representation of the *key*: 10000110

Plaintext 'F'	Key 'V'	Ciphertext
0	1	1
1	0	1
1	0	1
1	0	1
0	0	0
0	1	1
0	0	0
0	1	1

What is XOR encryption?

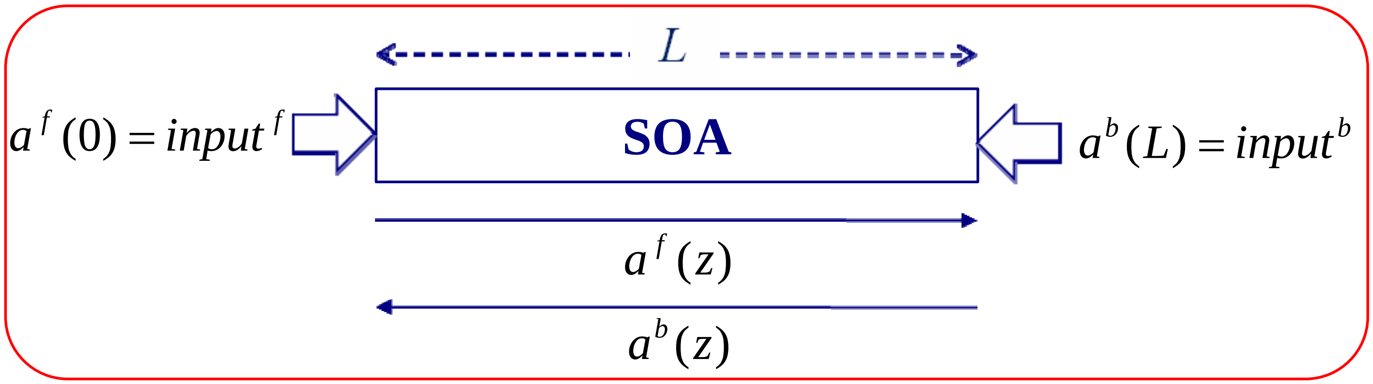
❑ Converting *Ciphertext* to *Plaintext* with XOR Encryption

- XOR encryption is a symmetric algorithm. This means that we can use the encryption key as the decryption key.
- Let's decrypt our *ciphertext* to recreate our original *plaintext*.
- Many encryption algorithms utilize the XOR operator as part of their operations.

Ciphertext	Key 'V'	Plaintext
1	1	0
1	0	1
1	0	1
1	0	1
0	0	0
1	1	0
0	0	0
1	1	0

Problem definition of steady state simulation

Let $a^f(z)$ be forward propagating E-field and $a^b(z)$ be backward propagating E-field
And also let forward input be $input^f$ and backward input be $input^b$



Field propagation equation can be written as differential equation form like below

$$\frac{da^f(z)}{dz} = f(a^f, a^b, z) \qquad a^f(0) = input^f$$

$$\frac{da^b(z)}{dz} = g(a^f, a^b, z) \qquad a^b(L) = input^b$$

➔ Boundary value problem of simultaneous ODE (ordinary differential equation).

Shooting method for solving boundary value problems of ODE

In order to solve this problem, *Shooting* method can be used, namely it can be solved by iteration of '*guess and check*'.

$$\frac{da^f(z)}{dz} = f(a^f, a^b, z) \qquad a^f(0) = input^f$$
$$\frac{da^b(z)}{dz} = g(a^f, a^b, z) \qquad a^b(L) = input^b$$

First of all, we assume $a^b(z) = input^b$

Then, the problem becomes initial value problem of ODE like Eq(1).

Initial value problem can be solved by well-known *Euler* or *Runge-Kutta* method.

$$\frac{da^f(z)}{dz} = f(a^f, a^b, z) \qquad a^f(0) = input^f \qquad (1)$$

With obtained $a^f(z)$ form Eq. (1), solve initial value problem of Eq. (2)

$$\frac{da^b(z)}{dz} = g(a^f, a^b, z) \qquad a^b(L) = input^b \qquad (2)$$

With obtained $a^b(z)$ form Eq. (2), solve initial value problem of Eq. (1) again.

Picard iteration method for solving boundary value problems of ODE

As another choice, *Picard* iteration method can be used.

$$\frac{da^f(z)}{dz} = f(a^f, a^b, z) \qquad a^f(0) = input^f$$
$$\frac{da^b(z)}{dz} = g(a^f, a^b, z) \qquad a^b(L) = input^b$$

First of all, we assume $a^f(z) = input^f$ and $a^b(z) = input^b$
We can calculate below equation,

$$a^f(z) = a^f(0) + \int_0^z f(a^f, a^b, z)$$
$$a^b(z) = a^b(0) + \int_0^z f(a^f, a^b, z) \qquad (1)$$

And calculate Eq. (1) again, with refreshed $a^f(z)$ and $a^b(z)$ obtained from Eq. (1).

Parameters & differential equations for real simulations

$$\frac{\partial a_l}{\partial z} = \frac{1}{2} g(N) \left[(1 - j\alpha) a_l - \sum_{m=cpp,shb,ch} \frac{(1 - j\beta_m)\varepsilon_m}{1 + j\Delta w_{ij}\tau_m} a_i^* a_j a_k \right] - \frac{\gamma_{sc} a_l}{2}$$

$$\frac{dN}{dt} = \frac{J}{qd} - \frac{N}{\tau_s} - \frac{g(N)}{\hbar \omega_0} |E|^2$$

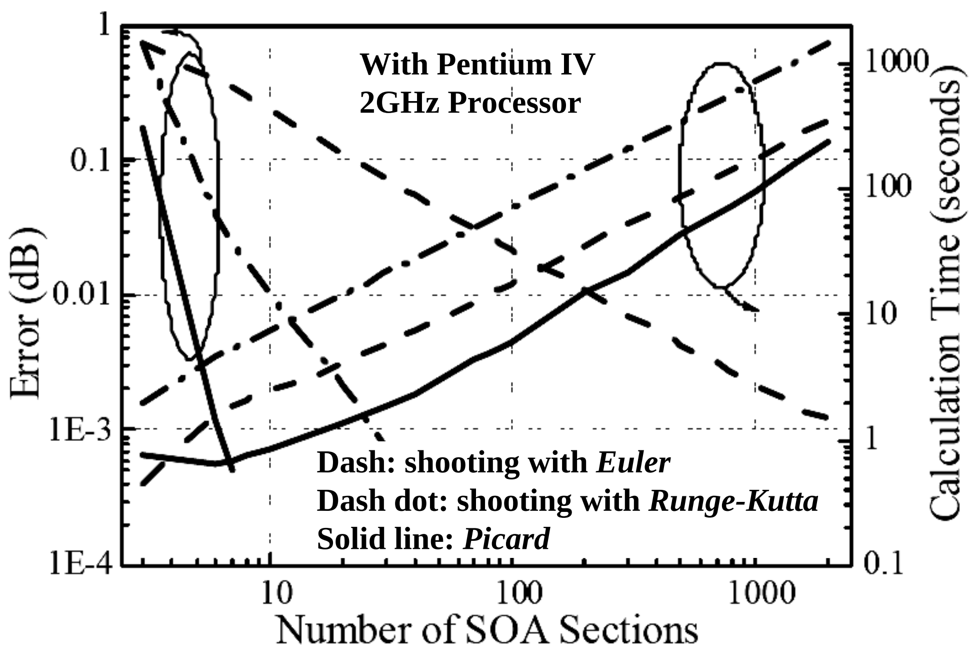
$$Where \quad \tau_s = \frac{1}{A + BN + CN^2}$$

Ref :IEEE, JSTQEL, Vol. 5, No. 3, pp. 839-850, 1999

$a_l(z)$	complex amplitudes of the signal fields	
z	propagation axis	
N	carrier density	
$g(N)$	modal gain	
α	linewidth enhancement factor	10
γ_{sc}	scattering loss per unit length	34 cm^{-1}
'i, j, k, l'	index of different wavelengths	
$\Delta\omega_{ij}$	frequency difference $(\omega_i - \omega_j)$	
ε_m	inverse saturation powers from the nonlinearity	shb:0.91 W^{-1}, ch:1.62 W^{-1}
β_m	contributions of linewidth enhancement factor	shb:0.21 W^{-1}, ch:2.812 W^{-1}
τ_m	relaxation times	`shb:0.036 ps, shb:0.52 ps
index m	carrier population pulsation (*cpp*), spectral hole burning (*shb*) and carrier heating (ch)	
J	current density	
q	electron charge	
d	active layer density	
A, B, C	recombination coefficient	A: $1x10^8$ s^{-1}, B: $2.5x10^{-11}$ cm^3s^{-1}, C: $1x10^{-28}$ cm^6 s^{-1}

Calculation efficiency of the simulation method

- According to our previous work (Jung, Optics express 2006), for the same accuracy, *Picard* iteration method is the fastest method in the case of calculating bidirectional signals.



Convergence error and required computation time plotted as a function of number of SOA segments

OPERATING CONDITION

Driving current = 500mA

SOA length=500μm

Input power = 10/8dBm (forward/backward)

Wavelength = 1549.2/1550.8 nm (forward/backward)

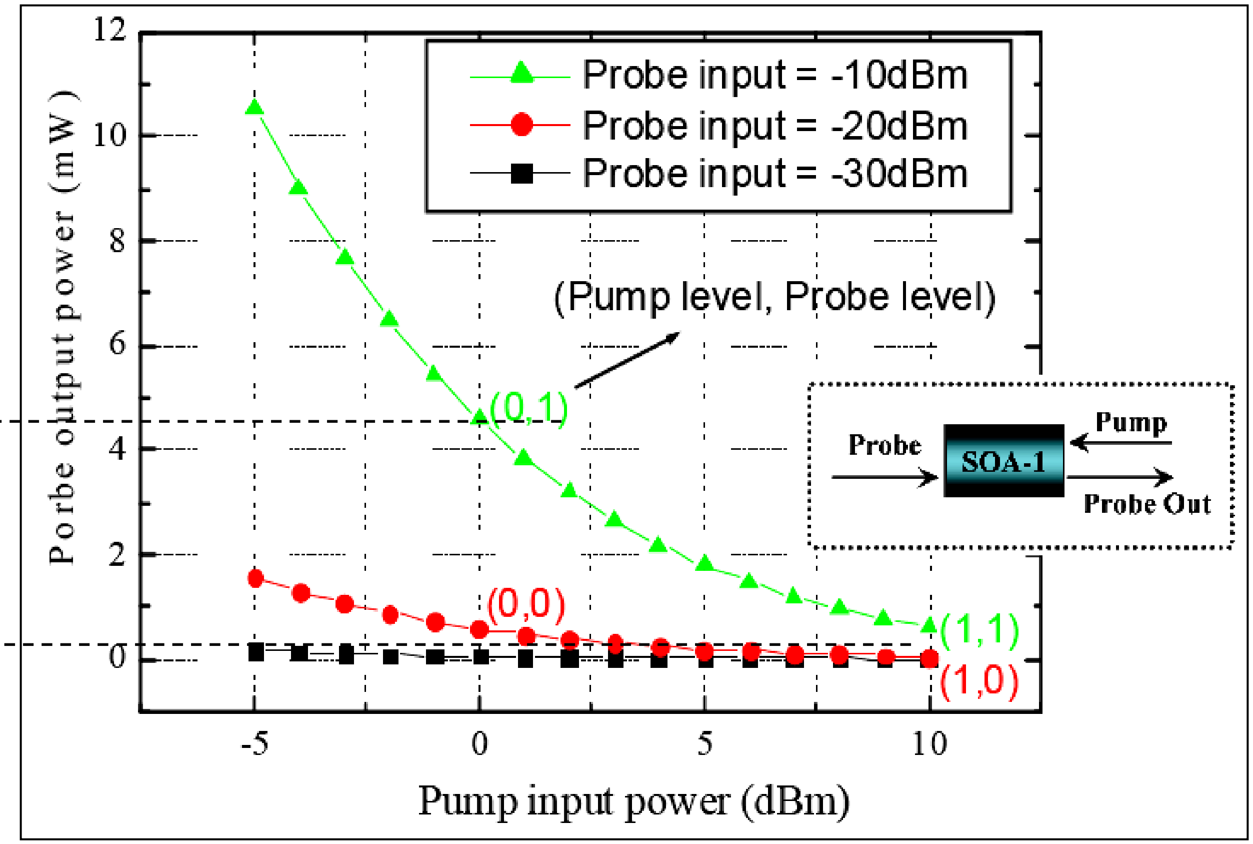
Wavelength resolution= 0.04 nm

Simulation study of cross gain modulation characteristics in a SOA

Assume,
Pump power of
***'0-level'* is 0dBm**
and ***'1-level'* is 10dBm**
Probe power of
***'0-level'* is -20dBm**
and ***'1-level'* is -10dBm**

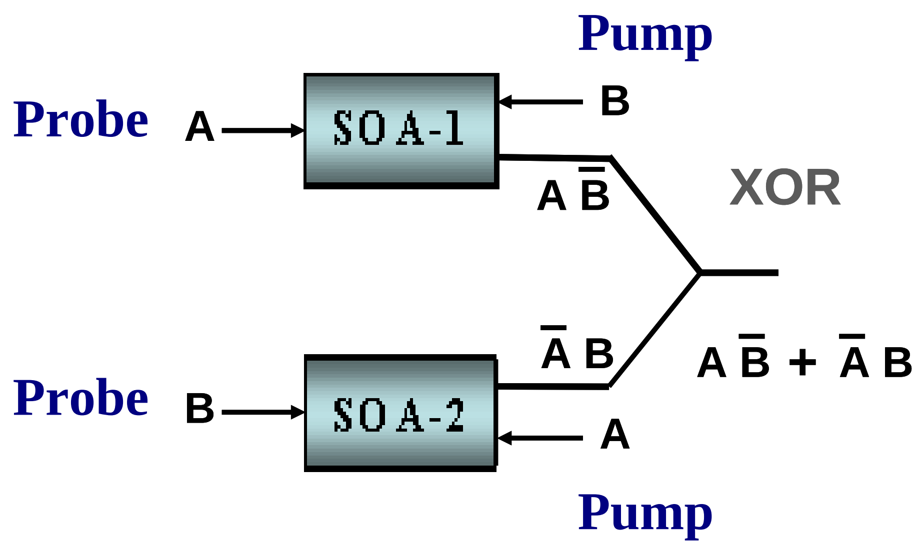
Probe out *'1-level'*

Probe out *'0-level'*



pump	*probe*	***probe out*** = $probe \cdot \overline{pump}$
0	0	0
0	1	1
1	0	0
1	1	0

Operation Principles of Single XOR Gate Utilizing Cross Gain Modulation in SOAs

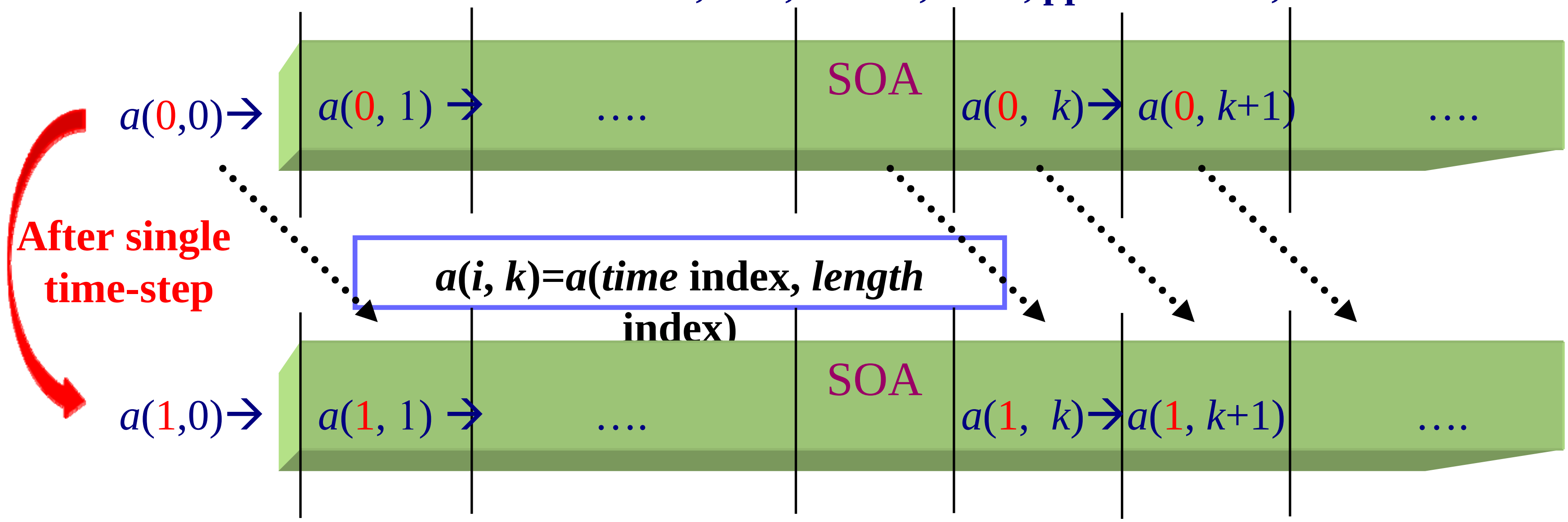


A	B	$A\bar{B}$	$\bar{A}B$	$XOR\ (A\bar{B}+\bar{A}B)$
0	0	0	0	0
0	1	0	1	1
1	0	1	0	1
1	1	0	0	0

Dynamic simulation method

❑ Transfer Matrix Method

- We can divide SOAs with small sections and calculate E-field(a) at each section **Ref : IEEE, JLT, Vol. 20, No. 8, pp. 1350-1356, 2002**



$$\frac{\partial a(z,t)}{\partial z}+\frac{\partial a(z,t)}{v_g \partial t}=f\left[a(z,t),Variables\right] \Rightarrow \frac{a(z,t+\Delta t)-a(z,t)}{v_g \Delta t}=f\left[a(z,t),Variables\right]$$

For a same section

with index notation

$$a(i+1,k)=a(i,k)+f\left[a(i,k),Variables\right]\times v_g \Delta t$$

Dynamic simulation method

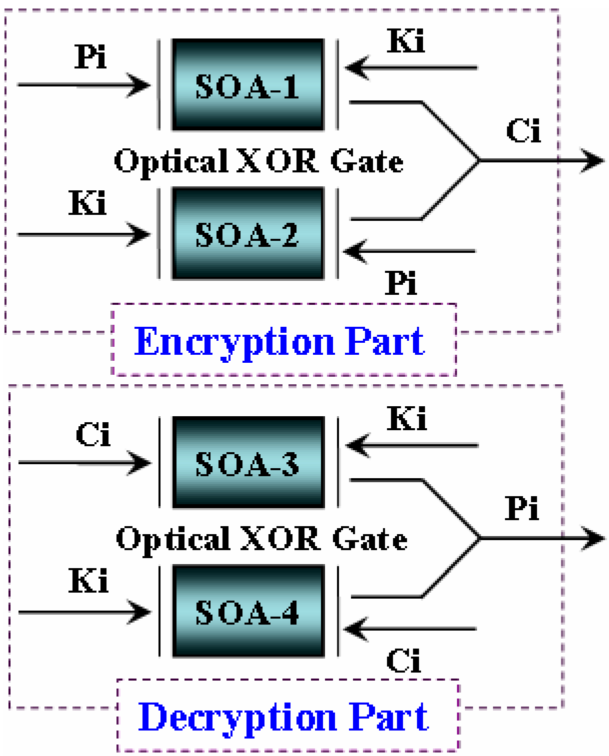
- On the contrary to steady state analysis that is finding final state as fast as possible, many calculation times were required because fields at all of time steps have to be calculated sequentially in the dynamic simulation.

$$a_l(i+1,k) = a_l(i,k) + \frac{1}{2} g(N) \begin{bmatrix} (1-j\alpha) a_l(i,k) \\ -\sum_{m=cpp,shb,ch} \frac{(1-j\beta_m)\varepsilon_m}{1+j\Delta w_{ij}\tau_m} a_i^*(i,k) a_j(i,k) a_k(i,k) \end{bmatrix} - \frac{\gamma_{sc} a_l(i,k)}{2} \times v_g \Delta t$$

$$\frac{dN}{dt} = \frac{J}{qd} - \frac{N}{\tau_s} - \frac{g(N)}{\hbar\omega_0} |E|^2 \qquad \tau_s = \frac{1}{A + BN + CN^2}$$

Schematics for encryption and decryption

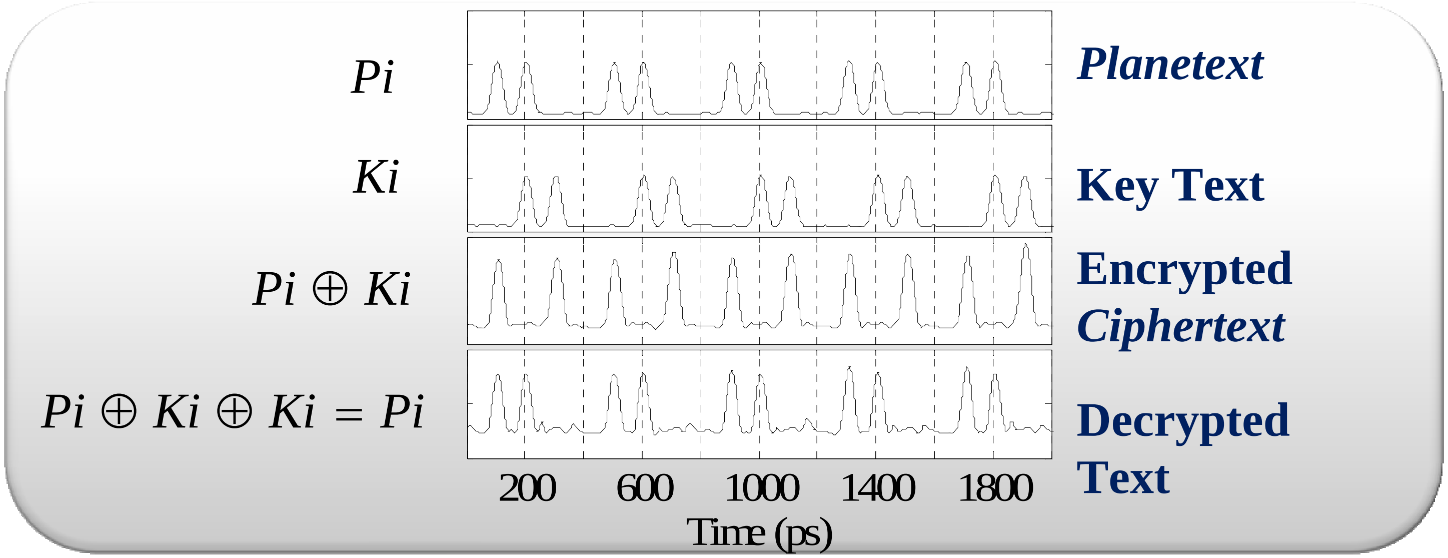
- Schematics and applied signal for calculations
  - In the calculation, OSNR for all of *Pi* and *Ki* was assumed as 10dB
  - All of the SOAs were assumed that have length of 300μm and 300*mA* bias current



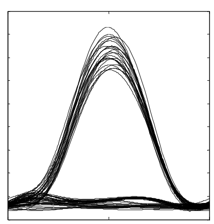
Signals for Calculations		Average power	Extinction Ratio
SOA1	Pi	-13dBm	10dB
	Ki	7dBm	10dB
SOA2	Pi	7dBm	10dB
	Ki	-13dBm	10dB
Encrypted	Ci	3dBm	7dB
SOA3	Ci	-13dBm	7dB
	Ki	7dBm	10dB
SOA4	Ci	5dBm	7dB
	Ki	-13dBm	10dB
Decrypted	Pi	2dBm	5.5dB

Calculated signal patterns and eye-diagrams of encrypted and decrypted signals

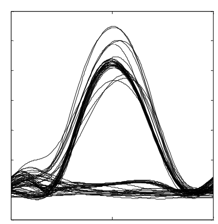
- Regular 10Gbps RZ pattern having ‘1100’ was applied for *Pi* and *Ki*



- In order to consider bit pattern effects, we also obtained eye-diagrams with 127bit PRBS patterns for *plaintext* and *ciphertext*.
  - Calculated Q-factor of decrypted signal was about 5.4 after all of processes.



Encrypted signals

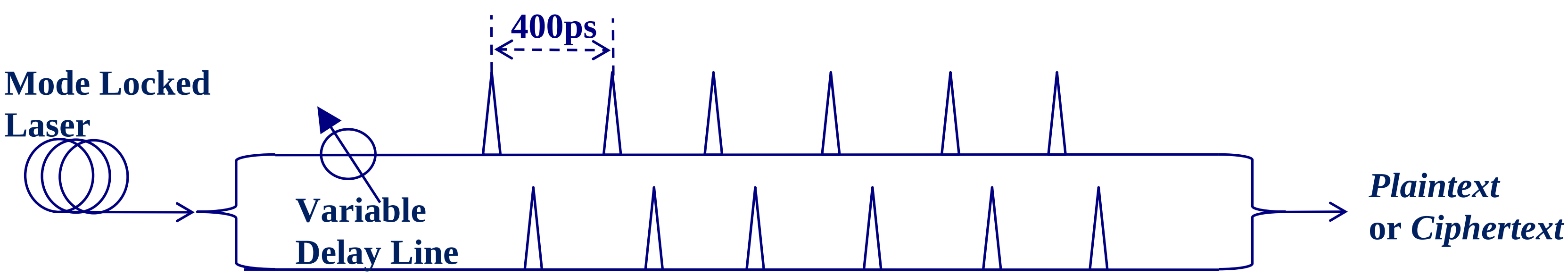


Decrypted signals

Experimental setup

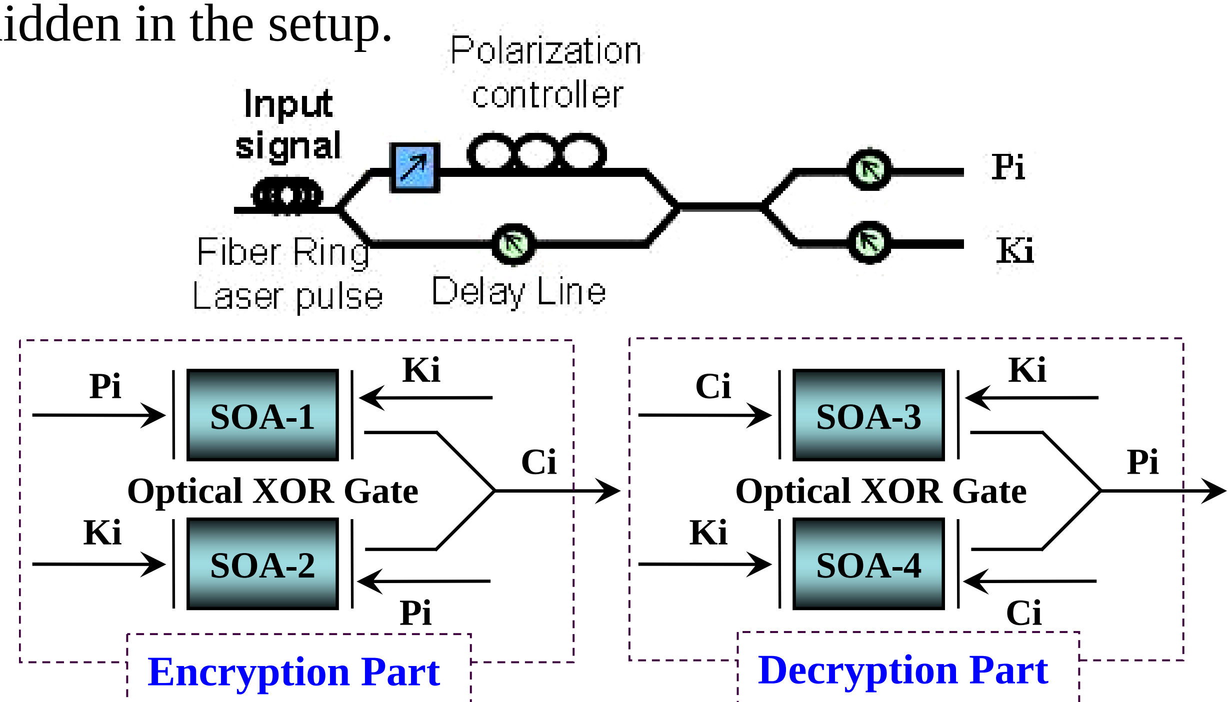
❑ Procedures to make signals

- Mode-locked fiber ring laser was used to generate short pulses with 400ps repetition rate
- After that, RZ pattern of '1100' was made with a sum of patterns of '1000' and '0100'



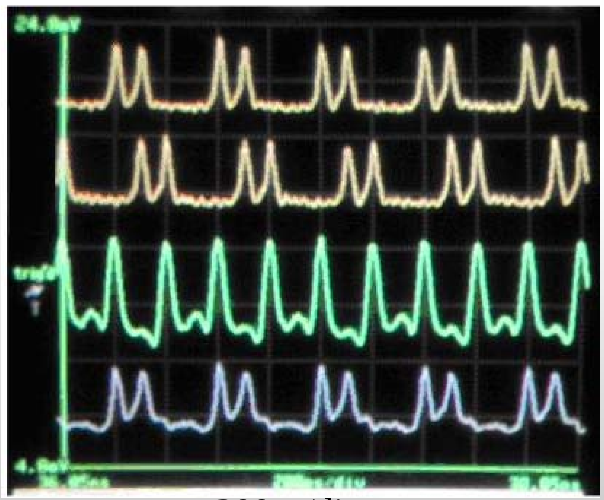
Experimental setup

- Experimental setup
  - With appropriate delay, all of synchronized signal was applied for the system.
  - EDFAs /attenuators were used for optimize the power levels of propagating signals for the efficient XGM processes even these were hidden in the setup.



Experimental results

- Experimental results show two cascaded NOR-gates (serially connected encryption and decryption parts) actually keep signal shape

Pi		***Planetext***
Ki		**Key Text**
$Pi \oplus Ki$		**Encrypted** ***Ciphertext***
$Pi \oplus Ki \oplus Ki = Pi$		**Decrypted Text**

200ps/div

Conclusion

- We have investigated encryption/decryption system based on cross gain modulation in SOAs with the numerical simulation.
  - In order to reduce required calculation time, the integral equation approach was adopted for the steady state analysis and the transfer matrix method was employed for the dynamic simulations.
  - Simulation /experimental results show that serially connected two XOR-gates can act as encryption and decryption system for the 10Gbps RZ patterns without any additional regenerator.

Thank you for your attention….