《연구논문》 Hankook Kwanghak Hoeji, Volume 19, Number 3, June 2008 DOI: 10.3807/HKH.2008.19.3.237

반도체 광 증폭기 XOR 논리게이트를 이용한 10 Gbps 전광 암호화 시스템의 구현

정영진 · 박남규

서울대학교 전기컴퓨터 공학부

㊞ 151-742 서울시 관악구 관악로 599

전영민 · 우덕하 · 이 석†

한국 과학기술 연구원

㊞ 136-791 서울시 성북구 월송길 5

길상근

수원대학교

㊞ 445-743 경기도 화성시 봉담읍 와우리 산 2-2

(2008년 5월 23일 받음, 2008년 6월 8일 수정본 받음, 2008년 6월 9일 게재 확정)

전자 논리회로에서 이용되는 전자신호 암호화와 같은 방법으로, 반도체 광 증폭기 XOR논리 게이트를 이용한 전광 암호화 시스템을 제안하였다. 시스템의 변수를 최적화 하고 전체 디자인 과정을 빠르게 수행하기 위해 정상상태와(steady state) 과도상태에(dynamic) 대한 전산모사가 차례로 이루어졌다. 심각한 신호 왜곡이 없이 10 Gbps 속도에서 일반적인 반도체 광 증폭기의 연속적 연결을 통해 전광 신호에 대한 암호화와 해독이 수행될 수 있음을 전산모사와 실험에 의한 결과를 통해 보여주었다.

주제어: Logic-based optical processing, Optical logic, Semiconductor optical amplifiers

I. 서 론

복잡한 초고속 논리회로는 많은 연구원들의 의욕적인 연구 주제로 여겨지고 있다. 그리고 초고속 비선형 광학을 이용할 때 10 Gbps 이상의 신호처리를 이용할 수 있는 장점들을 이용해 전자 논리회로를 전광 회로로 바꾸는 연구에 대한 관심은 계속해서 커져가고 있다. 대표적인 예로 광 아날로그 디지털 컨버터(all optical analog to digital converter),[1] 전광 읽기 전용 메모리(all optical read only memory)[2] 그리고 전광 암호화(all optical encryption)[3-5] 등이 있다. 그러나 여전히 이러한 광 회로 시스템의 동작원리는 기존에 잘 발달되고 확립되어있는 전자회로 디자인 법칙과는[6] 동떨어져 있어 실용화를 원하는 연구원들에게 어려움을 남기고 있다. 또한, 광 회로 시스템의 하드웨어를 일반적인 전자 회로 디자인 법칙으로 이해하기 어렵고, 이미 확립되어있는 전자회로 디자인 법칙을 이용해 좀더 높은 레벨의 광 회로를 디자인 하는데 어려움이 있다. 본 연구에서는 전광 XOR게이트를 기본 구성 소자로 사용하여, 기존의 매우 간단한 전자회로 암호화 원리를 그대로 이용한 XOR 암호화 시스템을 구현해 보았다. 반도체 광 증폭기의(SOA: semiconductor optical amplifier) 상호 이득변조를(XGM: cross gain modulation) 이용한 전광 XOR 논리 게이트를 이용하여[7-9] 우리는 10 Gbps의 속도로 데이터의 암호화 복호화가 가능함을 보여 주었으며 전산모사를 통해 자세한 디자인 과정과 성능에 영향을 미치는 요소들을 분석하였다.

†E-mail: slee@kist.re.kr

II. 디자인원리와 전산모사분석

제안하는 암호화 복호화 시스템은 그림 1에 설명되어 있으며 여기서 *Pi*, *Ki*와 *Ci*는 각각 원(plaintext), 키텍스트(keytext), 암호문을(ciphertext) 나타낸다. 암호화 과정을 살펴보면, 두 개의 반도체 광 증폭기를(SOA-1, SOA-2) 이용해 "*Pi XOR Ki*" 연산이 수행되며 그 원리는 다음과 같다. 먼저 $Pi \cdot \overline{Ki}$ 불 연산이 SOA-1에서 수행되고(SOA-1에 대해 프루브(probe)신호로는 *Pi*, 펌프(pump)신호로 *Ki*가 사용됨) 동시에 SOA-2에서 $\overline{Pi} \cdot Ki$이 수행된다(SOA-2에 대해 프루브(probe)신호로 *Ki* 펌프(pump)신호로 *Pi*가 사용됨). 그리고 광 커플러를 통해 $Pi \cdot \overline{Ki}$와 $\overline{Pi} \cdot Ki$ 두 신호가 더해져서 *Ci*가 얻어지며 이때 "*Ci* =

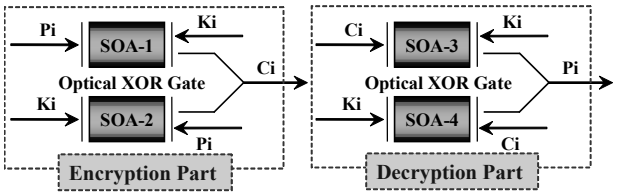

그림 1. 제안된 암호화/복호화 시스템의 구조도. 쌍을 이루고 있는 반도체 광 증폭기는(SOA-1 & SOA-2, SOA-3 & SOA-4) 하나의 XOR 게이트를 구성하며 암호화와 복호화에 사용되고 있다.

Pi XOR Ki"가 된다. 다음으로 복호화에 대해서 살펴보면, 같은 원리를 통해서 SOA-3과 SOA-4에서 *Ci*와 *ki*에 대해 XOR 연산이 이루어질 수 있음을 알 수 있다. 정리하면 식 (1)과 같은 연산을 통해 암호화가 수행되고 식 (2)와 같은 연산에 의해 복호화된 신호를 얻을 수 있음을 알 수 있다.

$$Ci = Pi\ XOR\ Ki \tag{1}$$

$$Pi = Ci\ XOR\ Ki = (Pi\ XOR\ Ki)\ XOR\ Ki \tag{2}$$

반도체 광 증폭기의 상호 이득변조특성을 분석하기 위해 우리는 식 (3)과 식 (4)에서와 나타낸 진행방정식과(propagation equation) 비율방정식을(rate equation) 이용하여 정상상태 전산모사를 수행하였다.[10] 이때 우리는 계산 효율을 높이기 위해 식 (5)와 같이 적분형으로 진행 방정식을 변형하여 전산모사를 수행 하였다.[11]

$$\pm\frac{da_l}{dz} = \frac{1}{2}g(N)\begin{bmatrix}(1-j\alpha)a_l \\ -\sum\limits_{m=cpp,shb,ch}\dfrac{(1-j\beta_m)\varepsilon_m}{1+j\Delta w_{ij}\tau_m}a_i^* a_j a_k\end{bmatrix} - \frac{\gamma_{sc}a_l}{2} \tag{3}$$

$$\begin{aligned}&\frac{dN}{dt} = \frac{I}{qV} - \frac{N}{\tau_s} - \frac{g(N)}{\hbar\omega_0}|E|^2 \\ &where\quad \tau_s = \frac{1}{A+BN+CN^2},\quad |E|^2 = \sum_i |a_i|^2 / A_x\end{aligned} \tag{4}$$

$$\begin{aligned}&\pm a_l(z) = a_l(0) + \\ &\int_0^z \frac{1}{2}g_l(N)\begin{bmatrix}(1-j\alpha)a_l \\ -\sum\limits_m\left(\sum\limits_{\Delta\omega_{ij}}\dfrac{(1-j\beta_m)\varepsilon_m}{1+j\Delta\omega_{ij}\tau_m}a_i^* a_j a_k\right)\end{bmatrix} - \frac{\gamma_{sc}a_l}{2}dz\end{aligned} \tag{5}$$

표 1은 반도체 광 증폭기의 전산모사에 사용된 매개변수들을 나타내고 있다.[10] 진행하는 광 파워와 주입전류에 따라 변하는 매개변수 ε_{cpp}와 τ_{cpp}에 대해서는 잘 알려진 수식 $\varepsilon_{cpp} = \Gamma a\tau_{cpp}/\hbar\omega_o$와 $\tau_{cpp} = 1/(A+BN+CN^2+(\Gamma a/\hbar\omega_o)|E|^2)$를 이용해 계산되었다. 참고로 전산모사 모델은 여러 개의 파장에 대해 수행 가능하지만 우리는 하나의 파장만을 이용하였으며 1550 nm로 수행 되었다. 300 μm길이의 반도체 광 증폭기에 대해 300 mA의 구동 전류를 가정하여 상호이득 변조 특성이 분석되었다. 10 dB 소광비의 펌프신호와("1" = 10 dBm, "0" = 0 dBm) 프루브신호를("1" = -10 dBm, "0" = -20 dBm) 주입시켜 주었을 때 출력으로 얻어지는 신호의 정상상태 소광비는 대략 8 dB정도로 측정 되었다. 그림 2를 통해 프루브 출력에서 '$\overline{펌프}$·프루브' 불 대수 연산 값을 얻게 되는 것을 확인 할 수 있다. 즉, 펌프 입력값이 "0"이고 프루부 입력값이 "1"인 경우에만 프르부 출력이"1"이 되는 것을 알 수 있다. 식 (3)~(5)에서 알 수 있듯이 펌프입력 신호와 프루브 입력 신호의 합이 충분이 커서 이득으로 쓰이는 전자가 모두 고갈되어 이득이 모자랄 때 상호 이득 변조가 일어나는 점을 감안하면서 펌프 신호와 프루브 신호의 파워를 결정할 때 주의를 기울여야 한다. 즉 그림 2에서 보는 바와 같이 원하는 상호이득변조 기울기가 있는 영역에서 입력전류와 광 파워의 레벨을 결정해 주어야 한다.

정상상태 응답으로부터 결정된 최적의 펌프와 프푸브 파워를 이용해 암호화와 복호화 성능을 분석하기 위해 과도상태(dynamic) 전산모사가 수행 되었으며 이때 식 (6)을 이용한 행렬 전달법이(transfer matrix method) 사용되었다.[12,13]

표 1. 반도체 광 증폭기의 매개변수들

$a_l(z)$	complex amplitudes of the signal fields
q	electron charge
N	carrier density
z	propagation axis
I	current
i, j, k, l	index of different wavelengths
$\Delta\omega_{ij}$	frequency difference ($\omega_i - \omega_j$)
$g(N)$	modal gain $g(N) = \Gamma a(N - N_0)$
a	material gain = 2.7×10^{-9} cm^2
Γ	confinement factor = 0.4
N_0	Transparent carrier density = 1.9×10^{18} cm^{-3}
α	linewidth enhancement factor = 10
γ_{sc}	scattering loss per unit length = 34 cm^{-1}
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, *ch*: 2.81, *cpp*: 10
τ_m	relaxation times *shb*: 0.036 ps, *ch*: 0.52 ps
index m	carrier population pulsation (*cpp*), spectral hole burning (*shb*) and carrier heating (*ch*)
V	volume of the SOA active region = 5.04×10^{-11} cm^3
A_x	cross-sectional area of the SOA active region = 1.68×10^{-9} cm^2
A, B, C	recombination coefficient A: 1×10^8 s^{-1}, B: 2.5×10^{-11} cm^3·s^{-1}, C: 1×10^{-28} cm^6·s^{-1}

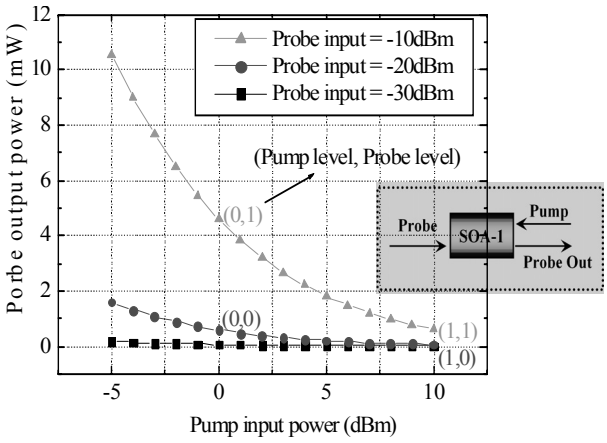

그림 2. 반도체 광 증폭기의 상호이득변조 정상상태 응답.

$$\frac{\partial a_l}{\partial z}+\frac{\partial a_l}{v_g \partial t}=\frac{1}{2}g(N)\left[(1-j\alpha)a_l-\sum_{m=cpp,shb,ch}\frac{(1-j\beta_m)\varepsilon_m}{1+j\Delta w_{ij}\tau_m}a_i^* a_j a_k\right]-\frac{\gamma_{sc}a_l}{2} \quad (6)$$

참고로 *Pi*와 *Ki*에 대해 ASE 잡음을 더해주어 대략 OSNR이 35 dB가(0.1 nm 대역폭에 대해) 되도록 하였으며 ASE 잡음은 시간 축에서 만들어져서 필터를 통과시킨 후 더해 주었다. 시간 축에서 암호화와 복호화된 신호를 보기 위해 10 Gbps 슈퍼 가우시안(super-Gaussian) RZ 형태의 데이터를 넣어 주었다. 그림 3에서 볼 수 있듯이 암호화/복호화된 양질의 광 신호가 10 Gbps로 얻어진 것을 알 수 있다. 표 2에서 볼 수 있듯이 하나의 XOR 논리 게이트에 대해 대략 3 dB정도의 과도응답 소광비 손해가 있는 것을 알 수 있었다. 아이 다이어그램을(eye-diagram) 얻고 Q값을 예측해 보기 위해 127비트 PRBS(Pseudo-random bit sequence) 입력 신호를 넣어 주었으며 그림 3과 같은 결과를 얻었다. 고속 동작에서 신호의 질을 떨어뜨리는 가장 큰 요인은 전자의 공핍이 빠른 시간 안에 채워지지 못하는 데서 오는 것을 식 (6)을 살펴보면 알 수 있다. 따라서 이득 매질 내에 충분한 전자밀도가 유지 되어야 하며 이를 위해서는, 입력전류가 높아야 하고 반도체 광 증폭기의 길이가 짧아야 한다. 전산모사에 사용된 입력 전류 300 mA와 300 μm의 길이를 가지는 반도체 광 증폭기에 대해서 분석해 본 그림 3의 결과를 볼 때, 복호화된 신호에서 패턴 영향이(pattern effect) 발견 되는 것은 암호화와 복호화를 거치는 동안 반도체 광 증폭기의 이득 회복시간의(gain recovery time: 계산에 이용된 반도체 광 증폭기의 경우 대략 30 ps정도로 RZ 신호의 상승/하락 시간과 비슷하다.) 축적에 따른 것으로 보이며 또한, 암호화에서 줄어든 소광비가 복호화 부분에서 영향을 미친 것으로 보인다.

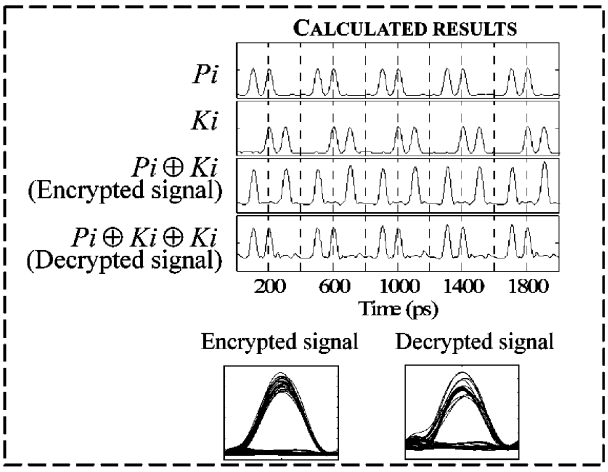

그림 3. 암호화/복호화된 신호의 패턴과 아이 다이어그램.

표 2. 입력된 신호와 그에 따른 출력 신호들에 대한 파워와 소광비

Signals for calculations		Peak power	Extinction ratio
SOA1	Pi	-10 dBm	10 dB
	Ki	10 dBm	10 dB
SOA2	Pi	10 dBm	10 dB
	Ki	-10 dBm	10 dB
Encrypted	Ci	6 dBm	7 dB
SOA3	Ci	-10 dBm	7 dB
	Ki	10 dBm	10 dB
SOA4	Ci	8 dBm	7 dB
	Ki	-10 dBm	10 dB
Decrypted	Pi	5 dBm	5.5 dB

아이 다이어그램으로부터 계산된 복호화된 신호의 Q값은 대략 5.4로 측정 되었다. 전광 신호 재생기나[14] FEC등의(forward error correction) 추가적인 신호처리 한다면 통해 더 나은 출력 신호를 얻을 수 있을 것으로 판단된다.

III. 실 험

4개의 상용 반도체 광 증폭기를(Samsung-OA40B3A 2개, Genoa-G111 2개) 기본 소자로 이용하여 XOR 광 암호화/복호화 시스템을 실험을 해 보았다. 입력 신호를 만들기 위해 충분한 소광비를 얻기 위해 2.5 Gbps의 주기를 가지는 모드 잠김 광섬유 링 레이저(mode-locked fiber ring laser)의 출력을 이용했다. (이상적인 경우 10 Gbps 펄스를 만들어 펄스패턴 발생기를 통과시켜 원하는 패턴을 만들 수 있어야 하지만 이 경우는 충분한 소광비를 얻는데 어려움이 있다. 따라서 우리는 충분한 소광비를 가지는 2.5 Gbps의 신호를 이용하여 10 Gbps의 일정한 패턴을 가지는 신호를 만들어 주었다. 따라서 PRBS 신호에 대해 신호의 질을 평가할 수 없었고 이는 앞의 전산모사를 이용한 분석으로 대신했다.) 그림 4와 같이 반복 주기가 2.5 GHz인 신호를 50:50 광섬유 커플러에 주입하여 두 신호로 나누어준 후 하나의 신호는 100 ps 시간지연장치를 통과 시키고, 다시 두 신호를 더해 주어 10 Gbps의 주기적인

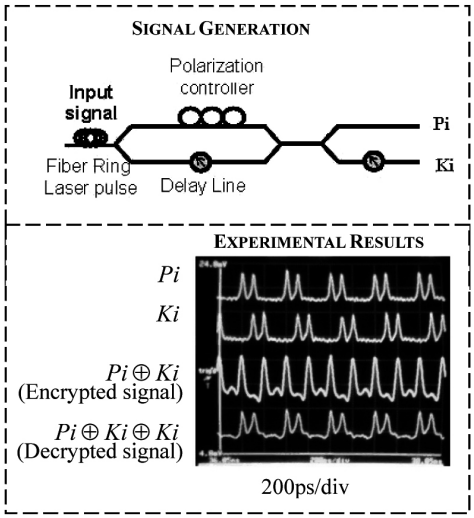

그림 4. 위: 신호발생을 위한 실험셋업, 아래: *Pi*, *Ki*, 암호화된 신호 그리고 복호화된 신호의 패턴.

"1100" 패턴을 얻었다. 그리고 얻어진 이 패턴의 신호를 다시 시간 지연을 주어 동기화된 "1001" 패턴을 얻었으며 얻어진 두 종류의 패턴을 각각 *Pi*와 *Ki*신호로 사용 하였다. 그림에는 나타내지 않았지만 반도체 광 증폭기의 효율적인 상호이득변조를 위해 어븀첨가 광섬유증폭기와(EDFA: erbium doped fiber amplifier) 소광기를(attenuator) 사용하여 광 파워를 조절해 주었다. 모드 잠김 광섬유 링 레이저로부터 나오는 신호의 소광비는 정해져 있기 때문에 신호의 파워 크기를 조절하여 상호 이득변조가 최적화 되도록 하였다. *Pi*, *Ki*, 암호화된 신호 그리고 복호화된 신호에 대한 패턴이 그림 4에 나타나있으며 최종적으로 얻어진 복호화된 신호의 소광비는 대략 6.1 정도로 측정 되었다. 상호이득변조가 잘 되도록 반도체 광 증폭기를 특별히 주문 제작하지 않았고 기존에 상용화된 반도체 광 증폭기를 이용하였지만 10 Gpbs 데이터 신호에 대해 제안된 암호화/복호화 시스템에 대해 실험적으로 증명이 가능하였다.

IV. 결 론

우리는 고속의 전광 암호화/복호화 시스템을 제안하고 분석하였다. 전광 논리회로를 만들기 위해 반도체 광 증폭기의 상호 이득변조를 이용한 XOR 전광 논리 게이트를 기본 소자로 사용 하였으며 확립된 디지털 전자회로 디자인 방법이 사용되었었다. 정상상태 응답과 과도상태 응답에 대한 전산모사 분석을 통해 제안된 시스템의 가능성과 한계를 제시하였다. 그리고, 10 Gbps 데이터에 대해 상용 반도체 광 증폭기를 이용하여 실험적인 증명을 수행 하였다. 이러한 결과는 앞으로 전광 논리 게이트들을 이용한 높은 수준의 전광 논리회로 개발에 기반이 될 것으로 기대 된다.

참고문헌

[1] George C. Valley, "Photonic analog-to-digital converters," *Optics Express*, vol. 15, no. 5, pp. 1955-1982, 2007.

[2] C. A. Barrios and M. Lipson, "Silicon photonic read-only memory," *Journal of Lightwave Technology*, vol. 24, no. 7, pp. 2898-2905, 2006.

[3] F. F. Froehlich, C. H. Price, T. M. Turpin, and J. A. Cooke, "All-optical encryption for links at 10 Gbps and above," *IEEE. MILCOM.* vol. 4, pp. 2158-2164, 2005.

[4] O. Buskila, A. Eyal, and M. Shtaif, "Secure communication in fiber optic systems via transmission of broad-band optical noise," *Optics Express*, vol. 16, no. 5, pp. 3383-3396, 2008.

[5] C. R. Mirasso, "Chaotic optical communications," *IEEE. LEOS News Letter*, vol. 19, no. 1, pp. 12-14, 2005.

[6] B. Schneier, Applied Cryptography (2nd Ed). John Wiley & Sons, 1996.

[7] J. H. Kim, Y. M. Jhon, Y. T. Byun, S. Lee, D. H. Woo and S.H. Kim, "All-optical XOR gate using semiconductor optical amplifiers without additional input beam," *IEEE. Photonics Technology Letters*, vol. 14, no. 10, pp. 1436-1438, 2002.

[8] Q. Wang, G. Zhu, H. Chen, J. Jaques, J. Leuthold, A. B. Piccirilli, and N. K. Dutta, "Study of all-optical XOR using Mach-Zehnder Interferometer and differential scheme," *IEEE. Journal of Quantum Electronics*, vol. 40, no. 6, pp. 703-710, 2004.

[9] M. Zhang, L. Wang, and P. Ye. "All optical XOR logic gates: technologies and experiment demonstrations," *IEEE. Communication Magazine*, vol. 43, no. 5, pp. s19-s24, 2005.

[10] M. A. Summerfield and R. S. Tucker, "Frequency-domain model of multiwave mixing in bulk semiconductoroptical amplifiers," *IEEE. Journal of Selected Topics in Quantum Electronics*, vol. 5, no. 3, pp. 839-850, 1999.

[11] Y. J. Jung, P. Kim, J. Park, and N. Park, "Integral equation approach for the analysis of high-power semiconductor optical amplifiers," *Optics Express*, vol. 14, no. 6, pp. 2398-2403, 2006.

[12] M. G. Davis and R. F. O'Dowd, "A transfer matrix method based large-signal dynamic model for multielectrode DFB lasers," *IEEE. Journal of Quantum Electronics*, vol. 30, no. 11, pp. 2458-2466, 1994.

[13] H. Lee, H. Yoon, Y. Kim, and J. Jeong, "Theoretical study of frequency chirping and extinction ratio of wavelength-converted optical signals by XGM and XPM using SOA's," *IEEE. Journal of Quantum Electronics*, vol. 35, no. 8, pp. 1213-1219, 1999.

[14] Y. J. Jung, J. Park, and N. Park, "Wavelength-transparent nonlinear optical gate based on self-seeded gain modulation in folded tandem-SOA," *Optics Express*, vol. 15, no. 8, pp. 4929-4934, 2007.

Demonstration of 10 Gbps, All-optical Encryption and Decryption System Utilizing SOA XOR Logic Gates

Young Jin Jung and Namkyoo Park

School of EECS, Seoul National University, 599 Gwanangno, Gwanak-gu, Seoul, 151-742, South Korea

Young Min Jhon, Deok Ha Woo, and Seok Lee†

Korea Institute of Science and Technology, 5 Wolsong-gil, Seongbuk-gu, Seoul, 136-791, South Korea

†*E-mail: slee@kist.re.kr*

Sangkeun Gil

University of Suwon, San 2-2 Wau-ri, Bongdam-eup, Hwaseong-si, Gyenggi-do, 445-743, South Korea

(Received May 23, 2008; Revised manuscript June 8, 2008; Accepted June 9, 2008)

An all-optical encryption system built on the basis of electrical logic circuit design principles is proposed, using semiconductor optical amplifier (SOA) exclusive or (XOR) logic gates. Numerical techniques (steady-state and dynamic) were employed in a sequential manner to optimize the system parameters, speeding up the overall design process. The results from both numerical and experimental testbeds show that the encoding/decoding of the optical signal can be achieved at a 10 Gbps data rate with a conventional SOA cascade without serious degradation in the data quality.

OCIS codes: (200.3760) Logic-based optical processing; (200.4660) Optical logic; (250.5980) Semiconductor optical amplifiers.