SANDIA REPORT

SAND 2003-4474
Unlimited Release
Printed December 2003

Photonic Encryption using All Optical Logic

Jason D Tang, Thomas D Tarman, and Lyndon G Pierson
Ethan L. Blansett and G. Allen Vawter
Perry J. Robertson and Richard Schroeppel

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.doe.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2003-4474
Unlimited Release
Printed December 2003

Photonic Encryption using All Optical Logic

Jason D. Tang, Thomas D. Tarman, and Lyndon G. Pierson
Advanced Networking Integration Department

Ethan L. Blansett and G. Allen Vawter
RF Microsystems Technologies

Perry J. Robertson
RF and Opto Microsystems

Richard C. Schroeppel
Crypto and Info Systems Surety

Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0806

Abstract

With the build-out of large transport networks utilizing optical technologies, more and more capacity is being made available. Innovations in Dense Wave Division Multiplexing (DWDM) and the elimination of optical-electrical-optical conversions have brought on advances in communication speeds as we move into 10 Gigabit Ethernet and above. Of course, there is a need to encrypt data on these optical links as the data traverses public and private network backbones. Unfortunately, as the communications infrastructure becomes increasingly optical, advances in encryption (done electronically) have failed to keep up. This project examines the use of optical logic for implementing encryption in the photonic domain to achieve the requisite encryption rates.

In order to realize photonic encryption designs, technology developed for electrical logic circuits must be translated to the photonic regime. This paper examines two classes of all optical logic (SEED, gain competition) and how each discrete logic element can be interconnected and cascaded to form an optical circuit. Because there is no known software that can model these devices at a circuit level, the functionality of the SEED and gain competition devices in an optical circuit were modeled in PSpice. PSpice allows modeling of the macro characteristics of the devices in context of a logic element as opposed to device level computational modeling. By representing light intensity as voltage, “black box” models are generated that accurately represent the intensity response and logic levels in both technologies. By modeling the behavior at the systems level, one can incorporate systems design tools and a simulation environment to aid in the overall functional design. Each black box model of the SEED or gain competition device takes certain parameters (reflectance, intensity, input response), and models the optical ripple and time delay characteristics. These “black box” models are interconnected and cascaded in an encrypting/scrambling algorithm based on a study of candidate encryption algorithms. We found that a low gate count, cascadeable encryption algorithm is most feasible given device and processing constraints. The modeling and simulation of optical designs using these components is proceeding in parallel with efforts to perfect the physical devices and their interconnect. We have applied these techniques to the development of a “toy” algorithm that may pave the way for more robust optical algorithms. These design/modeling/simulation techniques are now ready to be applied to larger optical designs in advance of our ability to implement such systems in hardware.

[this page left intentionally blank]

Table of Contents

1. Introduction

As existing transport networks evolve into intelligent all-optical networks, end-to-end connections are beginning to look like virtual fibers. The elimination of optical-electrical-optical (OEO) conversions within network equipment allows for a vast increase in network capacity due to enabling technologies such as dense wavelength division multiplexing (DWDM). This is an important trend for Sandia and the DOE complex due to the increasing need to interconnect high performance computing and visualization platforms, often in a "network protocol agnostic" fashion. However, as signaling and switching technologies progress towards an all-optical architecture, network encryption technology, which remains in the electrical domain, fails to keep pace. Because network encryption is paramount to the Sandia/DOE mission, the lack of encryption mechanisms for all-optical networks seriously limits our ability to utilize these exciting new technologies and to reach bit rates currently not viable under electronic methods.

Over the past five years, Sandia has been developing all-optical devices that perform Boolean logic functions on optical inputs and produce optical outputs without intermediate electrical conversion. These all-optical logic gates are built upon two distinct technologies – self electro-optic effect devices (SEED) and gain competition technologies. These devices form logical building blocks suitable for a designing a photonic encryptor. However, optical logic gates are just now maturing into a state of discrete operation and have yet to be demonstrated in monolithic arrangements and present a few limitations (e.g., limited cascade depth, fanout, etc.) when applied in an encryption algorithm.

We are developing a technically feasible design for a photonic encryptor that is based on a simple, but useful encryption algorithm that can be built within the limitations of the SEED and/or gain competition devices. The encryptor will be able to process an optical data stream with known characteristics and will exhibit scaling properties to bit-rates unreachable through traditional OEO methods. By designing a set of Boolean logic elements with all optical logic, we can use them in conjunction with low gate count encrypting/scrambling algorithms to demonstrate an all-optical encryptor. Because there is no known software that can model these devices at a circuit level, we have modeled the functionality of the SEED and gain competition devices in an optical circuit in PSpice. PSpice allows us to model macro characteristics of the devices in context of a logic element as opposed to device level computational modeling.

This project has examined cryptographic algorithms in detail and determined innovative implementation approaches that can be implemented within the constraints of current optical logic gate technology. In addition, novel encryption approaches that utilize other photonic properties (e.g., dispersion, polarization, etc.) that may be modulated by these devices are also being explored.

As of the end of FY03, we are currently modeling the devices in PSpice as well as investigating novel low gate count algorithms. Items for FY04 include cryptographic synchronization and generating a library of logic elements (both SEED and gain competition) that can be applied to our experimental "toy" encryption algorithm. Future work may apply the lessons learned from these activities to larger, more complex optical systems.

2. Photonic Encryptor Usage

Figure 1 shows the photonic encryptor designed under this project, and how it fits into a generalized photonic network architecture.

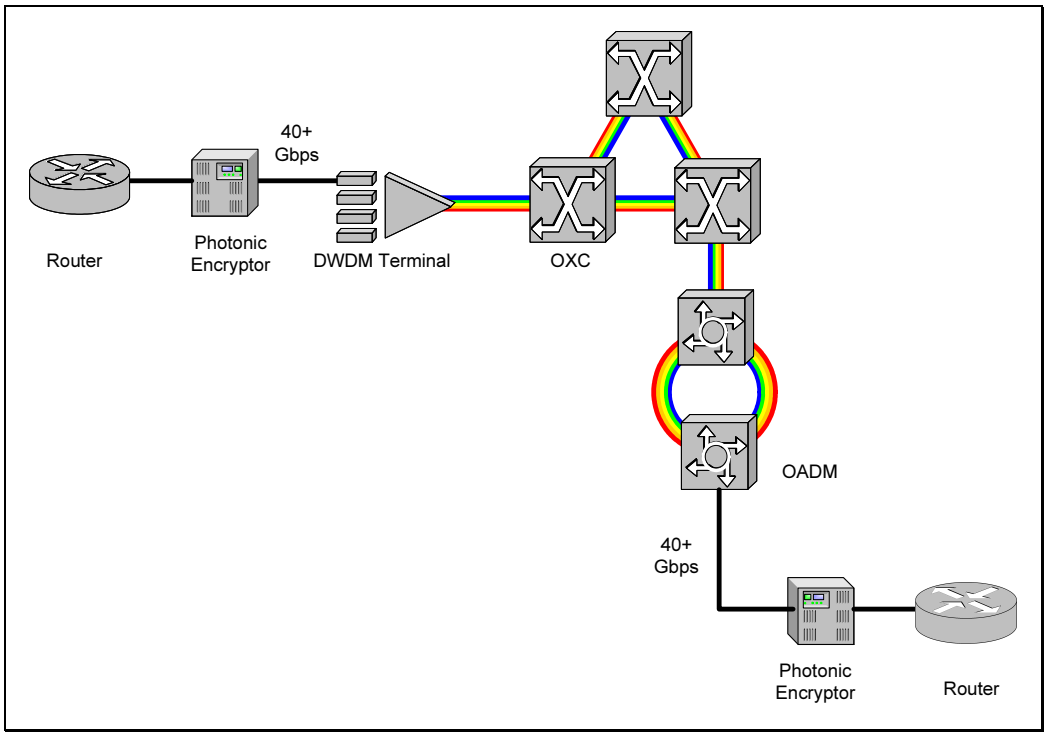

Figure 1: Photonic encryptor placement in all-optical network

In general, a photonic network may consist of the following components:

- **Dense Wave Division Multiplexer (DWDM)**
  This device takes multiple inputs with known wavelengths and framing protocols, wavelength-converts the inputs, and multiplexes the converted wavelengths onto a single fiber. These devices are typically connected to each other via a single, point-to-point connection.

- **Optical Add-Drop Multiplexer (OADM)**
  This device takes a single input with known wavelength and framing protocol, wavelength-converts it, and multiplexes the converted wavelength onto a single fiber that carries other wavelengths. In the de-multiplexing direction, this device isolates a single wavelength from a collection of wavelengths and converts it to a specified wavelength on the output interface. These devices are typically connected to each other in a ring topology.

- **Optical Crossconnect (OXC)**
  An OXC is an all-optical switch. As such, it isolates a wavelength on its input port, wavelength-converts it, and multiplexes it onto the output port. These devices can be interconnected in an arbitrary mesh.

The photonic encryptor designed in this project operates on a single wavelength with known framing protocol, as shown in Figure 1. Therefore, it is meant to connect to the input/output of a DWDM terminal

or an OADM. Although techniques for broadband (multi-wavelength) encryption were considered, they were rejected for the following reasons:

- Asynchronous key stream and data stream. In general, the data channels on each wavelength in a WDM network are not synchronized with each other. Therefore, a single key stream that would encrypt all wavelengths at once would be asynchronous with the data on all of the wavelengths. This is a departure from conventional cryptographic techniques, in which the key stream is synchronous with the data stream, and could present cryptanalytic challenges that this project is not prepared to accept.

- Possibility for sub-rate encryption. Encryption of an arbitrarily formatted data stream with unknown bit rate could lead to a situation where the bit rate of the data stream is faster than the bit rate of the key stream. This results in re-use of key stream, which is taboo from a cryptanalytic perspective. This situation is likely for broadband encryption, as devices that can switch or operate on multiple wavelengths (e.g., micro-mirrors) are typically too slow to switch at the rates required for encryption of 40+ gigabits per second.

- Wavelength constraints of photonic logic. Although other devices (e.g., micromirrors, chaotic mode-locked lasers, etc.) were considered, the speed requirements for this project called for the use of photonic logic. However, these devices operate at fixed wavelengths (usually 850 nm).

For the reasons listed above, the encryptor is designed to operate on a single wavelength with known protocol. Furthermore, the encryptor is designed to transparently pass an optical path [1]. However, the optical framing protocol that is encrypted might have overhead information (e.g., for OA&M purposes) that must bypass encryption. If so, then techniques such as those developed for optical label swapping can be used to suppress encrypted headers and substitute plaintext header information [2]. Other techniques for processing optical headers are also possible [3].

Although the single wavelength with known protocol restriction may appear to limit the encryptor's usefulness in photonic networks, it is actually a realistic configuration that would have interesting application in high speed communications. One can easily envision subscribing to a carrier's wavelength service, where the framing protocol and rate are known, but are beyond the capabilities of today's electrical domain encryption devices. By implementing photonic encryption at the point of presence, bulk encryption can be realized. Furthermore, it is expected that the techniques developed for photonic encryption will facilitate scaling of encryption data rates more readily than today's electronic implementations.

3. Overview of S-SEED Device Performance and Logic

The symmetric self electro-optic effect device (S-SEED) is a bistable device consisting of two diodes in series with a constant bias voltage set across the two diodes, as shown in Figure 2. The two states are characterized by having about zero volts across one diode and the remaining voltage across the other and vice versa. The absorption of each photodiode depends upon the voltage across it, and therefore the state of the S-SEED is transferred to the incident equal power optical pulses through differential absorption. These equal power optical power pulses are the clock pulses that read out the state of this S-SEED. The resulting beams, with unequal power, can be used as inputs to another stage of S-SEEDs. The two states of the S-SEED are set with a larger power beam on either diode A or B.

Related Sandia work[1] has demonstrated an 865-nm S-SEEDs having a switching time of about 7 ps, and that a design for 1550-nm S-SEEDs shows promise for similar behavior. Sandia has demonstrated that the 865-nm S-SEEDs can be cascaded so that the output of one S-SEED can drive the input of another. The design included an additional S-SEED and performed an XOR logic function with three S-SEEDs. We are currently pursuing methods for interconnecting S-SEEDs at the wafer level. Our primary thrust is to use diffractive optic lenses on a fused-silica substrate mated to the SEED substrate. Efforts have also begun to accomplish monolithic integration by using GaAs waveguides grown beneath the SEED active region.

Described below are some results in measuring sweep-out time of 1550-nm SEEDs, cascading 865-nm S-SEEDs, performing an XOR logic function, and designing a diffractive optic interconnect experiment.

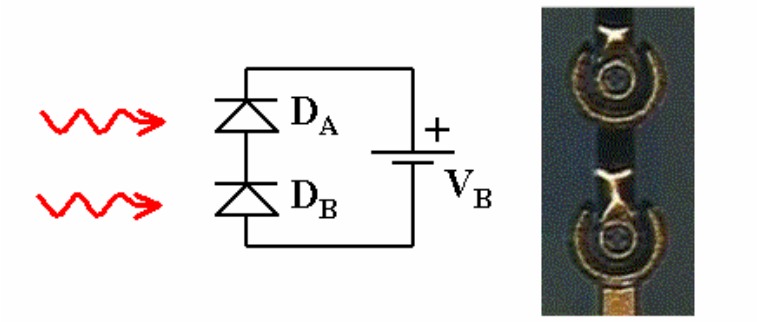

Figure 2: Symmetric self electro-optic effect device (S-SEED). A constant bias voltage, V_B, is placed across two diodes in series. The system is bistable in that an optical beam incident on either diode will experience either low or high absorption depending on the state. The image on the right shows a fully processed S-SEED.

[1] This work is supported by the Department of Defense through grant EAO MOD 706897.

3.1. Carrier Sweep-out Time Measurements of 1550-nm SEEDs

The carrier sweep-out time is roughly the sum of the carrier escape time from the quantum wells and the carrier drift time across the nominally undoped MQW region. The goal of carrier sweep-out measurements is to verify that the carrier escape time from the extremely shallow quantum wells is short, consistent with rapid LO phonon excitation out of the wells. If the wells are too deep, the LO phonon energy will not be sufficient to excite carriers out of the wells, and the escape time will be limited by a relatively slow tunneling rate. We have measured the sweepout time for our 1550-nm SEEDs to be as low as 2.4 ps, which suggest that the wells are shallow enough for rapid carrier escape.

The epitaxial layers were deposited by MOCVD onto an InP substrate. For electrical contact, n-type and p-type layers were grown above and below the intrinsic (undoped) MQW region. The intrinsic region is 0.5- m thick and is filled with extremely shallow quantum wells (25 pairs of 10-nm $In_{0.53}Ga_{0.435}Al_{0.035}As$ wells and 10-nm $In_{0.53}Ga_{0.365}Al_{0.105}As$ barriers).

We performed a pump-probe measurement using a mode-locked Erbium-doped fiber laser that delivers approximately 500 fs pulses at a repetition rate of 15 MHz. The pump pulse energy was roughly 3 nJ. The probe pulse (attenuated to have about 2% of the pump pulse energy) was delayed relative to the pump pulse using a translation stage and the transmission of the probe pulse was measured as a function of this delay time. A constant reverse bias was applied to the upper and lower metal contacts of the SEED using electrical wafer probes.

Figure 3 shows the responsivity of a 1550-nm SEED as a function of wavelength for different reverse bias voltages. Note that near 1550 nm, the absorption at the exciton resonance wavelength decreases with increased reverse bias voltage, which is essential for proper S-SEED operation. The SEEDs are designed with extremely shallow quantum wells that permit the exciton feature at 1550 nm to exist at room temperature, yet allow for ionization of the exciton at relatively low bias voltages.

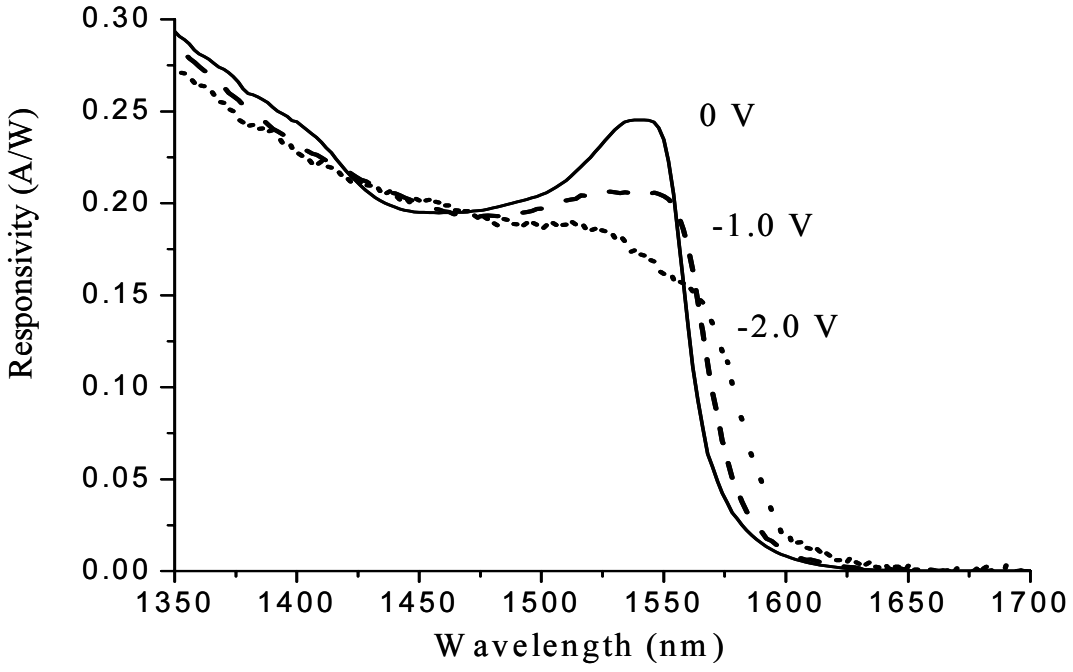

Figure 3: Responsivity of a 1550-nm InAlGaAs SEED as a function of wavelength for various bias voltages. Increased reverse bias leads to the ionization of the exciton resonance near 1550 nm.

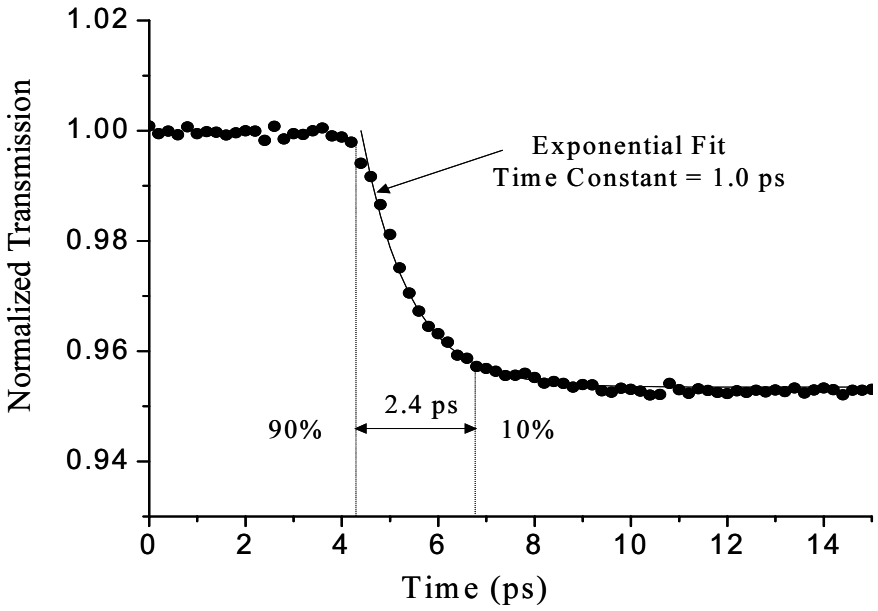

Figure 4: Normalized probe transmission as a function of time. The transmission decreases when carriers are swept out of the active region and temporarily screen the applied field, restoring the exciton absorption peak. The change in transmission can be fit with an exponential decay with a time constant of 1.0 ps. The change from 90% to 10% occurs in 2.4 ps.

The sweepout measurement result for an applied reverse bias of 3.0 V is shown in Figure 4. The pump pulse arrives at about 4.0 ps, at which point the transmission begins to decrease. The change in transmission corresponds closely to an exponential decay with a time constant of 1.0 ps. The 90% to 10% transition occurs in 2.4 ps. Results were similar for lower applied reverse bias voltages, but showed reduced contrast.

3.2. Cascading of Discrete S-SEEDs at 865 nm

We have demonstrated cascadeability (the output of one device driving the input of a second device) of 865-nm S-SEEDs using VCSELs and free-space optical connections. Figure 5 shows the experimental layout. The VCSELs were imaged onto the S-SEEDs in a one-to-one imaging configuration. The two SEEDs of each S-SEED and the two VCSELs of each VCSEL pair were spaced 250 microns apart and oriented horizontally, as illustrated in the inset of Figure 5. VCSELs 1A and 1B were alternately pulsed and acted as the set and reset optical pulses driving S-SEED 1. The drive current for VCSELs 2A and 2B was adjusted until the output power levels from these two VCSELs were equal. These “clock” VCSELs 2A and 2B were pulsed simultaneously and synchronized to arrive after the set pulse from VCSEL 1A and again after the reset pulse from VCSEL 1B. The reflected clock pulses returned to the polarizing beamsplitter (PBS) with opposite polarization due to the double pass through the quarter wave plate (QWP).

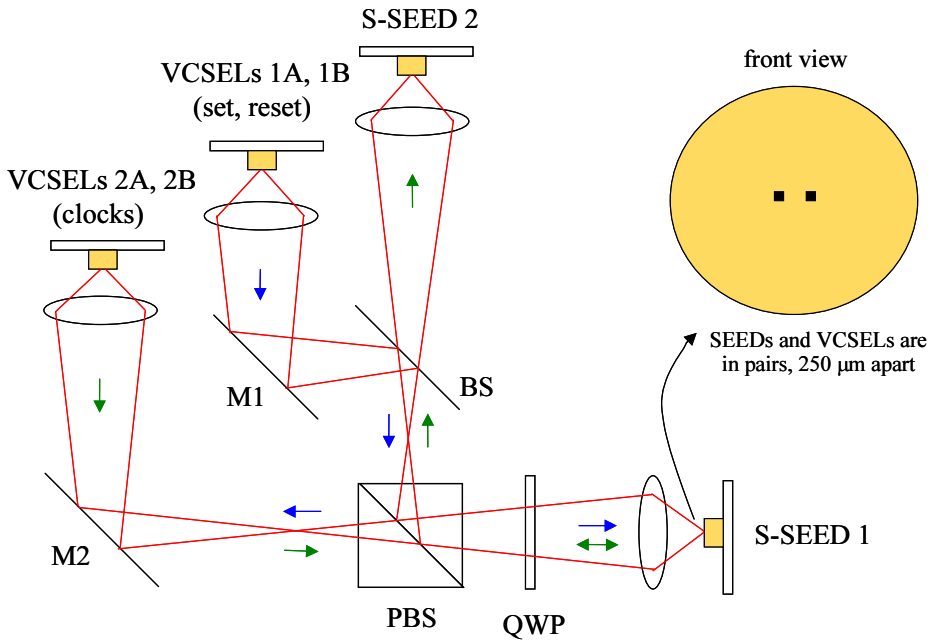

Figure 5: Cascaded 865-nm S-SEED experimental layout. Pulses from VCSELs 1A and 1B set and reset, respectively, the state of S-SEED 1. Simultaneous equal-power clock pulses from VCSELs 2A and 2B read out the state of S-SEED 1 and become inputs to S-SEED 2. In this arrangement S-SEED 2 is forced to follow the state of S-SEED 1 (with an inversion). The following abbreviations are used in the figure: M1 = mirror 1, M2 = mirror 2, BS = beam splitter, PBS = polarizing beam splitter, QWP = quarter-wave plate.

The reflected clock pulses from S-SEED 1 traveled to S-SEED 2 and acted as inputs that set its state. Since the pair of beams actually constitutes only a single differential input, it simply forces S-SEED 2 to switch to the current state of S-SEED 1 (with an inversion). These processes are described in more detail below and are illustrated with waveforms at various test locations.

Successful cascading of the two S-SEEDs is indicated in Figure 6, where the blue trace corresponds to the internal voltage of S-SEED 2. The 30% difference between the input pulse energies was sufficient for switching the state of S-SEED 2. However, the switching is slower for S-SEED 2 than for S-SEED 1 because the difference in the pulse energies of the two inputs was less than the total pulse energy in the set or reset pulses on S-SEED 1. Also, further losses were experienced due to imperfect alignment of the input pulses onto SEEDs 2A and 2B.

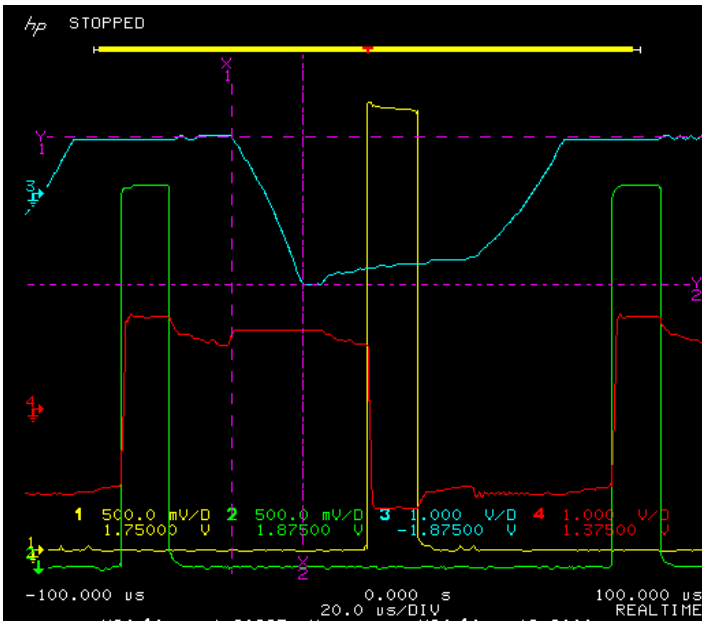

Figure 6: Oscilloscope image of the internal voltage of S-SEED 2 (blue) showing its state switching due to the reflected clock pulses from S-SEED 1 acting as inputs to S-SEED 2, indicating cascading of two S-SEEDs. The red trace indicates the switching of S-SEED 1. The green and yellow traces indicate when the set and reset pulses are incident on S-SEED 1A and 1B, respectively. The purple vertical dotted lines bracket the time period in which the inputs to S-SEED 2 are incident.

3.3. XOR Logic Gate Demonstration

We have added an additional S-SEED to create an exclusive OR (XOR) gate. In this demonstration, outputs from two S-SEEDs were combined as inputs to a third S-SEED as shown in Figure 6. In the cascading demonstration described above, S-SEED 1 acted as a set/reset flip flop, and S-SEED 2 acted as a single-input inverter. The XOR gate is far more complex and interesting because it requires AND/NAND and OR/NOR gates with two inputs each. Moreover, the two inputs to the third S-SEED gate come from the previous two S-SEED gates, so cascadeability is demonstrated in a much more rigorous fashion.

The table in the lower right in Figure 7 demonstrates the timing scheme used in our S-SEED optical logic. In the first time slot, the first stage is preset to act as NAND or NOR gates. In the second time slot, inputs are incident on the first stage as the second stage is preset. In the third time slot, the state of the first stage is read out with clock pulses and these pulses act as inputs to the second stage. The sequence then repeats and cascades to subsequent stages.

The oscilloscope waveforms demonstrating the XOR logic function are shown in Figure 8. The voltage drive pulses for Inputs 1A and 2A are included to indicate the value of the inputs. Recall that we are using differential logic, where 1A=high/1B=low (beam 1A is on and beam 1B is off) refers to a “1” and 1A=low/1B=high (beam 1A is off and beam 1B is on) refers to a “0”. The third and fourth waveforms, labeled “S-SEED1” and “S-SEED2”, correspond to the voltage at the midpoint of the S-SEED and indicate the logic function performed by the two S-SEEDs in the first stage. These show that the OR and AND functions were performed correctly. The “Clocks” waveform shows the time at which the clock pulses read out the states of S-SEEDs 1 and 2 and set the state of S-SEED 3. The last waveform shows the voltage at the midpoint of S-SEED 3, indicating that the XOR function was performed correctly.

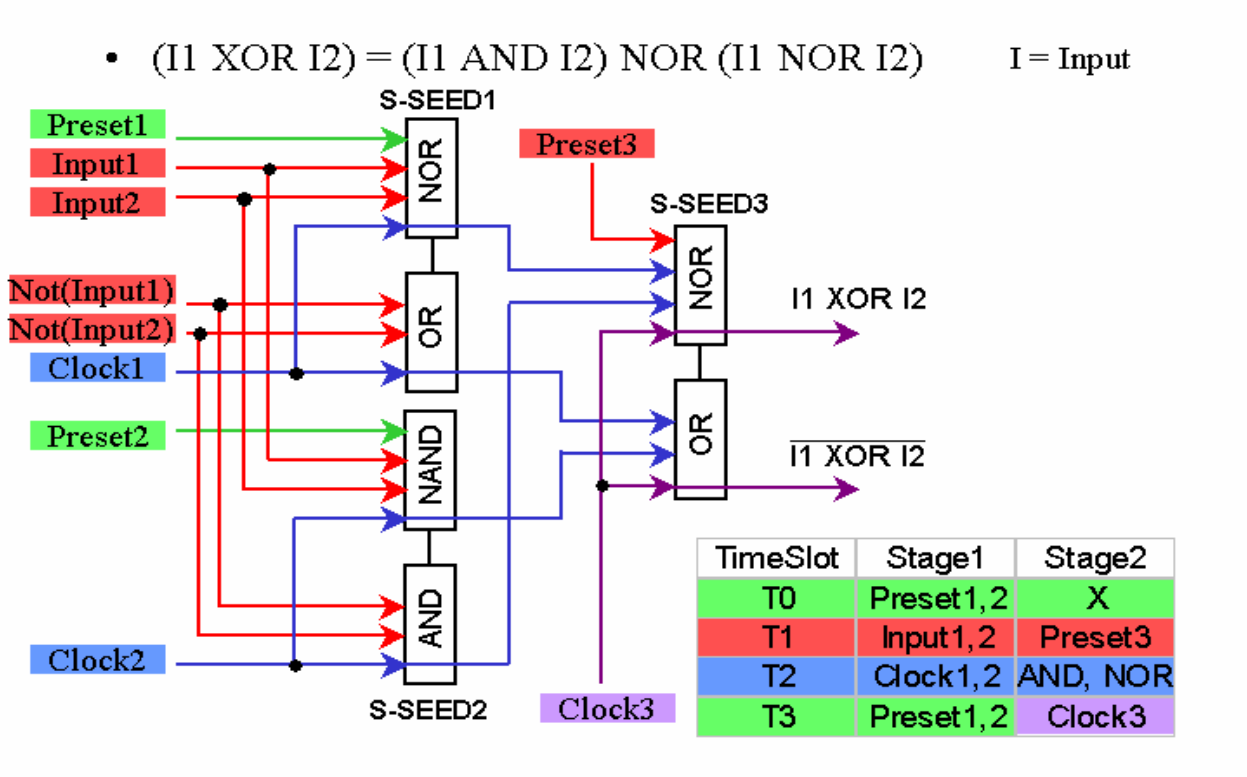

Figure 7: Diagram of the optical inputs and outputs used to demonstrate an XOR gate. The XOR function contains 3 S-SEED logic gates and involves the NOR of the AND and NOR of two input beams, I1 and I2.

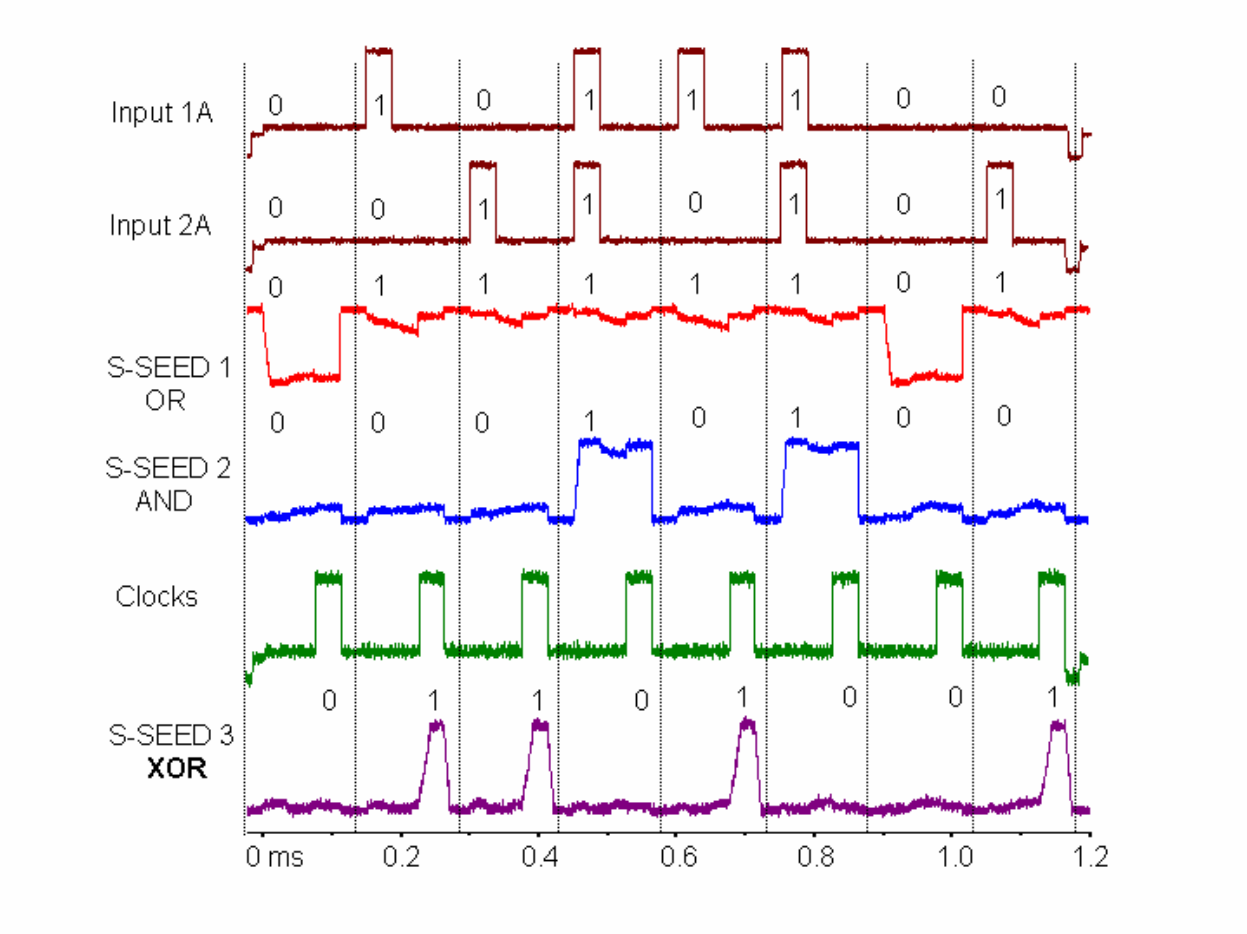

Figure 8: Oscilloscope waveforms demonstrating the XOR function. The OR and AND functions are performed when Inputs 1 and 2 are both incident on S-SEEDs 1 and 2. The Clock pulses indicate the time at which the states of S-SEED 1 and 2 are read out and the state of S-SEED 3 is set, performing the XOR function.

3.4. Substrate-Mode Microoptic Interconnects

In order to make S-SEED based logic into a useful technology, we need to demonstrate that we can optically interconnect devices using a wafer-scale fabrication technology in order to realize a true optical integrated circuit (OIC). The pursuit of OICs has been going for over 20 years and progress has been slow because of the great difficulties involved. Nonetheless, there have been successful demonstrations of small OICs containing relatively few components, and progress has recently accelerated due to improvements in microfabrication technology. While we have considered various approaches, we have focused mainly on using diffractive-optic based substrate-mode interconnects.

A substrate-mode interconnect is achieved using a transparent optical substrate, such as fused silica, within which each light beam bounces off the top and bottom surfaces repeatedly at roughly a 30-degree angle, thereby traveling in a zig-zag path in order to achieve a net horizontal displacement within the optical substrate. This optical interconnect substrate is attached above an active SEED wafer, and a microoptic lens on the bottom surface of the optical substrate couples reflected light from one SEED into the optical substrate, where it undergoes substrate-mode propagation to a second SEED, and a microoptic lens focuses the beam down onto the second SEED. A very simple substrate-mode optical

interconnect between 2 SEEDs is schematically depicted in Figure 9. Figure 9 also shows how the substrate-mode approach can readily handle inputs from and outputs to external optical fibers.

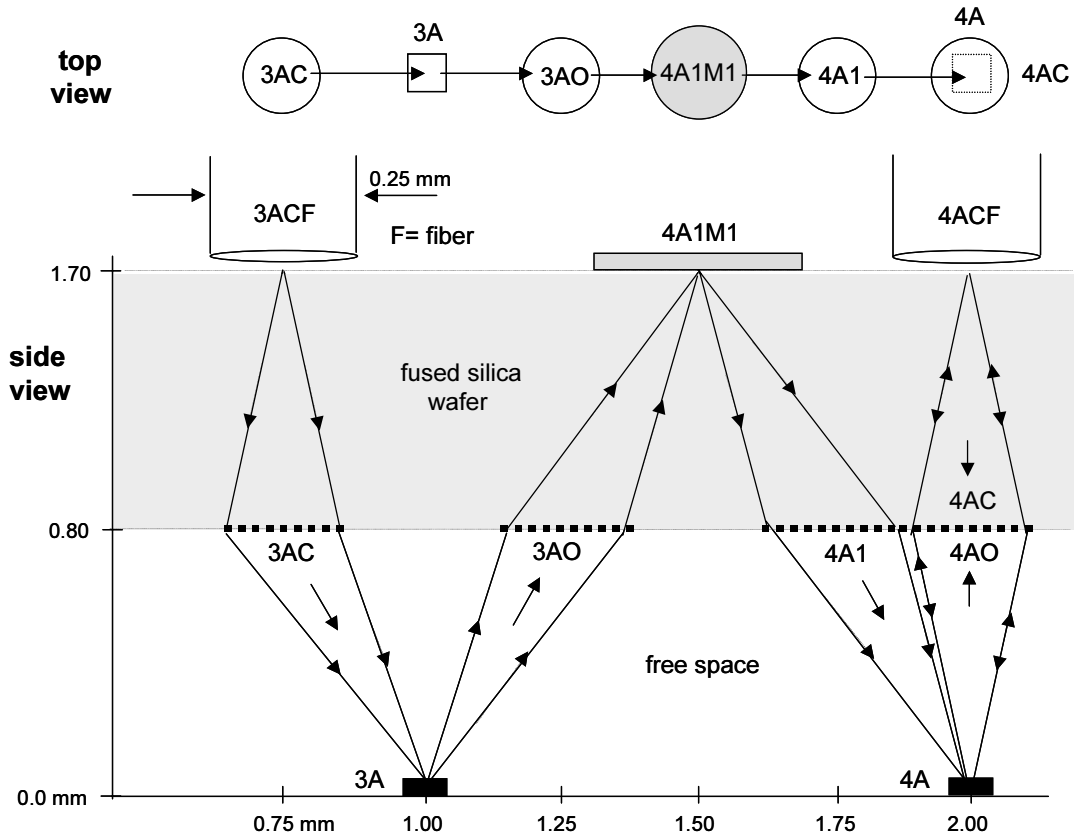

Figure 9: Full substrate-mode interconnect between two SEEDs. In order to simplify the design and fabrication, a single fiber 3ACF is used to carry both the logic input 3A1 and the clock input 3AC, which are distinguished only by their temporal positions.

We have designed simple substrate-mode interconnects and test structures to characterize their performance. We decided to do the initial fabrication and experiments using 865 nm SEEDs, because it is much easier to "see" the beams and do alignment of the substrate-mode optics using silicon-based CCD cameras, which only work up to a wavelength of 1100 nm. Fused silica is the optical substrate that we have the most fabrication experience with and it is transparent at any wavelength of interest for this project.

We are currently measuring the efficiencies of the diffractive optic lenses as well as constructing a set-up to mate together a 2x12 fiber array with the diffractive optic lens array and S-SEED devices. Future experiments will be performed to demonstrate interconnection of 1550-nm S-SEEDs. Goals for the future include increased functionality, such as an XOR gate, as well as high speed (50 to 100 Gb/s). The end goal is to increase the number of logic gates so that more sophisticated optical logic can be performed at high speed.

The simplest functionality implemented by an S-SEED pair is to invert. A single differential optical input on the S-SEED pair followed by equal power clock/read outs is needed to invert a signal. This arrangement uses two time slots to effectively deliver one logic cycle. Figure 10 shows the inverter implementation and Figure 11 describes the timing needed.

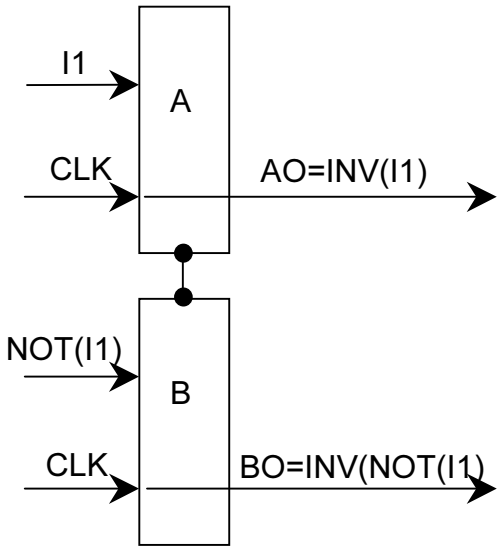

Figure 10: Inverter Implementation

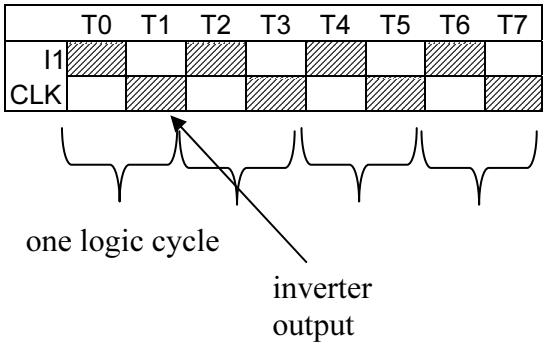

Figure 11: Timing Diagram for SEED inverter implementation

The buffer as implemented with SEED logic is shown in Figure 12. A buffer consists of two SEED pairs cascaded with output of the first pair fed into the input of the second pair. It is essentially an invert operation followed by another invert operation. Figure 13 shows that three time slots are required to perform the buffer functionality.

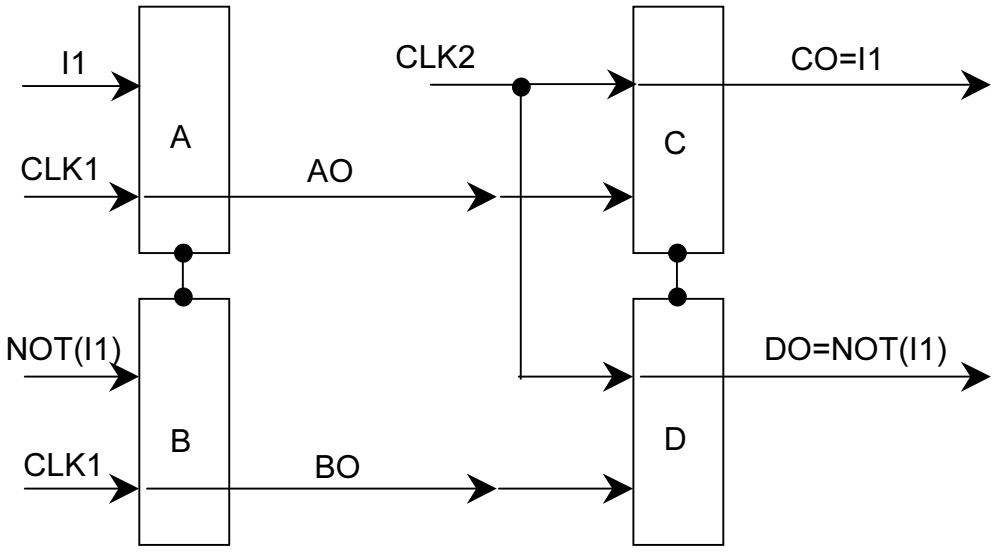

Figure 12: Buffer Implementation

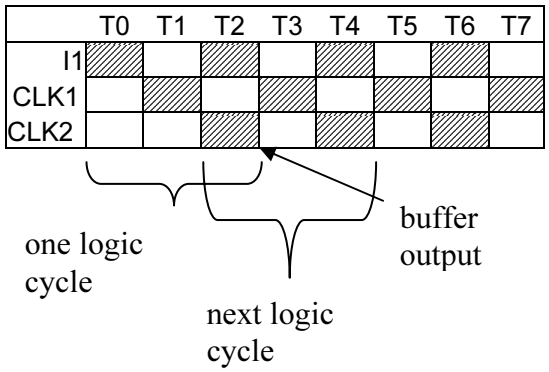

Figure 13: Timing Diagram for SEED buffer implementation

Using the building blocks (XOR, NAND, AND, OR, NOR, buffer, inverter) designed with SEED logic technology, we can build optical logic circuits to demonstrate a scrambler/encrypting algorithm.

4. PSpice modeling of S-SEED

4.1. PSpice Model

Our PSpice Model is similar to the Advice model presented by Lentine [5]. Like Lentine, a fifth order polynomial has been used to characterize the optical absorption of the p.i.n diode as a function of reverse bias voltage. However, Lentine chose to characterize the device as a three terminal device, with the diode terminals (cathode and anode) being two terminals and the third being the optical input. The PSpice model presented here characterizes the SEED as a four terminal device, two electrical and two optical. From the standpoint of the simulator, all terminals are electrical. The optical inputs and outputs are simply ideal electrical terminals where 1 V electrical potential is equivalent to 1 W optical power at the device.

4.2. Diode Electrical Model

The PSpice model is shown in Figure 14. The basic p.i.n. photodiode is modeled by a capacitor and parallel current source, G1. A lookup table is used to model the current versus voltage characteristic of the device (see Table 1). These values were taken from measured data. As can be seen in Figure 15, the piece wise linear model does a fair job of modeling the complex curve.

The diode model also contains a series resistor and series inductor whose values were derived experimentally. [6]

4.3. Responsivity Curves

The photoelectric currents are generated by each of the four beams that shine on the device. A and B are logic inputs, C is the clock input and P is the preset input. The gain for each is light input is modeled by a linear fit where the responsivity in the discharged state (approximately -0.5 V reverse biased) is .45 A/W and in the charged state (approximately +1.5 V reverse biased) is .35 A/W. The resulting line is shown in Figure 16 and the linear fit equation is

$$\mathrm{Re}s = .425 = .05V_r .$$

4.4. Reflectivity Curve

The reflectivity varies with the diode reverse bias voltage and can be represented quite accurately by a fifth order polynomial. This curve has been fitted to digitized data from an actual device. The data is given in Table 2. The equation is given by

$$R = 5.72 + 2.06X + .28X^2 - .665X^3 + .042X^4 + .057X^5 .$$

4.5. Gate Operation

The data is read out using a clock beam, C. The output light, Z, is determined by multiplying the incoming light level by the reflectivity value, R.

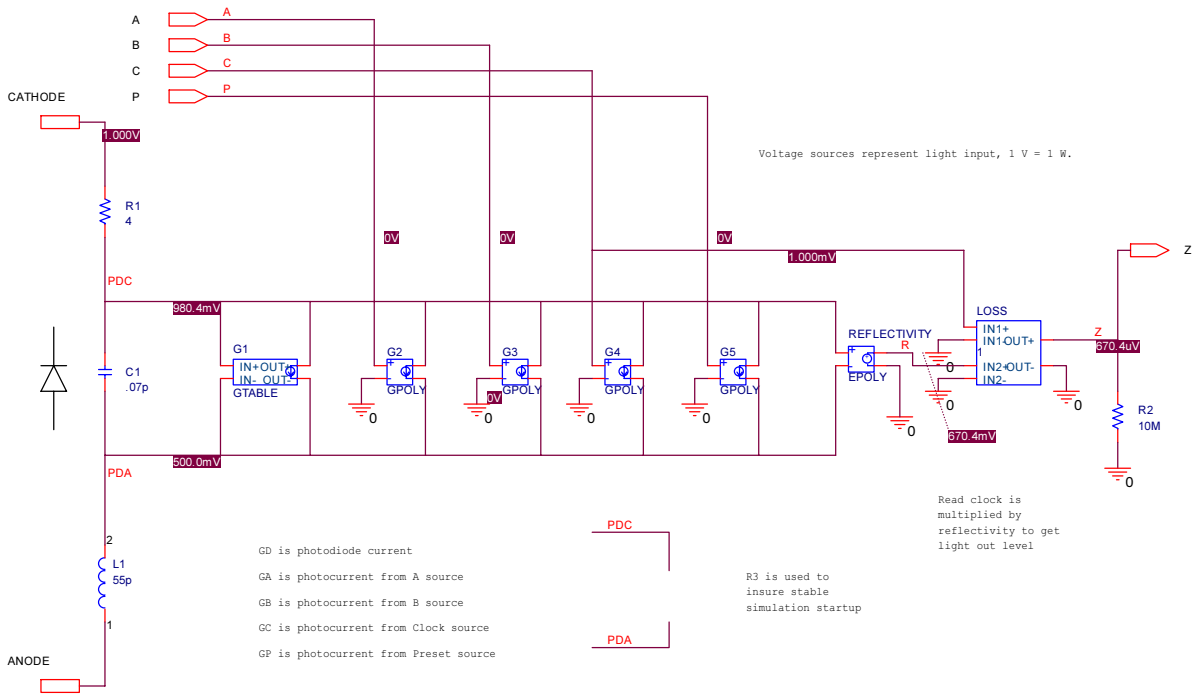

Figure 14: Schematic of SEED model.

Table 1. Measured SEED current versus voltage for input to model.

Reverse Voltage (V)	Reverse Current (mA)
-0.8254	0
-0.8254	0.80851
-0.824	1.617
-0.80952	2.2979
-0.79365	3.3191
-0.78	3.7021
-0.75603	4.0851
-0.74016	4.4255
-0.71828	4.7234
-0.71428	4.9362
-0.66667	5.1489
-0.63492	5.234
-0.60317	5.2766
-0.53968	5.3191
-0.47619	5.3191
-0.44444	5.2766
-0.39682	5.234
-0.25397	5.1489
-0.031745	4.9362
0.19048	4.766
0.44445	4.5106
0.66667	4.3404
0.90476	4.1702
1.1429	4.0426
1.3651	3.9574
1.6825	3.9149
1.9841	3.8723

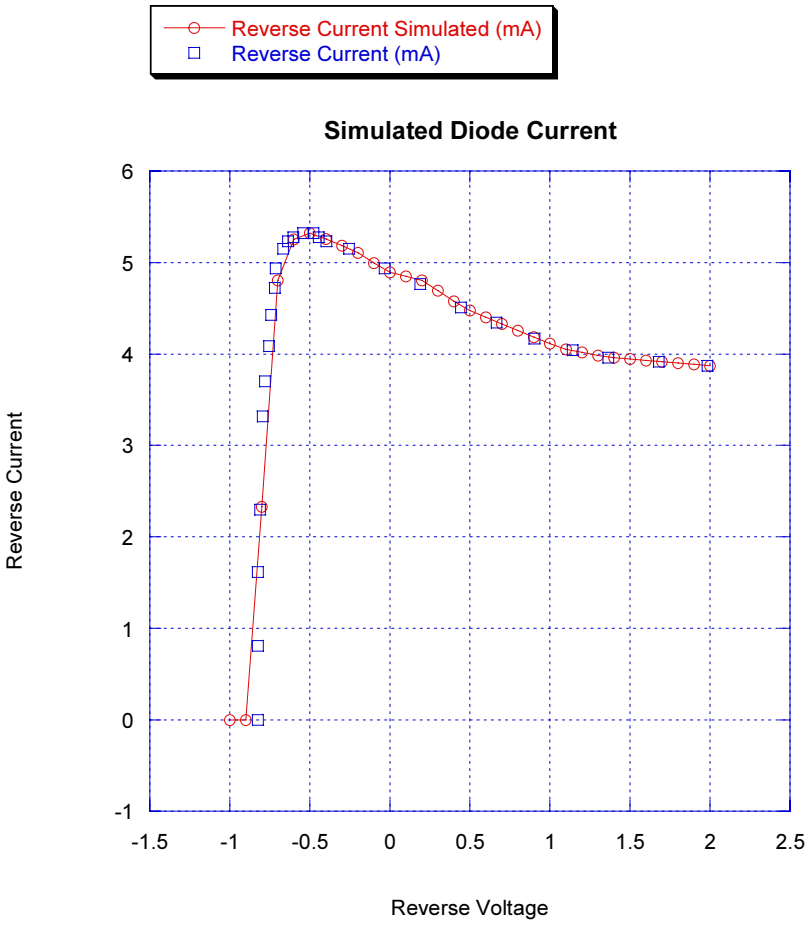

Figure 15: Simulated vs. measured p.i.n. diode current.

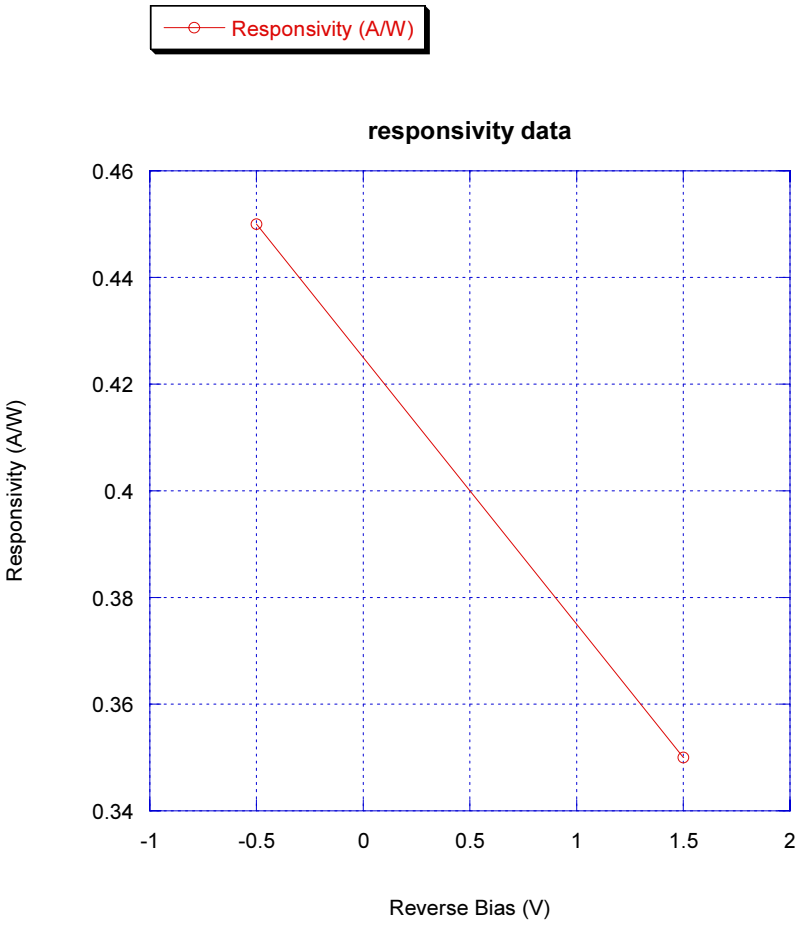

Figure 16: Responsivity curve.

Table 2. Measured reflectivity versus reverse voltage data.

Reverse Voltage (V)	Reflectivity (a.u.)
-1.00000	4.5714
-0.88889	4.5714
-0.82540	4.6032
-0.69841	4.6667
-0.60317	4.7302
-0.49206	4.8571
-0.39682	4.9841
-0.31746	5.1111
-0.25397	5.2381
-0.15873	5.3651
0.015874	5.7460
0.15873	6.0317
0.20635	6.1587

0.28572	6.3492
0.39683	6.5714
0.50794	6.7619
0.60318	6.9524
0.68254	7.0794
0.76191	7.2063
0.87302	7.3333
0.98413	7.4603
1.1111	7.5873
1.2222	7.6825
1.3492	7.7778
1.4762	7.8413
1.6667	7.9365
1.8889	8.0635
2.0000	8.1270

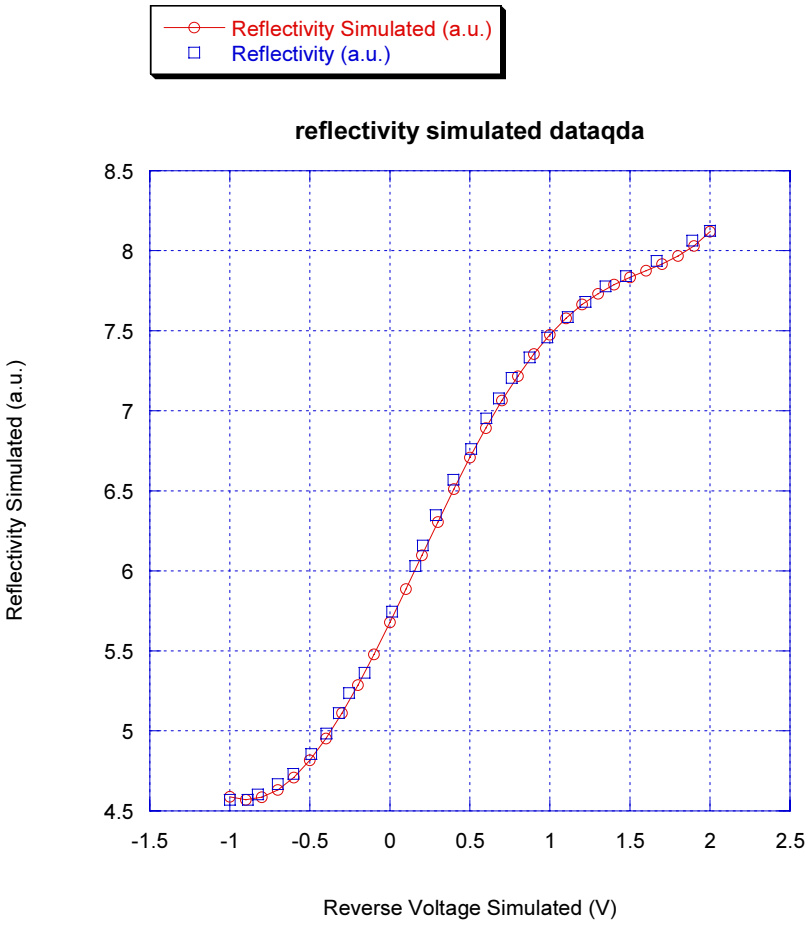

Figure 17: Reflectivity simulated data vs. measured.

5. S-SEED Switching Behavior

The switching characteristic of the S-SEED device was reported in a progress report [6]. The rise time of the S-SEED was 7ps with a settling time of over 75ps. The actual device is shown in Figure 18. The rise time was measured in Figure 19.

5.1. S-SEED Circuit

The circuit consists of two series SEED diodes (p.i.n. diodes are the two circular devices at the bottom of the picture) connected in parallel with a capacitor (the rectangular device at the top center of the picture) which was sized to provide transient current during switching. The two terminals were connected to a 1 V dc power supply. The PSpice schematic is shown in Figure 20.

5.2. Measurement Setup

The measured circuit has a train of light pulses, Pu1 and Pu2, which are shining on D1 and D2 respectively, at a 76 MHz rate. Pu1 and Pu2 are created from a common pump laser. Pu2 passes through a 1.8 meter delay line and arrives at the target delayed by 6 ns with respect to Pu1. Both pulses are vertically polarized by passing through a beam splitter. In operation, Pu1 discharges D1 and Pu2 discharges D2 6 ns later. In this way, the state of the logic gate is toggled continuously. The same beam splitter is used to create a horizontally polarized read signal, Pr1, which is itself delayed with respect to Pu1. The read signal is much smaller in intensity than either of the pulses so that it does not upset the state of the logic during the test. The read pulse is only applied to D2. The timing of these pulses is shown schematically in Figure 21.

5.3. Simulation Setup

The simulated circuit operates as follows. A 1 ps wide pulse, Pu2, is incident on D2 and discharges D2. The voltage across D2 approaches 0 V and, at the same time, the voltage on D1 approaches 1 V. A second 1 ps wide pulse, Pu1, is incident on D1 and discharges D1, thus switching the state of the circuit. The period between pulses is 200 ps. A constant read signal is applied to D2. The reflected output power of the circuit, POUT, is divided by the input power, Pr2, and scaled (by a factor of 10) resulting in a reflection coefficient measurement. The resultant waveforms are shown in Figure 22.

The output waveform has considerable ringing due to the series inductance in the device interconnect. By adjusting some of the model parameters, we can improve the device performance. For instance, if the series inductance is reduced from 55pH to 5pH, then the settling time improves from 100 ps to less than 10 ps. This also improves the rise time from over 5 ps to around 2 ps. There are two areas to target when reducing the series inductance in this experiment. First, the leads from the power supply probes can be shortened. Second, the interconnect between the two SEED devices can also be shortened. Building the circuit with an airbridge interconnect and widening the traces could lower the inductance.

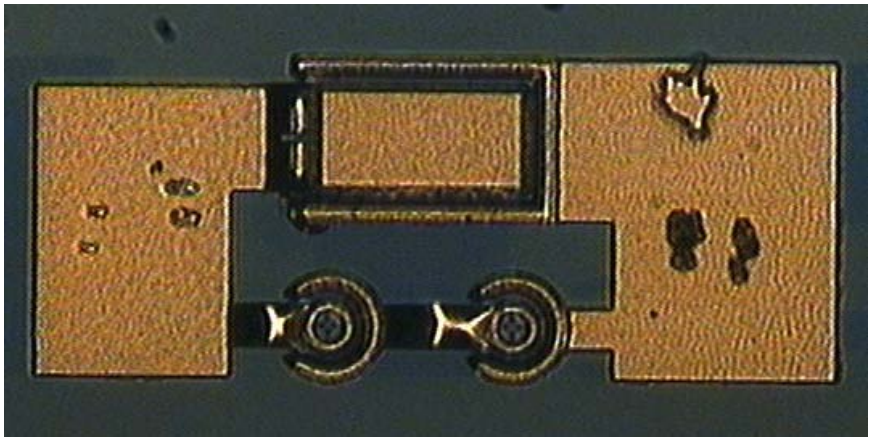

Figure 18: S-SEED photo.

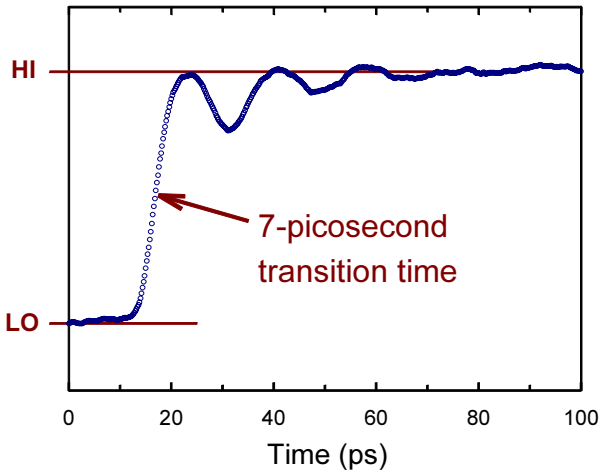

Figure 19: S-SEED switching characteristic.

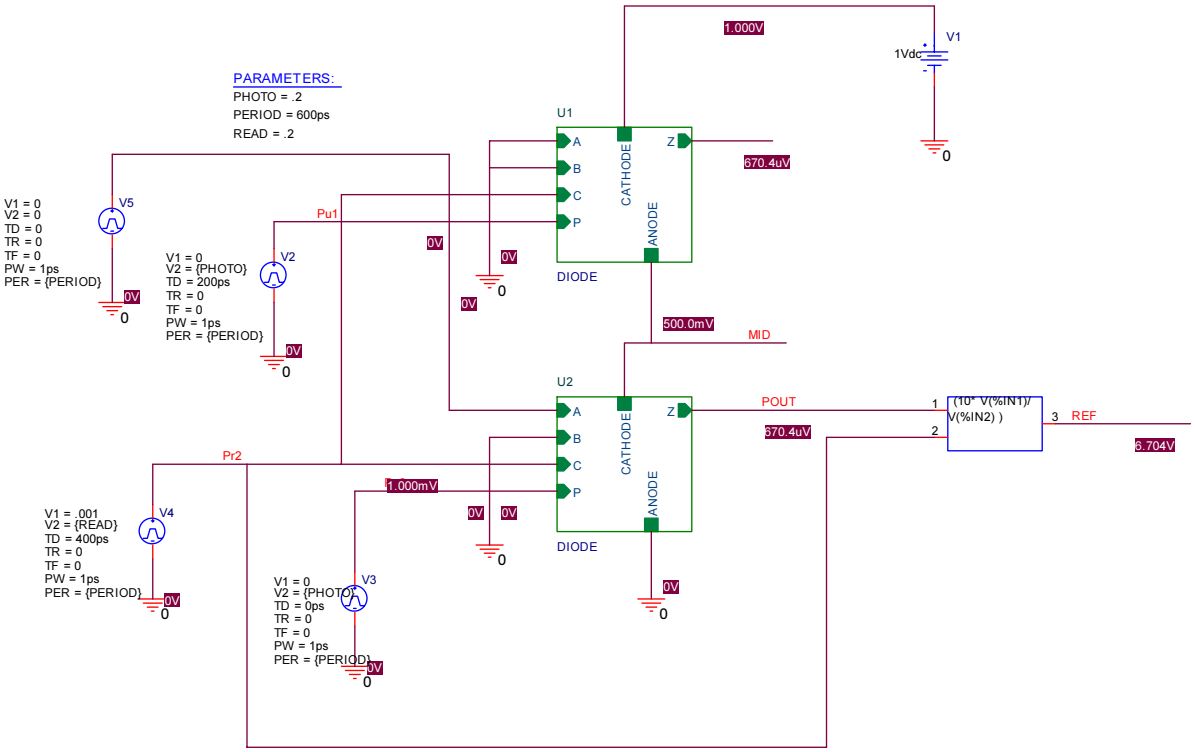

Figure 20: S-SEED switching speed PSpice circuit.

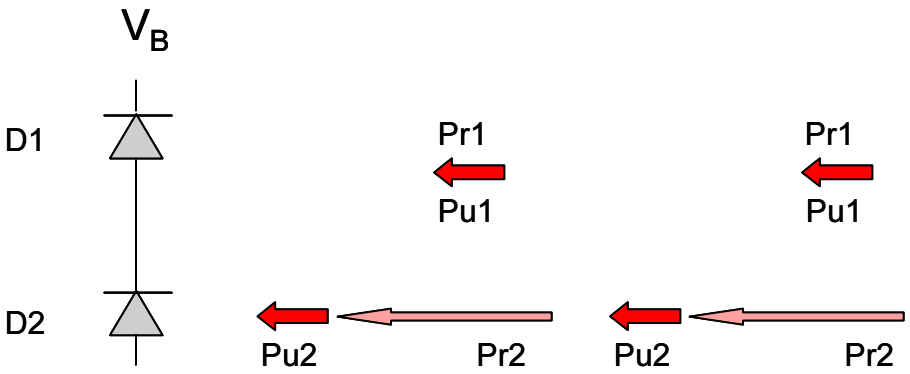

Figure 21: Pulse timing in S-SEED circuit.

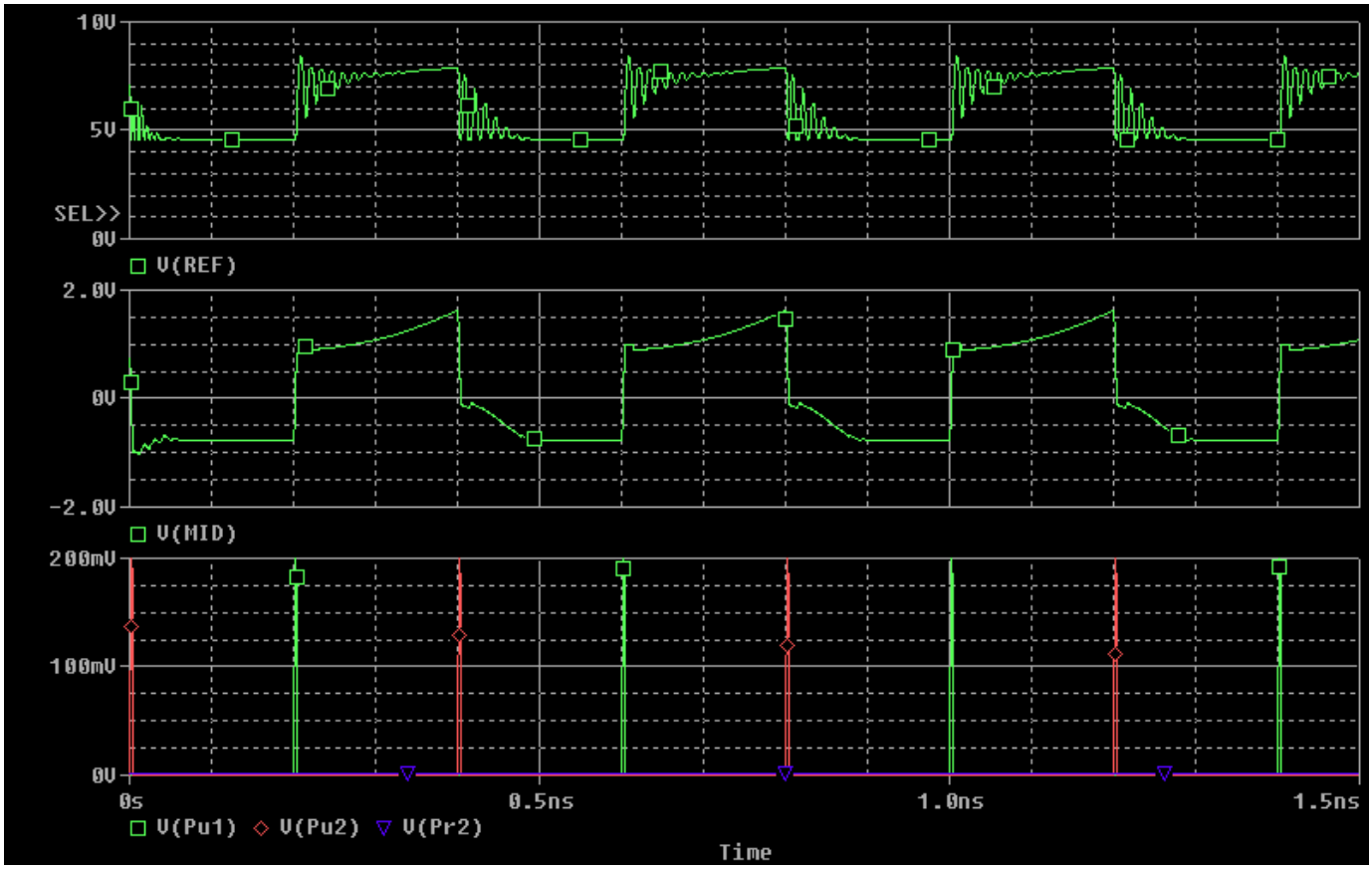

Figure 22: Switching speed simulation waveforms.

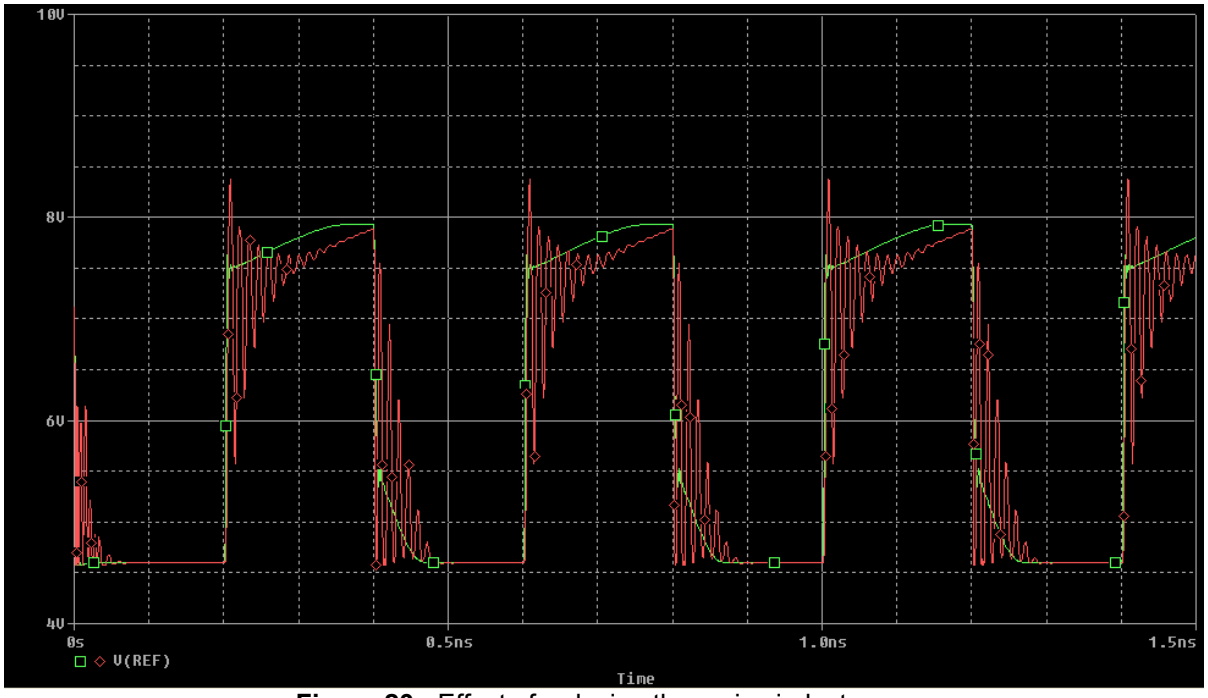

Figure 23: Effect of reducing the series inductance.

6. Characterization of the Optical Gate

Each digital logic gate will have a transfer characteristic and switching characteristic that describes the output waveform in terms of the input. In the case of the optical SEED logic gate it is more difficult to measure because the input and output signals are pulses of light. A series of simulations were used to measure the switching and transfer characteristics.

The simulation consist of an OR gate configuration (similar to Figure 26) with a single data input. The schematic is shown in Figure 24. The Preset input is used to discharge D1 (charging D2) and raising the voltage on MID. The data input, D, is pulsed to a maximum value which switches the gate and the magnitude of the output pulse is measured at POUT and POUTB during the clock pulse. The DB input (invert of D) has a maximum value that is .5625 * Dmax. This value represents the extinction ratio of the optical gate. The reflection of the clock input, C, is a function of the diode bias voltage ranging from a minimum of .45*C to .8*C. Since D is the true logic value, DB should be relatively dimmer by the extinction ratio.

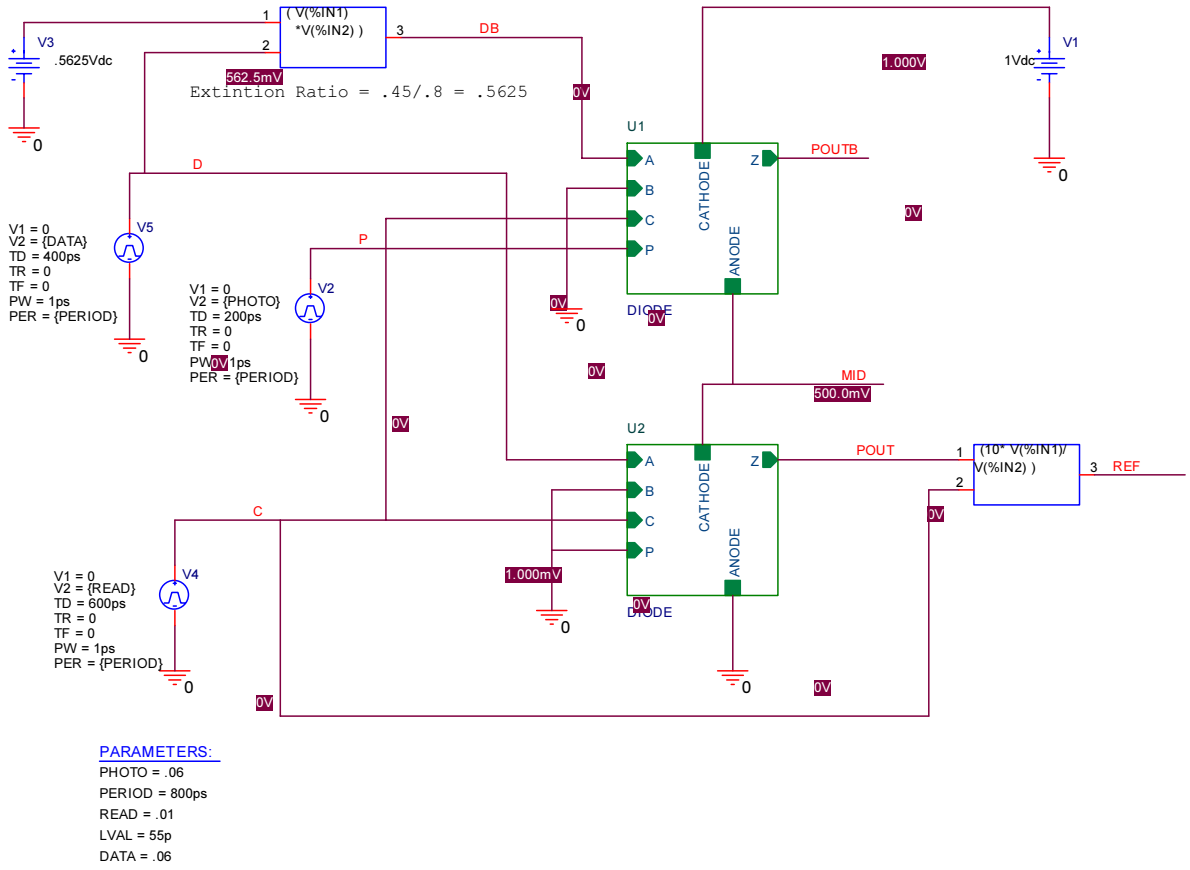

Figure 24: SEED Logic gate transfer characteristic schematic.

The circuit in Figure 24 was used to characterize the switching of the optical logic gate. The P input was used to alternatively switch logic states. The voltage on the electrical output MID varied from a high of 1.75V to a low of -0.75V. Depending on the amplitude of the input pulse, the signal exhibited overshoot. The input pulse was varied from .02 to .07 W and the rise/fall time of the pulse was measured. These values are given in Table 3. The goal was to find a pulse height that would generate just enough current to charge the alternate capacitor (of the diode) without having too much current and overcharging the capacitor. The result was that the 60 mW pulse appeared to have the fastest switching time without excessive overshoot exhibited with larger pulses. All pulses were 1ps in width. The switching

characteristic of the MID node for .06 W pulses is shown in Figure 25. This was the chosen pulse magnitude for future circuit design.

Table 3. Optical gate switching speed.

Pulse Height (mW)	Rise Time (pS)	Fall Time (pS)
20	no switch	no switch
30	no switch	no switch
40	100	100
50	33	32
60	23	23
70	20	20

Figure 25: NOR gate switching with .06 W pulses.

An actual logic input switches the gate differently than a preset pulse because the pulses are generated by previous logic gate for which the inverted and non-inverted outputs do not turn off completely. The low output is only 45% of the clock input while the high output is 80% of the clock input. An extinction ratio of about 56% is the result. Therefore, another series of simulations were performed to characterize the switching of the gates logic state by real optical inputs.

The resulting data from switching the gate using the D and DB inputs is given in Table 4. The characteristic of rise and fall switching times were symmetric. Slight overshoot began to appear around 140 mW. Therefore, 140 mW was used as the target input power for all data outputs to drive other gates.

The light loss through each gate is approximately 20%. The clock signal at each level of logic regenerates the logic levels. A clock pulse of 175 mW was used in future designs.

Table 4. Data input switch speed.

D Optical Input (mW)	DB Optical Input (mW)	Rise/Fall Time (pS)
60	34	no switch
80	45	136
100	56	72
120	68	26
140	79	22
160	90	21
180	101	20

7. Optical Logic Gate Simulation

A simple two input optical gate was designed and modeled from the S-SEED device models. The schematic of an OR gate and an AND gate are shown in Figure 26 and Figure 27respectively. The two diodes are connected in series with a 1 V power supply in reverse bias. Inputs A, B, AB, BB, C and P and outputs Q and QB are optical inputs and outputs simulated by PSpice as voltages where 1 V = 1 W optical power. Inputs AB and BB are inverted versions of the inputs A and B. MID is the electrical node connecting diodes D1 and D2.

The optical logic gate operation is based on a three phase clocking scheme shown in Figure 28. The following describes the operation of the OR gate. In the first phase, the logic of the gate (OR) is set using the P input. The P input will discharge D1 and charge D2. The voltage on node *MID* will rise toward VCC. In the second phase, the logic inputs (A, B, AB, BB) are applied to the two diodes. Unless both AB and BB are ON, the gate will not switch from the initial state set in phase 1. This performs the logic function. In phase three, the C input is applied to both diodes, and the light reflecting from the Q (charged diode) indicates the resulting of the logic function. The clock input is equal on both diodes and will not switch the state of the gate by itself. The simulated output of this logic gate is shown in Figure 29.

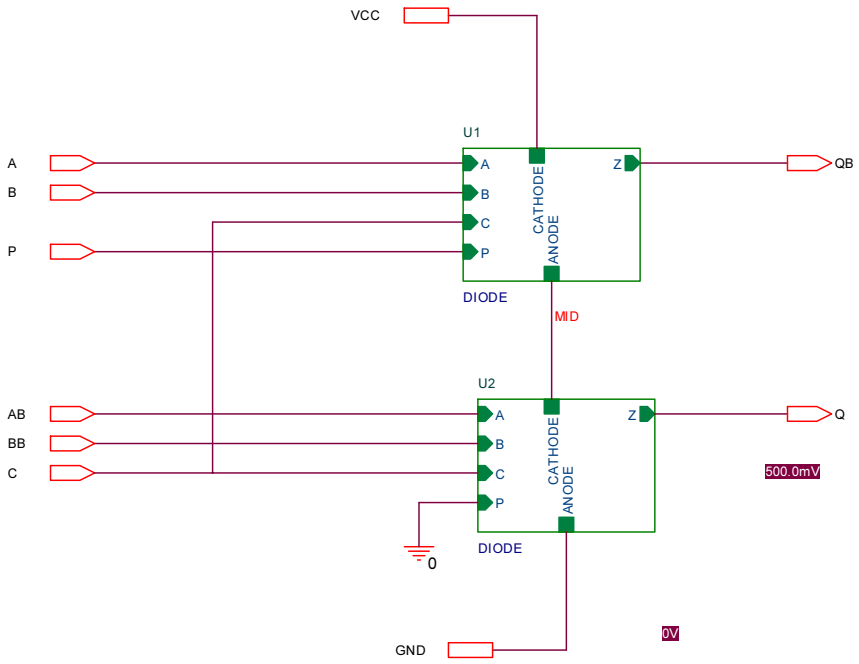

Figure 26: Two input optical OR gate.

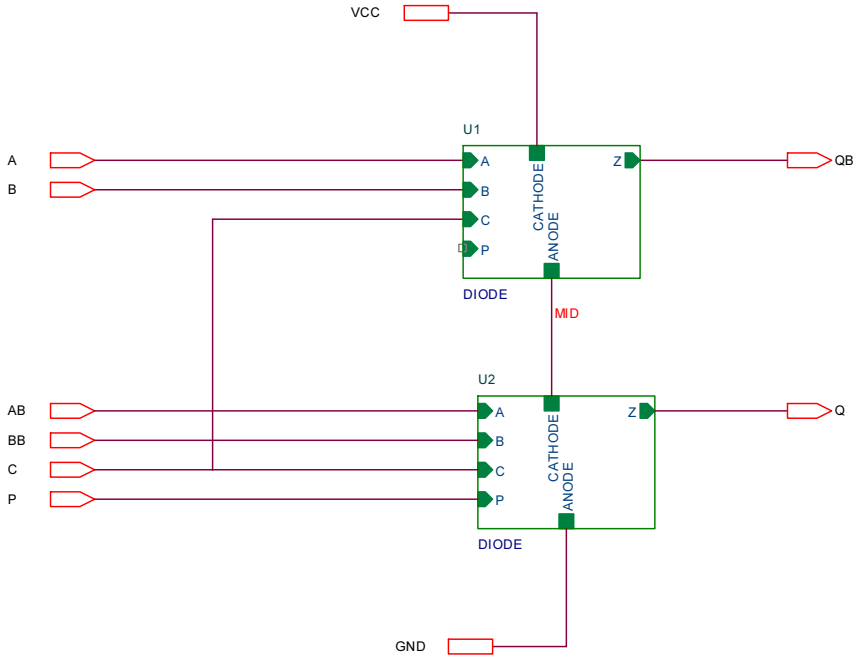

Figure 27: Two input optical AND gate.

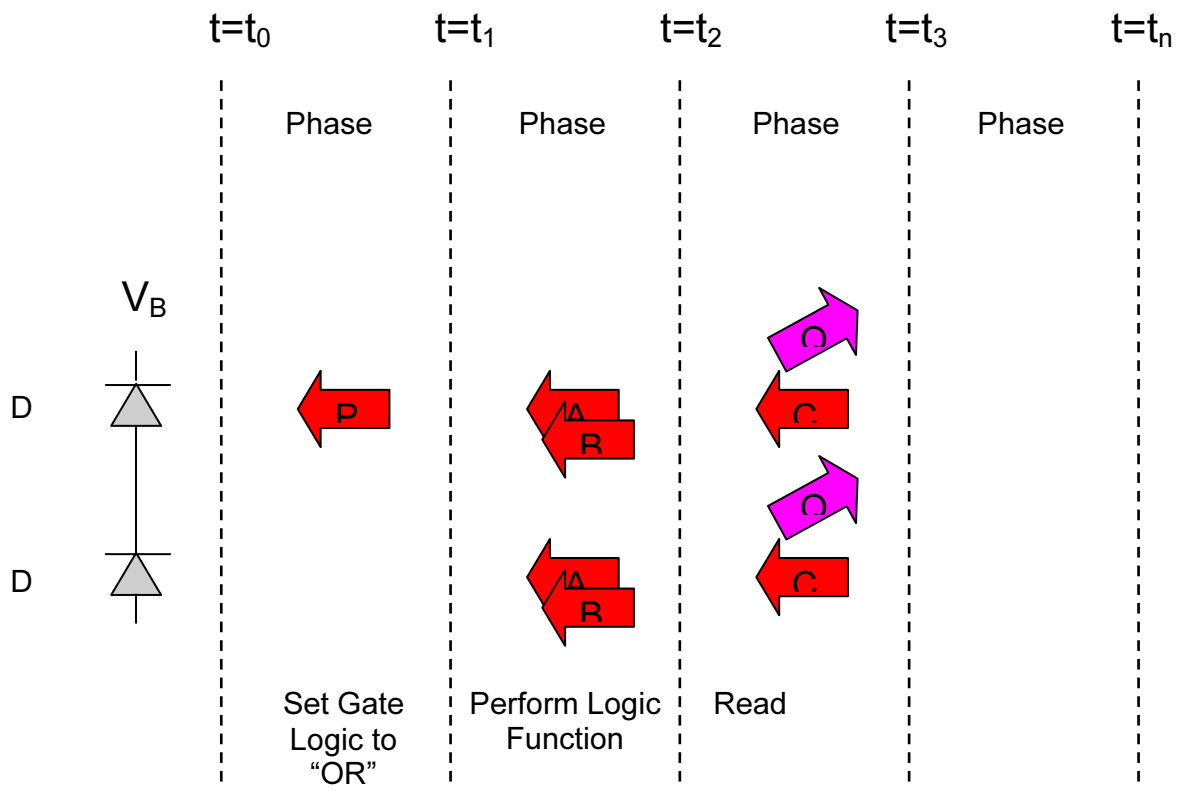

Figure 28: Three phase logic diagram.

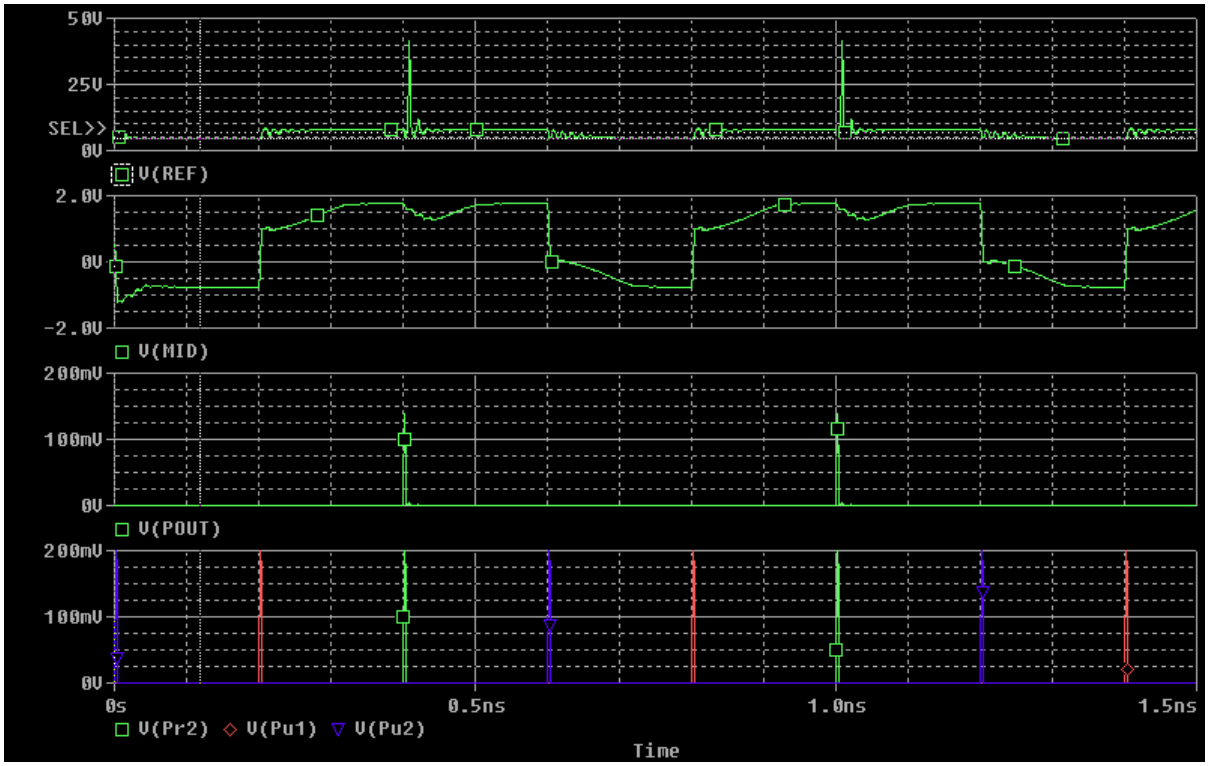

Figure 29: Simulated photonic logic gate operation.

8. Gain Competition Optical Logic

Semiconductor lasers are the primary optoelectronic devices used in optical communications systems today. These lasers operate by injecting current into the semiconductor allowing electron-hole pairs to recombine in the active region and generate photons. Photons (light) bounce in all arbitrary directions, or modes, in the laser cavity. Two parallel mirrors bound the cavity and the photons bouncing in the mode propagated by the mirrors undergo amplification from many passes through the active region. See Figure 30.

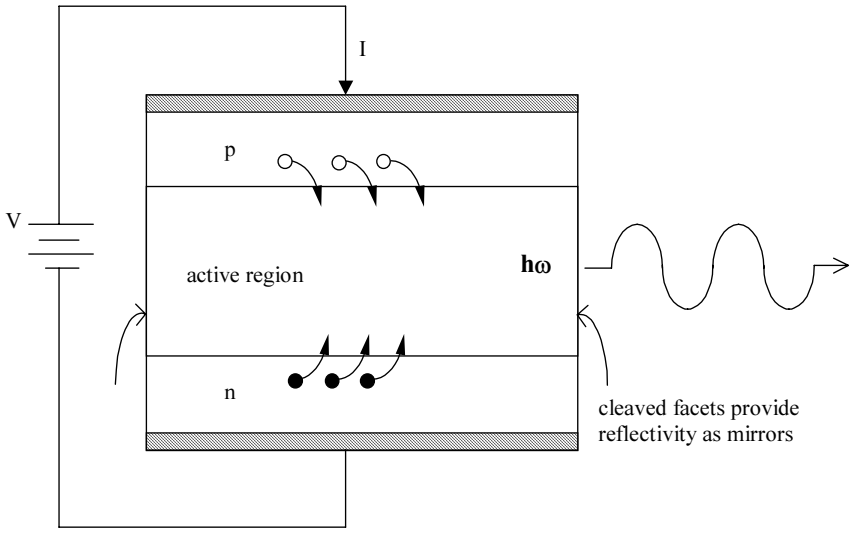

Figure 30: Cross section of double heterojunction semiconductor laser structure.

This dominant amplified mode is called the lasing mode or operational mode. Gain competition devices operate by injecting laser light into the cavity in a competing mode which "steals" carriers from the operational mode. Thus the simplest optical logic gate that is currently being fabricated is the inverter. In Figure 31, L_{SLAVE} is biased with a constant current and is controlled by L_{MASTER}. This configuration shows optional amplification in between lasers.

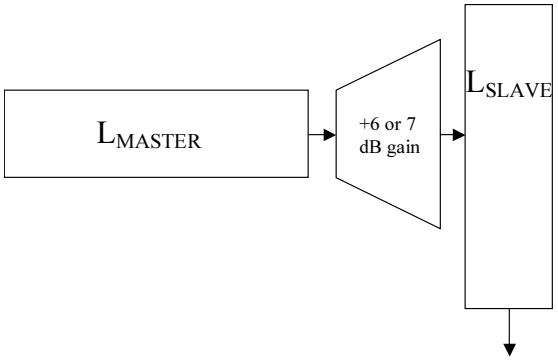

Figure 31: Master/Slave configuration of gain competition device.

The configuration shown can implement the following inverter waveform in Figure 32.

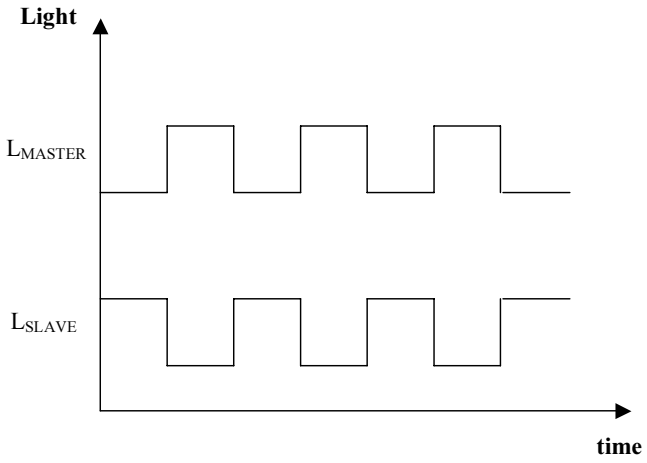

Figure 32: Inverter implementation.

The gain competition effect is dependent upon photon lifetime τ_p = 10-100 fs. This translates to a switching time currently at 1ps. The latency measured in the inverter gate has been measured around 20 ps. Fabrication density is estimated to be at 4-5 gates / μm^2. Currently the devices are operating at λ = 860 nm with plans to engineer the bandgap and effective wavelength of operation to λ' = 1550 nm. The longer wavelength device is ideal for optical networking equipment utilized in long haul transport.

8.1. Processing Challenges

Fabrication of a gain competition device requires precise etching and lithography specific to the device. Controlling the wall depth, device spacing, and alignment angles is paramount to decreasing the amount of loss through refraction. The spacing must be precise enough to produce a standing wave so that light passes into the next laser. See Figure 33.

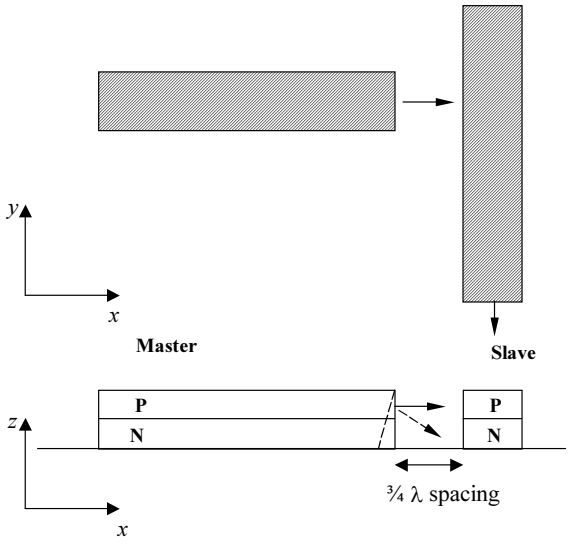

Figure 33: Cross sectional view of gain competition device.

8.2. Packaging and Interconnect Issues

Since these devices are edge emitting, fiber pigtails can be utilized for packaging and interconnecting devices. It is also feasible to bond gain competition devices to silicon PLCs (planar lightwave circuits). Silicon PLCs can be fabricated to monolithically provide routing, interconnections, filters, and integration of active and passive components. This has not been demonstrated yet. It is also estimated that there will be 1dB loss at a fiber-coupled interface and 1dB of mode loss from laser to laser. This places a constraint as to the number of gates that can be cascaded in an optical logic circuit design.

8.3. Future Developmental Directions

The concept of logical HI and logical LO is still undefined and is being developed. Current mathematical modeling done has shown different areas of operation (biasing conditions) which can be used to define thresholds of HI and LO seen in Figure 34.

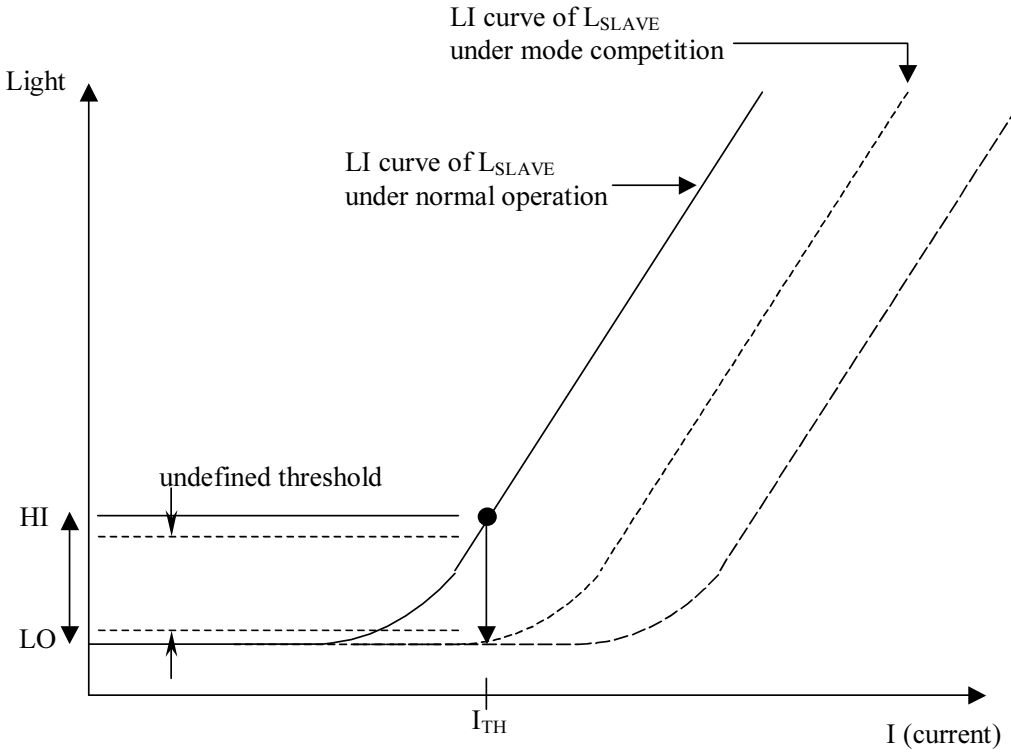

Figure 34: LI curve of L_{SLAVE}.

The threshold current $I_{TH} \alpha$ (gain – loss), where gain is controlled by L_{MASTER}. The proposed optical XOR logic gate would be built out of several cascaded devices arranged conceptually as shown in Figure 35. There would be input stages and output stages, each with gain and monolithic routing.

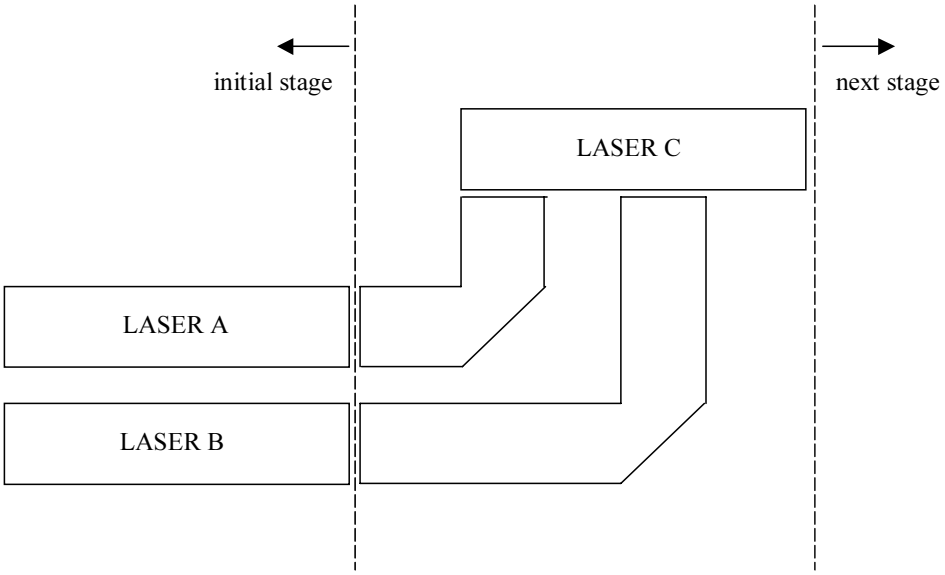

Figure 35: Conceptual optical logic circuit design.

As previously mentioned, output levels and definitions of HI and LO are still being modeled. For example, a two input gain competition device can be used to implement optical logic depending on what registers as high intensity and low intensity seen in Figure 36. Gain can be inserted between stages or at different input/output ports as defined by the device designers.

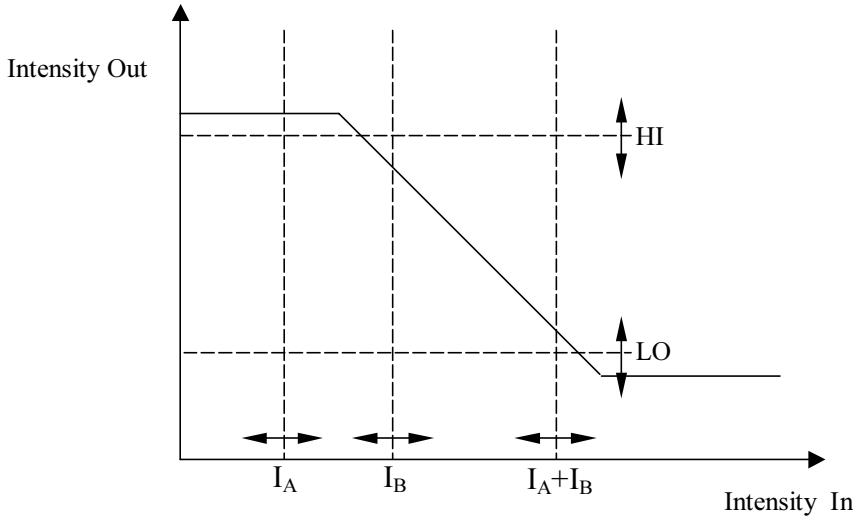

Figure 36: Intensity Out vs. Intensity In with varying logic levels (conceptual, not to be considered as actual implementation)

An XOR can be implemented with traditional boolean logic in two ways. One approach is to use a NOT-AND-OR set of gates to formally apply XOR = XY' + X'Y as shown in Figure 37. An alternate method of implementing the XOR is to use four NAND gates cascaded three deep as shown in Figure 38.

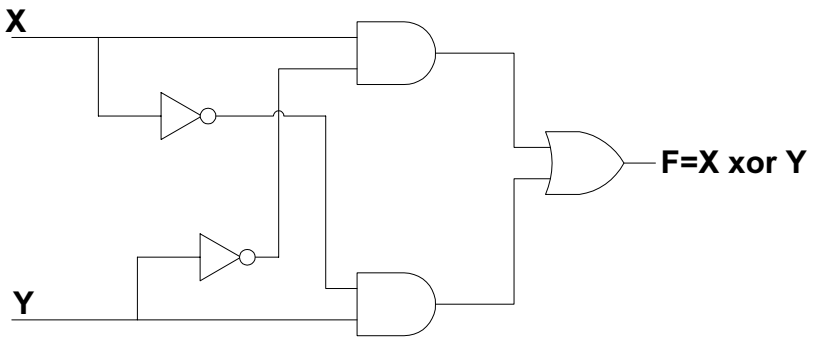

Figure 37: NOT-AND-OR implementation of XOR

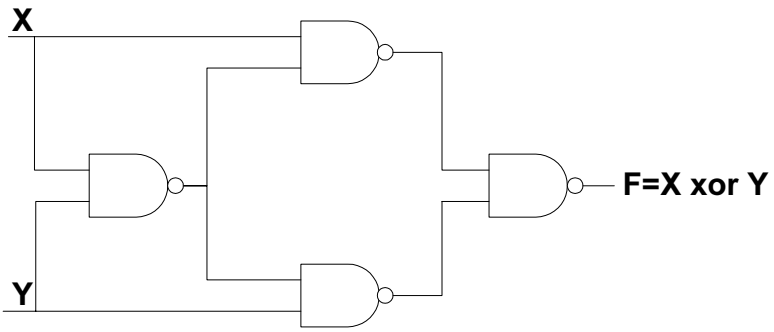

Figure 38: NAND-NAND-NAND implementation of XOR

A conceptual layout of a NOT-AND-OR implementation can be seen in Figure 39. A waveguide splitter is used in order to take the signals X and Y and fan out into two inputs, one a simple pass through and the other an invert. A waveguide with time delay is implemented so the path delay and synchronization match up with incoming signals from the opposite source. And NAND-NAND-NAND implementation can also be designed in the same manner. A planar lightwave circuit consisting of homogeneous two input / one output gain competition circuits provide a way of realizing NAND gate functionality. Figure 40 shows a conceptual layout of this implementation.

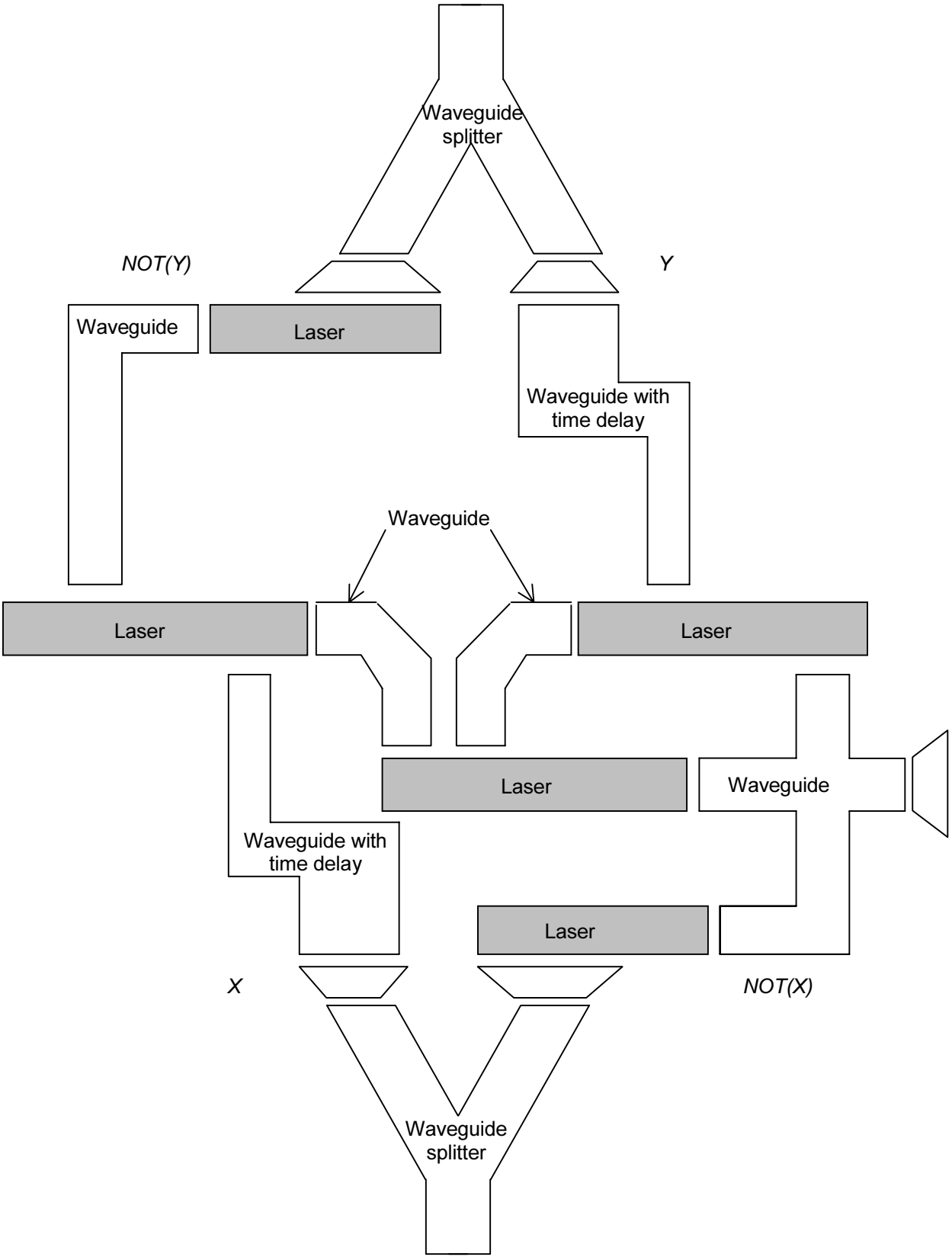

Figure 39: NOT-AND-OR layout of optical XOR

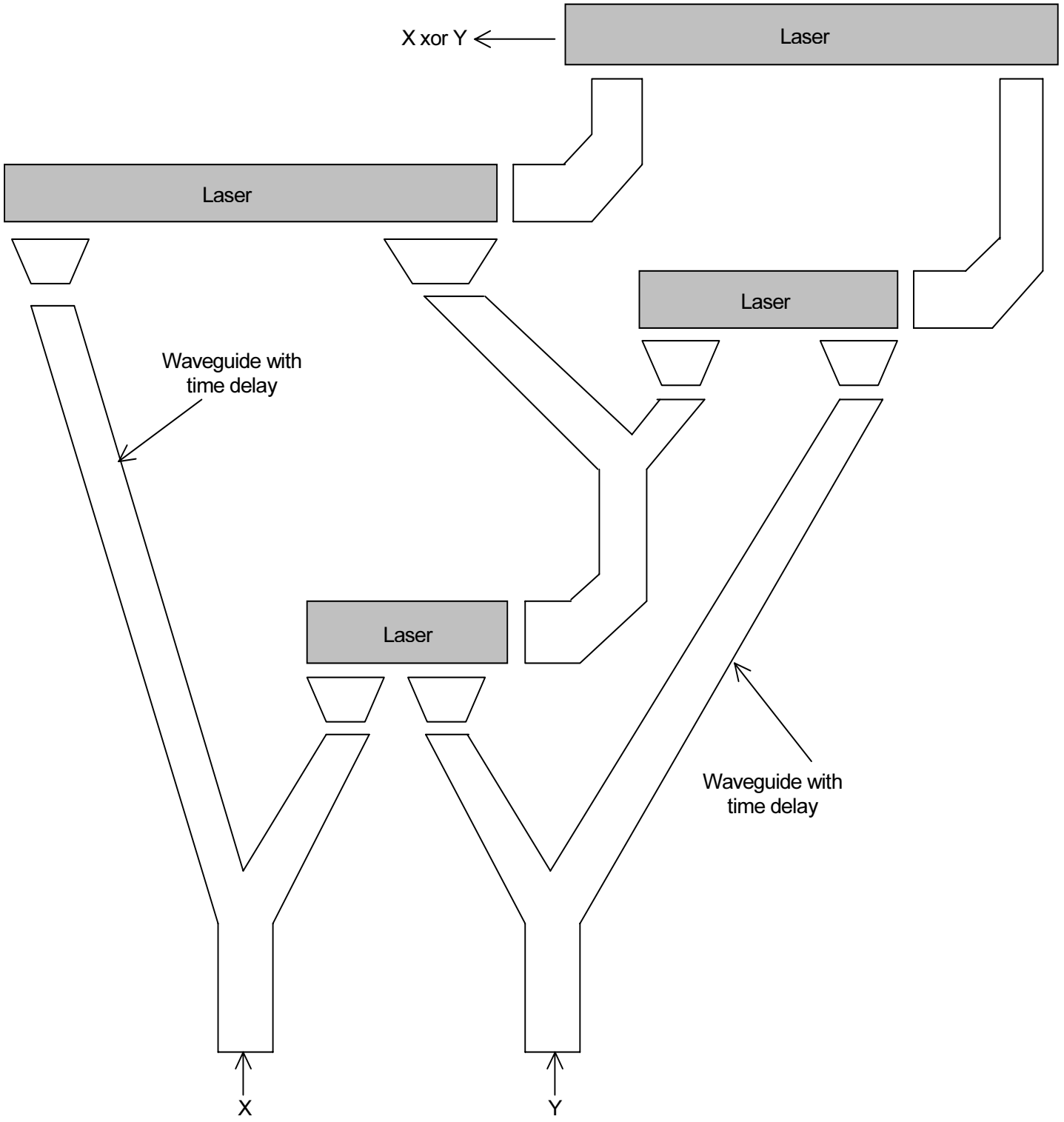

Figure 40: NAND-NAND-NAND implementation of XOR

We intend to perform the same type of behavioral modeling in PSpice for gain competition technology. By taking into account the propagation delays, intensity loss and gains, as well as laser switching times, we are trying to build a library of models which can then be cascaded and placed in different physical arrangements in an all-optical logic circuit.

9. Survey of Encryption Methods

In the design of a photonic encryptor, we consider multiple design methodologies. Given the device constraints of the optical logic gates, we have chosen to approach the problem from several different angles. One method is to do a strict electrical-to-optical translation of current encryptor designs. Another is to consider an encryption scheme capitalizing on purely optical properties of the bit stream and transmission method. Also, we consider a hybrid electrical/optical implementation with complex low-speed functions implemented via electronics and high-speed functions implemented in the photonic domain. Finally, we consider custom crypto-algorithms which allow for the design of an all-optical scaleable unit encryptor given the physical constraints of the optical logic devices.

9.1. Electrical-to-Optical Translation of Current Encryptor Designs

9.1.1. Conventional Block Ciphers

Many of today's algorithms that are regarded as "secure" are of the block cipher variety. These algorithms enjoy popularity among casual users and are recognized as federal standards for encryption in network communications.

Data Encryption Standard (DES): This is a standard outlined by FIPS 46-3 as the approved cryptographic algorithm originally intended for use in special purpose hardware devices for encryption of binary data. Since its adoption as the federal standard in 1977, it has been the predominant method of encrypting and decrypting information in storage and communications networks. One round of DES requires a minimum of 512 gates to implement. (Each DES s-box has 64 cells which require distinct gates to compute; there are 8 s-boxes.) A minimal DES implementation requires the 64-bit plaintext/middletext to be in a register, and clocked through the encryption logic 16 times for the 16 rounds of DES. DES is a block cipher that encrypts data 64-bits at a time. The cipher is a symmetric algorithm, meaning that the same key is used for both encryption and decryption. Functionally, the algorithm can be based on several different kinds of optical logic operations (AND, OR, XOR) for the s-boxes and is made up of clocked shift registers, flip-flops, and substitution for the key. Due to the parallel nature of the bit flow and the extensive number of logic gates, DES does not make a good candidate for implementation in optical logic given the algorithm's fan-out and timing requirements.

Advanced Encryption Standard (AES): This is the newest standard designed to eventually replace DES as the federal standard for encryption in communications devices. Specified in FIPS 197-1, the standard was the result of collaboration between the U.S. government, NIST, industry, and academic institutions around the world to find a cryptographically suitable replacement for future encryption requirements. AES is a symmetric key algorithm which can encrypt using 128, 192, or 256 bit keys. AES uses a more complex key scheduling than DES, requiring more logic to compute intermediate expanded-key bits. A strict optical translation of AES is problematic for the same reasons as the DES implementation. The sheer number of optical logic gates is currently not feasibly manufactured and interconnected.

Tiny Encryption Algorithm (TEA): A relatively new algorithm invented by David Wheeler and Roger Needham, it is a block cipher that operates on 64-bit blocks using a 128-bit key. This algorithm, which was designed primarily for efficient software implementation, achieves diffusion and confusion through a series of two orthogonal operations, the XOR and ADD. It is a fast and efficient crypto-algorithm which is resistant to differential cryptanalysis and well-known methods of attacks. Although the algorithm is compact and repeated many rounds, it still has a larger-than-desired gate count, and the necessity of operating in 64-bit blocks makes it unsuitable for our photonic encryptor [7].

9.1.2. Conventional Stream Ciphers

Most of the existing, “generally-regarded-as-safe” ciphers are block or stream ciphers. The data stream in a photonic encryptor design has no special block structure and would seem to lend itself to some sort of stream cipher implementation. However, there are inherent problems:

- **Acceptance:** There is currently no stream cipher with the widespread acceptance comparable to DES or AES. The European NESSIE project has several entries of the stream cipher variety, and none have survived cryptanalysis.

- **A5:** The best existing stream ciphers are from the A5 family. A5 is a stream cipher utilized to encrypt the link from mobile phones to cellular base stations in the European GSM (Group Special Mobile) standard. It employs three linear feedback shift registers (LFSRs) of length 19, 22, and 23 bits with sparse polynomials used in the feedback. Each LFSR is clocked according to its middle bit and the output of all three registers is XOR’d together. This cipher [8] is interesting because it was designed for implementation in hardware with minimal gate count. However, this cipher has been shown to be breakable with a desktop Pentium in less than one second.

- **Stuttering Characteristics:** The best design principle in stream ciphers that seems to have the most potential for thwarting analysis is to use a complex pattern of stuttering. Stuttering involves clocking shift registers with a complex irregular pattern. This is a good crypto ingredient, but is unnatural for our problem: Our optical logic device circuits are not congenial to stuttering registers.

9.2. Purely Optical Implementations

9.2.1. Chaotic Mode-Locked Lasers for Communications Encryption

The recent study of chaos in physical and biological systems has led to investigations into various real world applications. One of these engineering applications is the encryption of data for communications. When applied towards a modern crypto-system, there is a need to generate and confidently reproduce chaos, as well as a need for synchronization between transmitters and receivers. It has been shown that a semiconductor laser system can be driven into chaotic regimes of operation where the encryption of an optical bit stream is achieved. Bit rates upwards of 1GHz have been demonstrated in free space lab experiments [9]. In order to drive the transmitter and receiver into chaotic regime, they both must be fabricated from the same wafer, in effect coupling all transmit/receive pairs. This is an undesirable property to have in commercial communications systems. Also, chaotic mode locked lasers used as encryption devices have only been demonstrated using the free space communication channel. However, in modern fiber optical communication links, the dispersion property of fiber would destroy synchronization and make communications data unrecoverable. This would make chaotic mode-locked lasers unsuitable for high-speed data encryption in fiber optic networks.

9.2.2. Quantum Cryptography with Coherent State Noise

Another method of encryption of optical communications is by utilizing the fundamental quantum noise of coherent states. A shared secret key is used to set the polarization bases between a transmitter and receiver. An eavesdropper would then have to guess the alternating polarization bases on each bit. Without knowing the exact polarization state of the bit, the eavesdropper incorrectly reads the bit and reads optical noise. This technology has been demonstrated at 100kbps [10] but the ability to scale up to higher speeds is restricted by the polarization state generator.

9.2.3. Single Photon Quantum Cryptography

Quantum key distribution systems using single photon sources are also being explored as a method of optical communications encryption [11]. The premise is to securely transmit a key over a link with an optical bit stream consisting of a series of photons as bits. Each photon is transmitted with a certain quantum spin agreed upon by both receiver and transmitter. The security is based the theory that if an eavesdropper attempts to intercept a photon in transit and detect it, the physical act of detecting it alters its quantum number or spin, thus alerting the receiver that it has been compromised. Thus the system can change which way the photons are being generated and what "spin" is utilized. This method has been demonstrated experimentally but was necessitated by complete control of environmental variables. The variation in temperature, electromagnetic interference, and physical vibrations of the medium make this very fragile, and not robust enough for communications systems. Furthermore, this scheme cannot encrypt data at the required rates for optical networks.

9.3. Hybrid Electrical/Optical Implementation

9.3.1. Electric-to-optic Stream Cipher

The design methodology employed in the hybrid implementation is to generate the keystream in the electrical domain, multiplex it into the optical domain (creating a single composite keystream), and then optically XOR the composite key stream with a plain text stream of bits as shown in Figure 41. At the decryption end, the optical cipher-text bits are then XOR'd with an optical composite keystream that is identical and in phase with that used at the encryption end in order to recover the plain text. Ideally if the keystream is an endless stream of truly random bits, the cipher is as strong as XORing with a one-time pad. However, if the keystream is linear, generated deterministically using other methods, or repeated in any fashion, then the security of the cipher might be broken. The more random and non-linear the keystream can be, the more secure the algorithm becomes. The scheme capitalizes on commonly available Serializer/Deserializer (SerDes) technology when multiplexing the keystream from the electrical to optical domain.

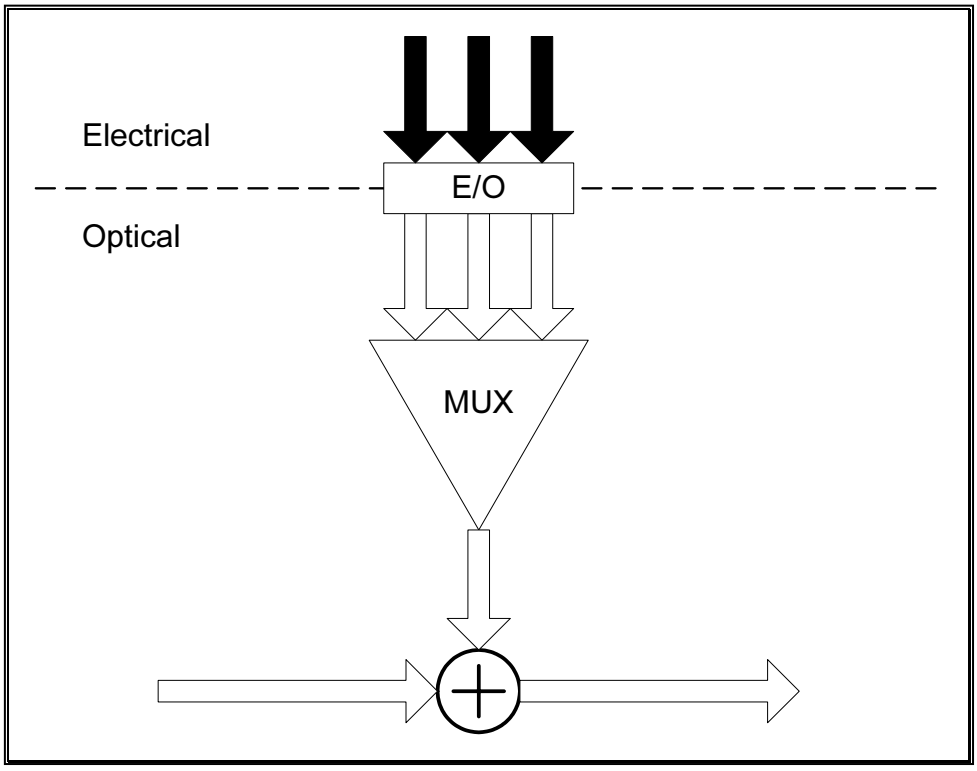

Figure 41: Hybrid electrical-optical encryption

10. Custom algorithm – Serial, cascadable, low gate count demonstration algorithm

A serially operated encryption circuit can be cascaded for increasing level of protection. The mode of operation in a unit block of a low gate count encryptor is Cipher Feedback Mode. A stream of plain text comes in, and is XOR'd with a stream of cipher text which has been passed through a simple logic function. The algorithm achieves the necessary security by cascading many of these unit blocks to provide "confusion and diffusion."

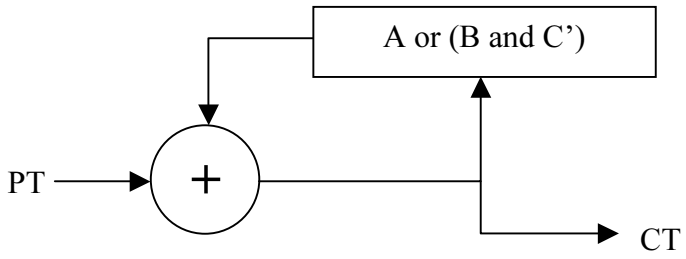

Figure 42: Unit Encryptor Cell

In Figure 42, the input plain text comes in from the left with the output cipher text leaving to the right. One bit of cipher text is determined by several bits of input. The result of the logic function is XOR'd into the input plain text stream to generate cipher text.

The unit decryptor cell operates by taking in cipher text from the left and tapping off appropriate bits to use in a corresponding logic function. This output is then XOR'd with the original CT to produce the recovered plain text. Figure 43 shows the flow of bits in the decryptor.

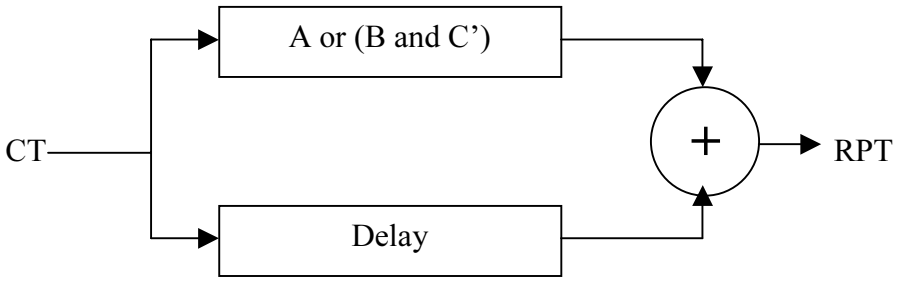

Figure 43: Unit Decryptor Cell

10.1. Key Inputs

Using a keystream generated by traditional E-O sources, we can control different elements of the encryption circuit itself. Five possible keying ideas are:

a) Have key–selectable complements on the inputs to the logic gates. This also means the logic function can be replaced with A or (B and C), maybe simplifying the gate slightly. It's also possible to key-selectably complement the output, although this might not be as effective.
b) Have key-selectable delays on the A,B,C inputs, or the gate output, perhaps having different delays on the inputs
c) Have key-selectable input choices, swapping or permuting the inputs to the gate.

d) One might vary the logic function used, based on the keying. This is relatively expensive, since the circuitry for both functions must be present, even though one circuit is idle. Although we may use a couple of different kinds of logic functions in the different cascaded stages of the cipher, we don't expect to have unused functions.
e) One might use the key to vary the routing of the middletext signal through different encryption stages. This idea would be most effective if there are several kinds of stages. Right now, we aren't planning to implement this idea.

10.2. Randomization

Using randomization in an encryption system is like having keyed encryption – it makes cracking the code more difficult for people with malicious intent – yet does not require transmitting a key to the receiver. A couple of different ways of randomizing are:

a) Initialize the contents of the internal delays in the logic inputs and outputs to have different random values.
b) Prepend a string of random bits at the front of the message, to accomplish the same result as letter a).

10.3. Cascading

In order to provide sufficient protection as an encryption algorithm, the unit encryption circuit can be cascaded many times. By chaining the cipher text into the plain text input of the next stage, we implement a "long and skinny" encryption algorithm as opposed to widely used parallel schemes in DES and AES. The encryption process is shown in Figure 44. Initial cryptanalysis has shown that the number of stages *n* needed may be between 32 and 128.

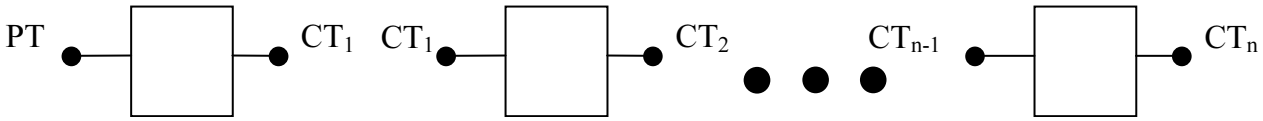

Figure 44: Cascaded Encryptor Design

The corresponding decrypting sequence would take reverse stage order. The recovered plaintext output of each decryption stage feeds into the cipher text input of the next stage. Figure 45 shows the corresponding decrypt process.

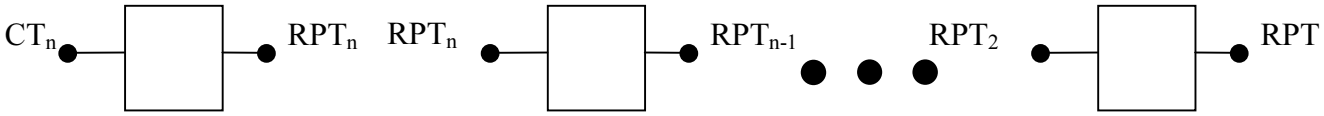

Figure 45: Cascaded Decryptor Design

Our cipher design differs from typical stream ciphers in one other respect: most stream ciphers generate a keyed pseudo-random bit stream, which is then XOR'd with the plaintext to produce ciphertext. The decryptor carries out the same operation. An active attacker can make a known modification to a message by XORing his modification into the message while it's in transit. If modification-in-transit is a realistic threat, messages must carry an authenticator, a hard-to-fake checksum. In contrast, our cipher doesn't have the easy-to-modify property. If a message is modified in transit, the decryption will be garbage at the place of modification and afterward for a few hundred bits. A simple checksum in the decrypted plaintext is sufficient, since an attacker can't figure out the right checksum.

10.4. Cryptanalysis Plan

- **Correlation Measurement:** We need to estimate the minimum secure number of stages. This will be based on simulation statistics. We will measure correlations between successive stages of message processing, and determine how effective each kind of stage is in reducing or destroying correlations.
- **Diffusion of Bit Influence:** we expect diffusion of bit influence to follow a simple model. Each encryption stage has a diffusion of a few bit positions (time steps) based on the width between the tapped bits, and any key-contributed variance in the stage delay. The addition formula for several stages is expected to be square-root-of-sum-of-squares, appropriate for convolved, cascaded filters. This formula needs to be confirmed.
- **Attack Model:** The block cipher world has several well developed attack models: chosen ciphertext, known plaintext, etc. We need to develop models appropriate to our stream cipher. We probably want to disallow an attacker from encrypting or decrypting two closely-related streams, say with single-bit differences.
- **Existing Stream Cipher Attacks:** Most stream cipher attacks are really attacks on the keyed pseudo-random bit stream. The opponent is assumed to have a large supply of stream available for analysis, and uses various statistical tools in his attack. Our situation is different. But we need to be aware of existing attack methods, and see which might be adaptable against our cipher. For example, our basic logic function A or (B and C') can be linearly approximated as simply A. We need to use enough stages of encryption to defeat attacks based on estimating the linear transfer function of the encryptor.
- **Related Key Attacks:** We are assuming that the key-setup for our encryptor is handled electronically, and that the key isn't changed at high speed. This allows us to assume that the actual key used to control the innards of the encryption is determined by hashing the external visible "user key." We can assume that even if two user keys are closely related, that the hashing stage will magnify even a single-bit difference into complete randomness within the encrypting device. A very practical benefit of this approach is that the keyed portions of the optical logic don't have their control inputs operating at high bandwidth.

11. Future Tasks

As we enter into the first quarter of FY04, we intend to accomplish the following tasks:

- Continued C programming of the demonstration algorithm. The project team will also refine the "lightweight yet nontrivial" scheme as well as investigate other low gate count, serial, cascadeable demonstration algorithms for encryption.
- Continued design of building blocks for a set of Boolean complete logic. The second half of this LDRD will focus on completing a set of XOR, NAND/AND, NOR/OR, inverter, and buffer gates for both the SEED and gain competition technologies.
- Development of a full proposal for Tier 2 funding from internal funding sources as well as external ones such as NSA. Completion of these tasks will incubate the project to a status suitable for Tier 2 level funding.

References

[1] S. Okamoto, “Photonic Transport Network Architecture and OA&M Technologies to Create Large-Scale Robust Networks,” IEEE Journal on Selected Areas in Communications, vol. 16, no. 7, September, 1998.

[2] D. Blumenthal, “Photonic Packet Switching and Optical Label Swapping,” Op. Nets. Mag., vol. 2, no. 6, November/December, 2001, pp. 54-65.

[3] S. Tarek, et. al., “Optical Packet Switching in Core Networks: Between Vision and Reality,” IEEE Communications, vol. 40, no. 9, September, 2002.

[4] S.L. Chuang, Physics of Optoelectronic Devices. New York, John Wiley & Sons, 1995.

[5] A. L. Lentine et. al, “Symmetric self-electrooptic effect device; optical set-reset latch, differential logic gate, and differential modulator/detector,” IEEE J. Quantum Electronics, vol. 25, no. 8, pp. 1928-1936, August 1989.

[6] D.K. Serkland, I.J. Fritz, T. Sullivan, J. H. Burkhart and J. F. Klem, “December 2, 1999 Intermediate Progress Report: Switching Speed Measurements of Symmetric Self-Electrooptic-Effect Device at 865 nm.”

[7] D.J. Wheeler and R. Needham, “TEA, A Tiny Encryption Algorithm,” Technical Report 355, “Two Cryptographic Notes,” Computer Laboratory, University of Cambridge, Dec 1994, pp. 1-3.

[8] B. Schneier, Applied Cryptography. New York, John Wiley & Sons, 1996.

[9] J. Paul, et. al., “GHz Bandwidth Message Transmission Using Chaotic Diode Lasers,” Electronics Letters, vol 38, no.1, pp. 28-29, January 2002.

[10] P. Kumar, G. Barbosa, and E. Corndorf, “Quantum Cryptography with Coherent State Light: Demonstration of a Secure Data Encryption Scheme Operating at 100kb/s,” QELS ’02 Technical Digest, pp. 189-190, May 2002.

[11] M.A. Nielsen and I.Chuang, Quantum Computation and Quantum Information. United Kingdom, Cambridge University Press, 2000.

DISTRIBUTION

1	MS 0801	A.L. Hale, 9300
1	MS 0801	M.R. Sjulin, 9330
1	MS 0801	W. F. Mason, 9320
1	MS 0806	L. Stans, 9336
1	MS 0806	J.P. Brenkosh, 9336
1	MS 0806	J.M. Eldridge, 9336
1	MS 0806	A.Ganti, 9336
1	MS 0806	S.A. Gossage, 9336
1	MS 0806	T.C. Hu, 9336
1	MS 0806	B.R. Kellogg, 9336
1	MS 0806	L.G. Martinez, 9336
1	MS 0806	M.M. Miller, 9336
1	MS 0806	J.H. Naegle, 9336
1	MS 0806	R.R. Olsberg, 9336
1	MS 0806	L.G. Pierson, 9336
1	MS 0806	T.J. Pratt, 9336
1	MS 0806	J.A. Schutt, 9336
1	MS 0806	T.D. Tarman, 9336
1	MS 0806	J.D. Tang, 9336
1	MS 0806	L.F. Tolendino, 9336
1	MS 0806	J.S. Wertz, 9336
1	MS 0806	D.J. Wiener, 9336
1	MS 0806	E.L. Witzke, 9336
1	MS 0806	P.C.R. Jones, 9322
1	MS 0813	R.M. Cahoon, 9327
1	MS 0874	D.W. Palmer, 1751
1	MS 0874	P.J. Robertson, 1751
1	MS 0874	K.L. Gass, 1751
1	MS 0603	C.T. Sullivan, 1742
1	MS 0603	E.L. Blansett, 1742
1	MS 0603	G.A. Vawter, 1742
1	MS 0603	D.K. Serkland, 1742
1	MS 0603	J. Guo, 1742
1	MS 0785	R.C. Schroeppel, 5516
1	MS 0785	T.S. McDonald, 5516
1	MS 9011	B.V. Hess, 8941
1	MS 9915	H.Y. Chen, 8961
1	MS 9019	Central Technical Files, 8945-1
2	MS 0899	Technical Library, 9616 (2)