



IEEE  
**GLOBECOM**  
2007  
GLOBAL TELECOMMUNICATIONS CONFERENCE  
COMMUNICATIONS, SIGNALS & SYSTEMS  
9-13 November 2007, Washington, DC, USA

**Presentation at GLOBECOM 2007**



**NuCrypt**  
Security. Privacy. Confidentiality. Integrity.

**After quantum keys are distributed:  
Physical-Layer Encryption Aided by Optical Noise**

By  
**Gregory Kanter and Prem Kumar**

**NuCrypt, LLC**  
1801 Maple Ave. #6322, Evanston, IL 60201-3135  
kanterg@nucrypt.net

**Funding Provided By:**



Approved for public release; distribution unlimited.

GLOBECOM 2007, Slide 1



**NuCrypt**  
Security. Privacy. Confidentiality. Integrity.

**Outline**

**General Cryptography:**

- Encryption vs. Key Generation
- Quantum Cryptography vs. Physical Cryptography
- Randomized Ciphers

**AlphaEta Encryption:**

- Basic principle/Security
- Simulations
- Experiments/Demonstrations

Approved for public release; distribution unlimited.

GLOBECOM 2007, Slide 2

| Report Documentation Page                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                    |                                     |                                                           | Form Approved<br>OMB No. 0704-0188                  |                                 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|-------------------------------------|-----------------------------------------------------------|-----------------------------------------------------|---------------------------------|
| Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. |                                    |                                     |                                                           |                                                     |                                 |
| 1. REPORT DATE<br><b>2007</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                    | 2. REPORT TYPE                      |                                                           | 3. DATES COVERED<br><b>00-00-2007 to 00-00-2007</b> |                                 |
| 4. TITLE AND SUBTITLE<br><b>After quantum keys are distributed: Physical-Layer Encryption Aided by Optical Noise</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                    |                                     |                                                           | 5a. CONTRACT NUMBER                                 |                                 |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                    |                                     |                                                           | 5b. GRANT NUMBER                                    |                                 |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                    |                                     |                                                           | 5c. PROGRAM ELEMENT NUMBER                          |                                 |
| 6. AUTHOR(S)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                    |                                     |                                                           | 5d. PROJECT NUMBER                                  |                                 |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                    |                                     |                                                           | 5e. TASK NUMBER                                     |                                 |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                    |                                     |                                                           | 5f. WORK UNIT NUMBER                                |                                 |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br><b>NuCrypt, LLC, 1801 Maple Ave. #6322, Evanston, IL, 60201-3135</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                    |                                     |                                                           | 8. PERFORMING ORGANIZATION REPORT NUMBER            |                                 |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                    |                                     |                                                           | 10. SPONSOR/MONITOR'S ACRONYM(S)                    |                                 |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                    |                                     |                                                           | 11. SPONSOR/MONITOR'S REPORT NUMBER(S)              |                                 |
| 12. DISTRIBUTION/AVAILABILITY STATEMENT<br><b>Approved for public release; distribution unlimited</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                    |                                     |                                                           |                                                     |                                 |
| 13. SUPPLEMENTARY NOTES<br><b>EEE Global Telecommunications Conference (IEEE GLOBECOM 2007), 26-30 November 2007, Washington, DC</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                    |                                     |                                                           |                                                     |                                 |
| 14. ABSTRACT                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                    |                                     |                                                           |                                                     |                                 |
| 15. SUBJECT TERMS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                    |                                     |                                                           |                                                     |                                 |
| 16. SECURITY CLASSIFICATION OF:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                    |                                     | 17. LIMITATION OF ABSTRACT<br><b>Same as Report (SAR)</b> | 18. NUMBER OF PAGES<br><b>8</b>                     | 19a. NAME OF RESPONSIBLE PERSON |
| a. REPORT<br><b>unclassified</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | b. ABSTRACT<br><b>unclassified</b> | c. THIS PAGE<br><b>unclassified</b> |                                                           |                                                     |                                 |

## Cryptography



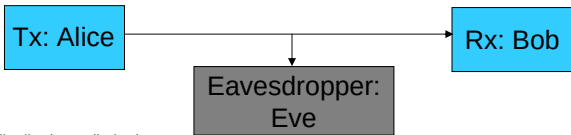
**Encryption:**

- Protects data from unauthorized observation
- Knowledge of a key (or some secret) identifies legitimate users
- Typically key is short (<1000 bits) while the message is long (>Gb)

**Key Distribution:**

- Generate shared key between two users
- Some initial shared information (secret) generally needed for authentication
- Traditionally use 'one-way' mathematical functions (make Eve factor large number or solve discrete logarithm)
- Quantum Key Distribution (QKD) uses quantum effects to try to bound the information that an eavesdropper can get

**Authentication, Non-Repudiation, etc.**



```

graph LR
    Alice[Tx: Alice] --> Bob[Rx: Bob]
    Eve[Eavesdropper: Eve] --> Alice
    Eve --> Bob
    
```

Approved for public release; distribution unlimited. GLOBECOM 2007, Slide 3

## Quantum Cryptography



**BB-84/ Ekert QKD:**

- Key Generation demonstrated
- Short distances (<~20dB loss)
- No optical amplifiers
- Low key-rate (kb/s) – need to use traditional encryption
- Quantifiable security model is a goal

**AlphaEta:**

- Practical **encryption** demonstrated
- Uses quantum noise, but not uniquely quantum effects
- Long distances (>200dB loss)
- Optical amplifiers, typical nonlinearity and network elements OK

- **BB-84** is an important key generation mechanism with limited applicability
- **AlphaEta** is a physical-layer optical encryption scheme compatible with current high speed fiber-optic networks

*Compatible (not competing) technologies*

Approved for public release; distribution unlimited. GLOBECOM 2007, Slide 4

### Standard (Traditional) Stream Cipher

PRBS: Pseudo-random bit generator

Assume PRBS is a simple linear feedback shift register (LFSR):

| Class of Attack        | Key Security               |
|------------------------|----------------------------|
| Ciphertext only attack | - Perfect                  |
| Statistical attack     | ?                          |
| Known plaintext attack | - Zero (for AES 'unknown') |

How do we really pin-down Eve's knowledge of plaintext statistics? Can only assume.

Approved for public release; distribution unlimited. GLOBECOM 2007, Slide 5

### Physical Encryption

- Some physical process obscures the data
  - not just mathematical manipulation
- Still share a secret — maybe in fabrication parameters
- Potentially high-speed, highly secure, difficult to record
- Performance / security / compatibility problems hamper their use

**Synchronized Chaotic Lasers:**

- Small signal under large chaotic fluctuation of laser
- Poor signal-to-noise ratio (SNR), nonlinearities set in early, not terribly fast

**OCDMA:**

- Data accessed via a modulation code
- Usually inherently insecure (small code-space)
- “Noise” (security) comes from multiple users
- Not compatible with typical systems (wide-band, poor performance)

Approved for public release; distribution unlimited. GLOBECOM 2007, Slide 6

### AlphaEta Encryption

- Use extended key (traditional encryption) to choose one of  $M$  basis states: adds a bias to each data bit
- Bob can subtract off bias — reads binary data
- Eve analyzes  $2M'$ ary signal set ( $2M > 4000$  demonstrated)
- Optical power level adjusted, so many states obscured by quantum noise
- Quantum noise can't be circumvented — not technology related
- Known Plaintext Attack → 'Lower-bounded' Statistical Attack

Approved for public release; distribution unlimited.

GLOBECOM 2007, Slide 7

### AlphaEta Block Implementation

Approved for public release; distribution unlimited.

GLOBECOM 2007, Slide 8

### AlphaEta Security

- ‘Lower bound’ noise levels for Eve’s statistical analysis known precisely
- Security ‘Level’ depends on:  
amount of noise, type of PRBS algorithm used, # basis states
- Still may not know exactly how hard system is to break  
(if optimal breaking algorithm unknown) but:
  - *worst-case security improved (even simple LFSR can offer useful security)*
  - *randomization adds qualitatively different type of security*
  - *nebulous problem of Eve’s statistical knowledge circumvented*
  - *additional measurement burden for attacker*

#### Class of Attack

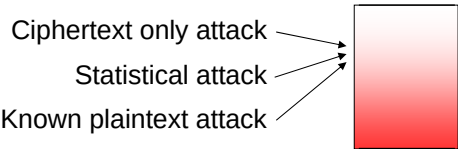
Ciphertext only attack

Statistical attack

Known plaintext attack

#### Key Security

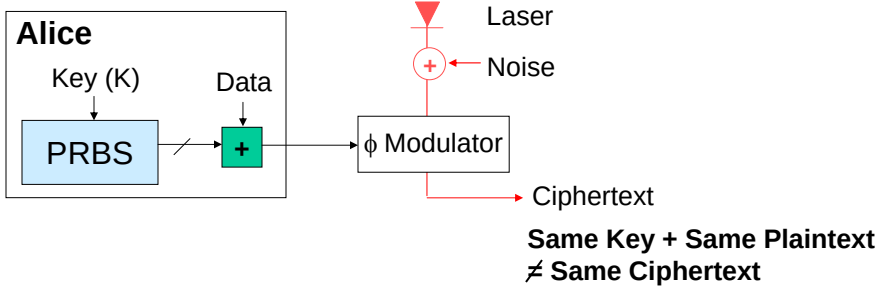
- Perfect Security
- Security ‘Level’
- LFSR-Zero Security (AES – unknown)



Approved for public release; distribution unlimited.

GLOBECOM 2007, Slide 9

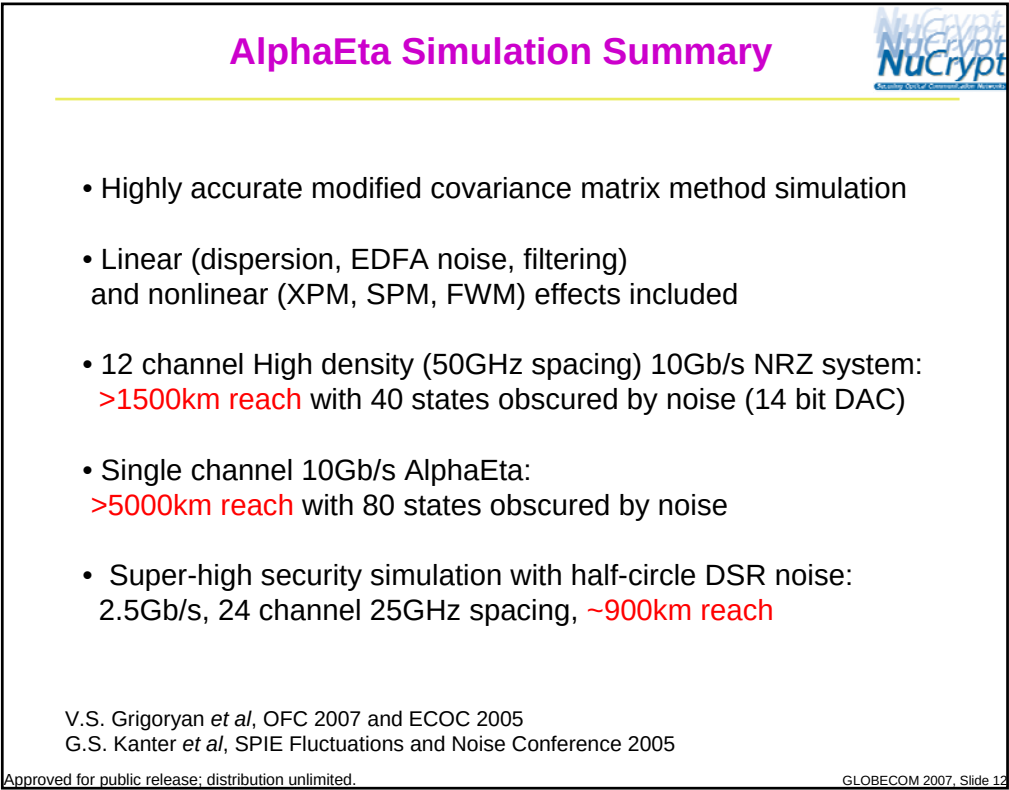
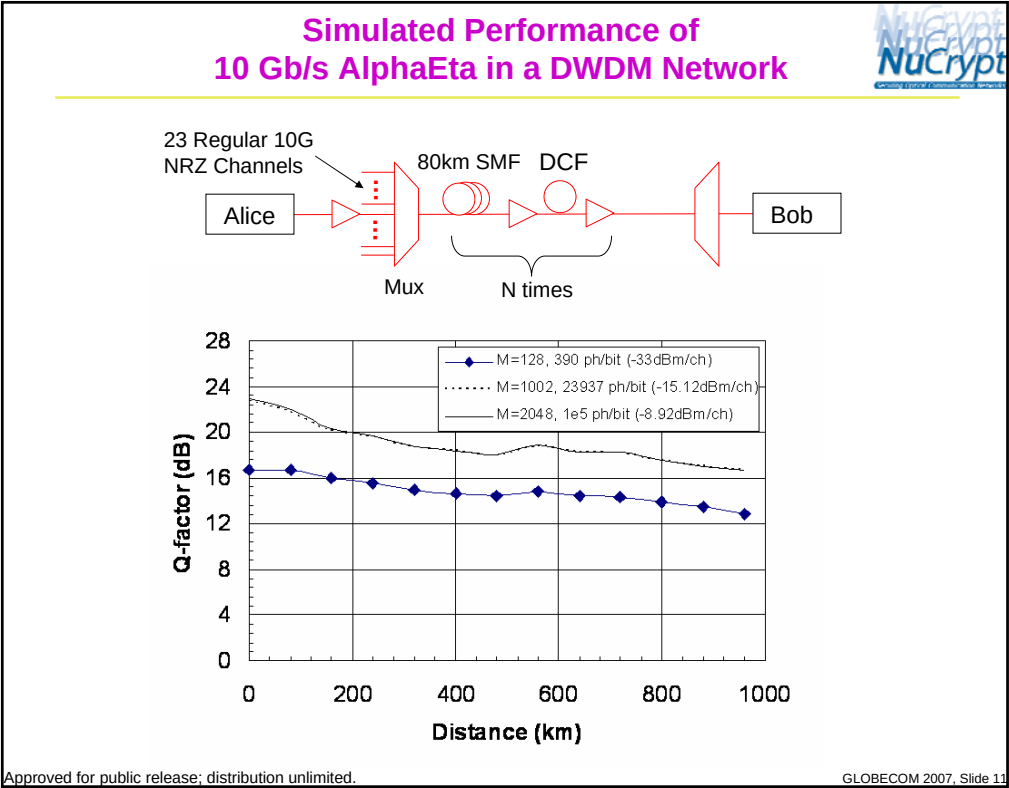
### AlphaEta Characteristics

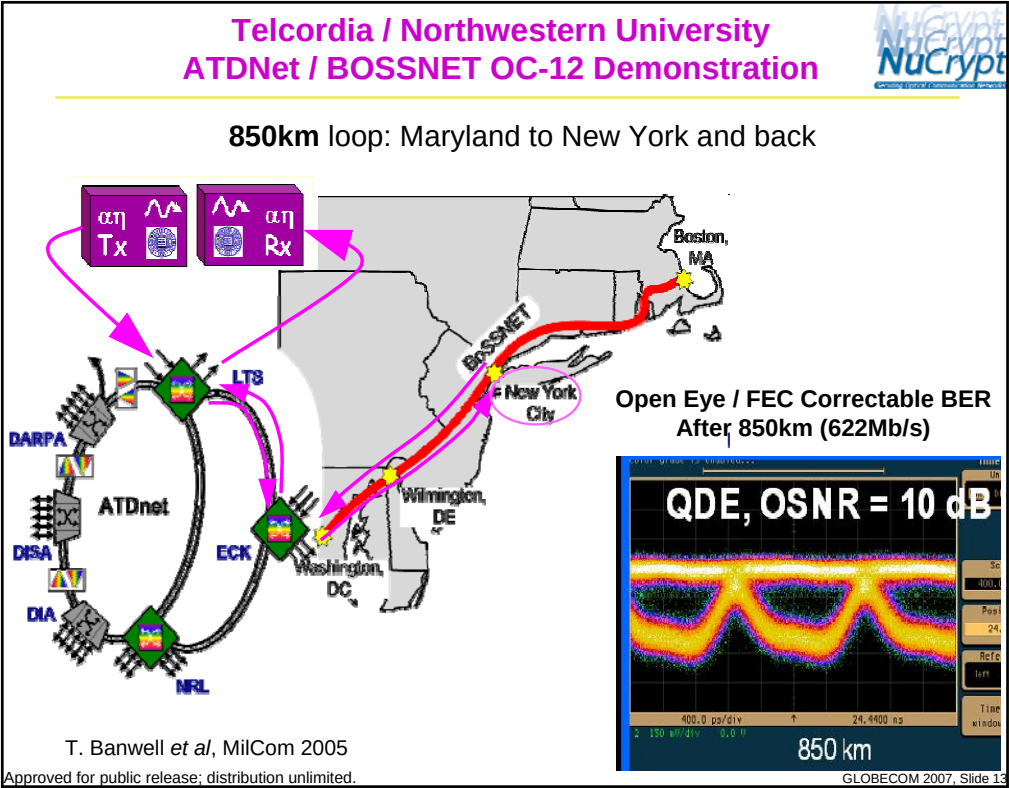


- **One class of key attack**
- **Compatible with current DWDM telecom infrastructure**
- **No direct attacks on the data (not true for all physical encryption schemes)**
- **Performance similar to DPSK signaling (1dB penalty observed)**
- **Combines traditional & physical encryption (high confidence, upgradeable)**
- **Noise levels controllable and set by quantum mechanics**  
— not technology related, quantifiable with no assumptions, truly random

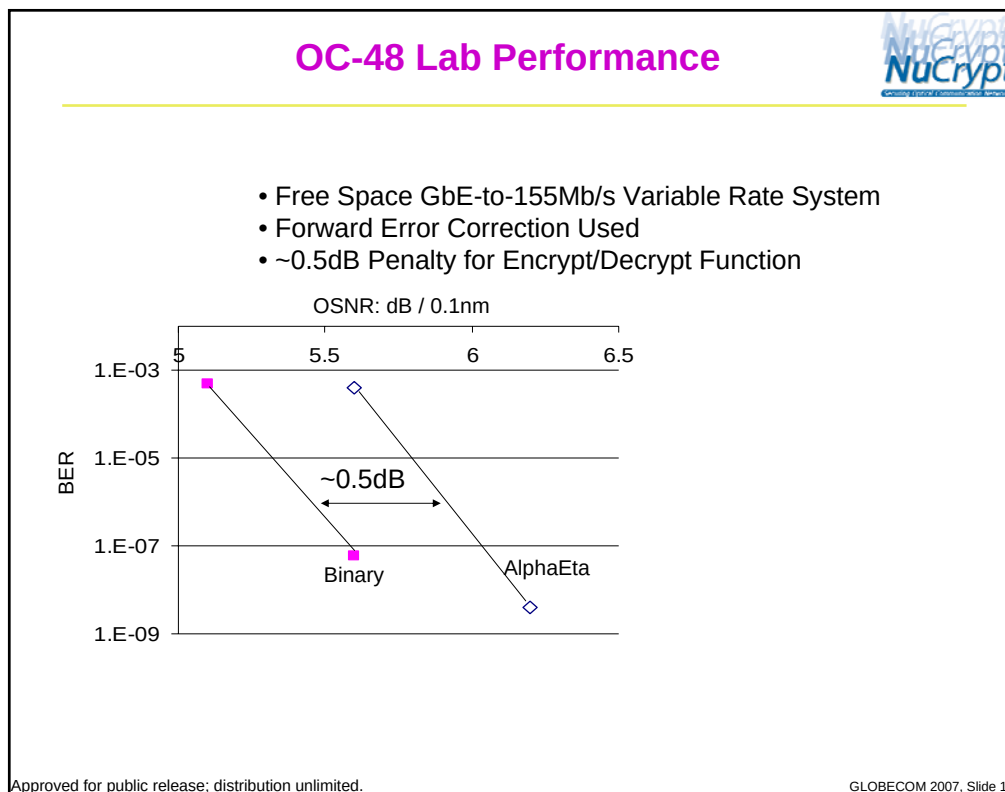
Approved for public release; distribution unlimited.

GLOBECOM 2007, Slide 10









### Summary



AlphaEta is a *practical* physical **encryption** system:

- Performance similar to standard systems: ~1dB performance reduction observed
- Uses off the shelf components
- Use best available traditional cryptographic algorithms
- Improved security via random noise / added complexity
- Known plaintext attack → low correlation statistical attack
- Lots of practical issues for Eve- How to phase-lock to a dense, noisy M-ary constellation?
- Demonstrated Drop-in compatibility with all-optical fiber networks- 850km in-ground demo
- 2.5Gb/s data rates attainable now

Approved for public release; distribution unlimited. GLOBECOM 2007, Slide 16