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

Outline

General Cryptography:
• Encryption vs. Key Generation
• Quantum Cryptography vs. Physical Cryptography
• Randomized Ciphers

AlphaEta Encryption:
• Basic principle/Security
• Simulations
• Experiments/Demonstrations
**After quantum keys are distributed: Physical-Layer Encryption Aided by Optical Noise**

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.

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

- Ciphertext only attack
- Statistical attack
- Known plaintext attack

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

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)
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

Bits shrouded in quantum-noise of light

EVE

Use of secret key unveils the shroud for Bob

BOB

AlphaEta Block Implementation

ALICE

- $K$
- $r$
- $r+1$
- $\phi$
- EDFA
- Quantum Noise
- (Encrypt)

BOB

- Data
- $\phi$
- MOD
- (Decrypt)
- DeMod
- Data OUT

EVE

Approved for public release; distribution unlimited.
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)

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
Simulated Performance of 10 Gb/s AlphaEta in a DWDM Network

Alice

N times Mux

23 Regular 10G NRZ Channels

80km SMF DCF

Bob

Simulated Performance of 10 Gb/s AlphaEta in a DWDM Network

- Highly accurate modified covariance matrix method simulation
- Linear (dispersion, EDFA noise, filtering) and nonlinear (XPM, SPM, FWM) effects included
- 12 channel High density (50GHz spacing) 10Gb/s NRZ system: >1500km reach with 40 states obscured by noise (14 bit DAC)
- Single channel 10Gb/s AlphaEta: >5000km reach with 80 states obscured by noise
- Super-high security simulation with half-circle DSR noise: 2.5Gb/s, 24 channel 25GHz spacing, ~900km reach

V.S. Grigoryan et al, OFC 2007 and ECOC 2005
G.S. Kanter et al, SPIE Fluctuations and Noise Conference 2005
Physical-layer encryption aided by optical noise

---

**Telcordia / Northwestern University**  
ATDNet / BOSSNET OC-12 Demonstration

850km loop: Maryland to New York and back

Open Eye / FEC Correctable BER  
After 850km (622Mb/s)

T. Banwell et al, MilCom 2005

---

**NuCrypt OC-48 (2.5Gb/s)**  
210 km Lab Test

DPSK Signal  
AlphaEta Encrypted/Decrypted Signal

18.1dB/0.1nm  
18.1dB/0.1nm
**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

---

Physical-layer encryption aided by optical noise