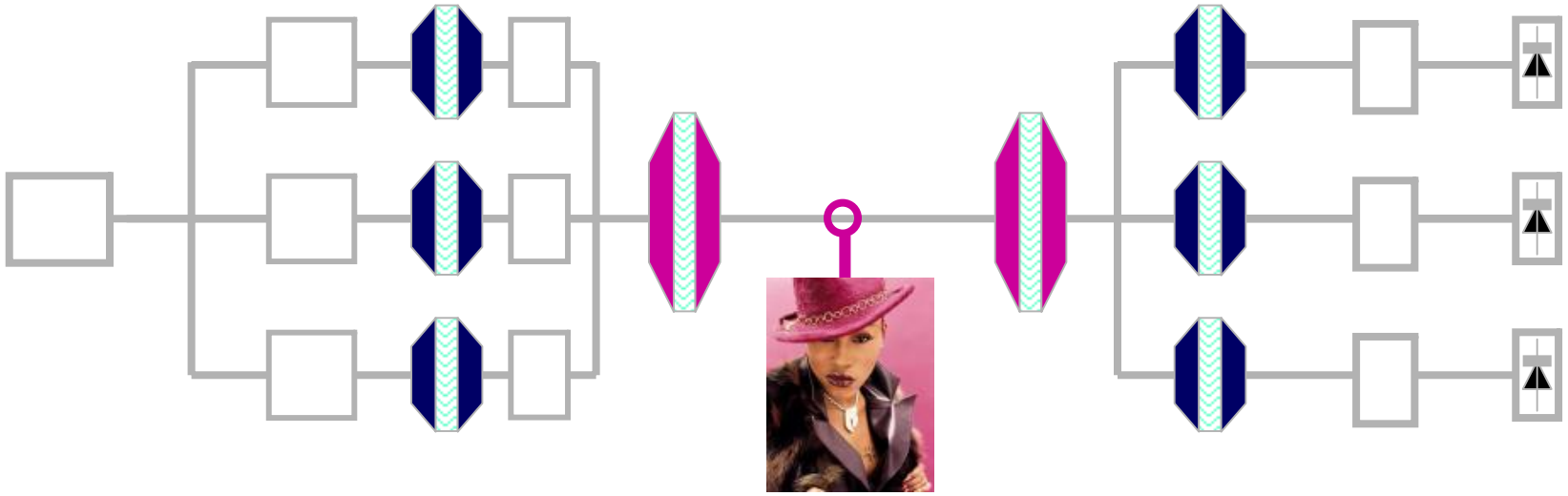
# Towards a Cryptanalysis of Scrambled Spectral-Phase Encoded OCDMA

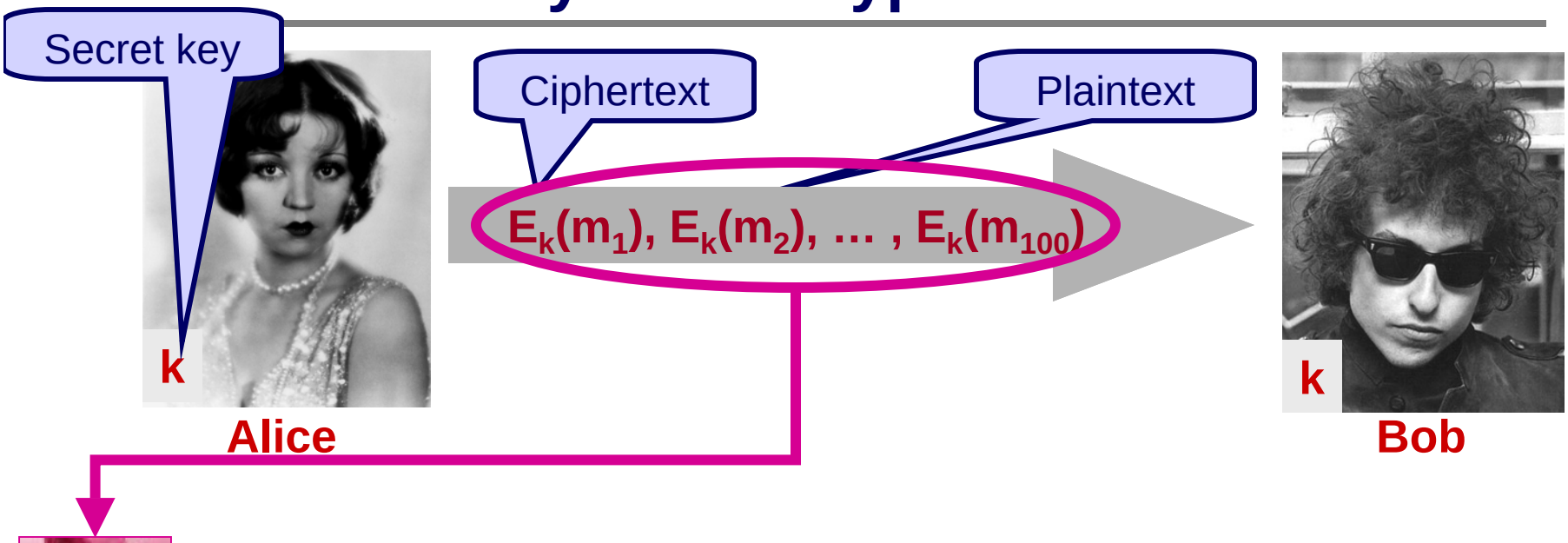


**Sharon Goldberg***

Ron Menendez**, Paul R. Prucnal*

*Princeton University, **Telcordia Technologies

# Security for Encryption Schemes




**Defining security:**

~~Ciphertext Only (COA): Given ciphertexts, Eve can't recover $m_1, \ldots, m_{10}$~~

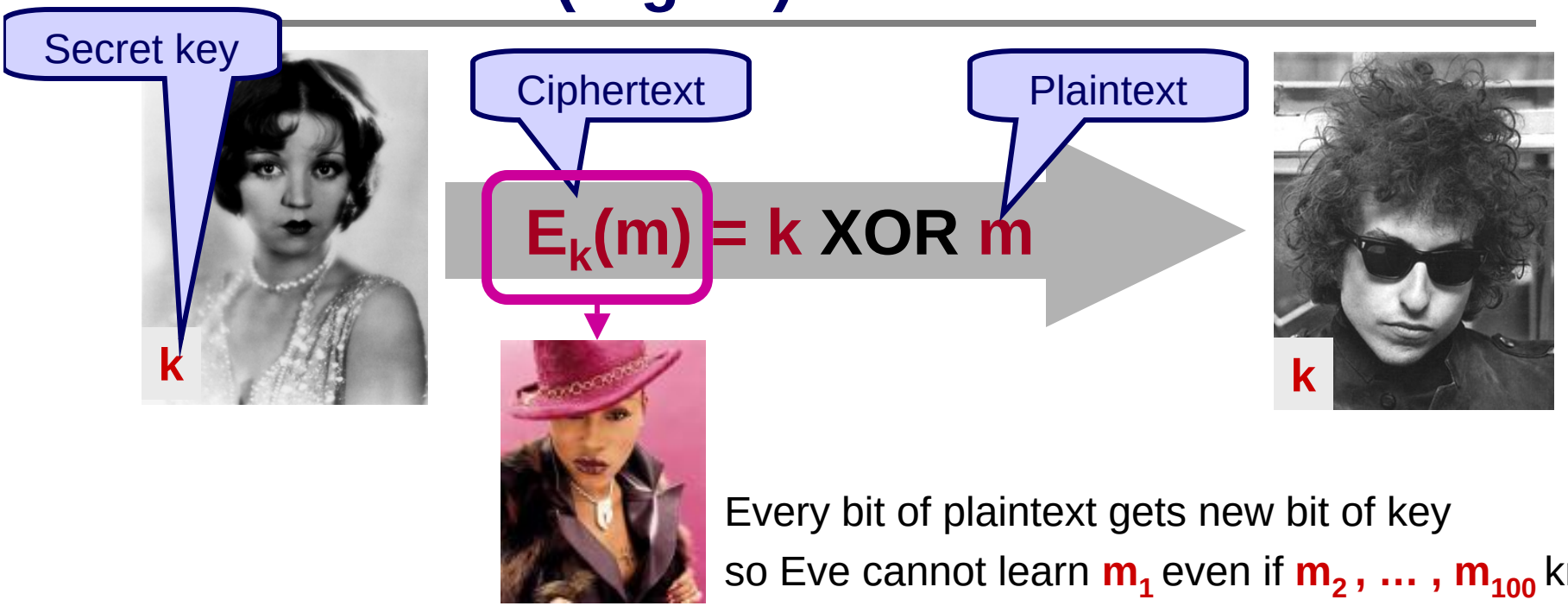
Known Plaintext (KPA): Given ciphertexts, Eve can't learn $m_1$ even if $m_2, \ldots, m_{100}$ known

*e.g.,* SONET header

*e.g.,* SONET payload

**Kerchoff's Principle (1883):** System should be secure even if encryption / decryption algorithms are known, as long as key is secret.

# The (Digital) One Time Pad




Every bit of plaintext gets new bit of key
so Eve cannot learn $m_1$ even if $m_2$ , … , $m_{100}$ known

**Major Limitation: key length = message length**

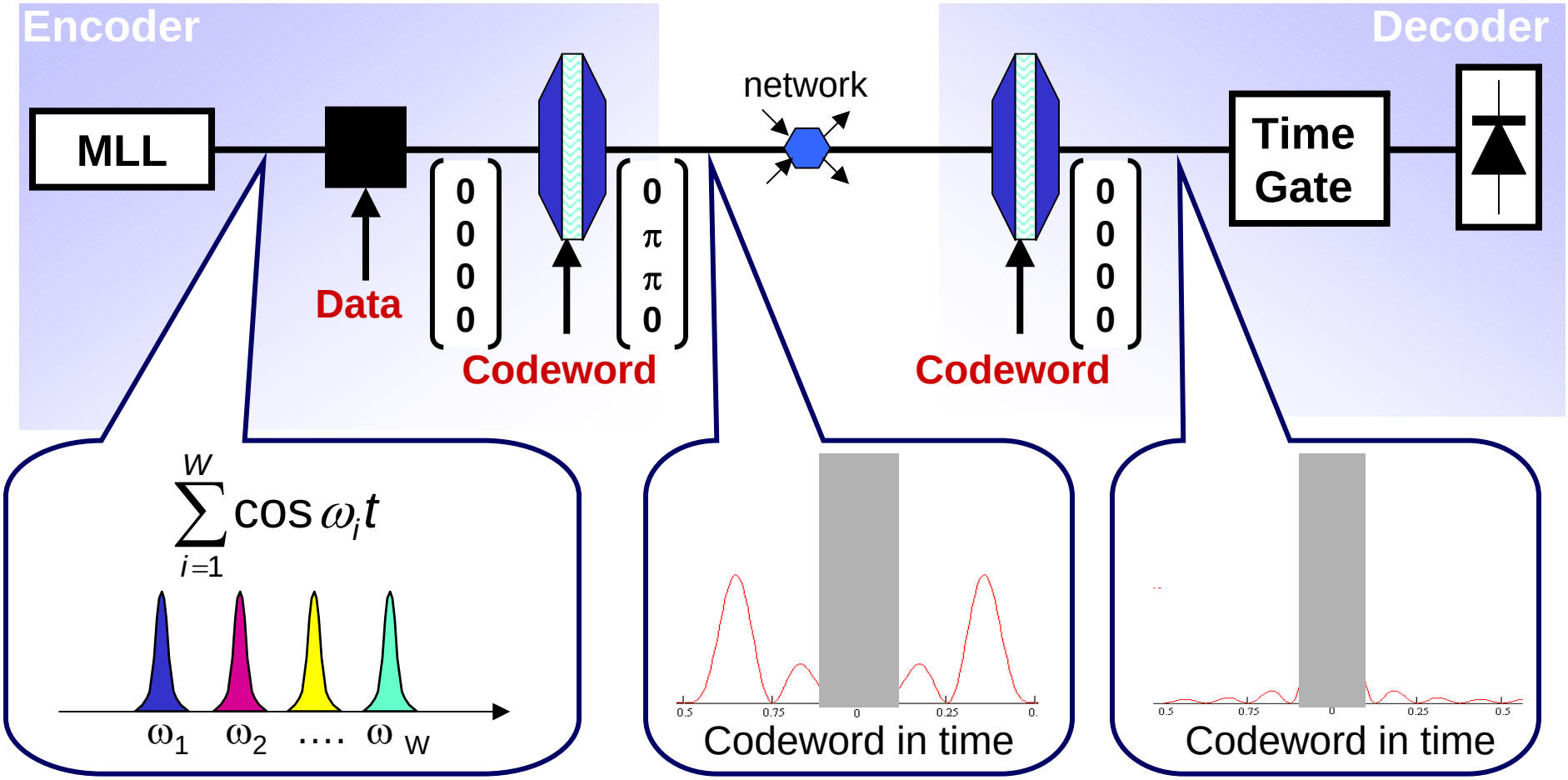
Generating and sharing the key is expensive

Digital solutions: Block ciphers like AES, Stream ciphers like RC4

**Can we encrypt at data optically faster than we could electronically?**

**Can optics do more than the digital one-time-pad?**

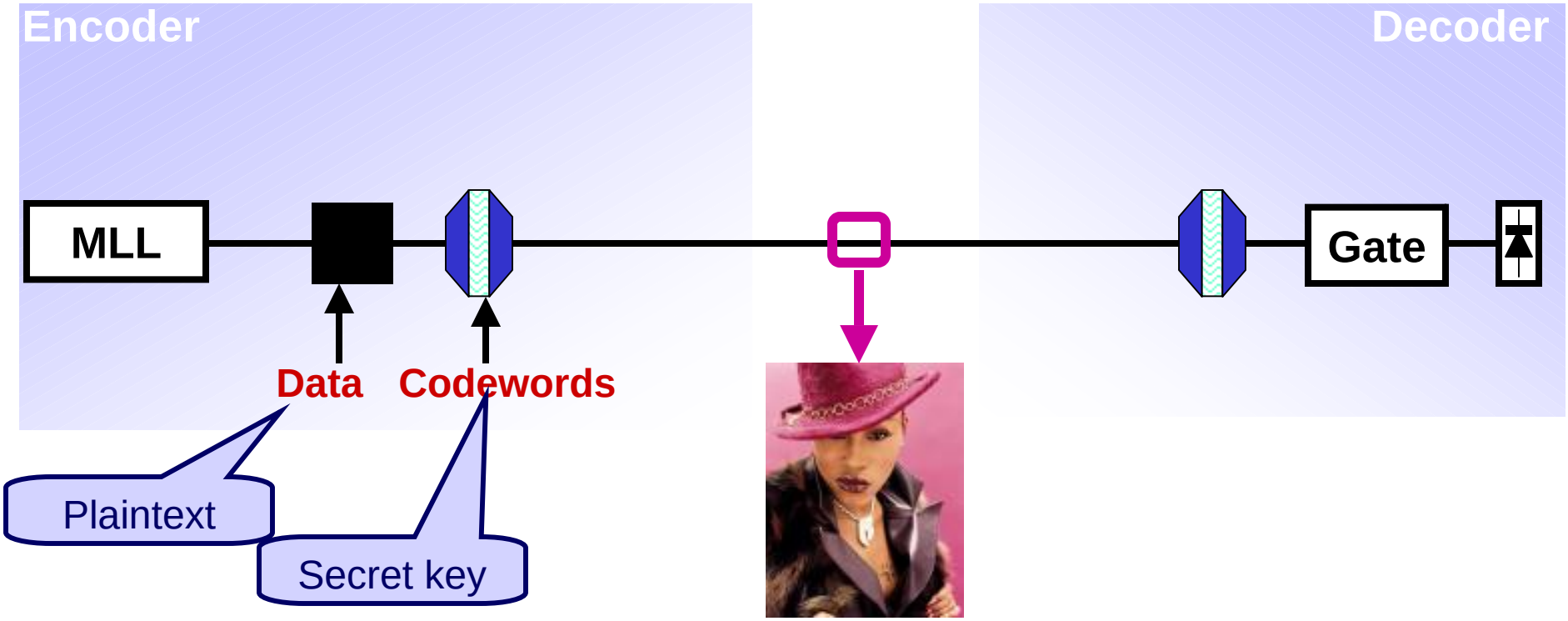
# Spectral Phase Encoded Optical CDMA (1)




Use orthogonal codewords

W frequencies → W codewords

# Spectral Phase Encoded OCDMA



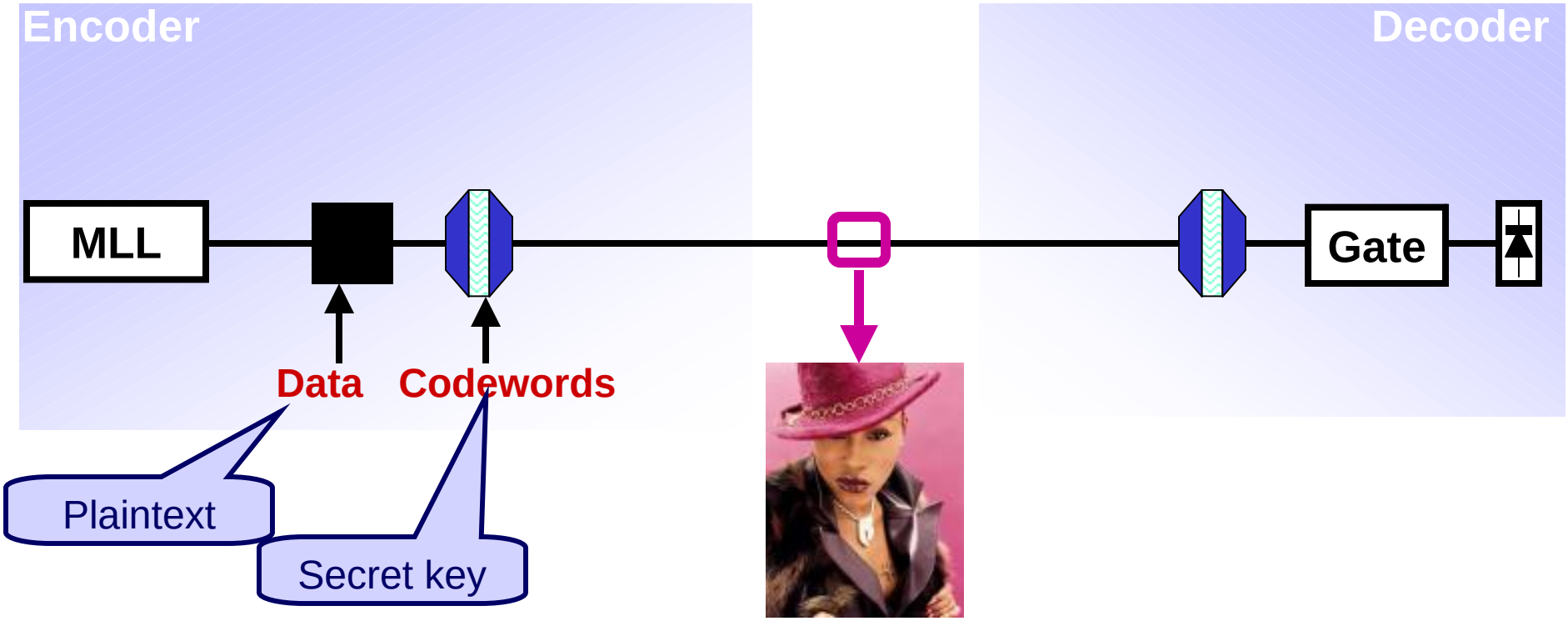

**Previous ciphertext-only attacks:**

**On-off-keying:** Eve uses energy detection to distinguish 0 & 1

**Isolated code:** Eve learns codeword by comparing adjacent phase elements **[Shake 05]**

Eve uses spectrum to distinguish 0 & 1 **[Leaird-Jiang-Weiner 05]**

# Spectral Phase Encoded OCDMA




**Previous ciphertext-only attacks:**

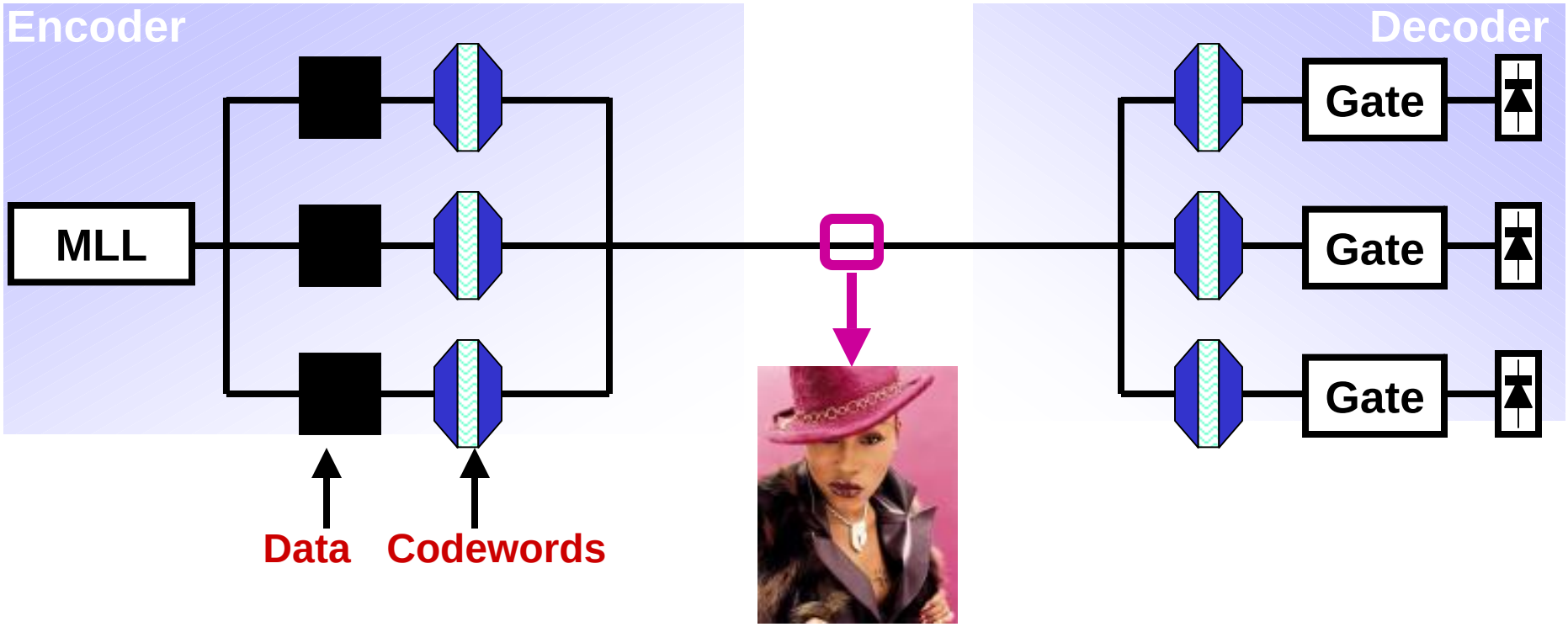
**On-off-keying:** Eve uses energy detection to di

**Use constant energy modulation**
(2-code-keying or PSK)

**Isolated code:** Eve learns codeword by comparing adjacent phase elements **[Shake 05]**

Eve uses spectrum to distinguish 0 & 1 **[Leaird-Jiang-Weiner 05]**

# Scrambled Spectral Phase Encoded OCDMA (1)




**Previous ciphertext-only attacks:**

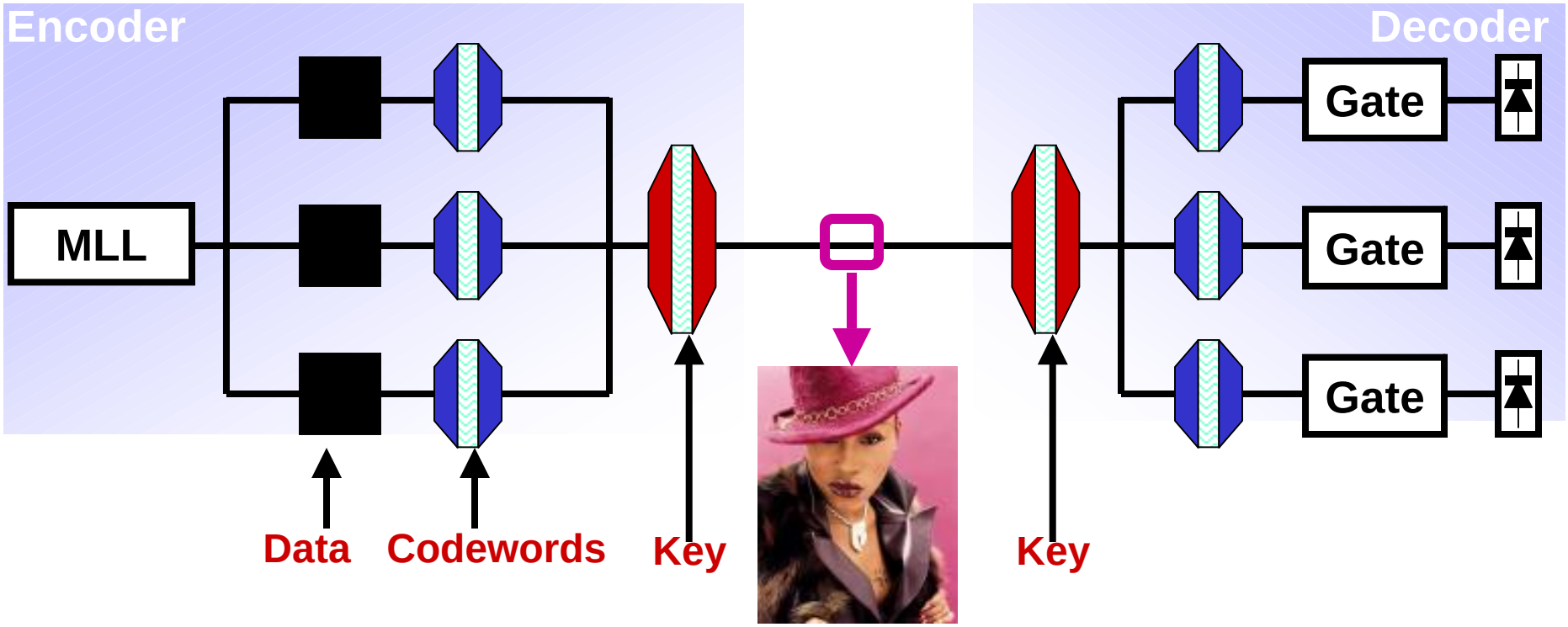
~~**On-off-keying:** Eve uses energy detection~~ → **Use constant energy modulation** (2-code-keying or PSK)

~~**Isolated code:** Eve learns codeword by compa~~ → **Use N tributaries** (Inverse Mux)

Eve uses spectrum to distinguish 0 & 1 **[Leaird-Jiang-Weiner 05]**

**Small codeset:** Eve builds detector, tries decoding with each of the **W** possible codewords

# Scrambled Spectral Phase Encoded OCDMA (1)




**Previous ciphertext-only attacks:**

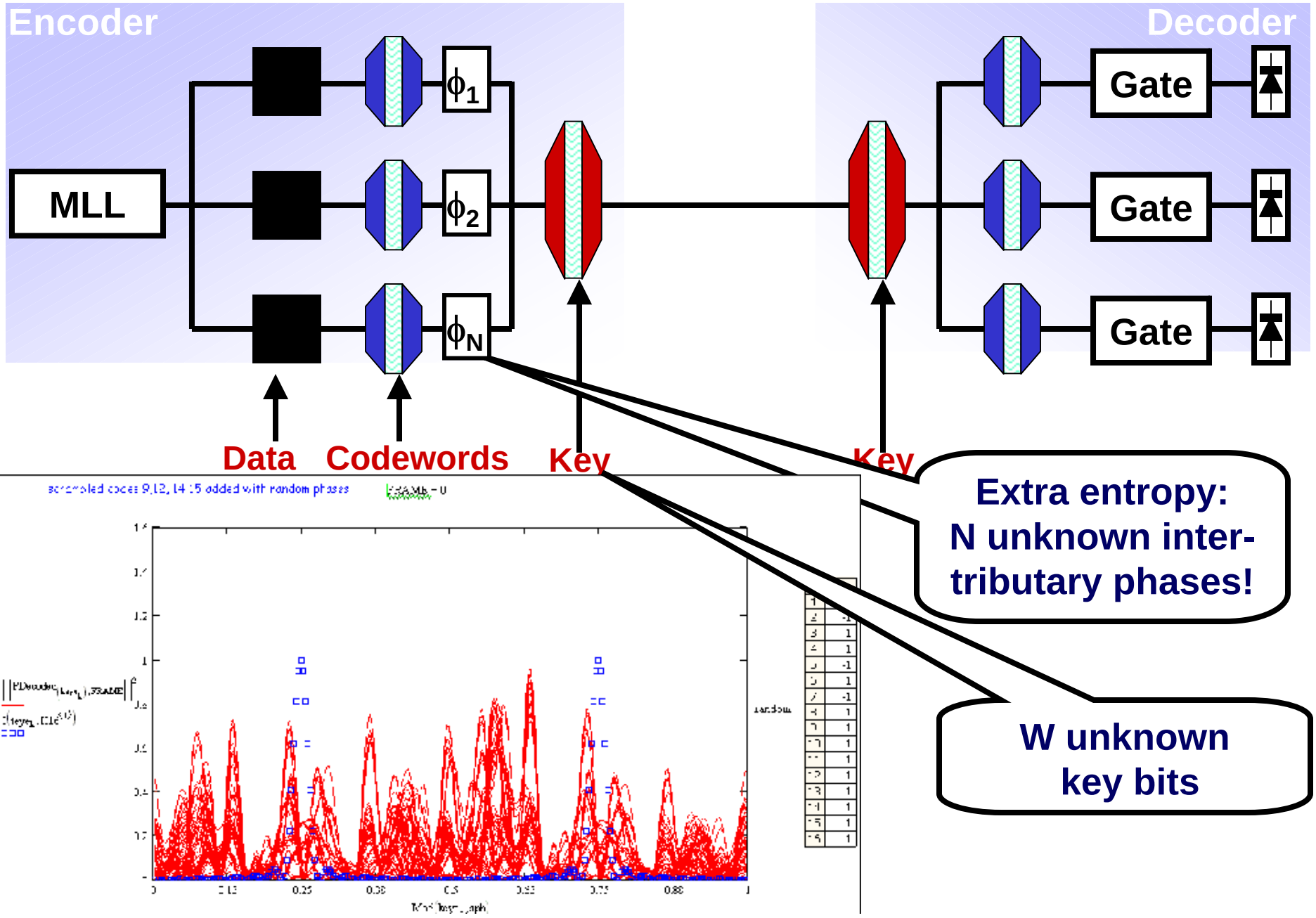
~~**On-off-keying:** Eve uses energy detection~~ → **Use constant energy modulation** (2-code-keying or PSK)

~~**Isolated code:** Eve learns codeword by compa~~ → **Use N tributaries** (Inverse Mux)

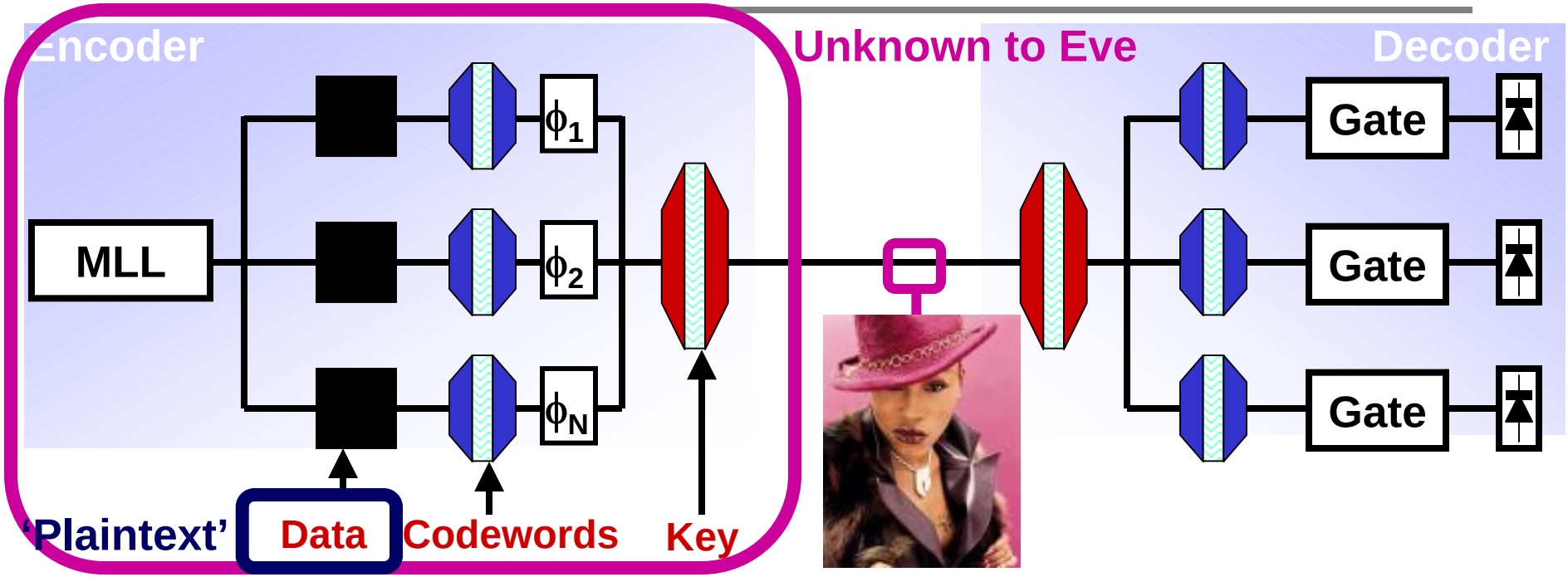
Eve uses spectrum to distinguish 0 & 1 [Le

~~**Small codeset:** Eve builds detector, tries decoding~~ with each of the **W** possible codewords → **Now there are $2^W$ codewords** [Menendez-et.al-2005] [Xue-Du-Yoo-Ding-2006]

# Scrambled Spectral Phase Encoded OCDMA (2)

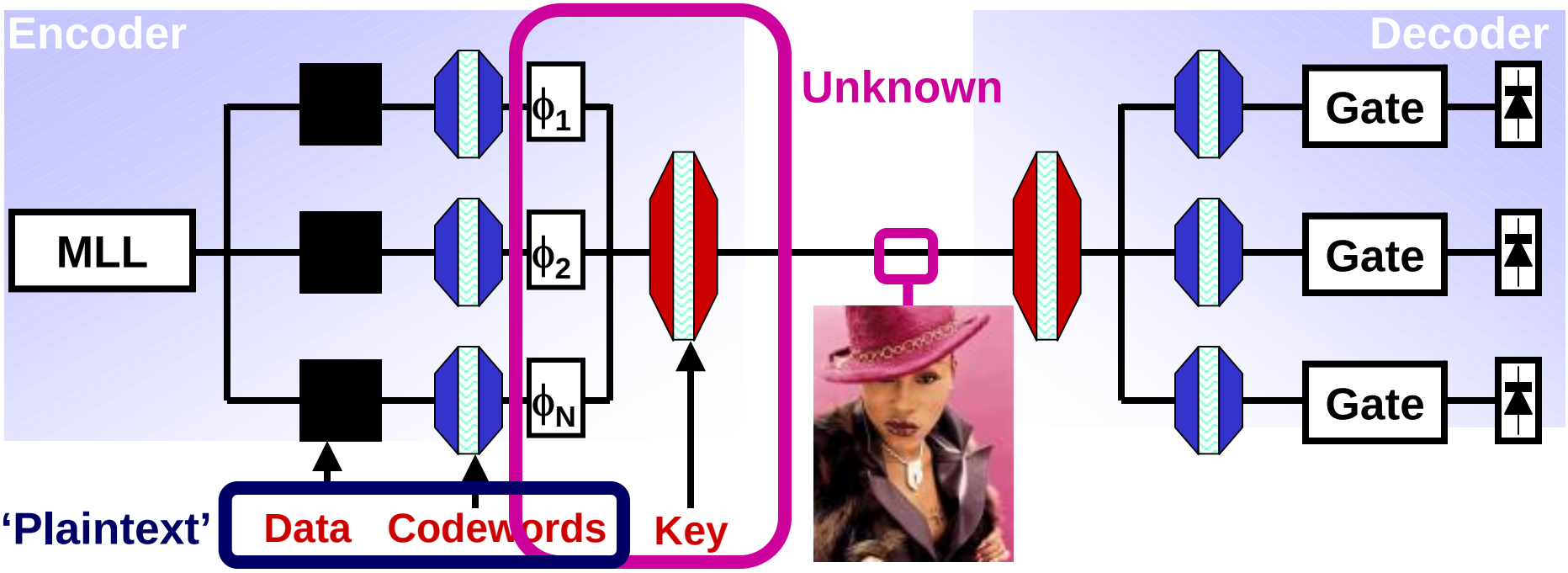


# Security of Scrambled SPE-OCDMA




**Brute Force:** Ciphertext-only exhaustive search thru $2^{\text{Frequencies}}$ keys

# Security of Scrambled SPE-OCDMA

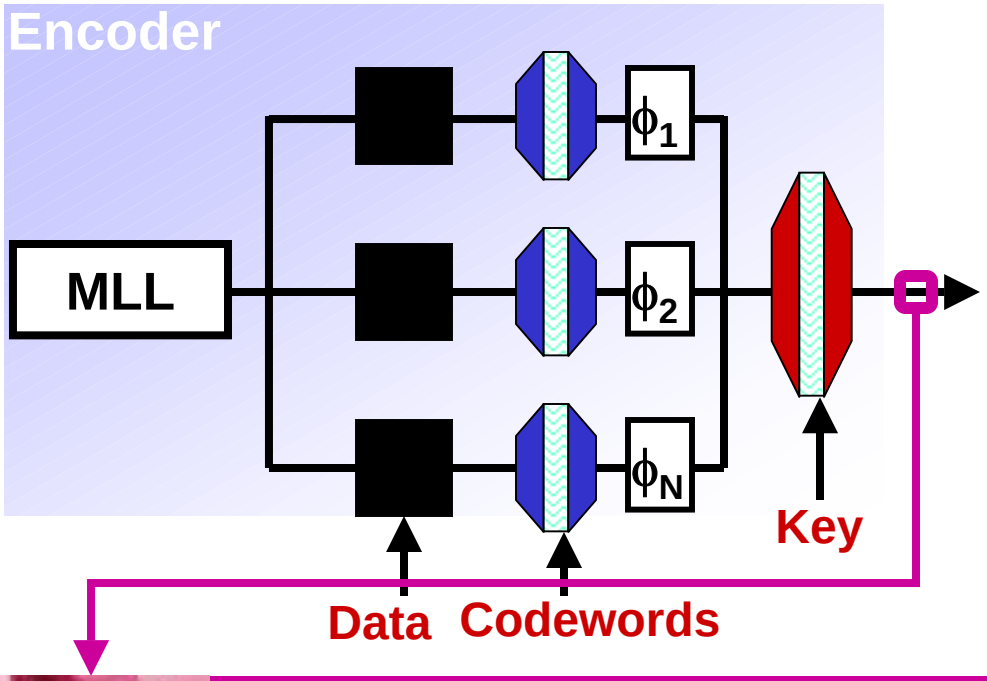



**Here we assume all secrecy in the system comes from the scrambler key.**

⇒ By Kerchoff's Principle, we assume that codewords are known to Eve.

| | |
|---|---|
| **Brute Force:** | Ciphertext-only exhaustive search thru $2^{\text{Frequencies}}$ keys |
| **Result 1:** | Known plaintext exhaustive search thru $2^{\text{Tributaries}}$ keys<br>Need 1 known plaintext and 1 "set of measurements" |
| **Result 2:** | Can immediately learn key without exhaustive search<br>Need 2 known plaintexts and 2 "sets of measurements" |

# Eve's 'set of measurements'




Electric field at frequency $\omega_i$

$$E_i(t) = k_i \sum_{j=1}^{N} \theta_{ij} d_j \cos(\omega_i t + \phi_j)$$

Key phases

Tributaries

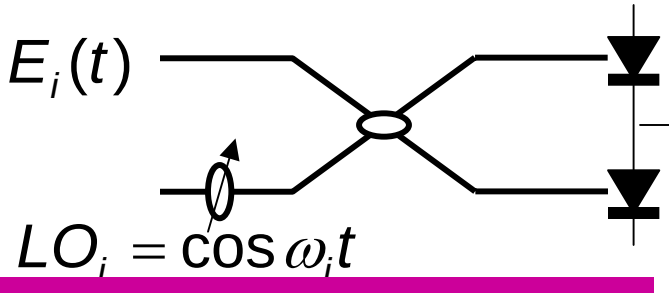
Codes

Inter-tributary phases

Data

**Plaintext**

Use balanced coherent detection at each frequency **[Shake 2005]**



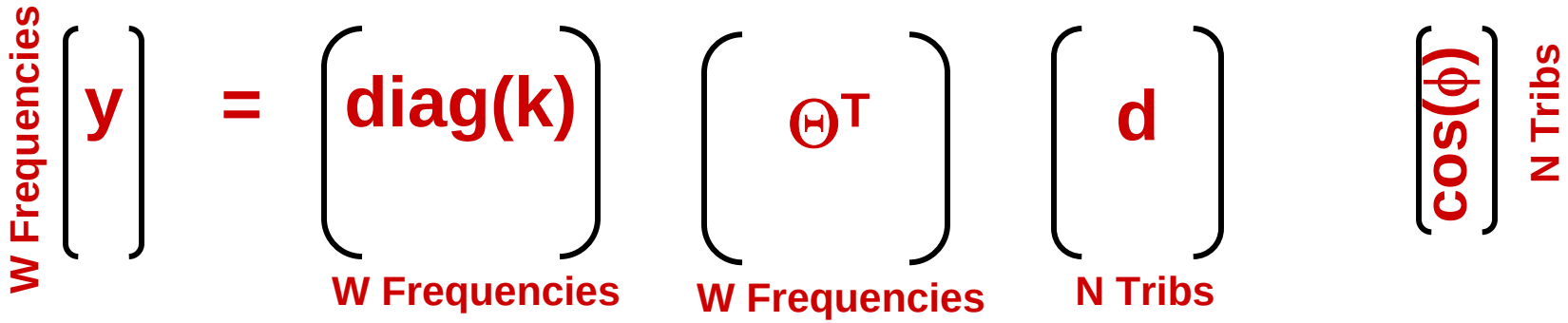

Obtain analog measure of current

$$I_i(t) \propto k_i \sum_{j=1}^{N} \theta_{ij} d_j \cos(\phi_j)$$

**Measurement**

**In our attacks:** For each known plaintext, we assume Eve gets **W** simultaneous (noise-free) current measurements

# Result 1: Reducing exhaustive search space




| **measurement** | **key** | **codes** | **plaintext** | **inter-trib phases** |
|---|---|---|---|---|
| real valued | discrete {1,-1} | discrete {1,-1} | discrete {1,-1} | real valued |
| ✓**known** | ?**secret** | ✓**known** | ✓**known** | ?**unknown** |

1. Eve obtains a **coherent measurement** set **y** and a known plaintext **d**
2. Eve has **W** equations in **W + N** unknowns
   **On computer**, guess just **N** key **bits** then solve for **W-N** remaining key bits
3. Eve tries the key on **decoder**. Stop if ungarbled data, else repeat step 2.

| | |
|---|---|
| **Brute Force:** | Ciphertext-only exhaustive search thru $2^{\text{Frequencies}}$ keys |
| **Result 1:** | Known plaintext exhaustive search thru $2^{\text{Tributaries}}$ keys |

# Result 2: Learning the key with 2 known plaintexts

$$\underset{\text{W Frequencies}}{\begin{bmatrix} y \end{bmatrix}} = \underset{\text{W Frequencies}}{\begin{bmatrix} \text{diag}(k) \end{bmatrix}} \underset{\text{W Frequencies}}{\begin{bmatrix} \Theta^T \end{bmatrix}} \underset{\text{N Tribs}}{\begin{bmatrix} d \end{bmatrix}} \underset{\text{N Tribs}}{\begin{bmatrix} \cos(\phi) \end{bmatrix}}$$

| **measurement** | **key** | **codes** | **plaintext** | **inter-trib phase** |
|---|---|---|---|---|
| real valued | discrete {1,-1} | discrete {1,-1} | discrete {1,-1} | real valued |
| ✓ **known changes** | ? **secret fixed** | ✓ **known fixed** | ✓ **known changes** | ? **unknown changes** |

1. Eve gets **2 coherent measurement / known plaintext** pairs **$(y_1, d_1)$ $(y_2, d_2)$**
2. Eve has **2W** equations in **W + 2N** unknowns where **$2N \leq W$**

   **On computer** solve the equations for the key **k**.

**What is dimension of solution space for this system of equations?**

If dimension **N**, there are **$2^N$** solutions and Eve learns nothing.
If there is a **unique** solution, Eve has learned the key

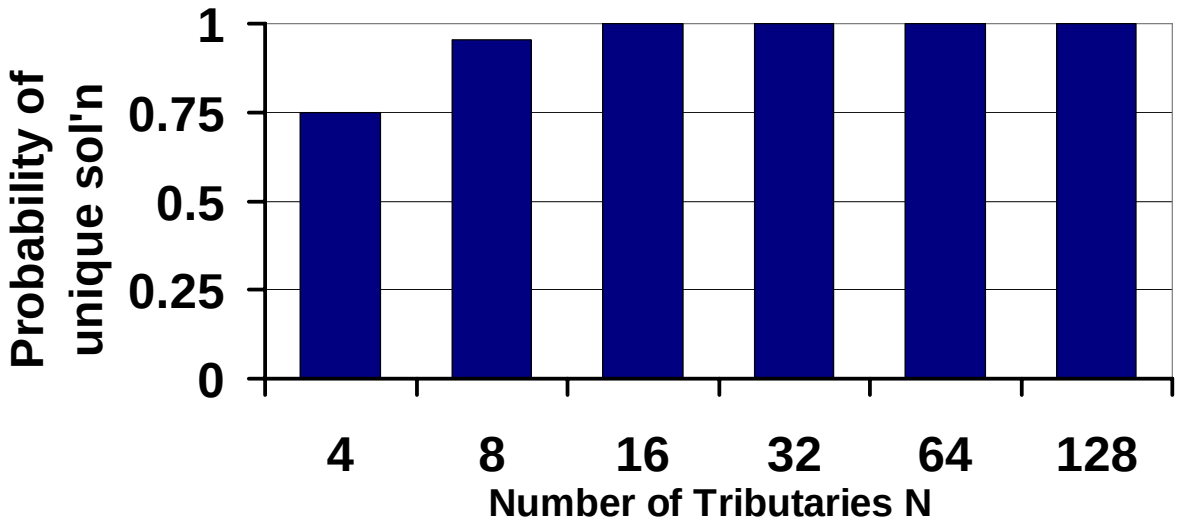
# Result 2: Learning the key with 2 known plaintexts

**What is dimension of solution space for this system of equations?**

If there is a **unique** solution, Eve has learned the key

For a system using Hadamard codes (e.g. [Menendez2005]) with **2N=W**

gets **2** plaintexts $\mathbf{d_1}$ , $\mathbf{d_2}$ chosen at random and **2** noise-free measurements




**Theorem:** If either known plaintext represents an odd number of '0' bits then there is a unique solution.

⇨at least 75% of plaintext pairs give a unique solution

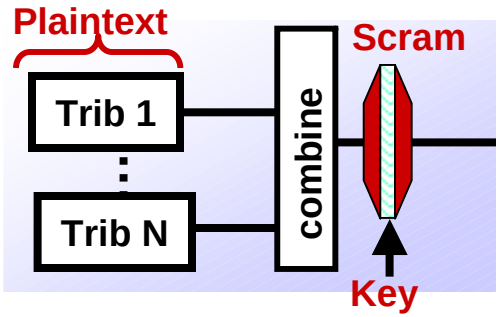
**Result 2:** Can immediately learn key (w.h.p.) without exhaustive search

Need 2 known plaintexts and 2 "sets of measurements"

# Conclusion and Open Problems

**Scrambled spectral-phase encoded OCDMA:**

- All secrecy from scrambler key ($2^{\text{Frequencies}}$ keys)
- Tributary codewords are known
- Binary scrambling phases




**Our Attacks**: Simultaneously measure electric field at $f_i$ for all $f_i$

- Co-polarized local oscillator phase- & time- synchronized with incoming signal
- Coherent balanced detection and noise-free analog current measurement

Parallelism is important!

**Result**

Known plaintext exhaustive search thru $2^{\text{Tributaries}}$ keys
(Need 1 known plaintext and 1 "set of measurements")

Can immediately learn key without exhaustive search
(Need 2 known plaintexts and 2 "sets of measurements")

**Open Issues:**

- **How often must the key be changed to secure the system?**
- Non-idealized measurements (noisy matrices / integer linear programming)
- Including the tributary codewords in the key (*i.e.*, make them secret)

## Thanks:

Boaz Barak

Jennifer Rexford

Moses Charikar

Eugene Brevdo

Parts of this work were supported by DARPA