Encryption at the Speed of Light?

Towards a cryptanalysis of an optical CDMA encryption scheme

Sharon Goldberg*

Ron Menendez**, Paul R. Prucnal*

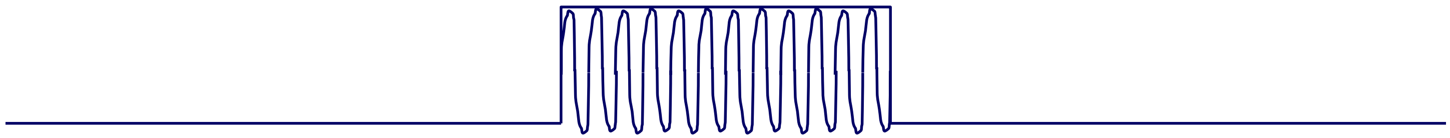
*Princeton University, **Telcordia Technologies

IPAM Workshop on Special purpose hardware for cryptography

Los Angeles, December 5, 2006

Optical Encryption?

Optical signals are **analog signals** at **frequencies in the THz**



Not feasible to measure all high frequency parts of optical signal

Key ideas behind optical encryption:

- Assume a realistic adversary that cannot measure all the high frequency portion of an optical signal.
- Hide information in the optical signal using secret key and noise

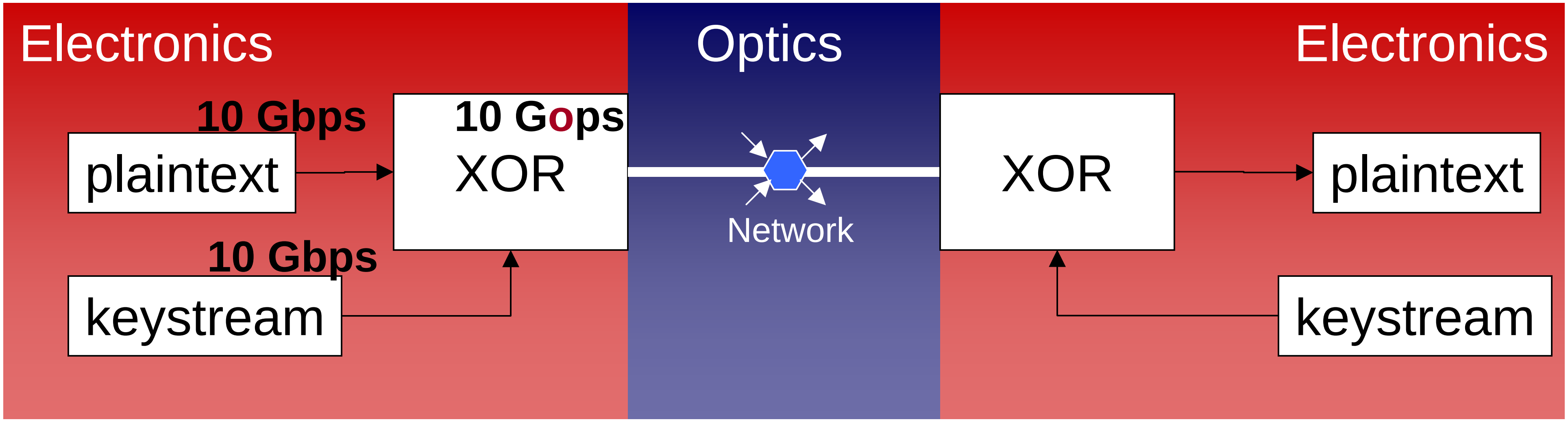
much interest in the **optics** community

- The hope: extremely fast encryption

Today we begin to **cryptanalyse** a variant of the promising **optical encryption** system of [Menendez, et.al., Oct. 2005]

…and we show situations where we learn key with 2 known plaintexts

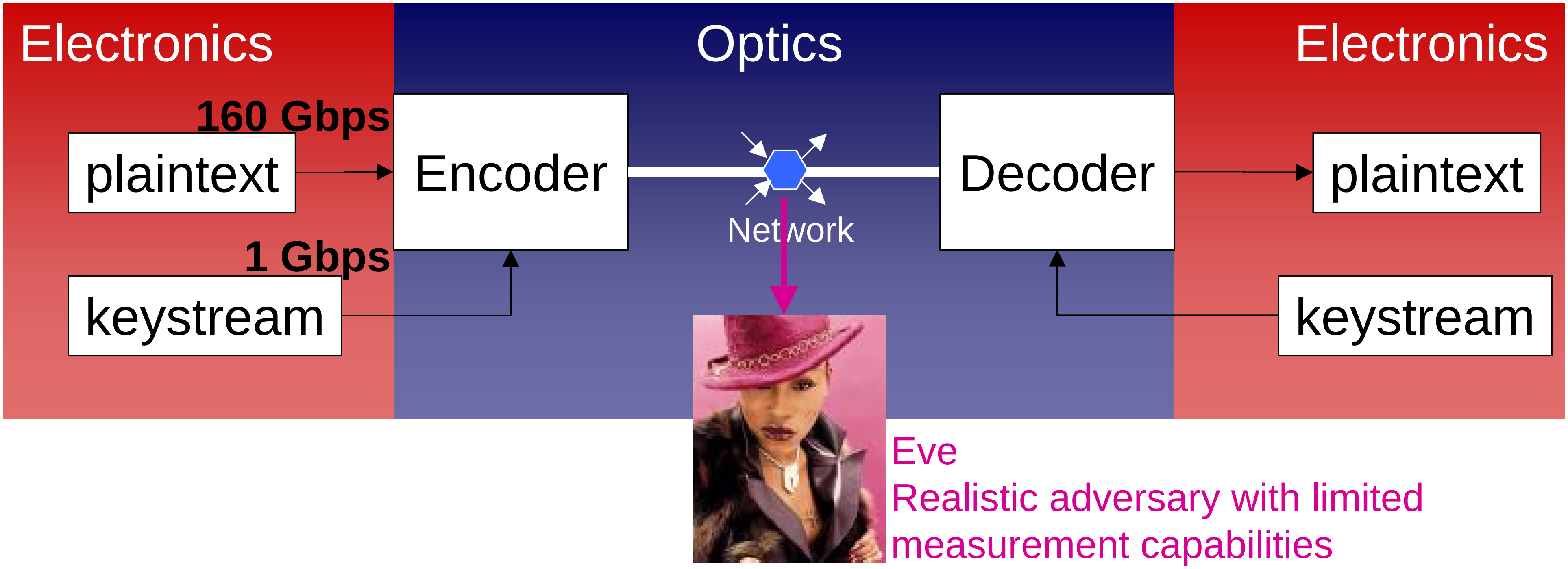
Why use optical encryption?   (1)



Electronic stream ciphers

rate of keystream = rate of data stream

Why use optical encryption?   (2)



The holy grail:

Encryption with data rates FASTER than crypto operation rates

rate of keystream << rate of data stream

Use properties of optical signals to do more than an electronic one-time-pad

Encryption with optical CDMA

Over 10 years of research by the optics community:

[Tancevski and Andonovic, Elec. Lett., 1994]

"… suitable for truly asynchronous highly secure LAN applications…"

DARPA Optical CDMA program (2002-Today):

"The benefits of the program will be optical communications systems with enhanced multi-level security, low probability of intercept, detection and jamming, traits which enhance the reliability and the survivability of military networks."

Some recent (independent) publications:

[TH Shake, J. Lightwave Technology, April 2005]

[R. Menendez et al., J. Lightwave Technology, Oct. 2005]

[F Xue, Y Du, B Yoo, and Z Ding, Optical Fiber Communication Conference, 2006]

[DE Leaird, Z Jiang, AM Weiner, Optical Fiber Communication Conference, 2006]

[BB Wu, EE Narimanov, Optics Express, 2006] & EE Times & ScienceDaily &&&&

Encryption with optical CDMA

Over 10 years of research by the optics community:

[Tancevski and Andonovic, Elec. Lett., 1994]

"… suitable for truly asynchronous highly secure LAN applications…"

DARPA (

"The ben … tems
with enha … etection
and jamm … ability of
military n

Some re

[TH Shake,

BUT

Very little work by the security or cryptanalysis community!

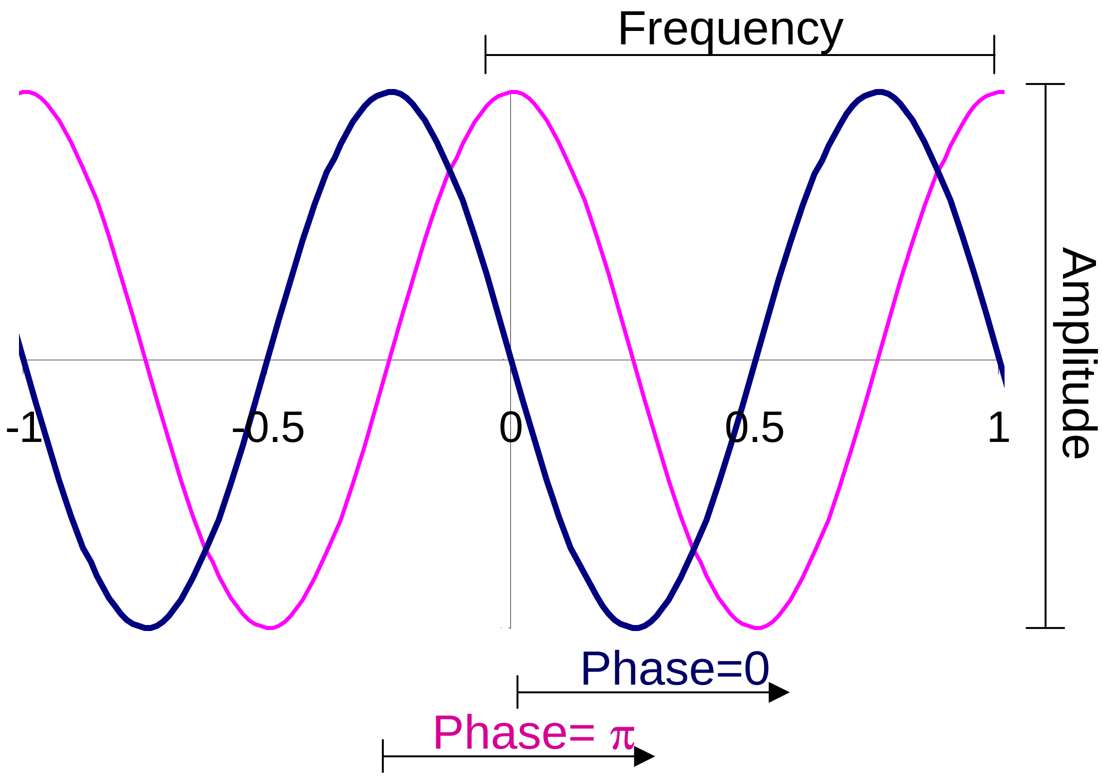
[R. Menendez et al., J. Lightwave Technology, Oct. 2005]

[F Xue, Y Du, B Yoo, and Z Ding, Optical Fiber Communication Conference, 2006]

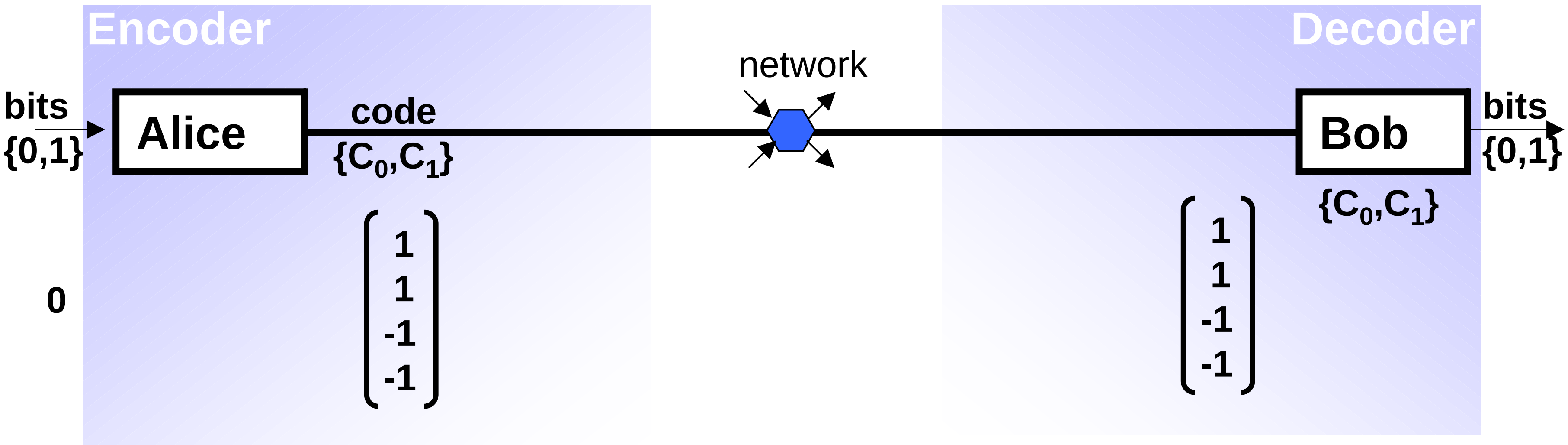
[DE Leaird, Z Jiang, AM Weiner, Optical Fiber Communication Conference, 2006]

[BB Wu, EE Narimanov, Optics Express, 2006] & EE Times & ScienceDaily &&&&

Optics 101



System overview: 1st (bad) attempt



Alice and Bob get a pair of unique codewords

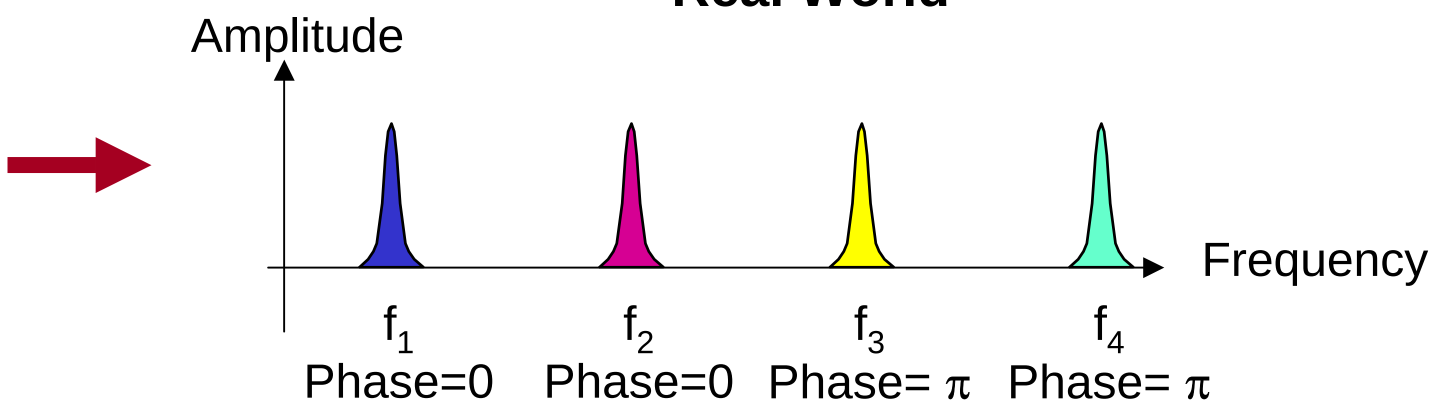
To send a **0** bit: **Alice** transmits codeword C_0

To send a **1** bit: **Alice** transmits codeword C_1

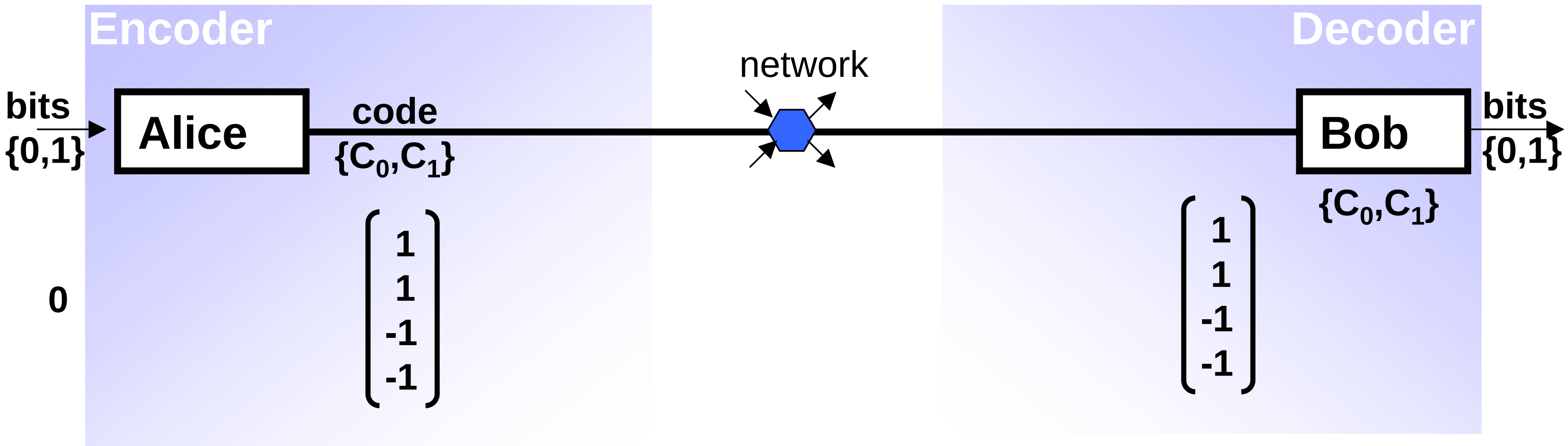
Abstraction

$$C_0 = \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix}$$

Real World



System overview: 1st (bad) attempt



Bob's (simplified) bit recovery algorithm

Check for a 0 bit:

1. Take dot product with C_0
2. Check for pulse of height 4

$$[\,1\ 1\ {-1}\ {-1}\,] \bullet \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix} = 4$$

Pulse!

Check for a 1 bit:

1. Take dot product with C_1
2. Check for pulse of height 4

$$[\,1\ {-1}\ {-1}\ 1\,] \bullet \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix} = 0$$

No Pulse!

System overview: 1st (bad) attempt

Encoder — **Decoder**

bits $\{0,1\}$ → **Alice** — code $\{C_0,C_1\}$ — network — **Bob** → bits $\{0,1\}$

Bob: $\{C_0,C_1\}$

0 (Plaintext)

Key: $\begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix}$ (Alice); $\begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix}$ (Bob)

Plaintext **Key**

[TH Shake, April 2005]
[DE Leaird, Z Jiang, AM Weiner, 2006]

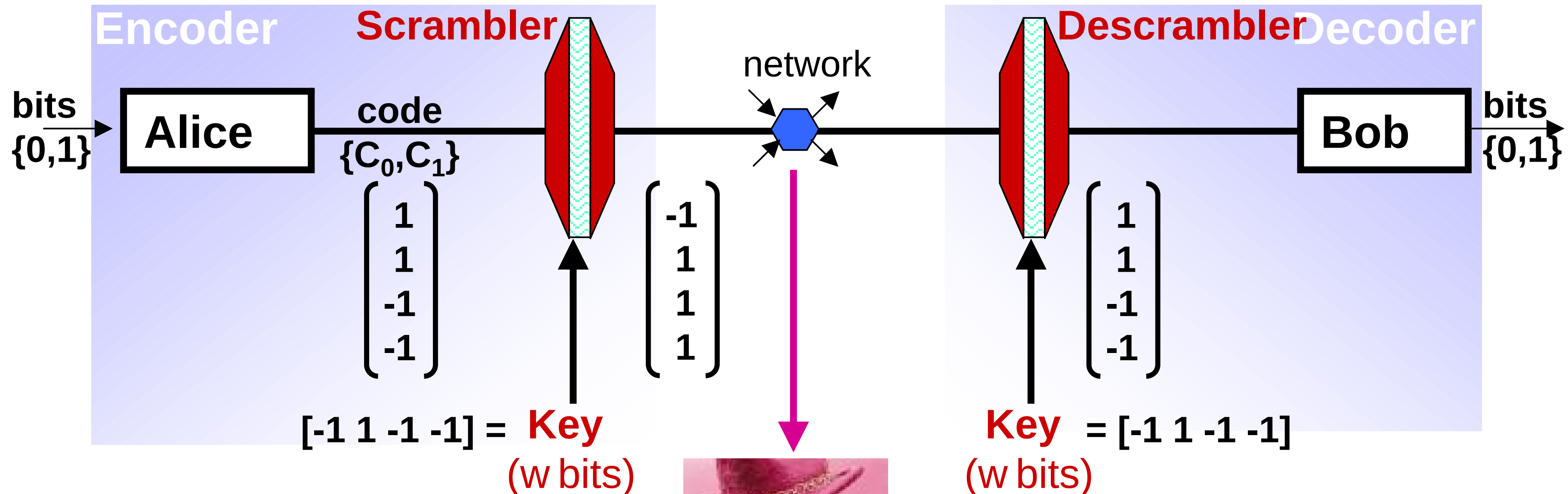
The many-time-one-time pad:
Eve can distinguish between $\mathbf{C_0}$ and $\mathbf{C_1}$ using her own 'Bob' detector with two random codewords

Bob's (simplified) bit recovery algorithm

Check for a 0 bit:
1. Take dot product with $\mathbf{C_0}$
2. Check for pulse of height 4

Check for a 1 bit:
1. Take dot product with $\mathbf{C_1}$
2. Check for pulse of height 4

System overview: 2^{nd} (still bad) attempt



Suppose key bits don't change

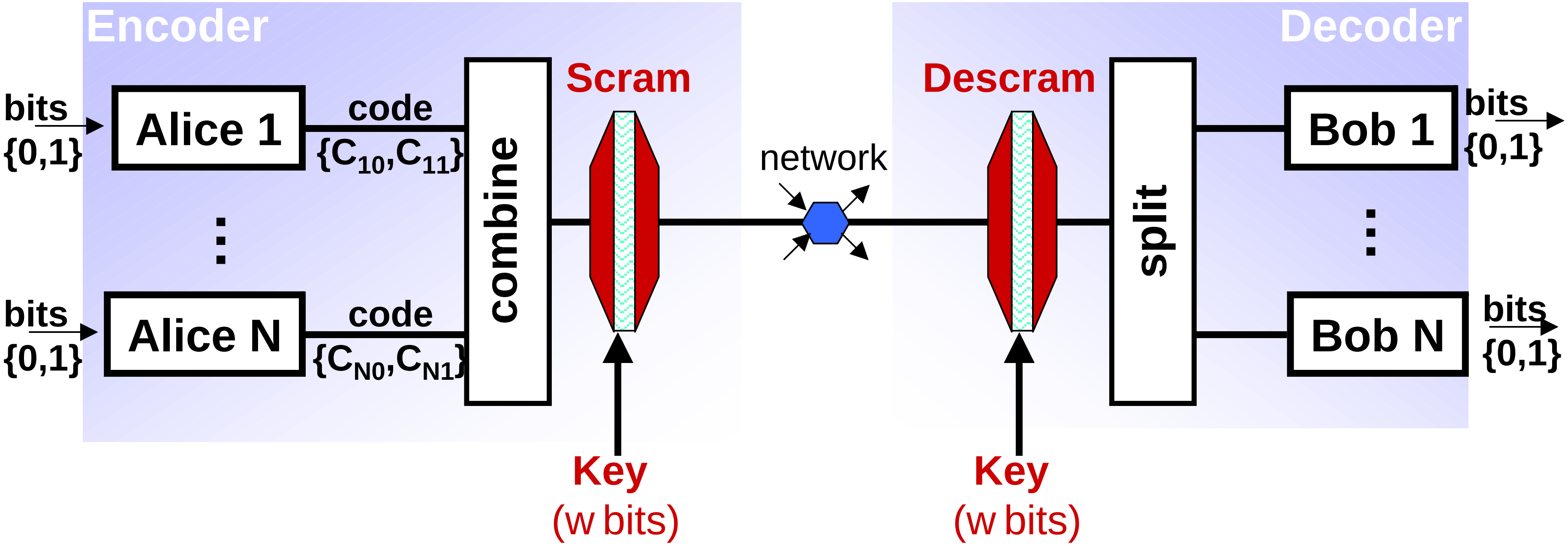
[TH Shake, April 2005]
[DE Leaird, Z Jiang, AM Weiner, 2006]

Still the many-time-one-time pad:
Eve can distinguish between $\mathbf{C_0}$ and $\mathbf{C_1}$ using her own 'Bob' detector with two random codewords

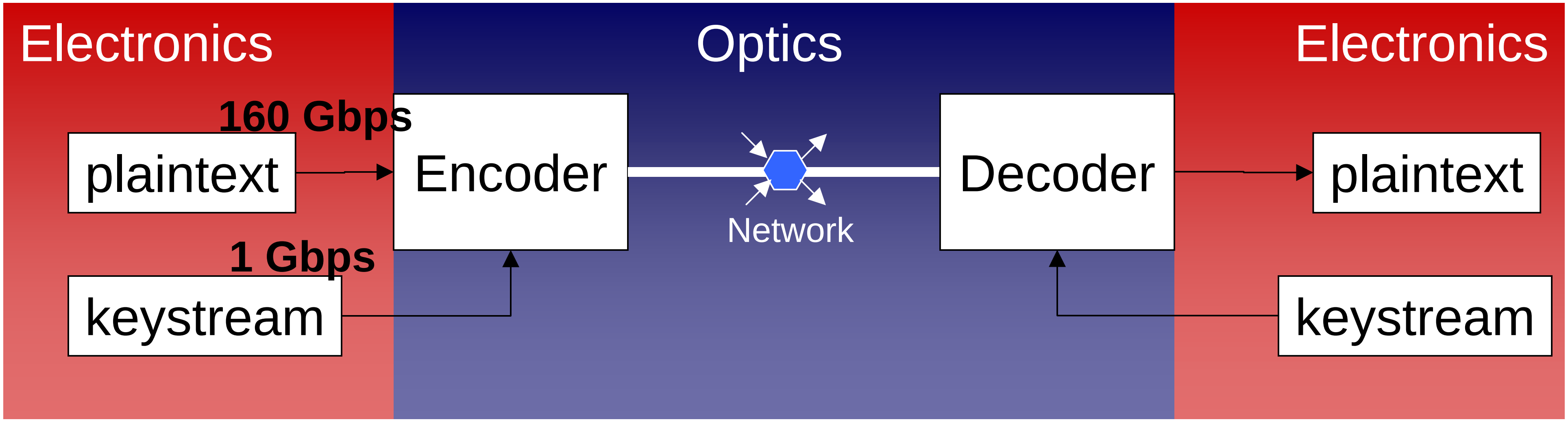
To secure this system:
Refresh key for each new bit of plaintext

Now it's a one-time pad BUT it's not particularly interesting

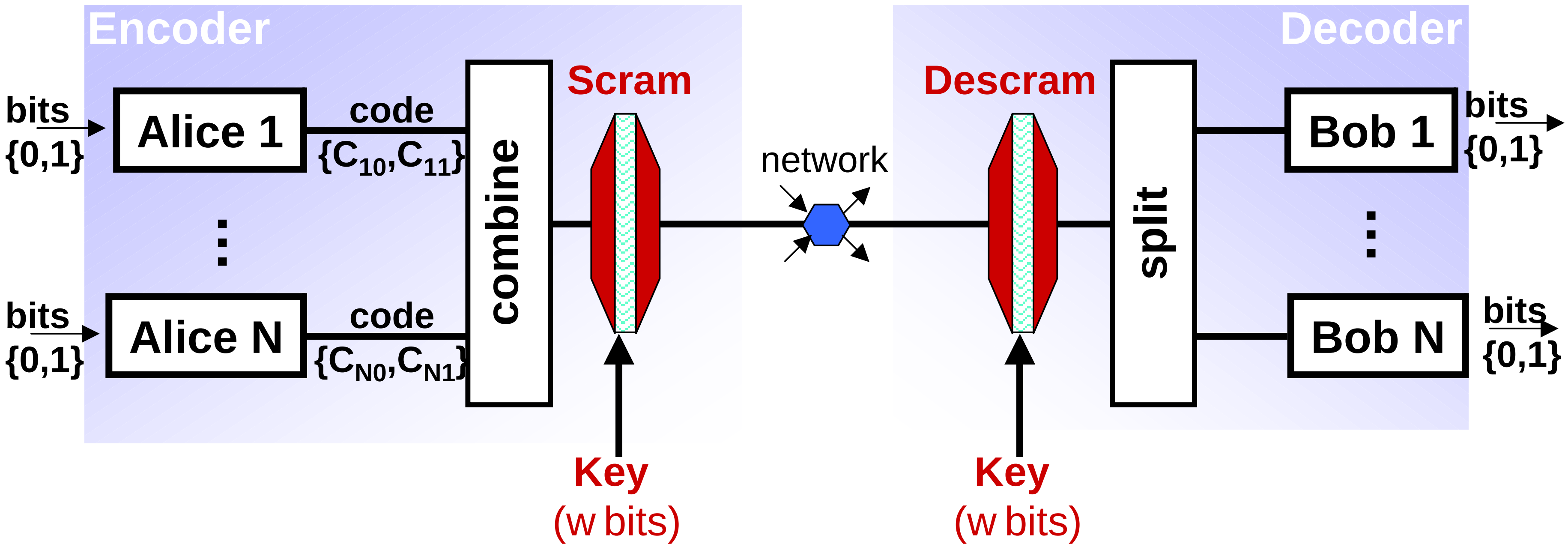
Overview of [Menendez2005]'s system



Encoding proceeds in three steps



Overview of [Menendez2005]'s system



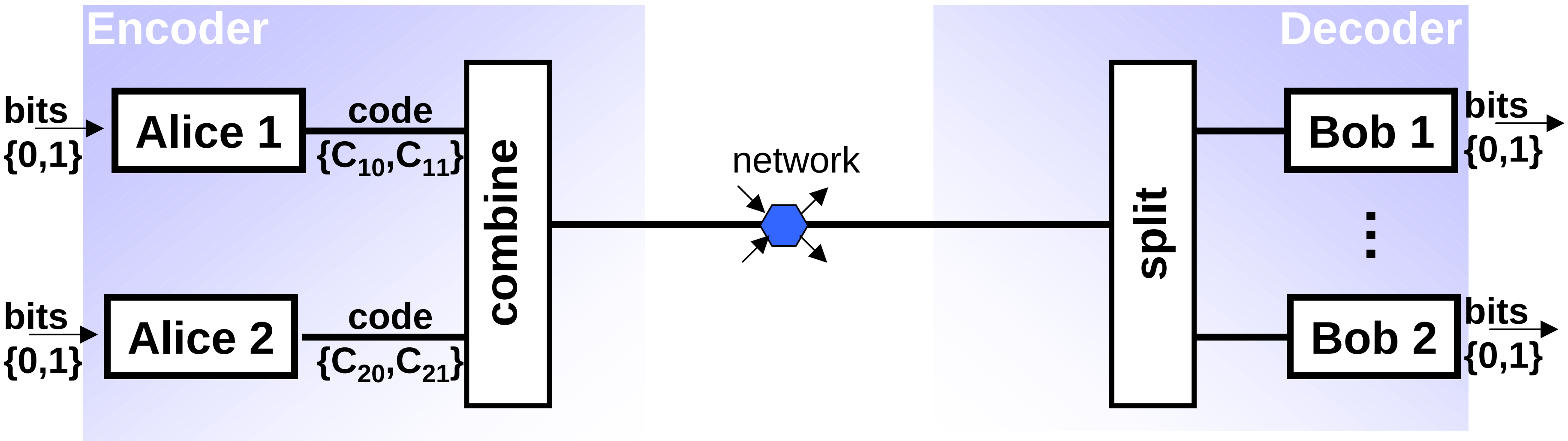
Encoding proceeds in three steps

Mapping: Each Alice maps an electronic bit to a unique optical codeword

Combining: Combine the optical signals from each Alice

Scrambling: Phase scrambling according to key is applied

[Menendez2005]'s system: Mapping



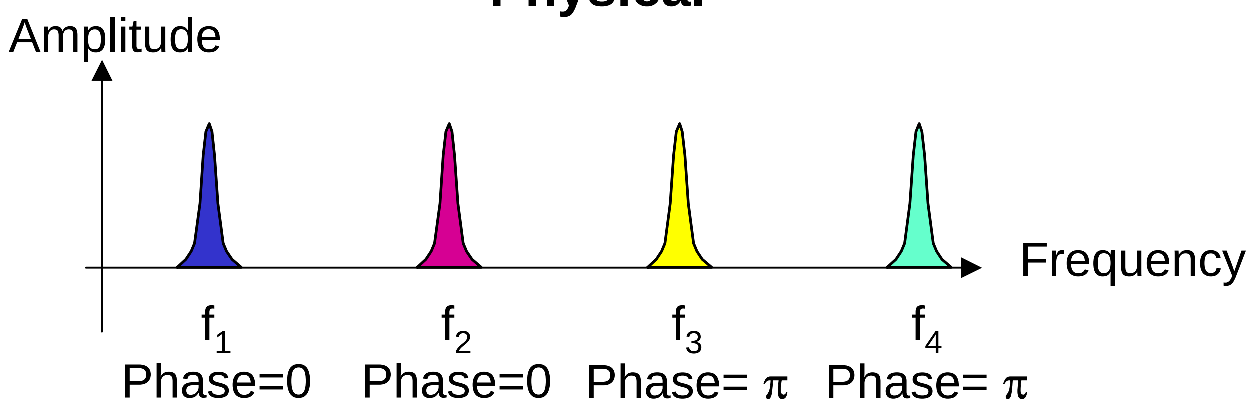
Each Alice-Bob get a pair of unique codewords

To send a **0** bit: **Alice1** transmits codeword $\mathbf{C_{10}}$
To send a **1** bit: **Alice1** transmits codeword $\mathbf{C_{11}}$

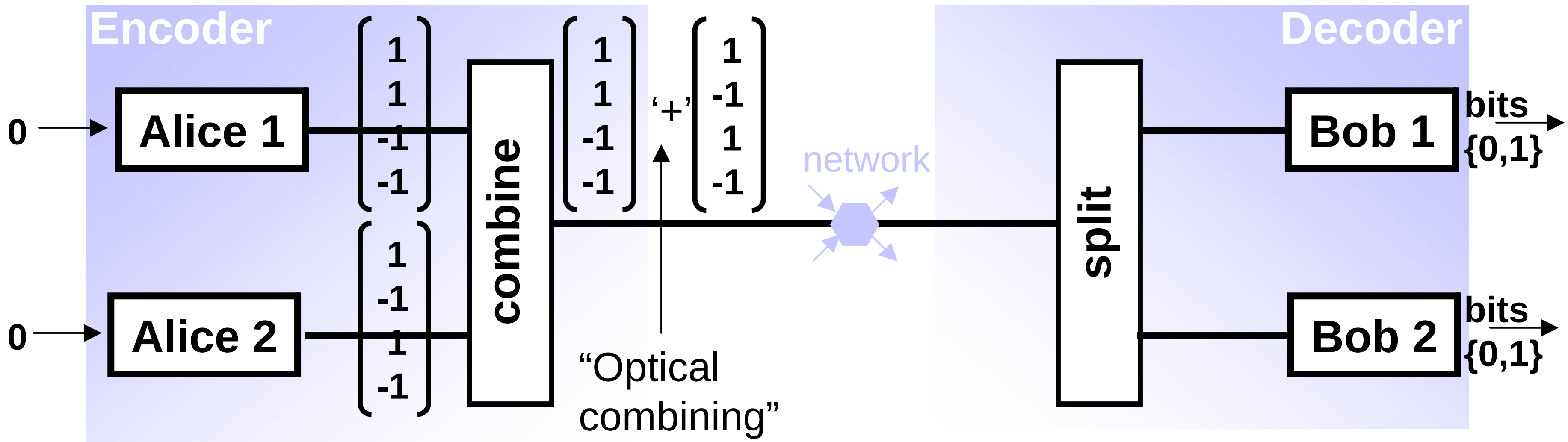
Abstraction

$$C_{10} = \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix}$$

Physical



[Menendez2005]'s system: Combining



Bob1's bit recovery algorithm

Check for a 0 bit:

1. Take dot product with C_{10}
2. Check for pulse of height 4

$$[\,1\ 1\ {-1}\ {-1}\,] \bullet \left(\begin{bmatrix}1\\1\\-1\\-1\end{bmatrix} \text{'+'} \begin{bmatrix}1\\-1\\1\\-1\end{bmatrix} \right) = 4\ \text{'+'}\ 0$$

Pulse!

Check for a 1 bit:

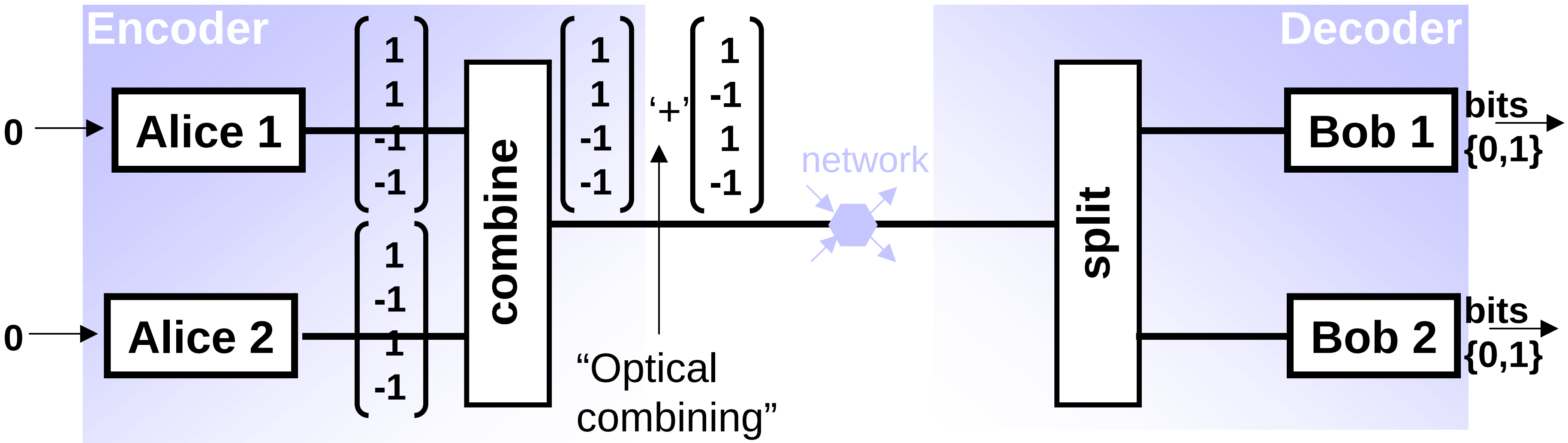
1. Take dot product with C_{11}
2. Check for pulse of height 4

$$[\,1\ 1\ 1\ 1\,] \bullet \left(\begin{bmatrix}1\\1\\-1\\-1\end{bmatrix} \text{'+'} \begin{bmatrix}1\\-1\\1\\-1\end{bmatrix} \right) = 0\ \text{'+'}\ 0$$

No Pulse

This works because we use orthogonal codes (e.g. Hadamard codes)

[Menendez2005]'s system: Combining



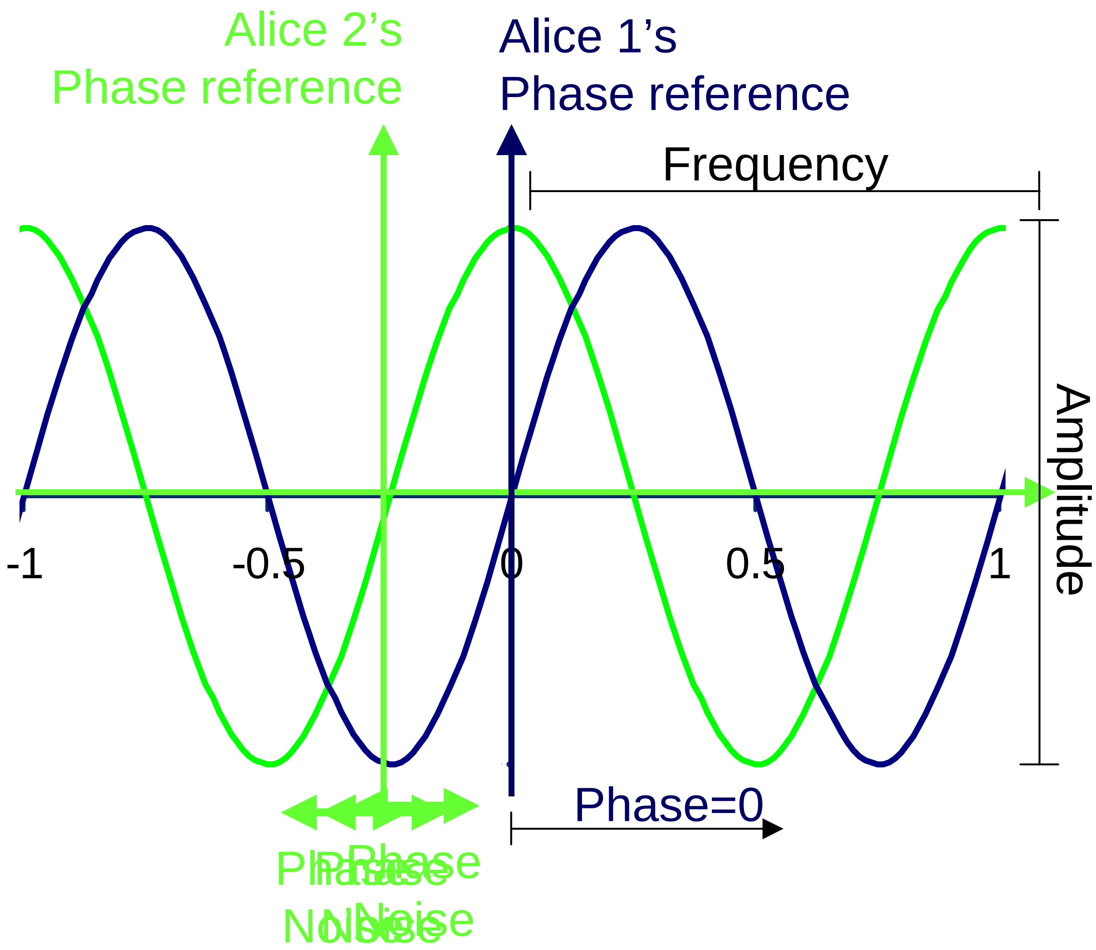
Bob1's bit recovery algorithm

This works because we use orthogonal codes (e.g. Hadamard codes)

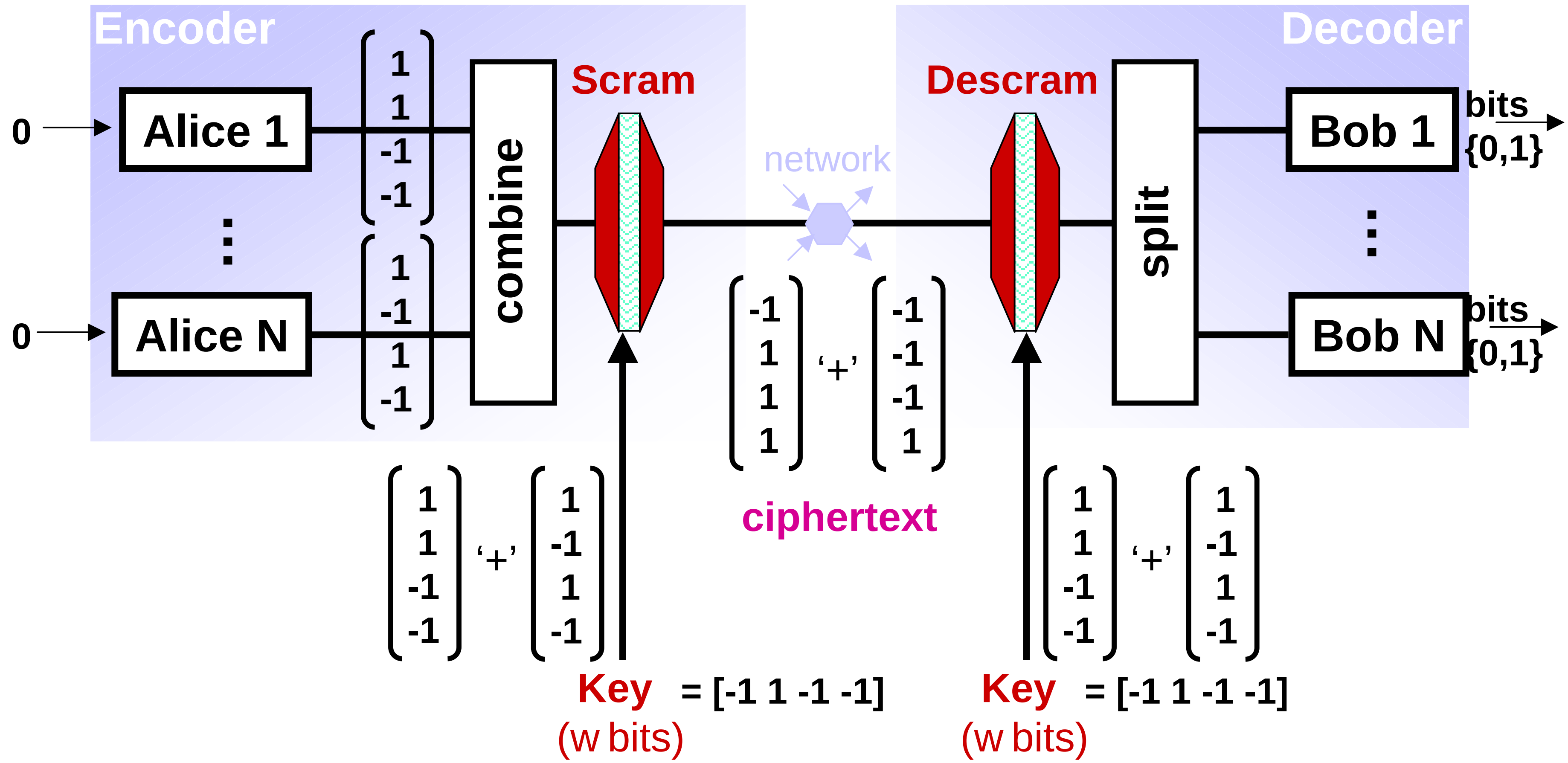
But the cardinality of orthogonal codes is small
(e.g. an orthogonal code of length **w** has only **w** codewords)

So Eve can learn plaintext by building her own Bobs

Optics 101


Alice 2's
Phase reference
Alice 1's
Phase reference
Frequency
Amplitude
-1
-0.5
0
0.5
1
Phase=0
Phase
Noise

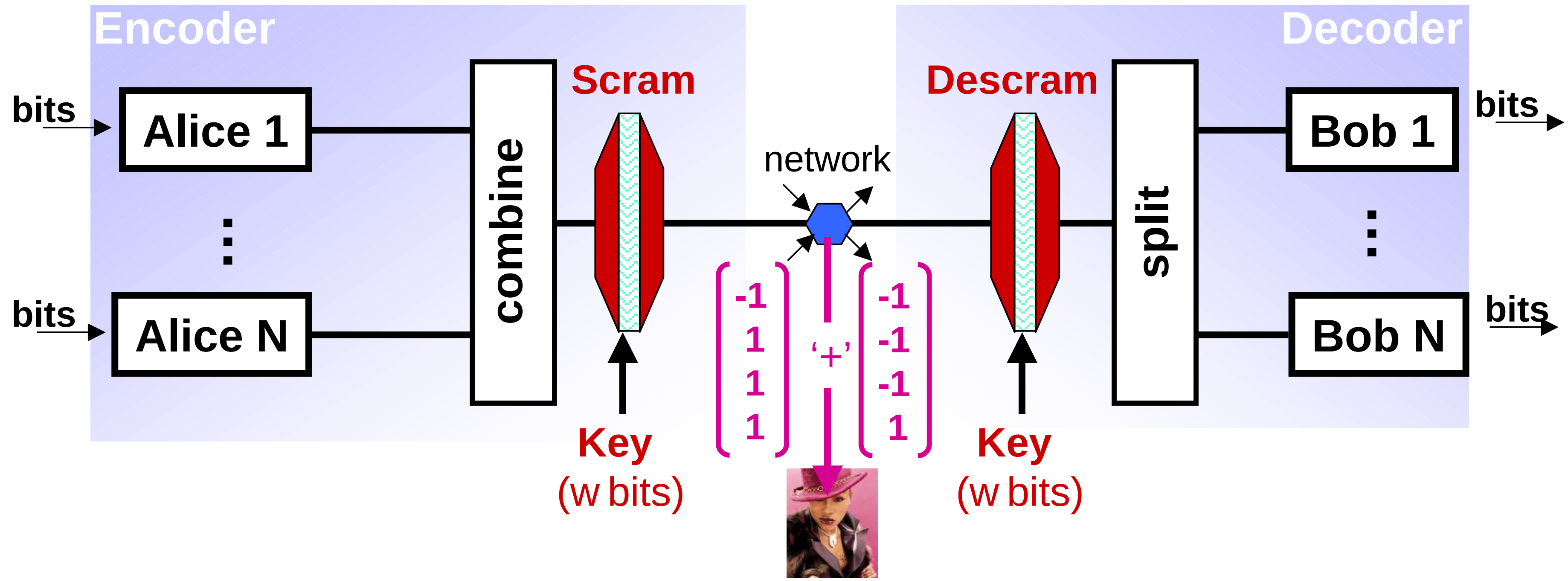
[Menendez2005]'s system: Scrambling



With orthogonal codes we had **O(w)** possible codewords (ciphertexts)

Adding scrambling gives **O(2^{w})** possible ciphertexts !

[Menendez2005]'s system: A One-Time-Pad?

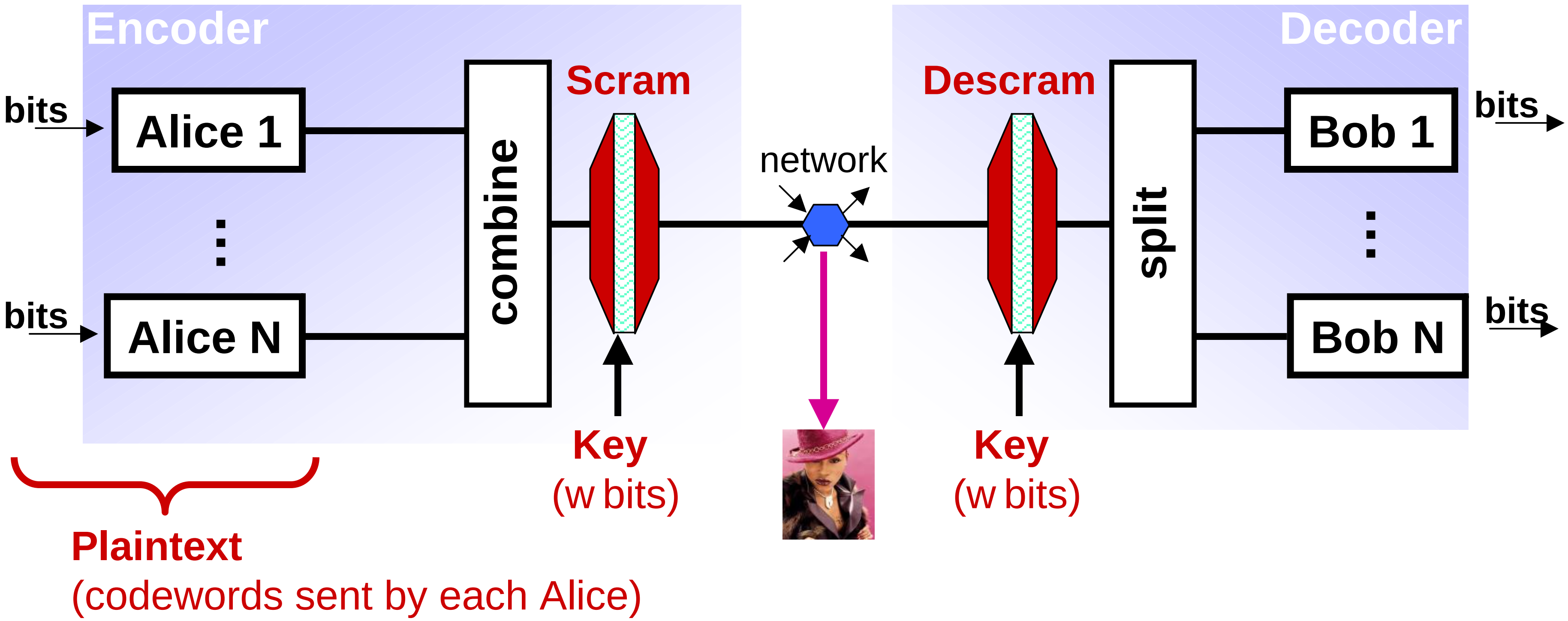


Suppose key bits don't change.
Do the attacks that we saw before still work?
Is this just the trivial one-time-pad used many times?

It is not trivial! We get extra entropy (in addition to key) from:

- Eve's inability to exactly measure the optical ciphertext
- Continuous random **phase noise** during the combining **'+'** operation

Overview of our results



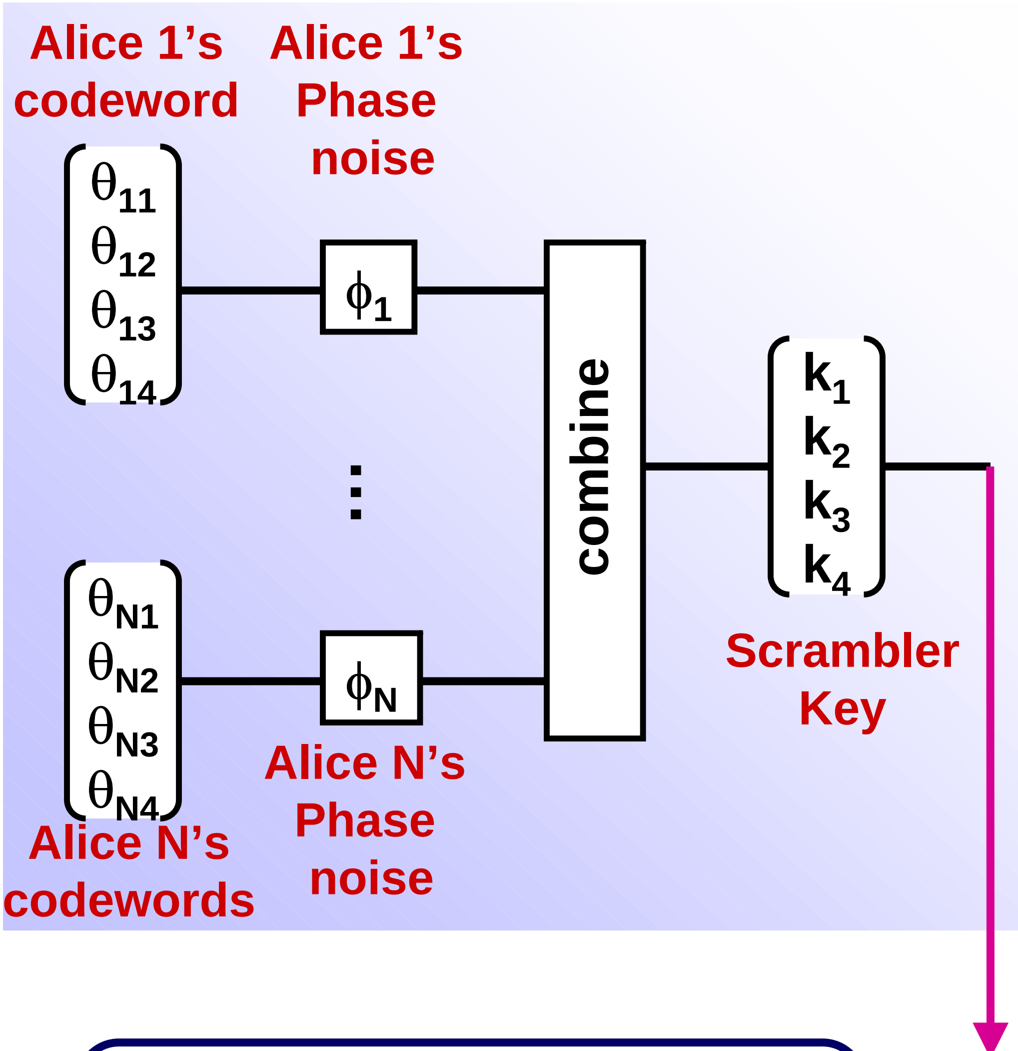
Folklore: ~~$2^{\text{frequencies}}$ brute force operations to learn key~~

Our result: Need 2^{Alices} brute force operations to learn the key

Folklore: ~~Only known way to learn key is via brute force search~~

Our result: Can learn the key (w.h.p) using only **2 known** plaintexts

Our attack: Step 1 - Abstract the encoder



plaintext matrix

$\Theta \in \{1,-1\}^{\text{Frequencies x Alices}}$

Discrete matrix elements set by the bits sent by each Alice

scrambler key vector

$k \in \{1,-1\}^{\text{Frequencies}}$

Discrete & Secret

phase noise vector

$x \in [1,-1]^{\text{Alices}}$

Unknown

Real-valued random process

Eve's measurement

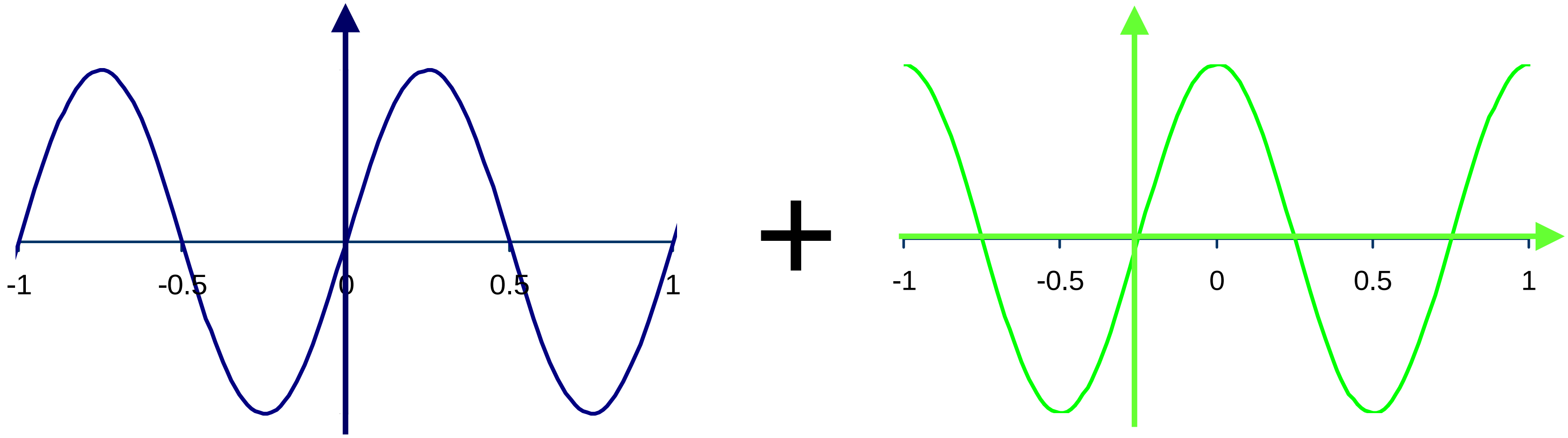
$y \in [N,-N]^{\text{Frequencies}}$

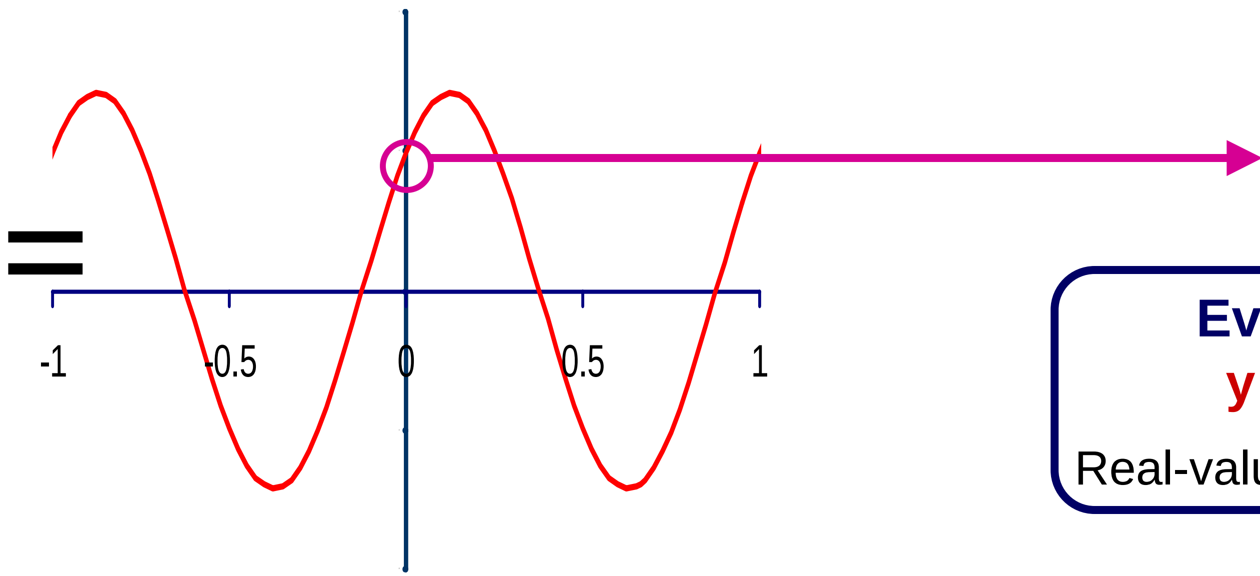
Real-valued measure of ciphertext

$$y = \mathrm{diag}(k) \cdot \Theta^T \cdot x$$

Assuming y is a noise-free amplitude measurement

Optics 101





Eve's measurement

$y \in$ [N,-N] Frequencies

Real-valued measure of ciphertext

Our attack: Step 2 - Brute force search space

$$\underbrace{\begin{bmatrix} y \end{bmatrix}}_{\text{W Frequencies}} = \underbrace{\begin{pmatrix} \mathrm{diag}(k) \end{pmatrix}}_{\text{W Frequencies}} \underbrace{\begin{pmatrix} \Theta^T \end{pmatrix}}_{\text{N Alices}} \underbrace{\begin{bmatrix} x \end{bmatrix}}_{\text{N Alices}}$$

measurement	**key**	**plaintext**	**phase noise**
real valued	discrete from {1,-1}	discrete from {1,-1}	real valued
✓**known**	?**secret**	✓**known**	?**unknown**

1. Eve (**optically**) obtains a measurement **y** and a plaintext **Θ**
2. Eve has **W** equations in **W + N** unknowns
   Offline, guess **N** key **bits**
   then solve for phase noise vector **x**
   then solve for **W-N** remaining key elements
3. Repeat step 2 (**offline**) until learning key

Folklore: $2^{\text{frequencies}}$ brute force operations to learn key

Our result: Need 2^{Alices} brute force operations to learn key

Our attack: Learning the key with 2 known plaintexts

$$\underset{\text{W Frequencies}}{\begin{bmatrix} y \end{bmatrix}} = \underset{\text{W Frequencies}}{\begin{pmatrix} \mathrm{diag}(k) \end{pmatrix}} \underset{\text{N Alices}}{\begin{pmatrix} \Theta^T \end{pmatrix}} \underset{\text{N Alices}}{\begin{bmatrix} x \end{bmatrix}}$$

measurement	key	plaintext	phase noise
real-valued	discrete from {1,-1}	discrete from {1,-1}	real-valued
✓ **known**	? **secret**	✓ **known**	? **unknown**
changes	**fixed**	**changes**	**changes**

---

1. Eve (**optically**) obtains a 2 measurement-plaintext pairs **(y_1, Θ_1) (y_2, Θ_2)**
2. Eve has **2W** equations in **W + 2N** unknowns where **$2N \leq W$**

   Offline 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

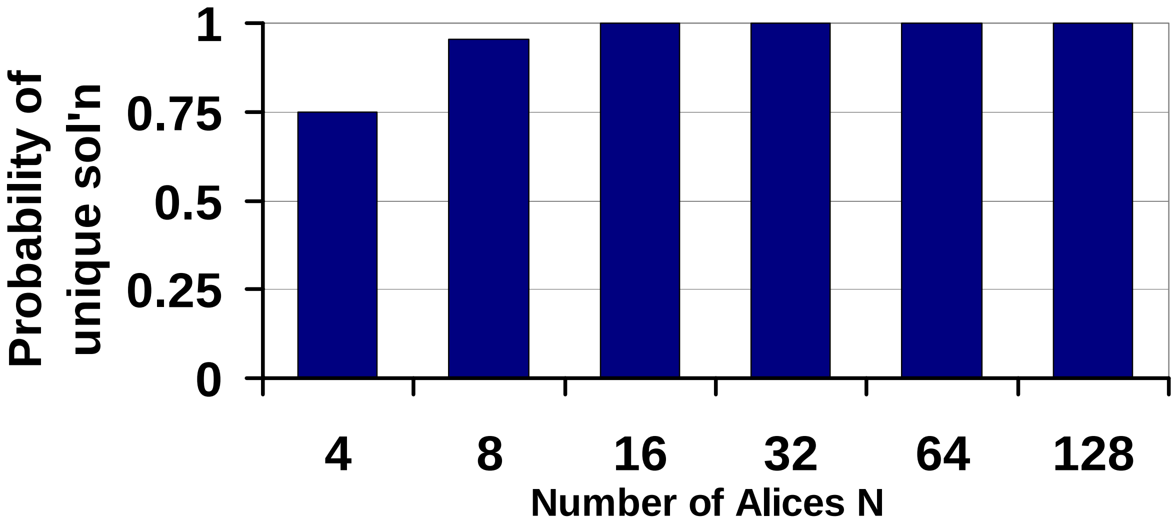
Our attack: Learning the key with 2 known plaintexts

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 Θ_1, Θ_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

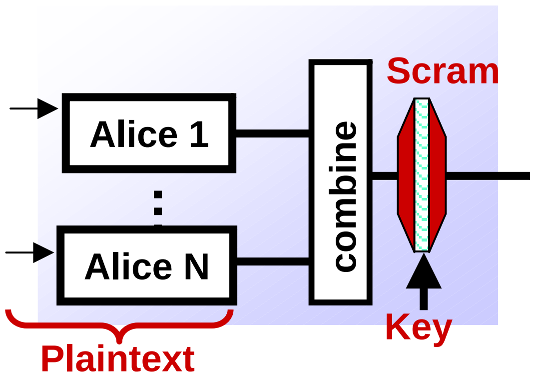
Folklore: Only known way to learn key is via brute force search

Our result: Can learn the key (w.h.p.) using only **2 known** plaintexts

Conclusion and Open Problems

The promise of optical encryption

- Limited measurement capabilities of adversary
- Extra entropy from noise
- Encryption faster than data rates



Known plaintext attacks on [Menendez 2005]

- If Eve can make noise-free measurements then:

Security depends on parallelism, not coding complexity

2 known plaintexts break system when Alices' codewords known

- Future: Attacks with noisy measurements

Some Open Problems:

- Cryptanalysis of Wu and Narimanov's scheme
- Extending bounded storage model to this setting
- Positive results for optical encryption!

Thanks:

Ron Menendez

Paul Prucnal

Boaz Barak

Jennifer Rexford

Moses Charikar

Eugene Brevdo

Parts of this work were supported by DARPA