Semantic Security for the Wiretap Channel

Stefano Tessaro

MIT

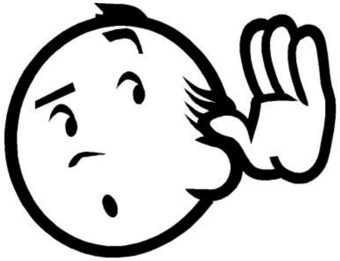
Joint work with

Mihir Bellare (UCSD)
Alexander Vardy (UCSD)

Cryptography today is (mainly) based on **computational assumptions.**

We wish instead to base cryptography on a **physical assumption.**

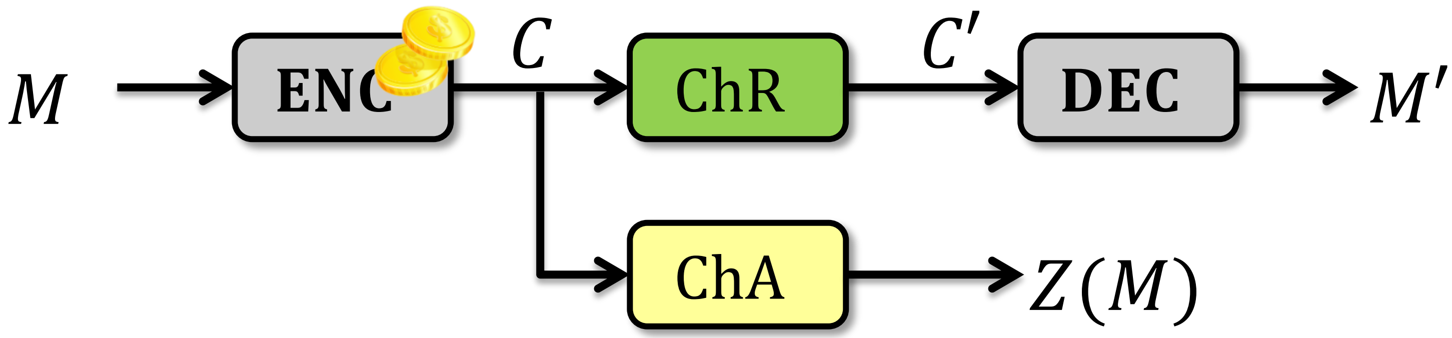
Presence of **channel noise**



Noisy channel assumption has been used previously to achieve **oblivious transfer**, **commitments** **[CK88,C97]**

But we return to an older and more basic setting …

Wyner's Wiretap Model [W75,CK78]



Goals: Message privacy + correctness

Assumption: ChA is "noisier" than ChR

Encryption is **keyless**

Security is **information-theoretic**

Additional goal: Maximize **rate** $R = |M|/|C|$

Channels

A **channel** is a randomized map $\mathrm{Ch}: \{0,1\} \to \{0,1\}$

$\dots, x_4, x_3, x_2, x_1$


$y_1, y_2, y_3, y_4, \dots$

We extend the domain of Ch to $\{0,1\}^*$ via
$\mathrm{Ch}(x_1 x_2 \dots x_n) = \mathrm{Ch}(x_1)\mathrm{Ch}(x_2) \dots \mathrm{Ch}(x_n)$

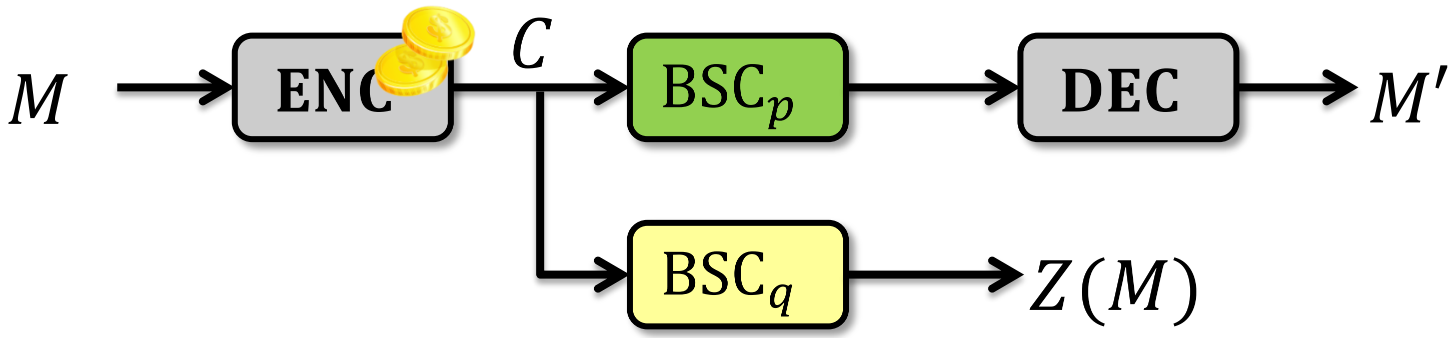
$$\begin{aligned} y_1 &= \mathrm{Ch}(x_1) \\ y_2 &= \mathrm{Ch}(x_2) \\ y_3 &= \mathrm{Ch}(x_3) \\ y_4 &= \mathrm{Ch}(x_4) \end{aligned}$$

Clear channel: $\mathrm{Ch}(b) = b$

Binary symmetric channel with error probability p:

$$\mathrm{BSC}_p(b) = \begin{cases} b & \text{with prob. } 1 - p \\ 1 - b & \text{with prob. } p \end{cases}$$

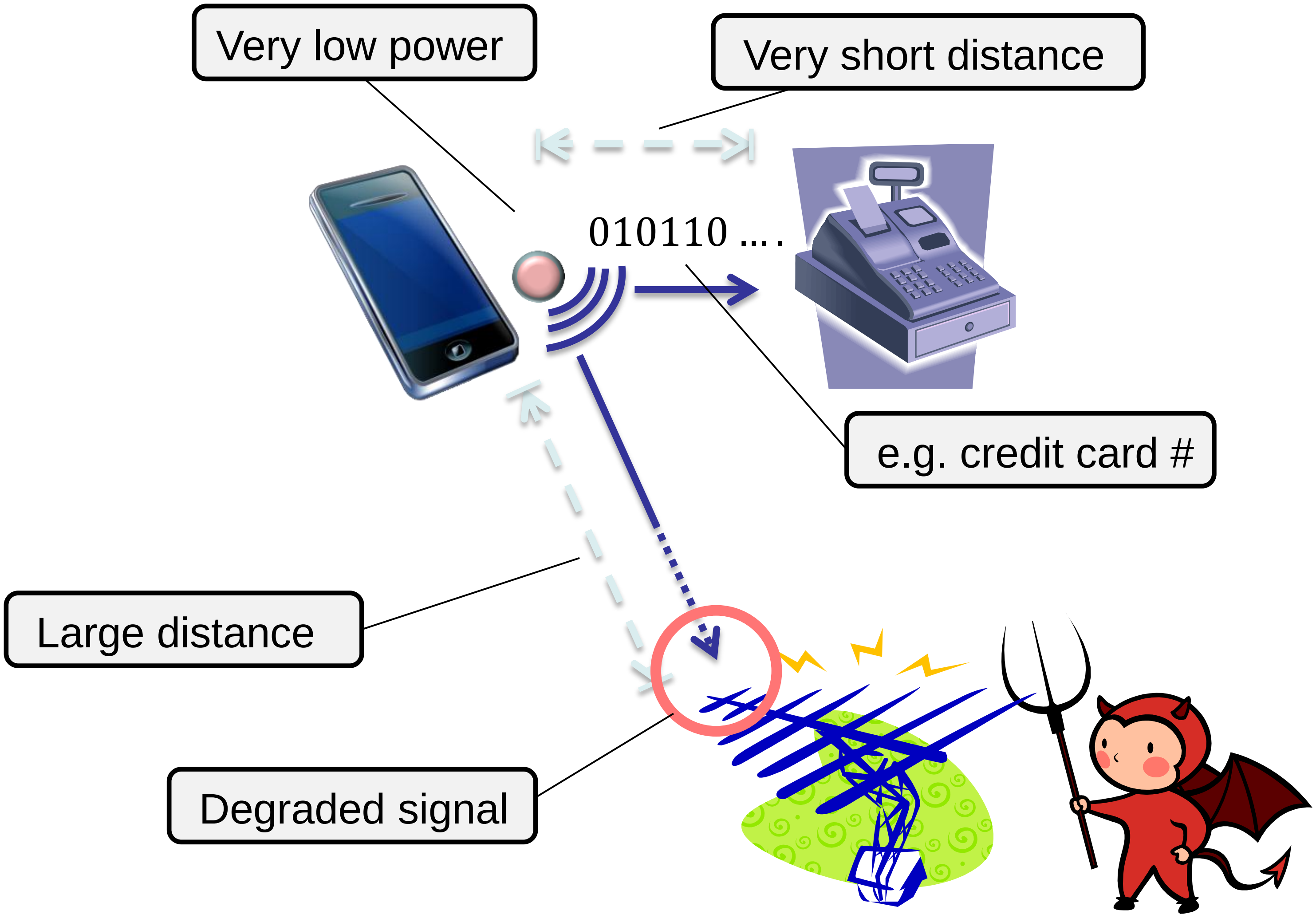
Wyner's Wiretap Model – More concretely



Assumption: $p < q \leq 1/2$

Wiretap channel – Realization

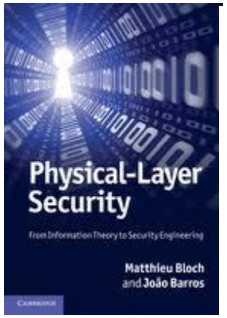
Increasing practical interest: Physical-layer security

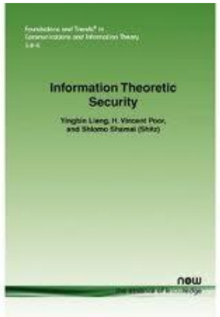


Wiretap Channel – Previous work

35 years of previous work:

Hundreds of papers/books on wiretap security within the information theory & coding community





Two major drawbacks:

1. **Improper privacy notions**
   Entropy-based notions
   Only consider random messages
2. **No polynomial-time schemes with optimal rate**
   Non-explicit decryption algorithms
   Weaker security

This work: We fill both gaps

Our contributions

1. New security notions for the wiretap channel model:

- **Semantic security, distinguishing security** following **[GM82]**
- **Mutual-information security**
- **Equivalence** among the three

2. Polynomial-time encryption scheme:

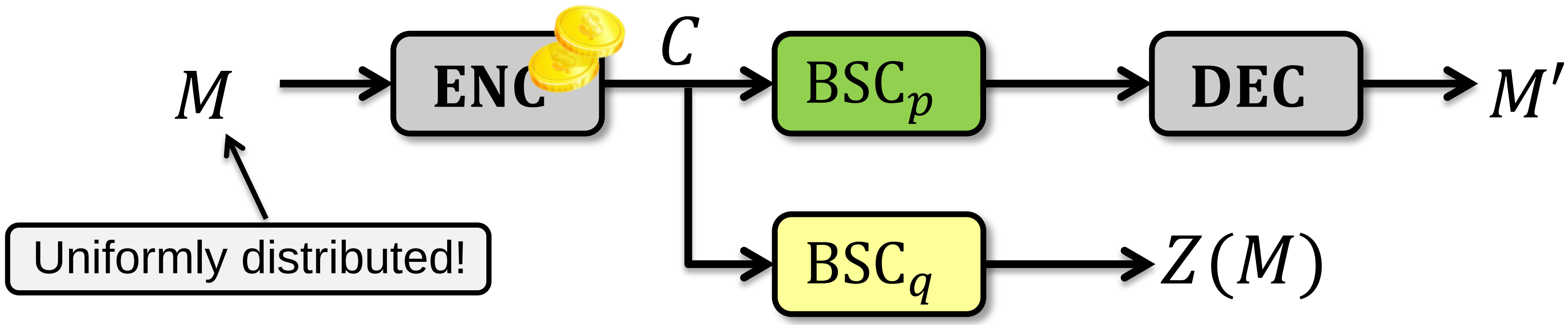
- **Semantically secure**
- **Optimal rate**

Outline

1. Security notions

2. Polynomial-time scheme

Prior work – Mutual-information security



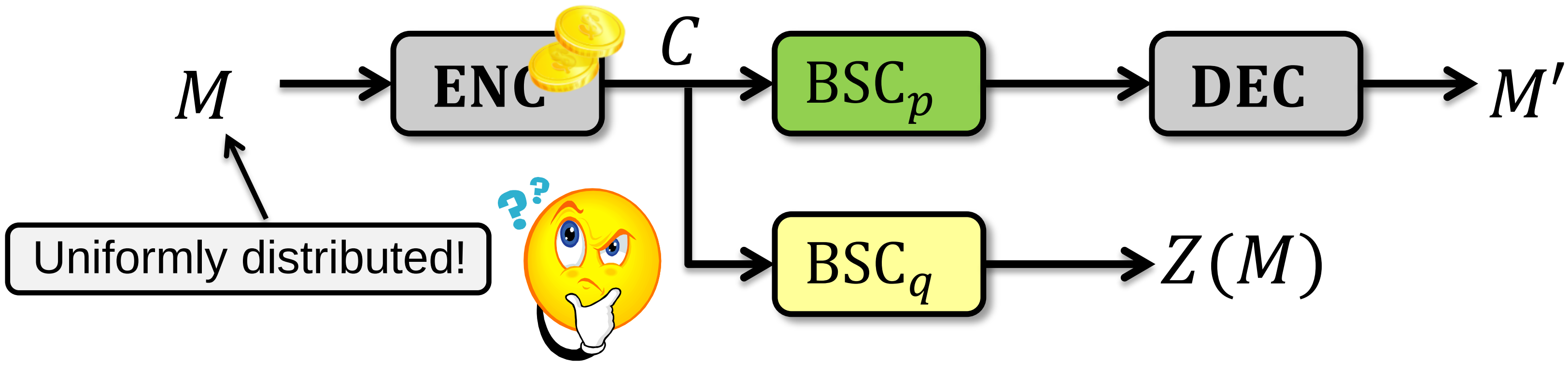
$$\mathbf{H}(M|Z(M)) = \mathbf{H}(M\ Z(M)) - \mathbf{H}(Z(M))$$

Definition: $\mathbf{I}(M; Z(M)) = \mathbf{H}(M) - \mathbf{H}(M|Z(M))$

Random Mutual-Information Security (MIS-R):

$$\mathbf{H}(M) = \sum_m \mathrm{P}_M(m) \cdot \log(1/\mathrm{P}_M(m))$$

Critique – Random messages



Common misconception: c.f. e.g. **[CDS11]**

*"[…] the particular **choice of the distribution on M as a uniformly random sequence will cause <u>no loss of generality</u>**. […] the **transmitter can use a suitable source-coding scheme to compress the source** to its entropy prior to the transmission, and ensure that from the intruder's point of view, M is uniformly distributed."*

Wrong! No universal (source-independent) compression algorithm exists!

We want security for arbitrary message distributions, following [GM82]!

Mutual-information security, revisited

~~Random Mutual-Information Security (MIS-R)~~

$$\cancel{\mathbf{I}(M;Z(M)) = \mathbf{negl}}$$

New: Mutual-Information Security (MIS)

$$\max_{\mathrm{P}_M} \mathbf{I}(M;Z(M)) = \mathbf{negl}$$

Maximize over **all** message distributions

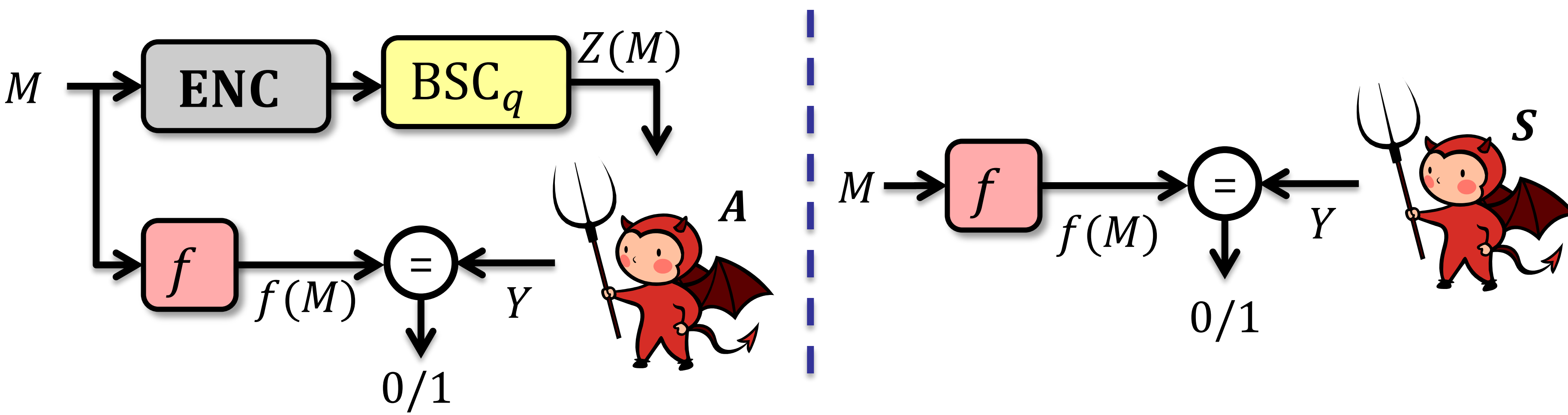
Critique: Mutual information is hard to work with / interpret!

Semantic security

Maximize over **all** functions + message distributions

Semantic Security (SS)

$$\max_{f,\mathrm{P}_M} \left| \boxed{\max_{\boldsymbol{A}} \Pr[\boldsymbol{A}(Z(M)) = f(M)]} - \boxed{\max_{\boldsymbol{S}} \Pr[\boldsymbol{S} = f(M)]} \right| = \mathbf{negl}$$



Distinguishing security

Uniform random bit B

Distinguishing Security (DS)

$$\max_{\boldsymbol{A}, M_0, M_1} \Pr[\boldsymbol{A}(M_0, M_1, Z(M_\mathrm{B})) = \mathrm{B}] = 1/2 + \mathbf{negl}$$

Fact:

$$\max_{A, M_0, M_1} \Pr[\mathrm{A}(M_0, M_1, Z(M_\mathrm{B})) = \mathrm{B}] = \frac{1}{2} + \mathbf{negl}$$

$$\Leftrightarrow \max_{M_0, M_1} \mathbf{SD}\big(Z(M_0); Z(M_1)\big) = \mathbf{negl}.$$

$$\mathbf{SD}(X; Y) = \frac{1}{2} \sum_{v} |\mathrm{P}_X(v) - \mathrm{P}_Y(v)|$$

Relations

Theorem. MIS, DS, SS are equivalent.

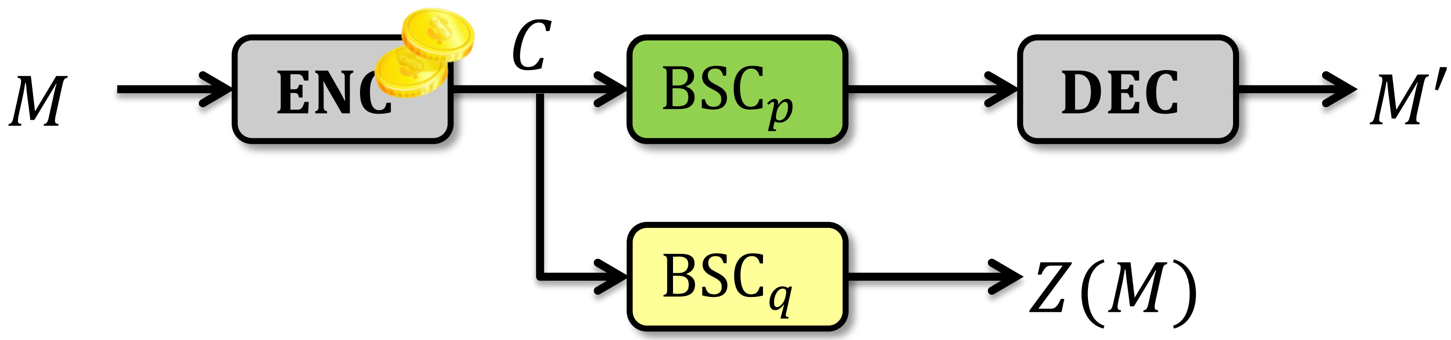
$$\begin{tikzcd}
\mathbf{MIS} \arrow[rrr, shift left] \arrow[d, shift left] & & & \mathbf{DS} \arrow[lll, shift left] \arrow[d, shift left] \\
\mathbf{MIS\text{-}R} \arrow[u, shift left, "/" marking] & & & \mathbf{SS} \arrow[u, shift left]
\end{tikzcd}$$

Outline

1. Security notions

2. Polynomial-time scheme

Polynomial-time scheme



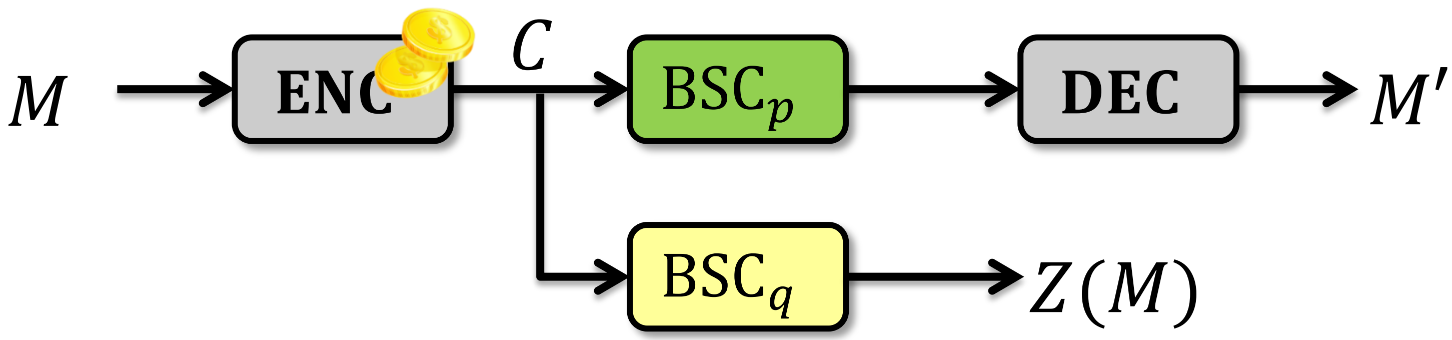
Goal: Polynomial-time ENC and DEC which satisfy:

1) **Correctness:** $\Pr[M \neq M'] = \mathbf{negl}$
2) **Semantic security**
3) **Optimal rate**

- We observe that **fuzzy extractors** of **[DORS08]** can be used to achieve **1 + 2.** (Also: **[M92,…]**)
- **[HM10,MV11]** Constructions achieving **1 + 3** or **2 + 3.**

This work: First polynomial-time scheme achieving **1 + 2 + 3**

What is the optimal rate?



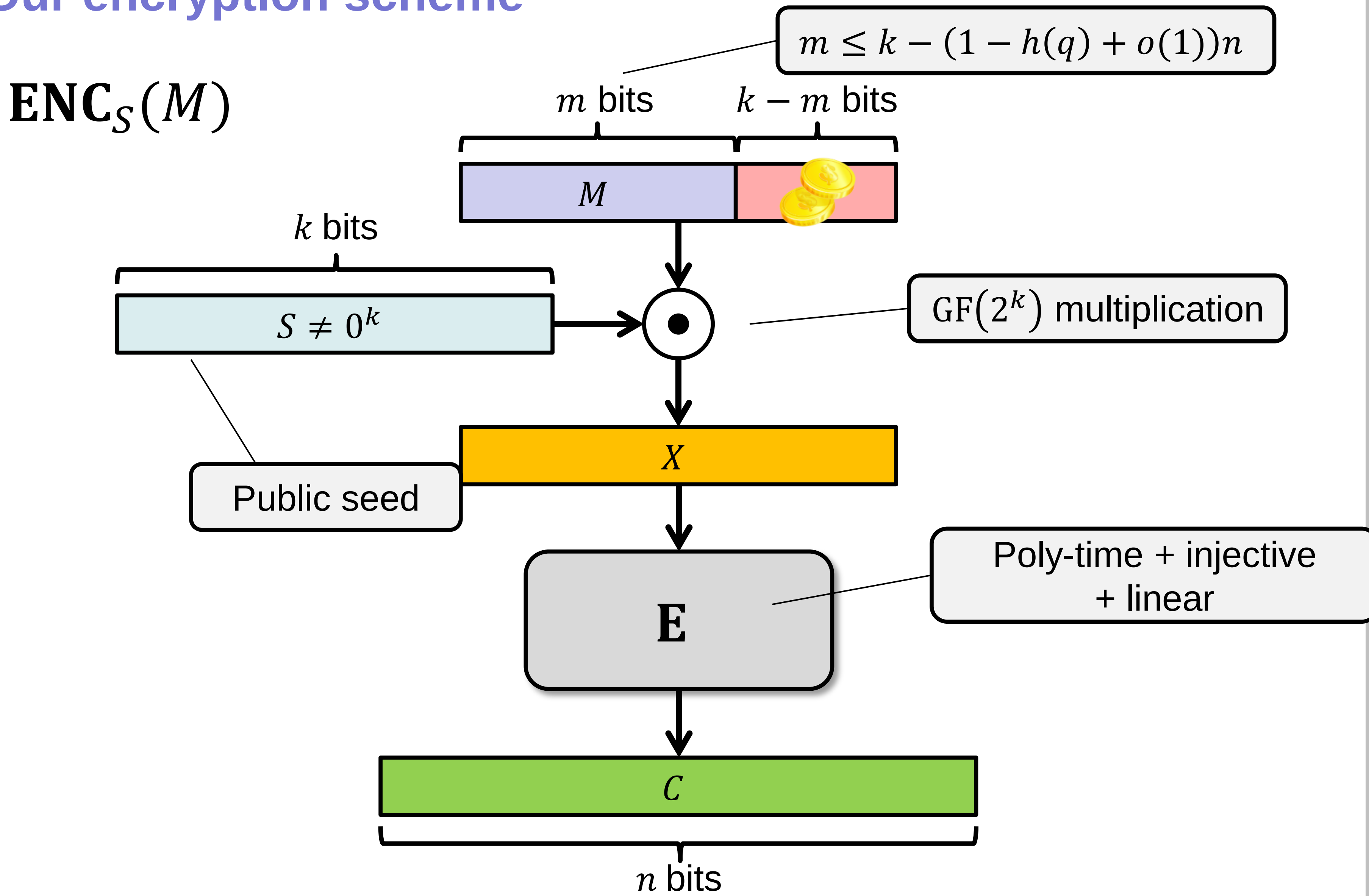
Definition: Rate $R = |M|/|C|$ $\boxed{h(x) = -x\log x - (1-x)\log(1-x)}$

Previous work: [L77] No MIS-R secure scheme can have rate higher than $h(q) - h(p) - o(1)$.

Our scheme: Rate $h(q) - h(p) - o(1)$

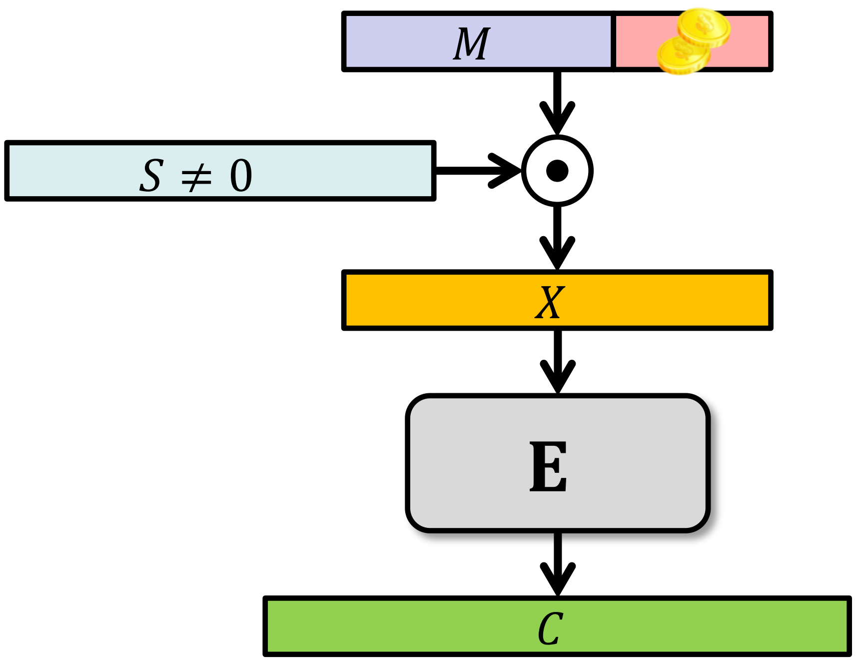
Hence, $h(q) - h(p) - o(1)$ is the **optimal rate** for all security notions!

Our encryption scheme



Our encryption scheme – Security

Theorem. $\mathbf{ENC}$ is **semantically secure**.



Challenge:
Ciphertext distribution depends on **combinatorial properties** of **E**.

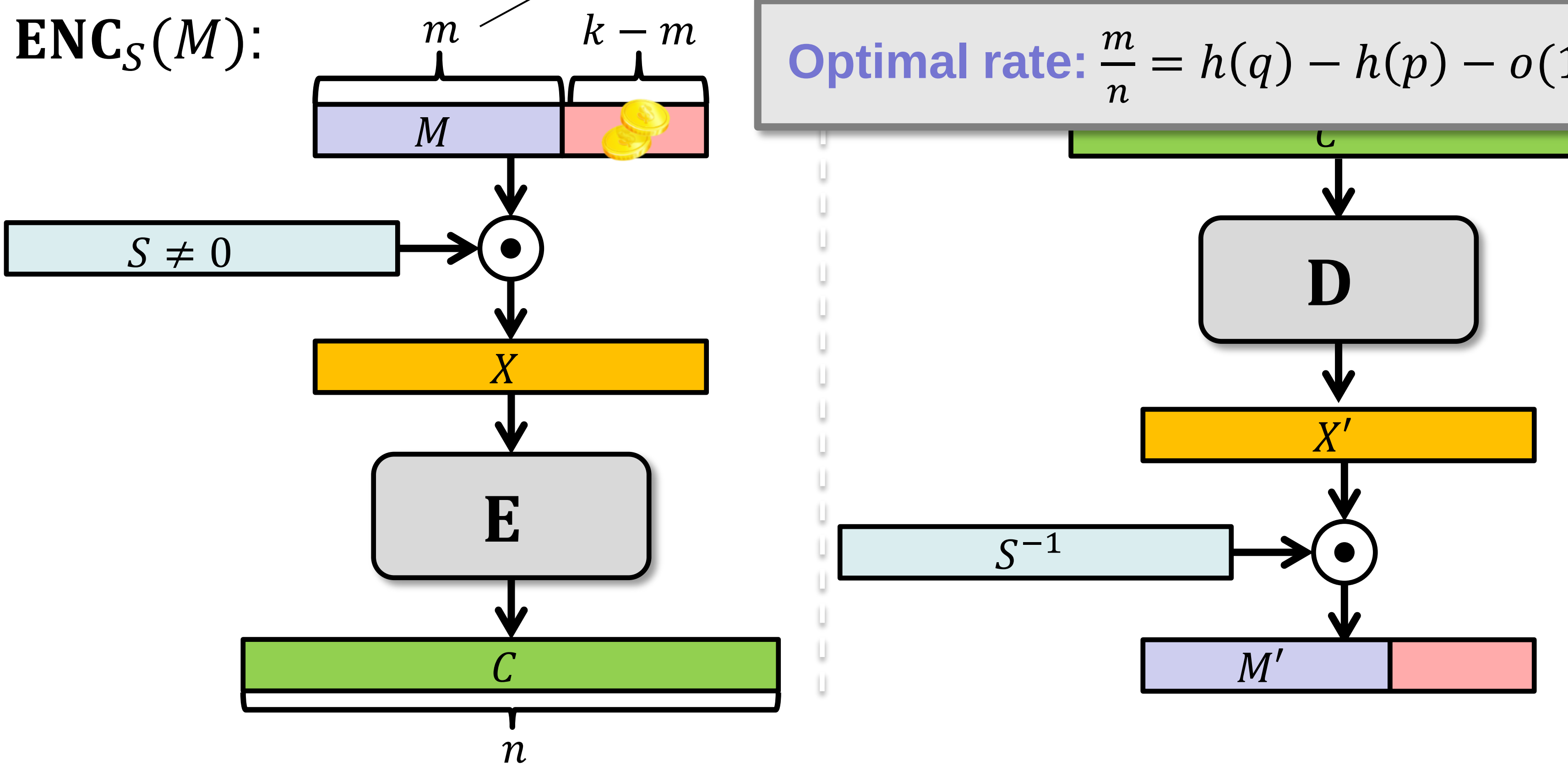
Two steps:

1. Reduce semantic security to **random-message security.**
2. Prove random-message security.

Our encryption scheme … rate

$m = k - (1 - h(q) + o(1))n$

Optimal rate: $\frac{m}{n} = h(q) - h(p) - o(1)$



Observation. If $(\mathbf{E}, \mathbf{D})$ are encoder/decoder of ECC for BSC_p, then correctness holds.

Optimal choice: Concatenated codes [F66], polar codes [A09]: $k = (1 - h(p) - o(1))n$

Concluding remarks

Summary:

- **New equivalent security notions for the wiretap setting:** DS, SS, MIS.
- **First polynomial-time scheme** achieving these security notions with optimal rate.
- Our scheme is **simple, modular, and efficient.**

Concluding remarks

Summary:

- **New equivalent security notions for the wiretap setting:** DS, SS, MIS.
- **First polynomial-time scheme** achieving these security notions with optimal rate.
- Our scheme is **simple, modular, and efficient.**

Additional remarks:

- We provide a **general and concrete treatment.**
- Scheme can be used on **larger set of channels.**

Concluding remarks

Summary:

- **New equivalent security notions for the wiretap setting:** DS, SS, MIS.
- **First polynomial-time scheme** achieving these security notions with optimal rate.
- Our scheme is **simple, modular, and efficient.**

Additional remarks:

- We provide a **general and concrete treatment.**
- Scheme can be used on **larger set of channels.**

Thank you!