



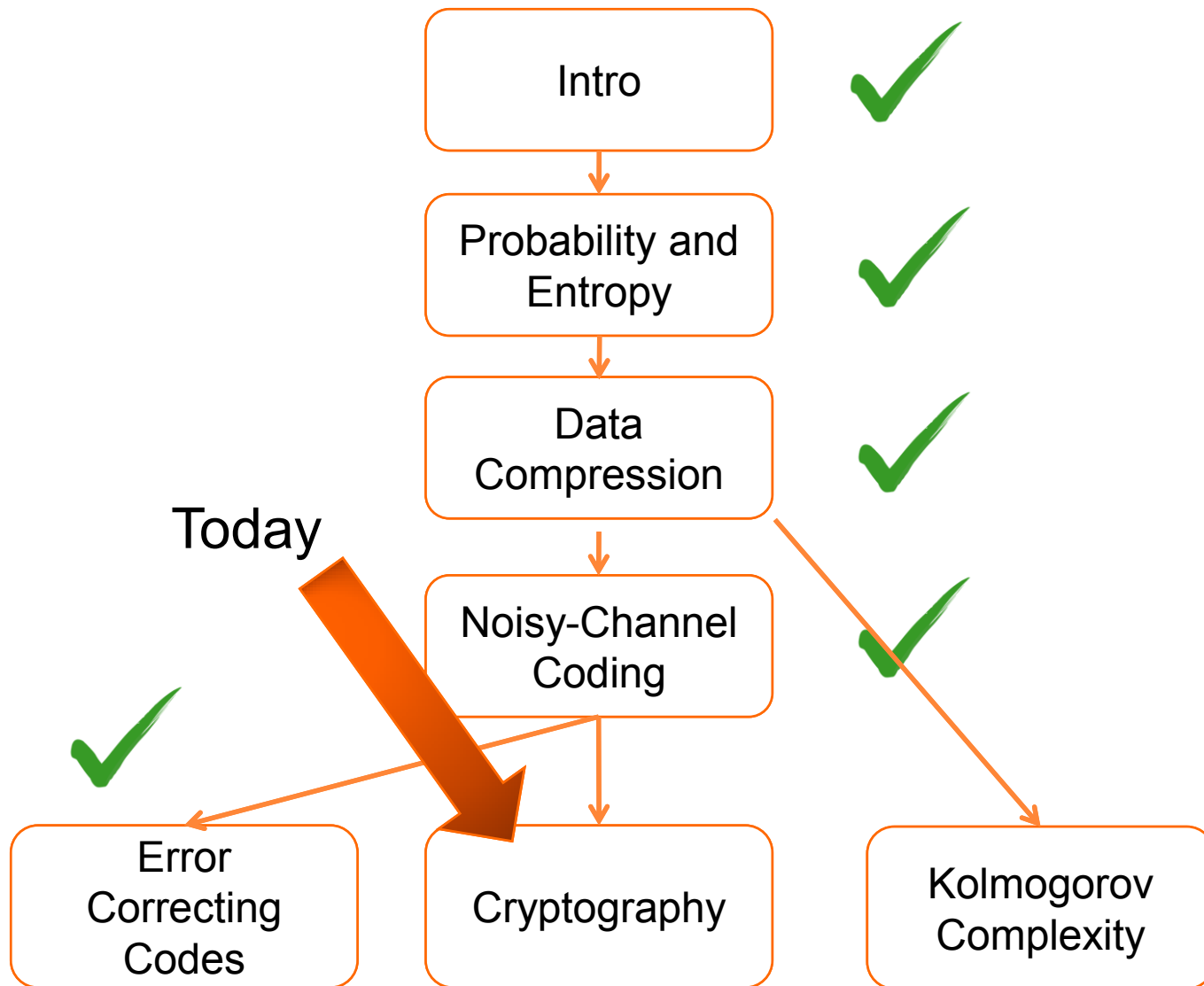
CS3236 INTRODUCTION TO INFORMATION THEORY

Lecture 11: Introduction to Cryptography

Course given by Pierre Senellart

Material by Stephanie Wehner, with additions by P. Senellart

WHERE DO WE GO FROM HERE?



WHAT WE'LL DO TODAY

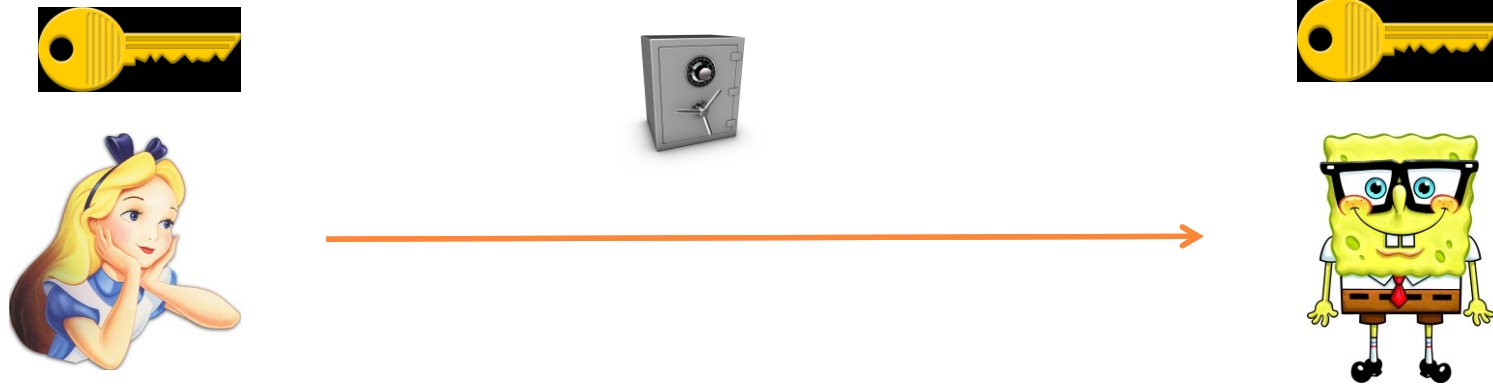
- Use of randomness in cryptography
- Entropy in cryptography
- Randomness extraction
 - Idea
 - Measure of success
 - Essential concepts




EXAMPLE: SENDING MESSAGES SECURELY



- Goal: The eavesdropper (Eve) should not gain any information about the message by listening to the communication.

EXAMPLE: ONE TIME PAD ENCRYPTION



	m_1	m_2	m_3	\dots	m_n
	\oplus	\oplus	\oplus	\dots	\oplus
	k_1	k_2	k_3	\dots	k_n
	$=$	$=$	$=$	\dots	$=$
	t_1	t_2	t_3	\dots	t_n

$$m_j, k_j, t_j \in \{0, 1\}$$

$$m_j \oplus k_j = m_j + k_j \pmod{2}$$

WHAT DOES IT MEAN THAT EVE DOESN'T KNOW THE KEY?

- Key should be “random”

$$P_K(k = k_1, \dots, k_n) = \frac{1}{2^n}$$

WHAT DOES IT MEAN THAT EVE DOESN'T KNOW THE KEY?

- Key should be “random”

$$P_K(\mathbf{k} = k_1, \dots, k_n) = \frac{1}{2^n}$$

- Eve is uncorrelated. For Eve's side information E

$$P_{KE}(\mathbf{k}, \mathbf{e}) = P_K(\mathbf{k}) \times P_E(\mathbf{e})$$

WHAT DOES IT MEAN THAT EVE DOESN'T KNOW THE KEY?

- Key should be “random”

$$P_K(k = k_1, \dots, k_n) = \frac{1}{2^n}$$

- Eve is uncorrelated. For Eve's side information E

$$P_{KE}(k, e) = P_K(k) \times P_E(e)$$

- Together we want that

$$P_{KE}(k, e) = \frac{1}{2^n} \times P_E(e)$$

HOW DO WE OBTAIN SUCH RANDOMNESS?

- Any key exchange protocol will
 - Need some source of randomness
 - Protect this randomness from Eve

The screenshot shows the top navigation bar of the New York Times website with links for HOME PAGE, TODAY'S PAPER, VIDEO, MOST POPULAR, and TIMES TOPICS. The main header features 'The New York Times' logo and 'Business Day Technology' section. Below this is a secondary navigation bar with links for WORLD, U.S., N.Y. / REGION, BUSINESS, TECHNOLOGY, SCIENCE, HEALTH, SPORTS, and OPINION. A blue button labeled 'More about our clients >>' is positioned below the navigation. The article title is 'Flaw Found in an Online Encryption Method' by JOHN MARKOFF, published on February 14, 2012, with 127 comments. The article text states: 'SAN FRANCISCO — A team of European and American mathematicians and cryptographers have discovered an unexpected weakness in the encryption system widely used worldwide for online shopping, banking, e-mail and other Internet services intended to remain private and secure.' A 'Readers' Comments' box indicates that readers have shared their thoughts on the article. On the right side, there is a social sharing menu with options for RECOMMEND, TWITTER, LINKEDIN, COMMENTS (127), SIGN IN TO E-MAIL, PRINT, REPRINTS, and SHARE.

HOME PAGE | TODAY'S PAPER | VIDEO | MOST POPULAR | TIMES TOPICS

The New York Times Business Day
Technology

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

[More about our clients >>](#)

Flaw Found in an Online Encryption Method

By JOHN MARKOFF
Published: February 14, 2012 | [127 Comments](#)

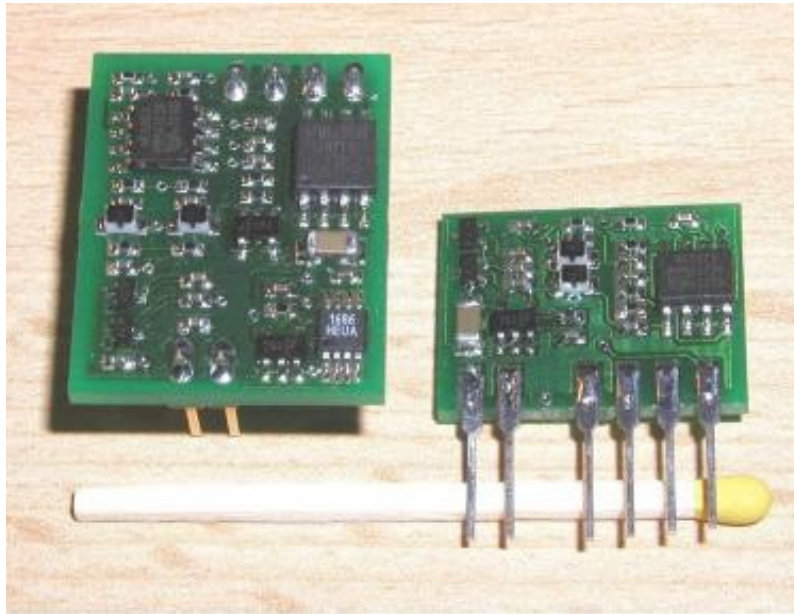
SAN FRANCISCO — A team of European and American mathematicians and cryptographers have discovered an unexpected weakness in the encryption system widely used worldwide for online shopping, banking, e-mail and other Internet services intended to remain private and secure.

Readers' Comments
Readers shared their thoughts on this article.
[Read All Comments \(127\) >>](#)

The flaw — which involves a small but measurable number of cases — has to do with the way the system generates random numbers, which are used to make it practically impossible for an

RECOMMEND
TWITTER
LINKEDIN
COMMENTS (127)
SIGN IN TO E-MAIL
PRINT
REPRINTS
SHARE

“GUARANTEED” RANDOMNESS IS HARD TO COME BY...



PRG210

PRG220



HOW DO WE OBTAIN SUCH RANDOMNESS?

Imagine a key generation machine



How can we quantify how much Eve knows about the output?

IDEA: USING ENTROPY



- We know that for the uniform distribution $H(X) = n$
- If Eve is uncorrelated $H(X) = H(X|E)$
- How about a somewhat imperfect source?

$$H(X) \geq \frac{n}{2}$$

SHANNON ENTROPY AS A CRYPTOGRAPHIC MEASURE

$$P_X(x) = \begin{cases} \frac{1}{2} & x = 111\dots 1 \\ \frac{1}{2} \cdot \frac{1}{2^{n-1}} & \text{otherwise} \end{cases}$$

X_1, \dots, X_n

- How useful is this box for generating keys?

MIN-ENTROPY

- Entropic measure used in cryptography

$$H_{\min}(X) = -\log \max_x \Pr_X(x) = \min_x (-\log \Pr_X(x))$$

- Measures how well Eve can guess x

$$\begin{aligned} H_{\min}(X | E) &= -\log \sum_e \Pr_E(e) \max_x \Pr_{X|E}(x | E = e) \\ &= -\log \Pr_{\text{guess}}(X | E) \end{aligned}$$

COMPARE ENTROPIES FOR OUR EXAMPLE

$$P_X(x) = \begin{cases} \frac{1}{2} & x = 111\dots 1 \\ \frac{1}{2} \cdot \frac{1}{2^{n-1}} & \text{otherwise} \end{cases}$$

X_1, \dots, X_n

$$H(X) \approx \frac{n}{2}$$

$$H_{\min}(X) = 1$$

COMPARE ENTROPIES FOR OUR EXAMPLE

$$P_X(x) = \begin{cases} \frac{1}{2} & x = 111\dots 1 \\ \frac{1}{2} \cdot \frac{1}{2^{n-1}} & \text{otherwise} \end{cases}$$

X_1, \dots, X_n

$$H(X) \approx \frac{n}{2}$$

$$H_{\min}(X) = 1$$

The min entropy is used to quantify how useful randomness is for the use in a cryptographic protocol

GENERATING RANDOMNESS FROM IMPERFECT SOURCES

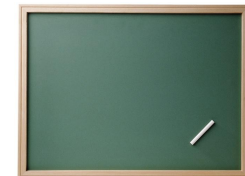
- Weak source of randomness: does not generate bits according to the uniform distribution



- Example: i.i.d. source $P_{X_j}(0) = \frac{1}{3}$ $P_{X_j}(1) = \frac{2}{3}$



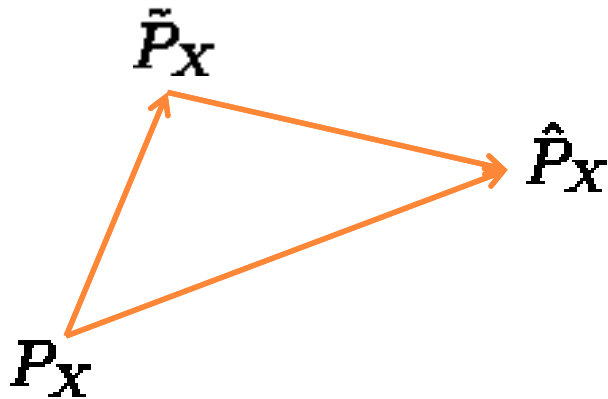
How can we produce one bit that is **more** random?
(i.e., closer to 50:50?)



MEASURE OF SUCCESS

- How do we measure “closer to uniform”?
- The statistical distance (or *total variation distance*) compares two distributions

$$\Delta(P_X, \hat{P}_X) = \frac{1}{2} \sum_x |P_X(x) - \hat{P}_X(x)|$$

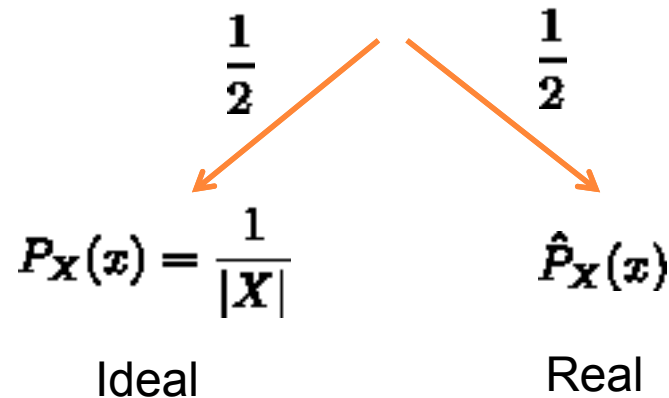


Properties of distance measure:

1. $\Delta(P_X, \hat{P}_X) \geq 0$
2. $\Delta(P_X, \hat{P}_X) = 0 \rightarrow P_X = \hat{P}_X$
3. $\Delta(P_X, \hat{P}_X) = \Delta(\hat{P}_X, P_X)$
4. $\Delta(P_X, \hat{P}_X) \leq \Delta(P_X, \bar{P}_X) + \Delta(\bar{P}_X, \hat{P}_X)$

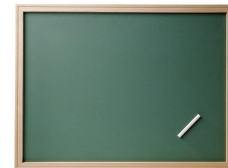
PROPERTY OF THE STATISTICAL DISTANCE

- Definition $\Delta(P_X, \hat{P}_X) = \frac{1}{2} \sum_x |P_X(x) - \hat{P}_X(x)|$
- Operational meaning: determines how well we can distinguish two distributions

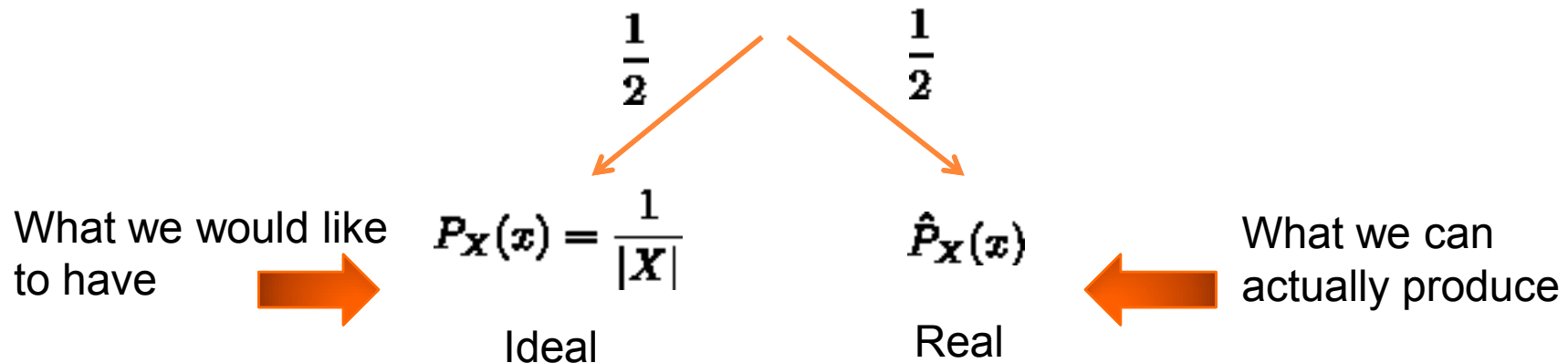


Let's show that

$$P_{\text{distinguish}} \leq \frac{1}{2} + \frac{\Delta(P_X, \hat{P}_X)}{2}$$



SIGNIFICANCE FOR CRYPTOGRAPHY



- When using randomness generated by the “real” process, we will assume in further analysis that we replaced the “real” by the “ideal” process.
- If the statistical distance is small, then the error thus incurred is small - otherwise the subsequent protocol would allow us to tell real from ideal but we know:

$$P_{\text{distinguish}} \leq \frac{1}{2} + \frac{\Delta(P_X, \hat{P}_X)}{2}$$

GOAL OF A RANDOMNESS EXTRACTOR

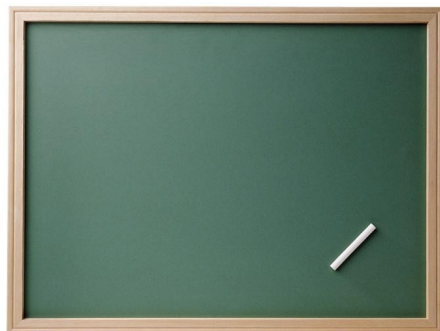
- Given a weak source of randomness X_1, \dots, X_n , produce a (possibly shorter) string K_1, \dots, K_ℓ

$$\Delta(P_K, \text{unif}(|K|)) \leq \epsilon$$

uniform distribution

acceptable error

- For our example: $\ell = 1, |K| = 2$



TYPES OF RANDOM SOURCES

- I.I.D. Source (von Neumann source)

$$P_X(\mathbf{x}) = P_{X_1}(x_1) \cdots P_{X_n}(x_n)$$

- Independent bit source

$$P_X(\mathbf{x}) = P_{X_1}(x_1) \cdots P_{X_n}(x_n)$$

- k-source

$$H_{\min}(X) \geq k$$

$$H_{\min}(X|E) \geq k$$

DETERMINISTIC RANDOMNESS EXTRACTOR

- In our example we applied a fixed function (parity)



- A deterministic randomness extractor is a function

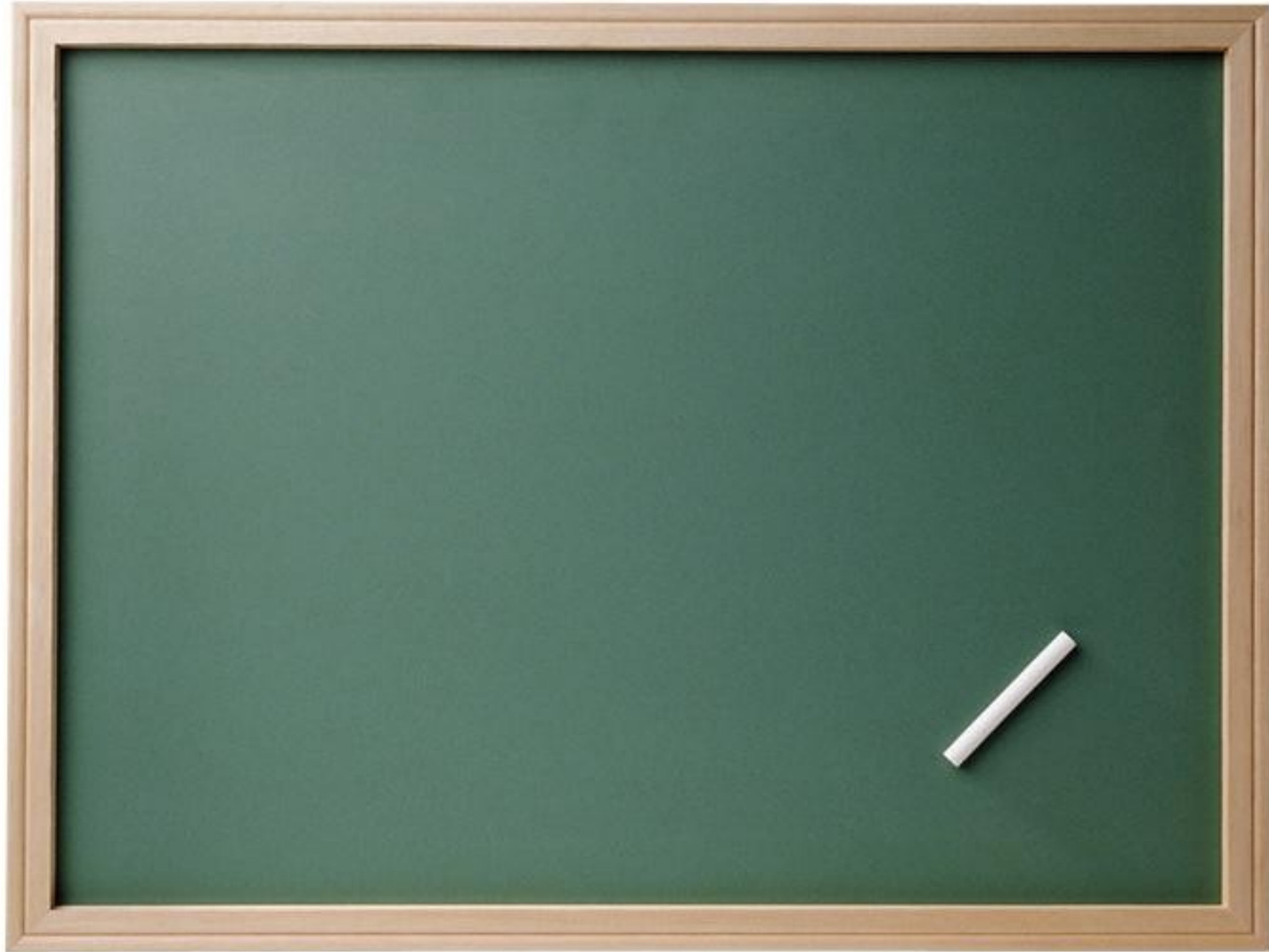
$$\text{Ext} : \{0, 1\}^n \rightarrow \{0, 1\}^\ell$$

- Is deterministic randomness extraction always possible?

IMPOSSIBILITY

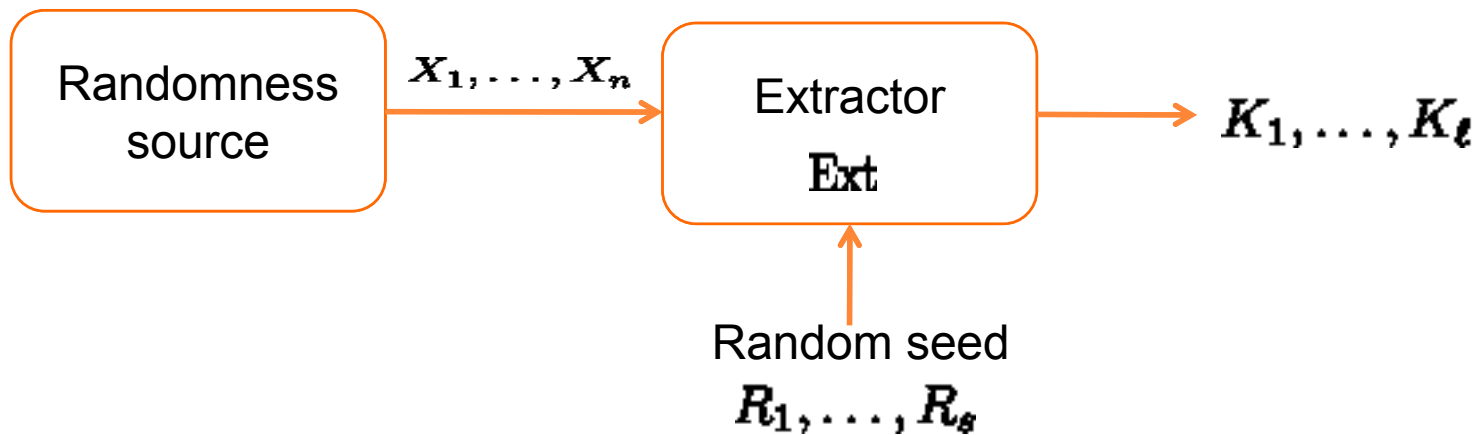
- There is no deterministic randomness extractor for an arbitrary k -source!
- Even if $H_{\min}(X) = \epsilon - 1$
- We show that for any function E there exists a source (probability distribution) such that we can predict the outcome perfectly!

PROOF OF IMPOSSIBILITY OF A PERFECT DETERMINISTIC EXTRACTOR



NOT ALL IS LOST.....

- Investing a random seed



- Can extract randomness this way!
- hardly surprising?

WEAK VS. STRONG EXTRACTORS

- Weak (k, ϵ) -extractor: If the source has min-entropy $H_{\min}(X) = k$ the output bits obey

$$\Delta(P_K, \text{unif}(|K|)) \leq \epsilon$$

$$\Delta(P_{KE}, \text{unif}(|K|) \times P_E) \leq \epsilon$$

- Strong (k, ϵ) -extractor: If the source has min-entropy $H_{\min}(X) = k$ the output bits obey

$$\Delta(P_{KER}, \text{unif}(|K|) \times P_{RE}) \leq \epsilon$$

Uniform (ie hard to predict) even given the random seed R!

HOW MUCH RANDOMNESS CAN WE GENERATE?

- Depends on
 - Seed size that we invest
 - Min-entropy of the source
- There exists extractors such that
 - Seed size $\log(n) - 2\log(1/\epsilon) + O(1)$
 - Output size $k - 2\log(1/\epsilon) + O(1)$
- The output size can never exceed the initial min-entropy

$$\ell \leq k = H_{\min}(X|E)$$

CONSTRUCTING STRONG EXTRACTORS

- Many constructions exist!
- Randomness extractors are equivalent to
 - List-decodable codes
 - Certain expander graphs
- A simple example: 2-universal hashing

$$F = \{f : \{0, 1\}^n \rightarrow \{0, 1\}^\ell\}$$
$$\forall x \neq x', \Pr_{f \in F}[f(x) = f(x')] \leq \frac{1}{2^\ell}$$

- The set of all possible functions is 2-universal ☺

LEFTOVER HASH LEMMA

- Imagliazzo, Levin and Luby
 - (Informal) Choosing f at random from a set of 2-universal hash functions yields a (k, ϵ) -strong randomness extractor with output length

$$\ell = k - 2 \log(1/\epsilon)$$

- Significant, since it tells us that we can actually generate roughly $k = H_{\min}(X|E)$ bits of randomness!

WHAT WE DID TODAY

- Cryptographic measure of entropy: min-entropy

$$H_{\min}(X) = -\log \max_x P_X(x)$$

- Randomness extractor

- Weak and strong extractors
- Measure of success

$$\Delta(P_{KER}, \text{unif}(|K|) \times P_{RE}) \leq \epsilon$$

- Basic example

READING FOR THIS LECTURE

- Lecture notes on statistical distance, min-entropy, and randomness extraction from IVLE (LN1statDistance.pdf, LN2minEntropy.pdf, LN3Randomness.pdf). Ignore references to homework and to quantum information.
- Homework due by Monday 2pm next week