Lecture 3 – Perfect Security and One-Time Pad

CS-466 Applied Cryptography
Adam O’Neill

Motivation

We saw that substitution ciphers cannot hope to achieve even the weakest privacy notion. → recover message from ciphertext

But what's the strongest privacy notion one can hope for? Is there a scheme achieving it?

recovering message from ciphertext is the weakest possible goal!

consider ~~recovering~~ some function of the message e.g. 1st bit

we want to formalize that ciphertext gives no information

knowledge before seeing ciphertext = knowledge after

Shannon's Work

Shannon (1948) addressed this in his landmark work, *A Mathematical Theory of Communication.*

This can be viewed as the birth of modern cryptography.

Shannon Security

Say $SE = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ with message-space $\mathcal{M}$, ciphertext-space $\mathcal{C}$, and coin-space $\mathcal{R}$ is SHANNON SECURE if:

We let $c \in \mathcal{C}$ be any ciphertext. It must hold that

$$\Pr_K[\mathcal{E}_K(m) = c]$$ is the same $\forall$ message $m \in \mathcal{M}$

Convince yourself this implies the adversary's knowledge before seeing a ciphertext == its knowledge after seeing a ciphertext.

Game

$K \xleftarrow{\$} \cancel{\mathcal{K}}$

$c' \xleftarrow{\$} \mathcal{E}_K(m)$

return $(c == c')$

probability the game ~~outputs~~ 1 is independent of m

may vary with c

One-Time Pad

Fix $k \in \mathbb{N}$

The one-time pad scheme with key-length k has key-space $\mathcal{K} = \{0,1\}^k$ and message-space $\mathcal{M} = \{0,1\}^k$ ie $\mathcal{K} = \mathcal{M}$ and coin-space $\emptyset$ is $OTP_k = (\mathcal{K}, \mathcal{E}, \mathcal{D})$

alg $\mathcal{K}$

$K \xleftarrow{\$} \{0,1\}^k$

return K

alg $\mathcal{E}(K, m)$

$c \leftarrow K \oplus m$

return c

alg $\mathcal{D}(K, c)$

$m' \leftarrow c \oplus K$

return m'

CORRECTNESS

$m' \leftarrow m \oplus K \oplus K$ ✓

bitwise XOR bits of K, m

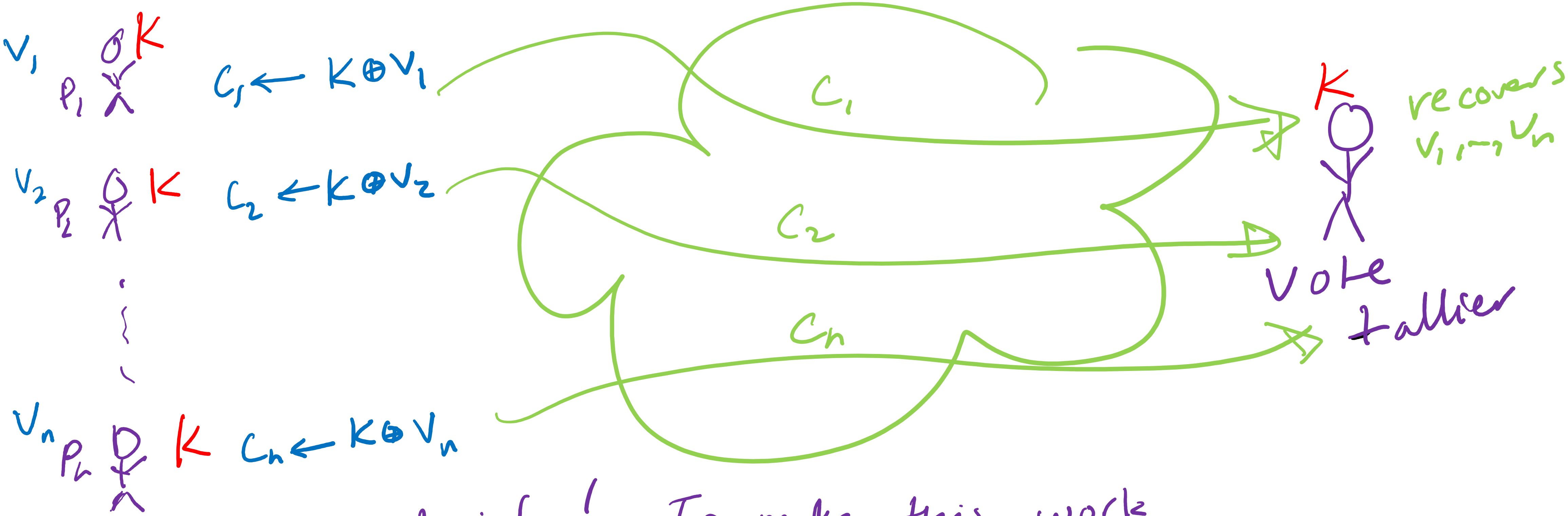
$K = K_1 \ldots K_k \quad m = m_1 \ldots m_k$

$K \oplus m = K_1 \oplus m_1 \| \cdots \| K_k \oplus m_k$

XOR

	0	1
0	0	1
1	1	0

Voting Example



tricky! To make this work we need $|K| = \sum_i |V_i|$ and

$c_i \leftarrow V_i \oplus \underbrace{K}_{K_i}$ means $K = K_1 \ldots K_n$

Lecture 3 – Perfect Security and One-Time Pad

CS-466 Applied Cryptography
Adam O’Neill

One-time Pad is Shannon Secure

Theorem. $\forall k \in \mathbb{N}$ OTP_k is Shannon Secure.

	0	1
0	0	1
1	1	0

Proof. It suffices to show SS for $k=1$.

Suppose we encrypt 0 under a random key

then $Pr[\mathcal{E}_k(0) = 0] = \frac{1}{2}$, $k \xleftarrow{\$} \mathcal{K}$

k here is one-bit

same for $\mathcal{E}_k(1)$

So probability distribution on ciphertexts is independent of m ✓

b/c OTP_k can be viewed as k parallel copies of OTP_1

proof of SS
assumes K is
as long as the
sum of the lengths
of every message
ever encrypted

$c_1 = K \oplus m_1$

$c_2 = K \oplus m_2$

$|K| = |m_1| = |m_2|$

Eve

Key Re-Use

Suppose the key is used twice. What can the adversary learn?

not Shannon Secure

can compute
$c_1 \oplus c_2 = m_1 \oplus m_2$

If you recover m_2 you get K

enough 00⋯0 in m_1 to learn bits of m_2

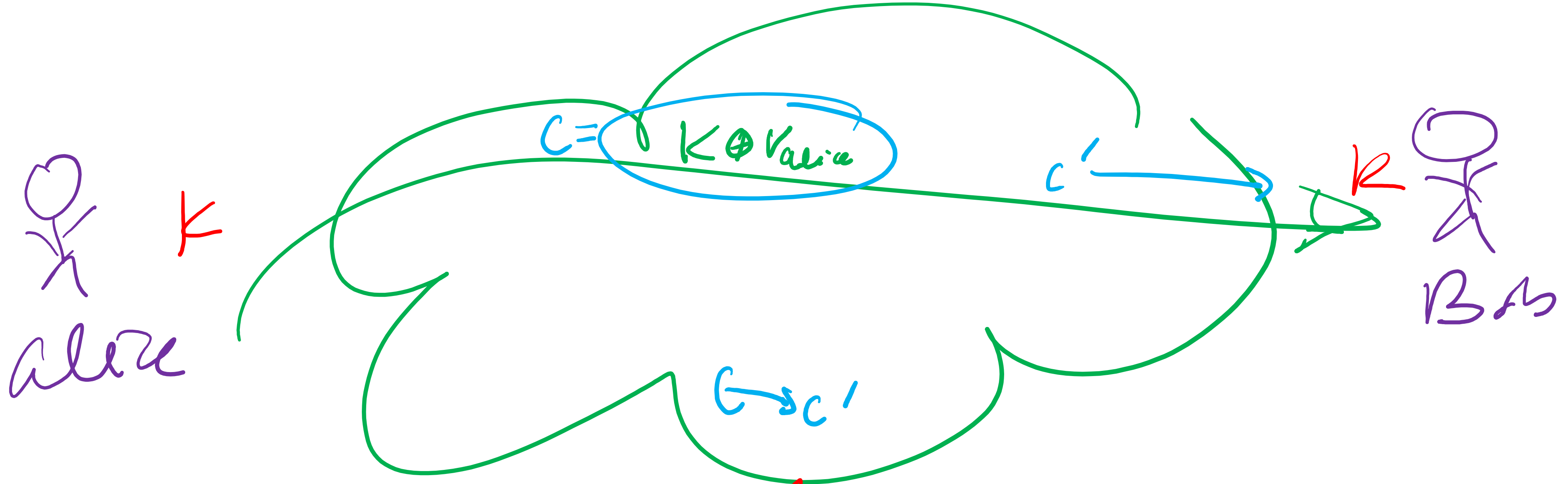
Project Venona

Another amusing story about the two-time pad is relayed by Klehr [65] who describes in great detail how Russian spies in the US during World War II were sending messages back to Moscow, encrypted with the one-time pad. The system had a critical flaw, as explained by Klehr:

> During WWII the Soviet Union could not produce enough one-time pads ... to keep up with the enormous demand .... So, they used a number of one-time pads twice, thinking it would not compromise their system. American counter-intelligence during WWII collected all incoming and outgoing international cables. Beginning in 1946, it began an intensive effort to break into the Soviet messages with the cooperation of the British and by ... the Soviet error of using some one-time pads as two-time pads, was able, over the next 25 years, to break some 2900 messages, containing 5000 pages of the hundreds of thousands of messages that had been sent between 1941 and 1946 (when the Soviets switched to a different system).

The decryption effort was codenamed project Venona. The Venona files are most famous for exposing Julius and Ethel Rosenberg and helped give evidence of their involvement with the Soviet spy ring. Starting in 1995 all 3000 Venona decrypted messages were made public.

One-Time Pad is Malleable



passive adversary:
No information about V_{alice}

active adversary

take compliment of ciphertext
→ encryption of opposite bit (w/o knowing the bit)

Optimality

Theorem: Suppose $SE = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is SS.
Then $|\mathcal{K}| = |\mathcal{M}|$.

proof: Suppose $|\mathcal{K}| < |\mathcal{M}|$. Fix c.
Then $\exists m_0, m_1$ st. $\exists k$ st. $\mathcal{E}_k(m_0) = c$
but $\nexists k$ st. $\mathcal{E}_k(m_1) = c$. So

$$\underbrace{\Pr_{k}[\mathcal{E}_k(m_0) = c]}_{> 0} \neq \underbrace{\Pr[\mathcal{E}_k(m_1) = c]}_{= 0}$$

Where To?

We have a scheme achieving perfect security and a proof that it’s optimal. (it’s very efficient, and one cannot do better in terms of key-length)

But key-length is completely impractical.

The main key idea of modern cryptography is that it is sufficient to consider efficient adversaries and allow “negligible” success (so small we feel comfortable with it for the foreseeable future)

Modern Cryptography: A Computational Science

In other words, security of a practical system must rely not on the impossibility but on the computational difficulty of breaking it.

Modern Cryptography: A Computational Science

(t, ε) - security

We might prove, e.g., no attack running in time (or resources) at most 2^{160} succeeds with probability greater than 2^{20}.

I.e., attacks could exist as long as it is prohibitive (in time/space, $$$) to mount them.

Algorithm Complexity

We measure the running-time of algorithms in the bit-length of their inputs. Not absolute value!

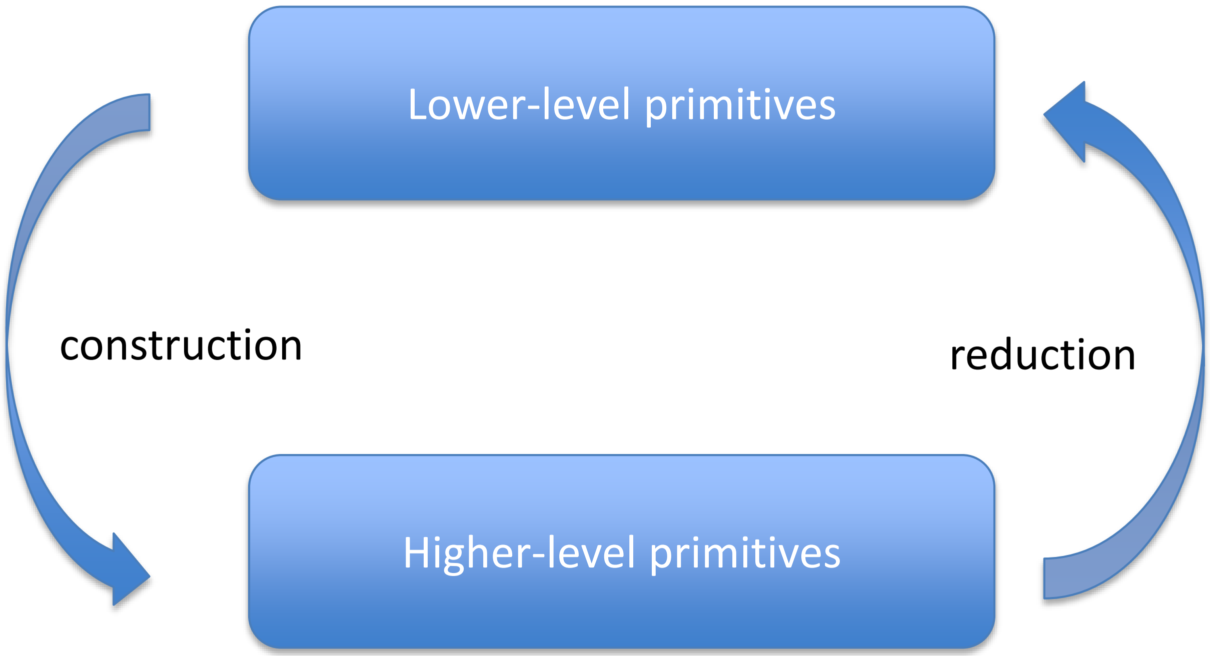
& memory usage

Efficient algorithms have code size, time and space use, etc. which is, e.g., polynomial in the input length (in a formal sense) and “feasible” (in an informal sense).

Factoring Example

https://en.wikipedia.org/wiki/Integer_factorization

Recall


Lower-level primitives
construction
reduction
Higher-level primitives

Quantitative Reductions

Where To?

Our first lower-level primitive, blockciphers.

Next time…