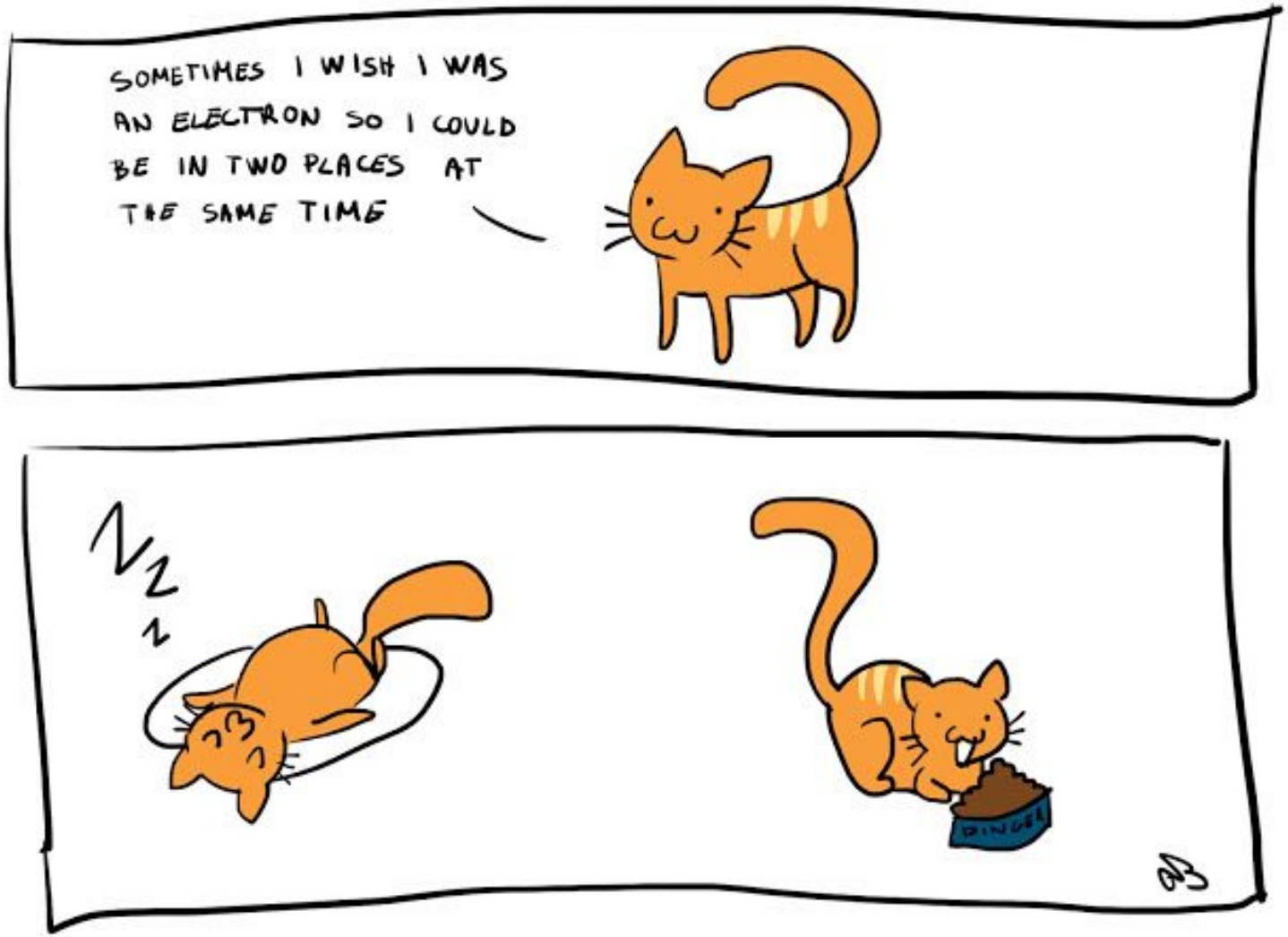
UCI University of California, Irvine

MITRE eCTF 2023-24

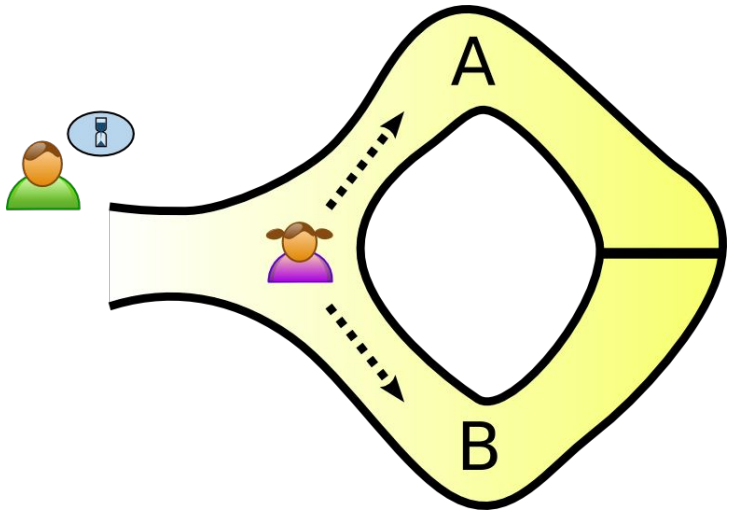
Kitten Postulation

MAX78000 Device–First Program Overview

Jinyao Xu (jinyaox@uci.edu)


SOMETIMES I WISH I WAS AN ELECTRON SO I COULD BE IN TWO PLACES AT THE SAME TIME
ZZZ
DINNER

Kitten Postulation (Not Proved Yet)



Cave ZKP:

- Chance for guessing one correct is ½
- Guessing two consecutive test ¼
- Geometric Series that converges to >1

Meaning:

The chances for playing correctly for at least once is greater than 1.

An NP Complete, reducible to SAT problem

Diverge Series:

- Guessing a password for the door, repeated enter and get feedback. Password never change–ZKP repeatedly testing it and probability becomes one over time.

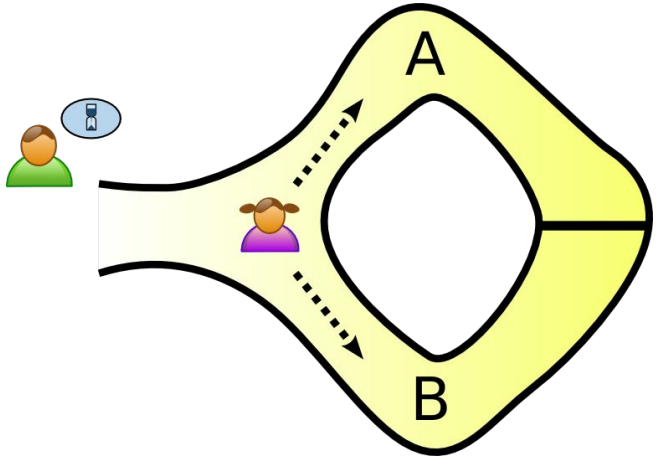
NOT NP Complete – Easy to see a polynomial time

Kitten Postulation (Weird Case)

- What happen if a series converge to >0 but <1?

Geometric Series:

- The coefficient A must be less than 1. → Meaning even if I have a correct solution, it may have error chances.
- eg the lock has a 80% chances not opening even if give correct password. So probability is 0.8/2. Two times will be 0.64/4, etc. It's greater than 0 for sure but less than 1.



Postulation: This is not solvable as a NP-Hard

DEMO FOR MAX78000FTHR

- Example 01: LED

- Example 02: UART with Computer

- Exception Registration

- Data Sheet and SPECS

Plain text = P

Encrypted text = C

Jet: $[k_{p_1}, k_{p_2}, k_{p_3}]$

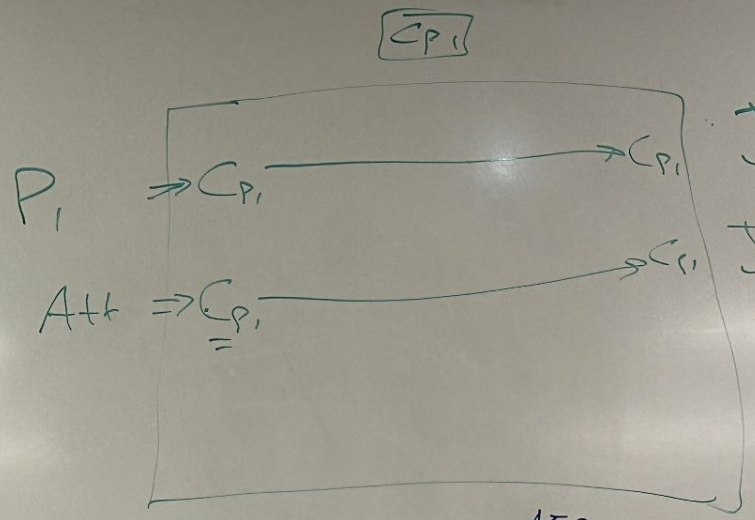
$P_1 : k_{p_1}$

$P_2 : k_{p_2}$

$P_3 : k_{p_3}$

$E(P \cdot k_{p_1} \cdot N) = C_{p_1}$

$D(C \cdot k_{p_1}) = P_{p_1}$



AES: 2 ms.

1. Goal 1 : Ciphertext indistinguishability.

CSV file.

- py. load procs.
- py. generate nonce.
- py. validate
- py. send out.

Interval: 0.1 sec.

100 ms.

JET

Pilot

- EEPROM STORE info. AES private key
- [Recieve Encrypt Send.] = Button push

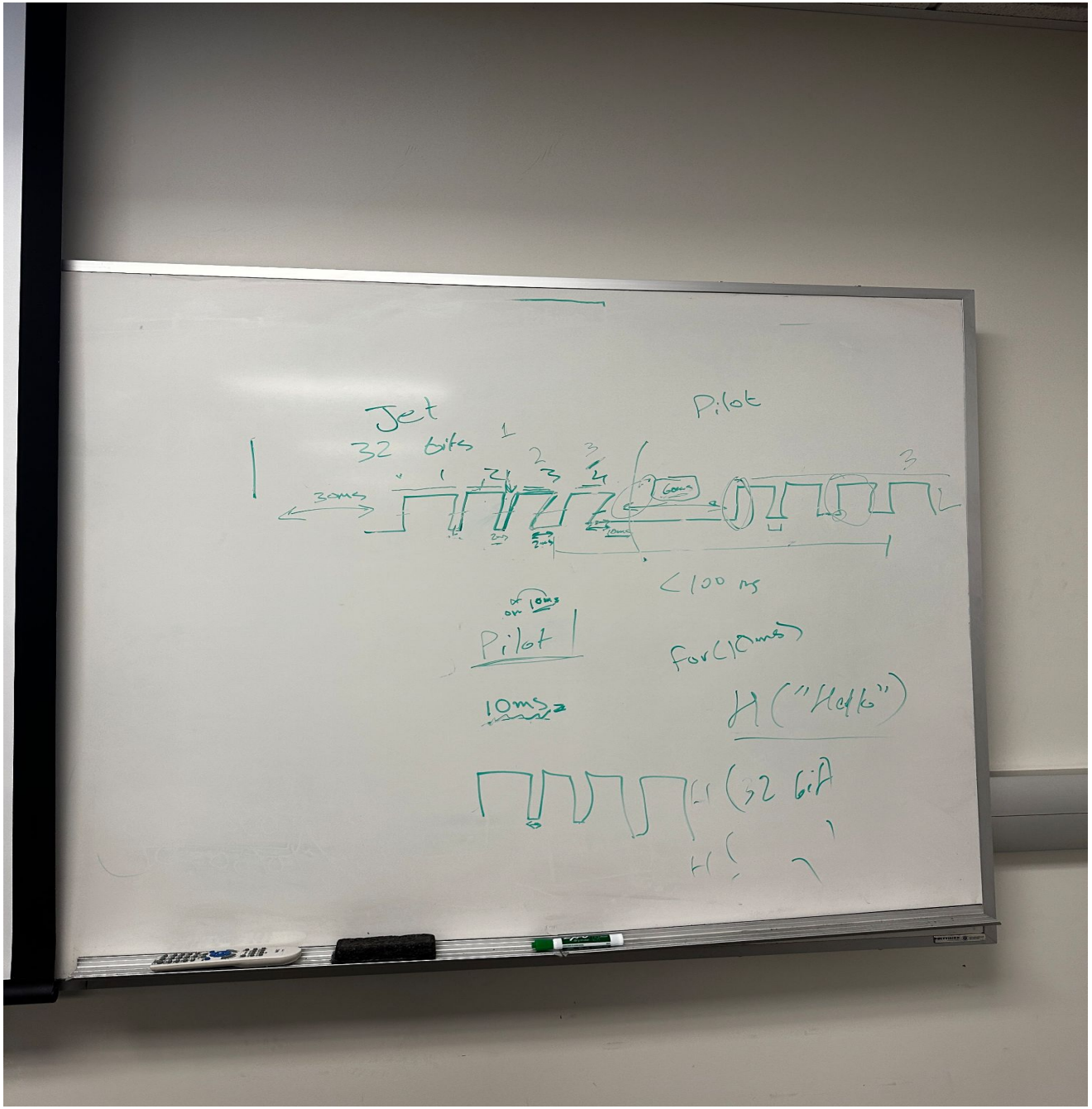
K_{P1} → 3 →

← C_{P1}

$D_{K1}(C_{P1}) = 3$

K_{P1} UART Rx AES Lib UART Tx

$E_{K1}(3) = C_{P1}$


Jet
32 bits
Pilot
30ms
< 100 ms
Pilot
10ms
for 10ms
H("Hello")