WiCS Fireside Chats : UG Interdisciplinary Research in CS @ Ashoka

# NeuroCrypt : CS and CogPsych

•••

Professor Debayan Gupta

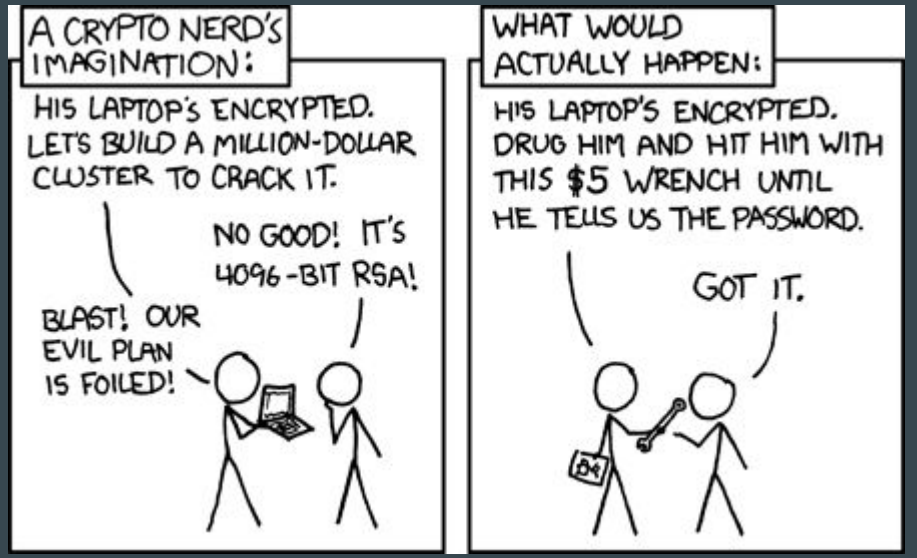
PhD - Arup Mondal

UG22 - Ritul Satish, Argha Chakraborty, Aditi Jain

UG23 - Niranjan Rajesh & Sristi Bafna

# Preliminary Information

- Motivation
- Supervisor
- Members on board
- Starting it off



# Background Information

- “Neuroscience Meets Cryptography” - Bojinov, Sanchez, Boneh and Lincoln

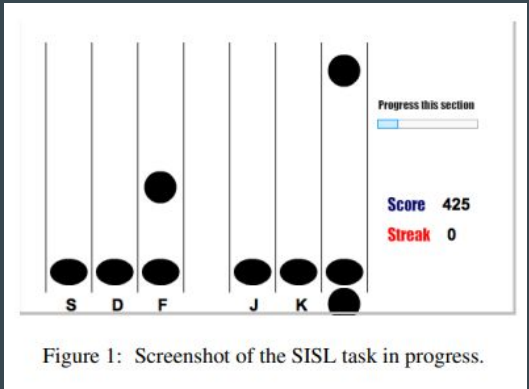
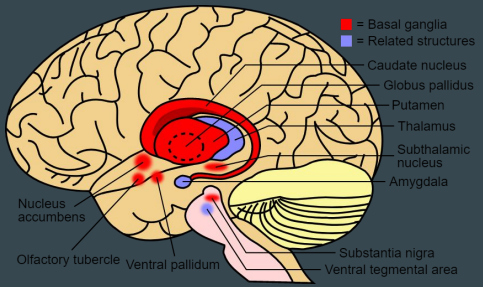


Figure 1: Screenshot of the SISL task in progress.



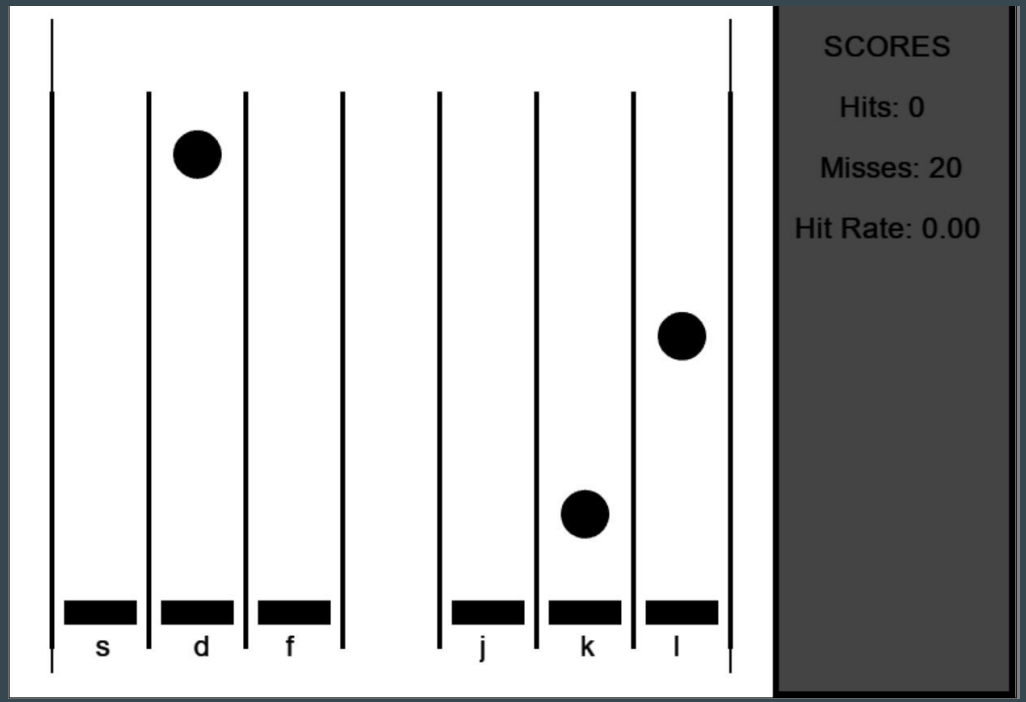

- Coercion attacks
- Implicit memory
- SISL task to leverage implicit memory
- Amazing idea but few shortcomings:
  - Long training period
  - Short retention period
  - Feasible as a real world-authentication system?

# Our Intended Contributions

- The product of an entire summer's literature review
- Engaging modalities from HCI:
  - Vision
  - Audition
- Reduce cognitive load
- Improve usability
- Improved retention

# The Experimental Game

https://sasta-guitar-hero-train-vid.netlify.app/

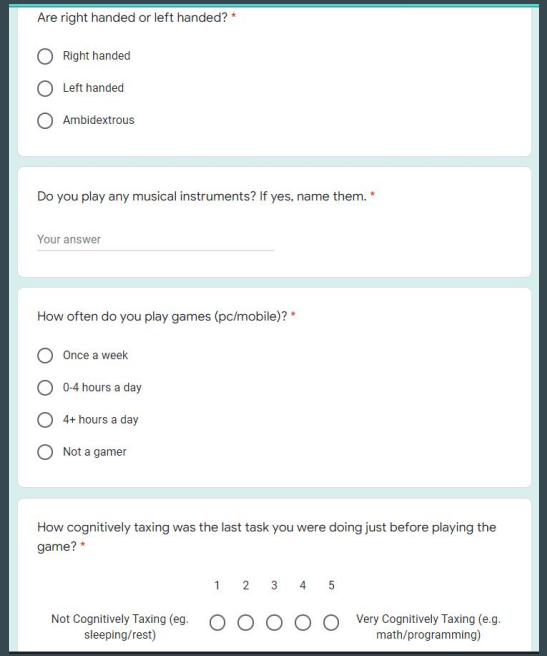



**Sasta Guitar Hero:**

- 7 blocks - 540 character long sequences [20 sec breaks]
- Audio:
  - White Noise
  - Note for each key (S,D,F,J,K,L)
- Visual:
  - Visual Separators
  - Flashing of cues
  - Color contrast between the cues
- Hit-Rate = hits/(hits+misses)
  - Displayed hit-rate to encourage better performance

# Experimental Procedure

1. IRB Approval for experimental study
2. Pilot experiment conducted online (remuneration for participants)
3. Offline experiments conducted last semester (4 iterations)
    a. Visual
    b. Audio
4. 30 people per session - same time every weekend
5. Training Session (45 mins), Auth1 (15 mins), Auth2 (15 mins)
6. Exit survey - To check explicit retention
    a. Languages
    b. Gaming experience
    c. Familiarity with musical instruments



# Passcode Generation

**Password Sequence ($P_a$)**

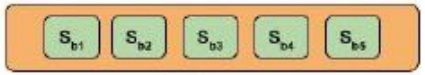
This 30 character long secret passcode sequence is generated from the set of Euler cycles from a directed graph G = (V, E) with each unique character in M as the vertexes.


**Sub Block gen($S_b$)**

The system assigned passcode $P_a$ is repeated thrice intermittently in an 18 character random sequence to make a 108 character sequence $S_b$ called sub-block.

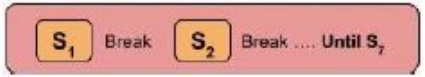

**Block gen(S)**

$S_b$ is followed by 4 more randomly generated $S_b$ to make S.

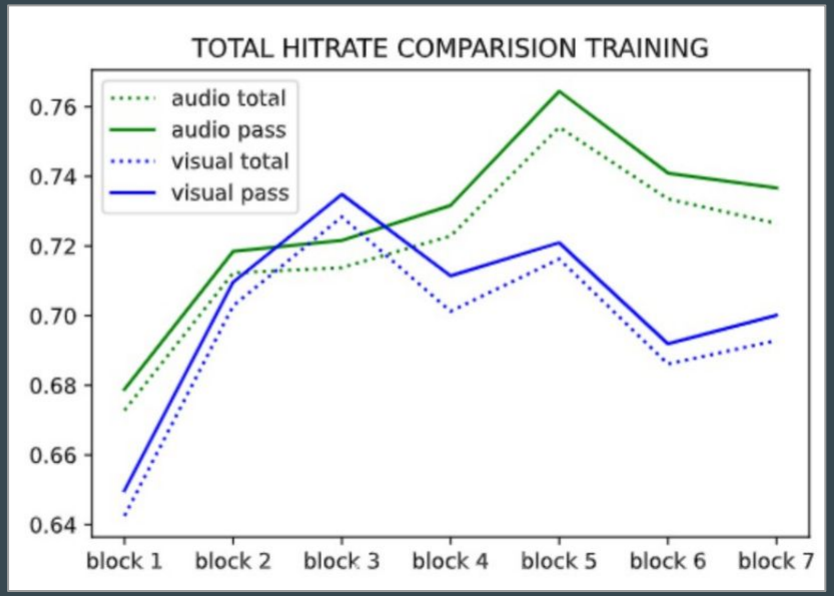


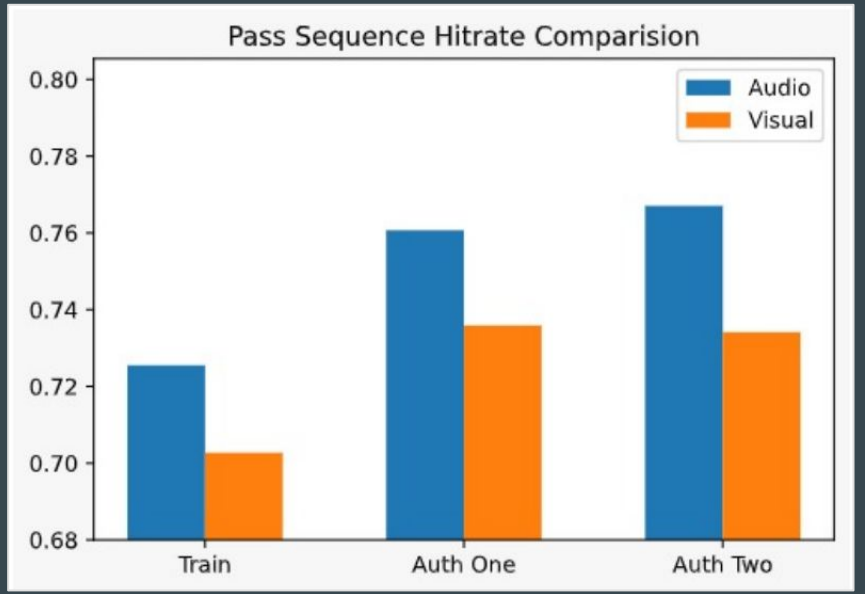

**Training sequence**

$S_b$ is followed by 4 more randomly generated $S_b$ to make S. S is repeated 7 times in the training phase. The user gets a 20 seconds break after every S called block.

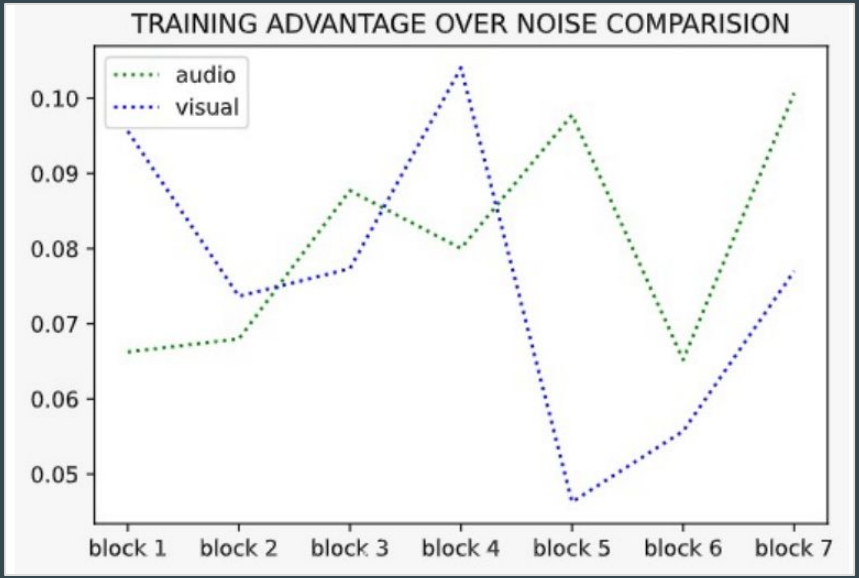


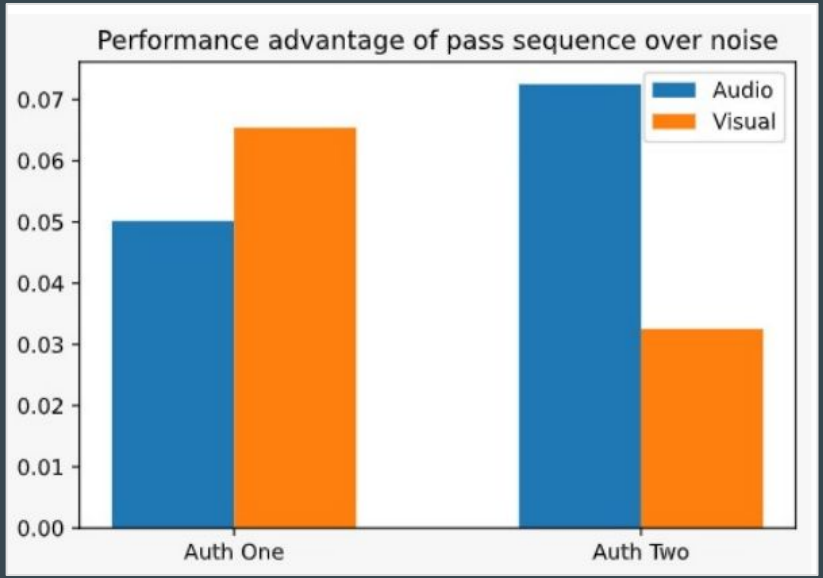
# Experimental Analysis



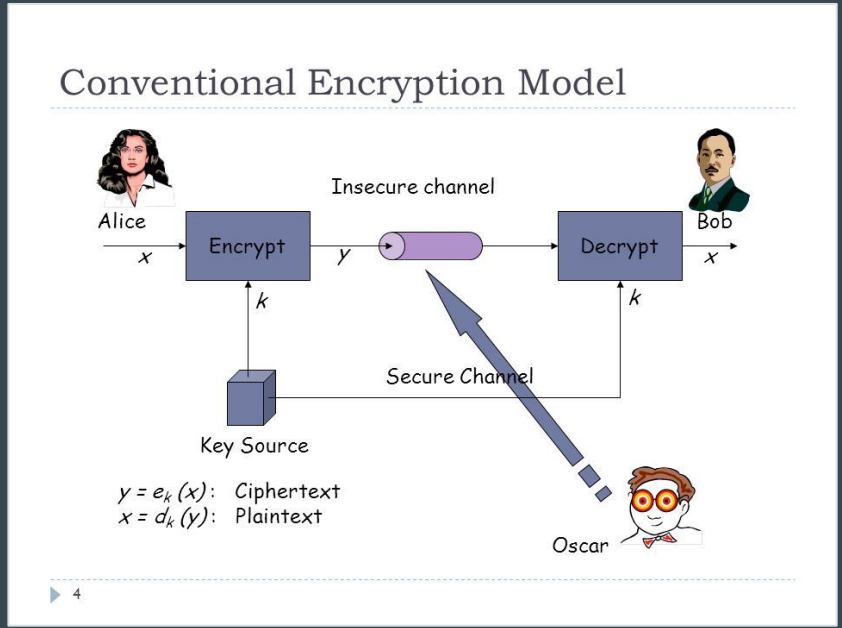
# Experimental Analysis



# Security & Usability Analysis

1. Basic threat vectors:
   a. User-interface attacks
   b. Inter-modal attacks
   c. Module attacks
   d. Template database attacks
2. Basic coercion threat model - Bob, Alice, Oscar
   a. Oscar coerces Alice
   b. Oscar takes the test himself
   c. Oscar recreates the sequence
3. Success probability shown for each



# Future Work & Conclusion

1. Haptic modality
2. Recreating parts of the sequence
    a. Boneh's results
3. Duress identification
    a. Skin conductance monitoring
    b. Eye-tracking software
4. Eavesdropping attacks:
    a. Client-side Malware
    b. Shoulder Surfing

# Publication

- AAAI 22 Poster Published!
- In process of applying to conferences and getting our entire paper published!

# NeuroCrypt: Coercion-Resistant Implicit Memory Authentication System

Ritul Satish  Niranjan Rajesh  Argha Chakrabarty  Aditi Jain  Sristi Bafna  Arup Mondal  Debayan Gupta

Ashoka University

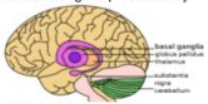
## Motivation

Coercion or Rubber-Hose attacks involve an adversary coercing a user to reveal the secret of an authentication system. To prevent this, proposed coercion-resistant models leveraged implicit memory to retain secrets instead of the traditional 'knowledge-based' password approach. However, the implementations of these systems lack in practicality and usability. To address these deficits, we propose NEUROCRYPT, an improved version of the Serial Interception and Sequence Learning (SISL) task that borrows concepts from cognitive psychology and Human Computer Interaction (HCI) to maximize implicit retention while minimizing the cognitive load on the user, thus improving such a system's practicality.

## Background Information

**Implicit Memory**

Implicit and explicit memory are the two main types of long term memory in humans. Implicit memory involves recollection of information unconsciously. The subject has no explicit recollection of the information stored in the mind. Motor tasks like riding a bicycle and typing on the keyboard leverage implicit memory.




**Sensory Modalities**

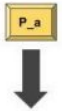
Modalities in HCI are channels of sensory information. In the context of our work, we intend to employ the **visual, auditory and haptic modalities** to reinforce the implicit learning that takes place. Three different modalities were chosen in order to employ **multimodal processing** to reduce **cognitive load** on the user.


## An Overview of Sequence Generation

Users undergo a training session in which they are trained with a 30 item long system assigned passcode sequence. The 6 keys that correspond to the six columns in the game are of the set S = {s, d, f, j, k, l}

**Password Sequence ($P_a$)**

This 30 character long secret passcode sequence is generated from the set of Euler cycles from a directed graph G = (V, E) with each unique character in M as the vertexes.

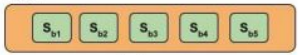



**Sub Block gen($S_b$)**

The system assigned passcode $P_a$ is repeated thrice intermittently in an 18 character random sequence to make a 108 character sequence $S_b$ called sub-block.


**Block gen(S)**

$S_b$ is followed by 4 more randomly generated $S_b$ to make S.




**Training sequence**

$S_e$ is followed by 4 more randomly generated $S_{e-1}$ to make S. S is repeated 7 times in the training phase. The user gets a 20 seconds break after every S called block.


## Authentication sequence (A)

The user is presented with $P_a$ along with two distinct untrained sequences $P_1$ & $P_2$ from the set of possible passwords. Each of the sequences in M = { $P_a$, $P_1$, $P_2$ } is presented to the user six times (two groups of three repetitions) with random ordering with no break.


## Stimuli from Modalities

**Auditory Stimuli**

Unique sounds played for each column/note to provide support in sequential learning according to 'the Scaffolding Hypothesis'.

White noise is played in the background and dynamically adjusted based on user performance to optimize user's attention in the game.

**Visual Stimuli**

To maximize visual perception and spatial differentiation of the cues, the colour contrast between the cues and the background is maximized and separators are added between columns.

To boost implicit sequence learning, a mild flashing in color of the visual cues are implemented.

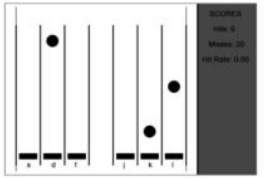
**Haptic Stimuli**

Haptic feedback administered to every keypress to reinforce implicit motor learning using motorized keys. Intensity of the vibration is chosen depending on the specific key from a set of two intensities in order to minimize explicit learning.

## Proposed Experimental Methodology

NeuroCrypt is a game played over three sessions, each seven days apart. Performance advantage of participants will be recorded for insights into implicit learning and retention which is crucial for corroborating the feasibility and promise of NeuroCrypt.

- **First Session (Training Session)**: Participants will be trained with a system-assigned passcode sequence for 45 – 50 minutes. After this, we will check explicit retention of the passcode sequence through a questionnaire.
- **Explicit Retention Test**: On a scale of 1 to 10 of familiarity, they will be asked to rate five videos of sequences (one system-assigned and four randomly generated sequences). For assessing correlation with other factors, we will inquire about their experience with gaming and instruments, their linguistic background, etc.
- **Subsequent Sessions (Authentication 1 & 2)**: Participant's implicit retention of the trained sequences will be tested in a 10 minute long session.




## Future Work

- Testing the extent of explicit recognition of the passcode sequence for the different modalities.
- Build a completely eavesdropping-resistant authentication scheme.

Author Contact: arup.mondal_phd19@ashoka.edu.in

Ashoka University, Rajiv Gandhi Education City, Sonipat, Haryana 131029

# THANK YOU!