Fighting Coercion Attacks in Key Generation using Skin Conductance
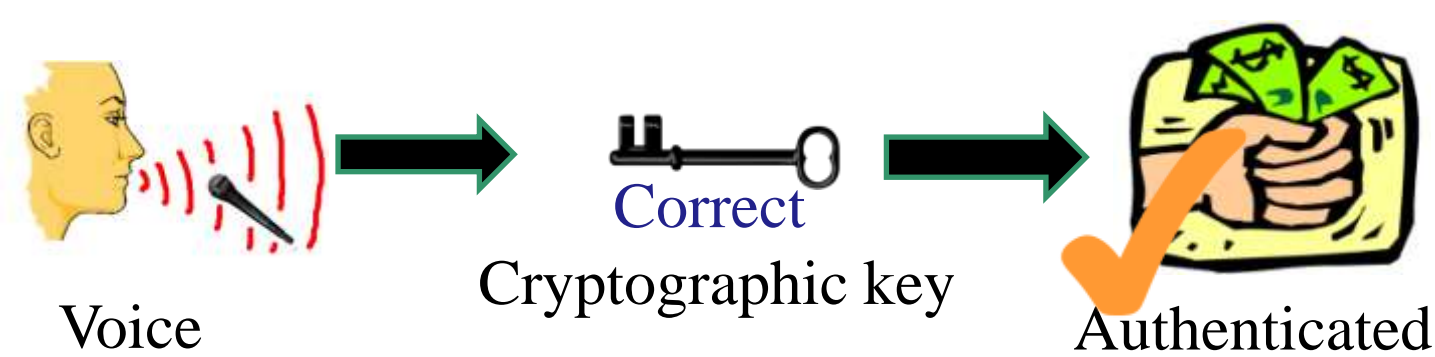
Payas Gupta, Assistant Professor Debin Gao

Example of Coercion Attacks

Bank's vault or safe Cockpit doors on airliners

Why Skin Conductance

- Measuring device is cheap and small in size
- Skin conductance and fingerprint can be measured simultaneously
- Skin conductance is the fastest responding measure of changes in stress

Existing Approaches to Generate Keys with Voice

Voice → Cryptographic key (*Correct*) → Authenticated

[Monrose et. al, 2001]

Key Generation

Skin Conductance — Features (*Amplitude*) → Feature Descriptor → Feature bit Vector (*0100*) → Lookup Table

Voice — (*MFCC*) Features → Feature Descriptor → Feature bit Vector (*0111*) → Lookup Table

Recover Key
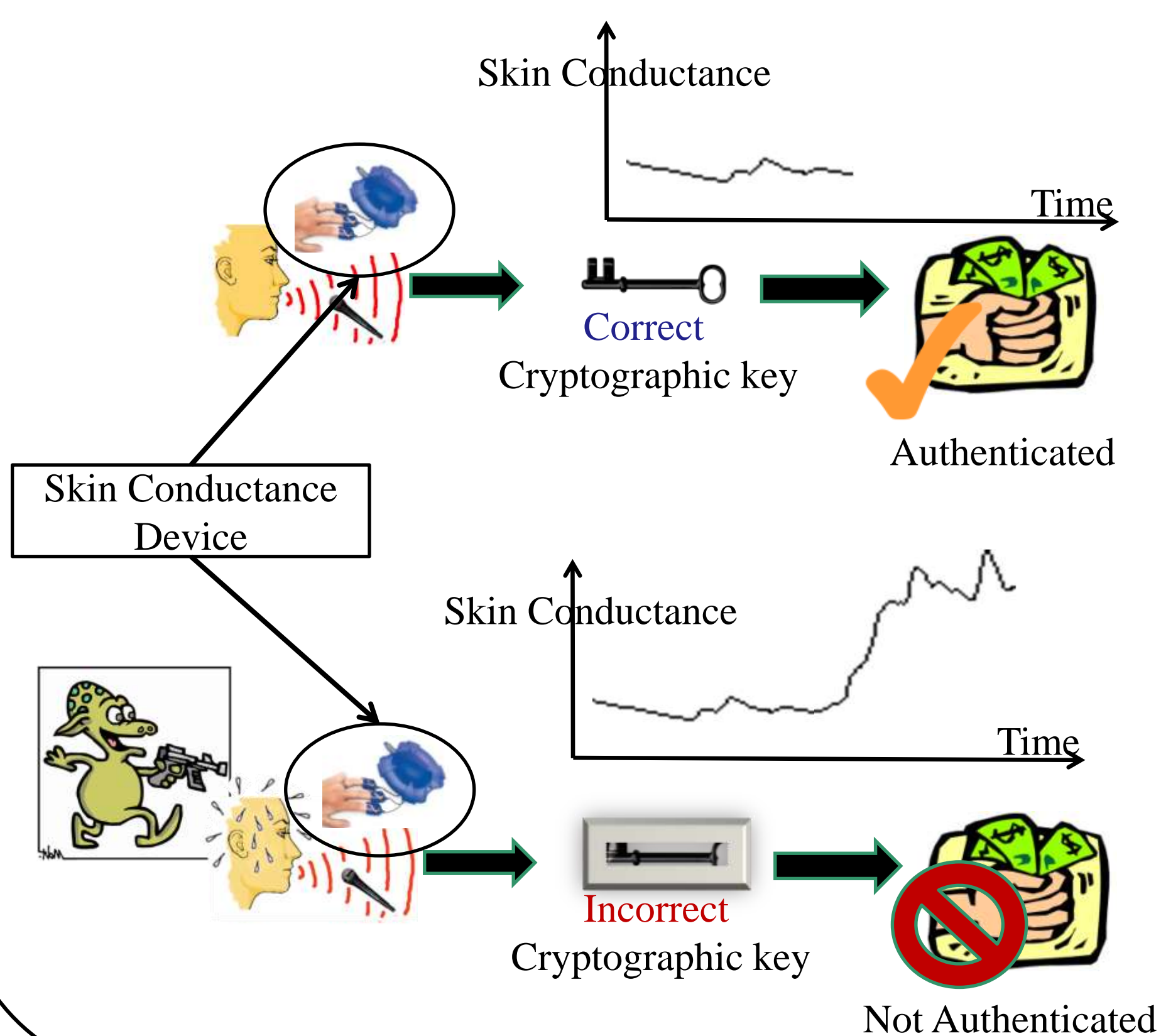
Coercion Resistance

- Properties we need
  - User does not have a choice
  - User does not have the capability under coercion
- No matter what the user does, the key generated will be wrong when user is under coercion
  - Assumption: attackers know how the system works
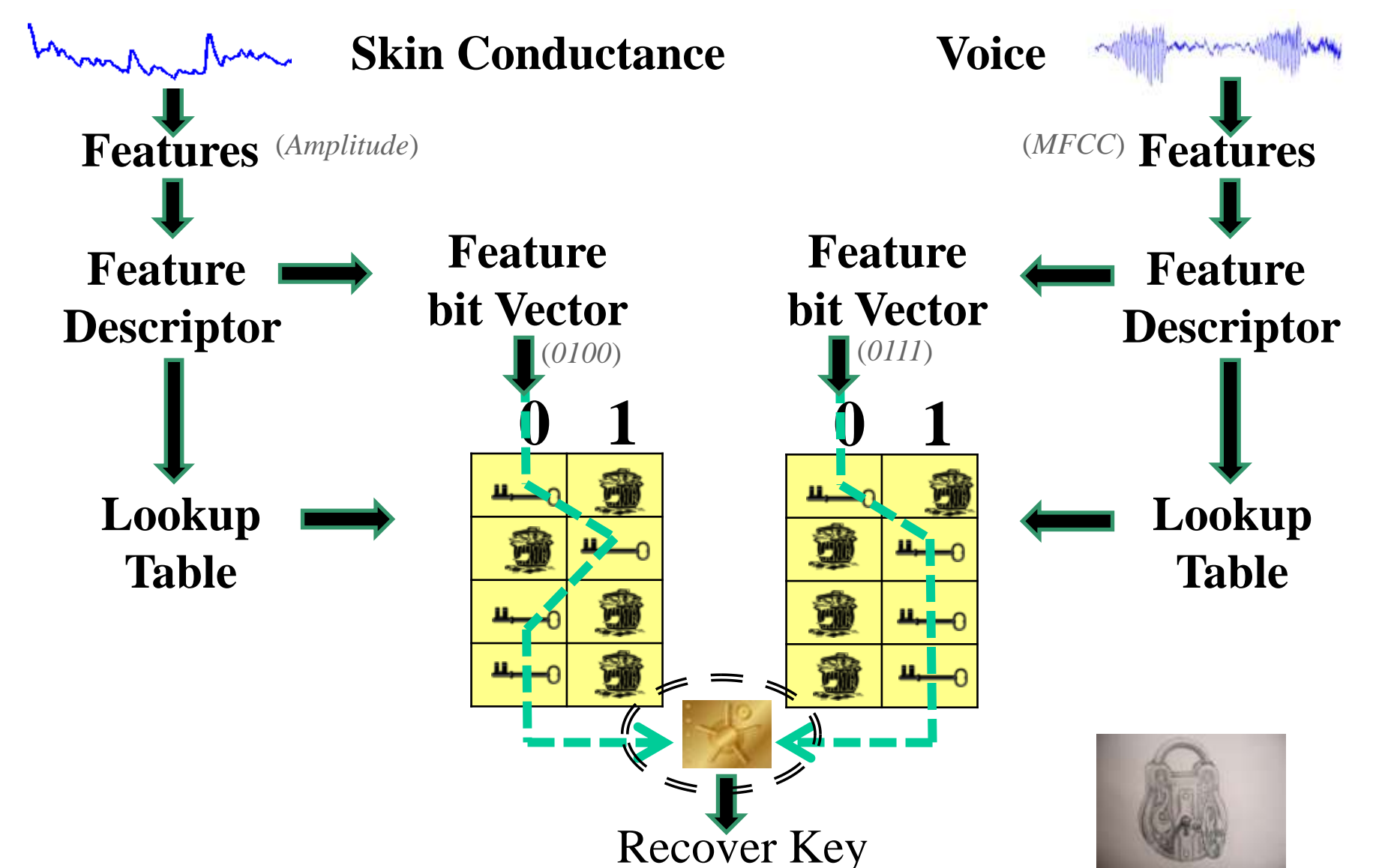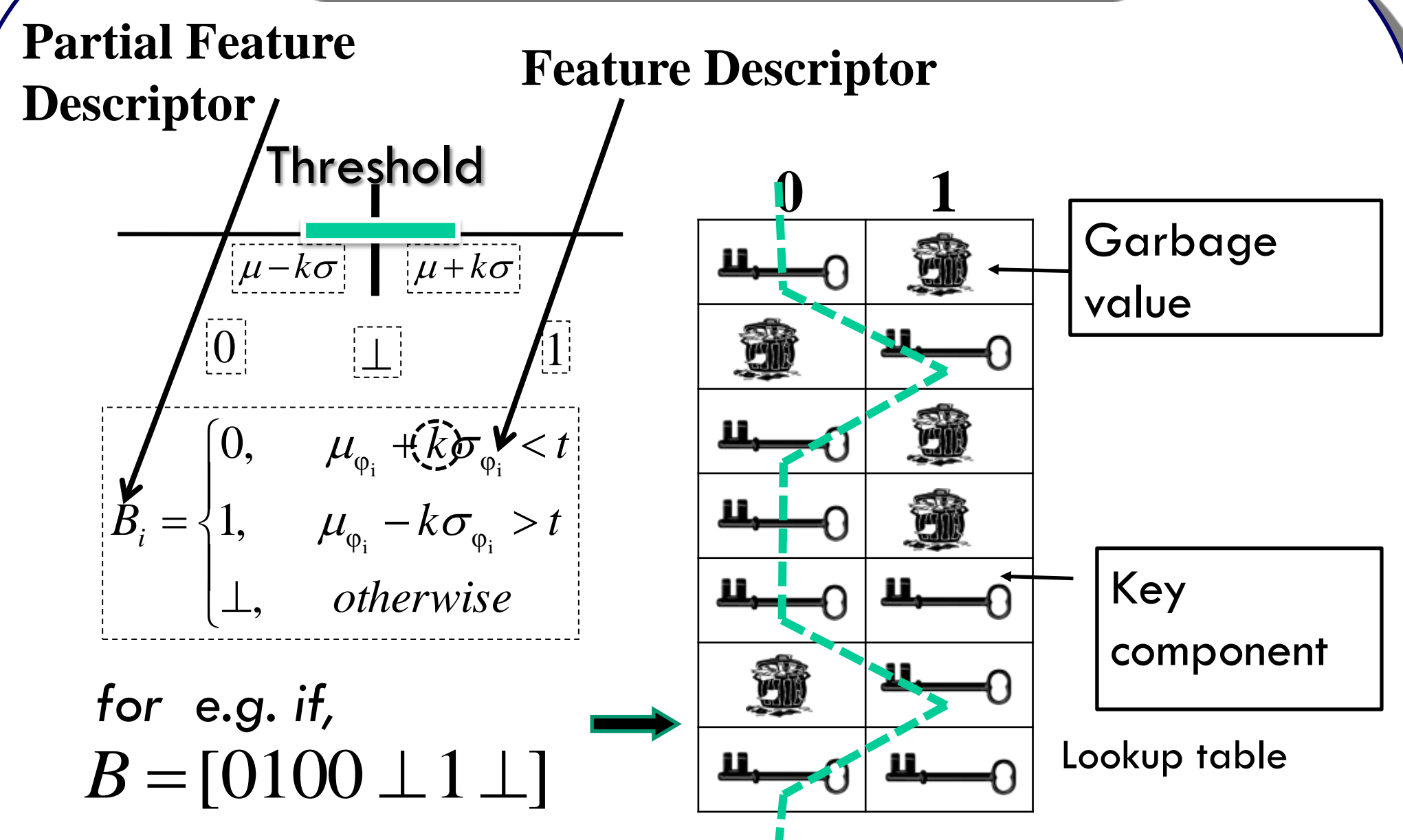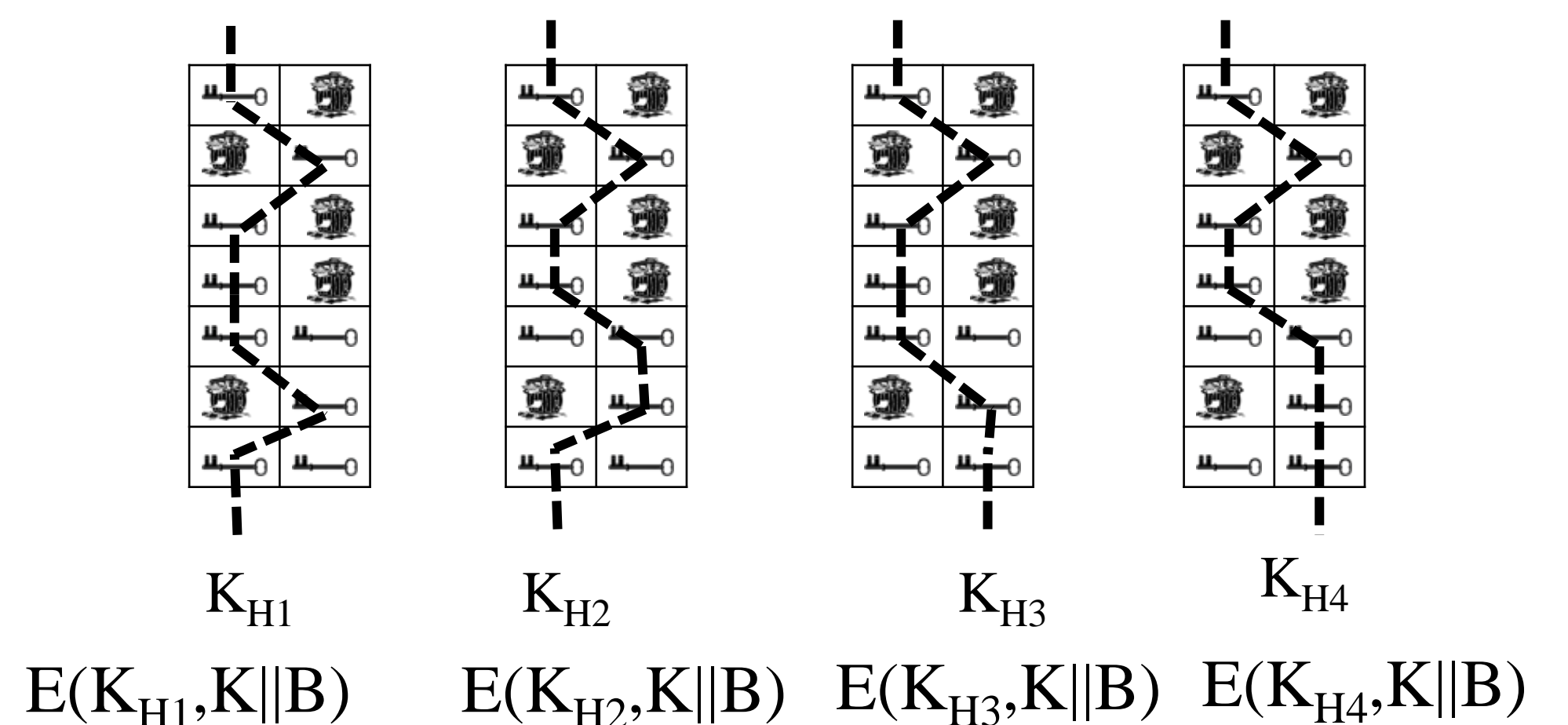 - Implication: attackers will not coerce the user

Lookup Table and Template Generation

Partial Feature Descriptor **Feature Descriptor**

Threshold

$\mu - k\sigma$ $\mu + k\sigma$

0 $\perp$ 1

$$B_i = \begin{cases} 0, & \mu_{\varphi_i} + k\sigma_{\varphi_i} < t \\ 1, & \mu_{\varphi_i} - k\sigma_{\varphi_i} > t \\ \perp, & otherwise \end{cases}$$

for e.g. if,

$$B = [0100 \perp 1 \perp]$$

0   1

Garbage value

Key component

Lookup table

K_{H1} K_{H2} K_{H3} K_{H4}

$E(K_{H1}, K\|B)$ $E(K_{H2}, K\|B)$ $E(K_{H3}, K\|B)$ $E(K_{H4}, K\|B)$

Random key **K** and Unique random number **B**

Template

$<<T_V \|\| T_{SC}>, <E(K_{H1}, K\|\|B), E(K_{H2}, K\|\|B), ..., E(K_{HZ}, K\|\|B)>, B>$

Our Proposal

Skin Conductance / Time

Voice → Cryptographic key (*Correct*) → Authenticated

Skin Conductance Device

Skin Conductance / Time

Cryptographic key (*Incorrect*) → Not Authenticated

Fighting Coercion Attacks in Key Generation using Skin Conductance

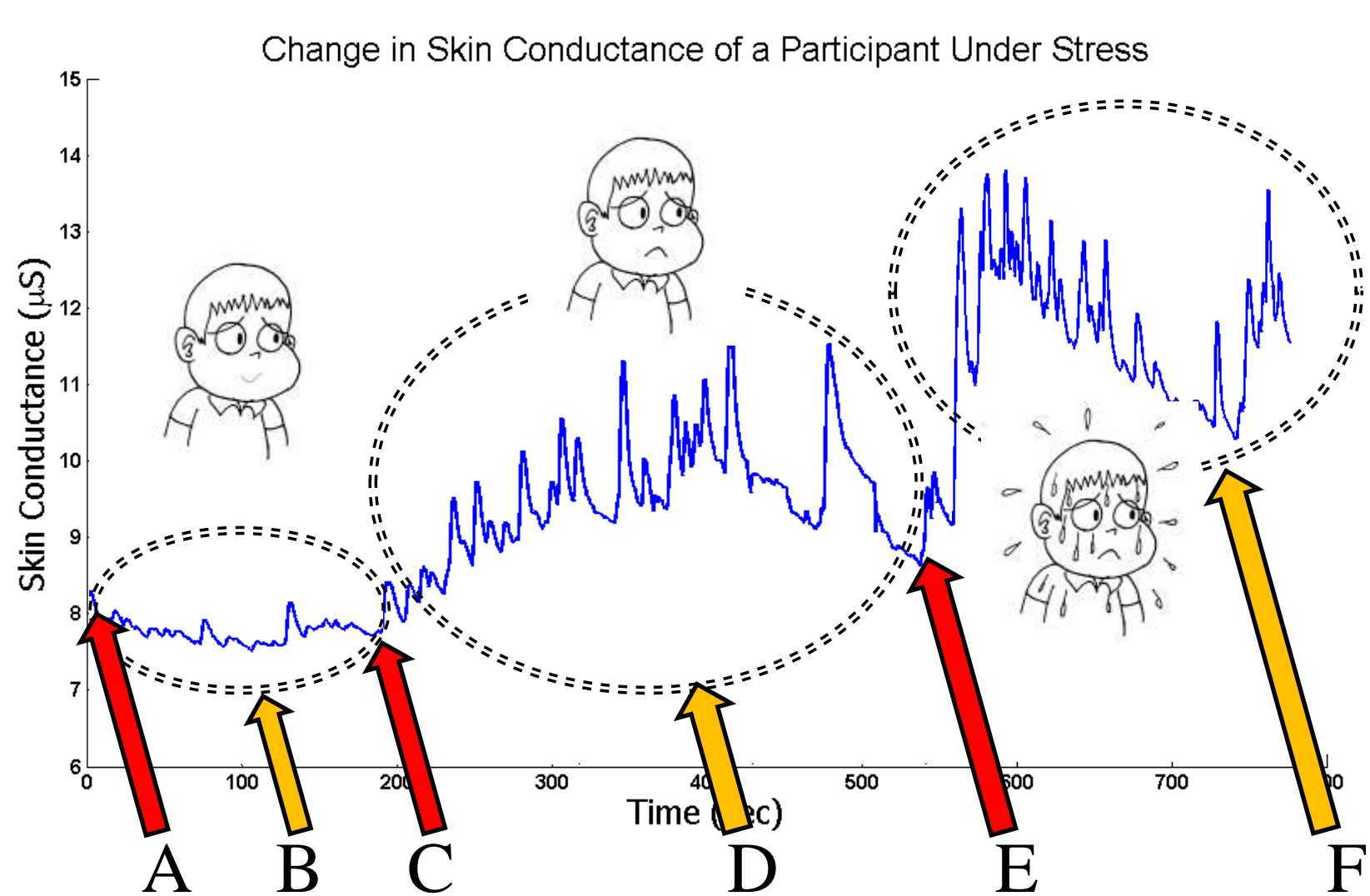**Payas Gupta, Assistant Professor Debin Gao**

User Study Demographics

- Undergraduate and graduate students in the age from 18 to 28.
- 43 participants
  - 4 participants removed the measuring device from their fingers when they were nervous during the experiment.
- Successful participants – 39
  - 22 male and 17 female

User Study

1. Do not touch the 'X' key of the keyboard
2. Hey I am back
3. It was your fault Who will pay for the device? How will I recover my data?
4.1. Yeah it was my mistake, I pressed the X key of your keyboard. I am ready to help you!!!
4.2. I am sorry, but I did not press X key.
4.3. Your experiment sucks, your laptop sucks, moreover you suck

Master Attacker

- To obtain normal skin conductance feature key from the following

Normal scenario feature key	Stress scenario feature key
01101101010000101	11101111010100111
01101101110001100	01101001010100011
01101010101000101	10100010100010111

Mapping of normal and stress skin conductance keys public database

Stress SC

Voice

Device and the algorithm

Original number of bits are 50

Events in the User Study

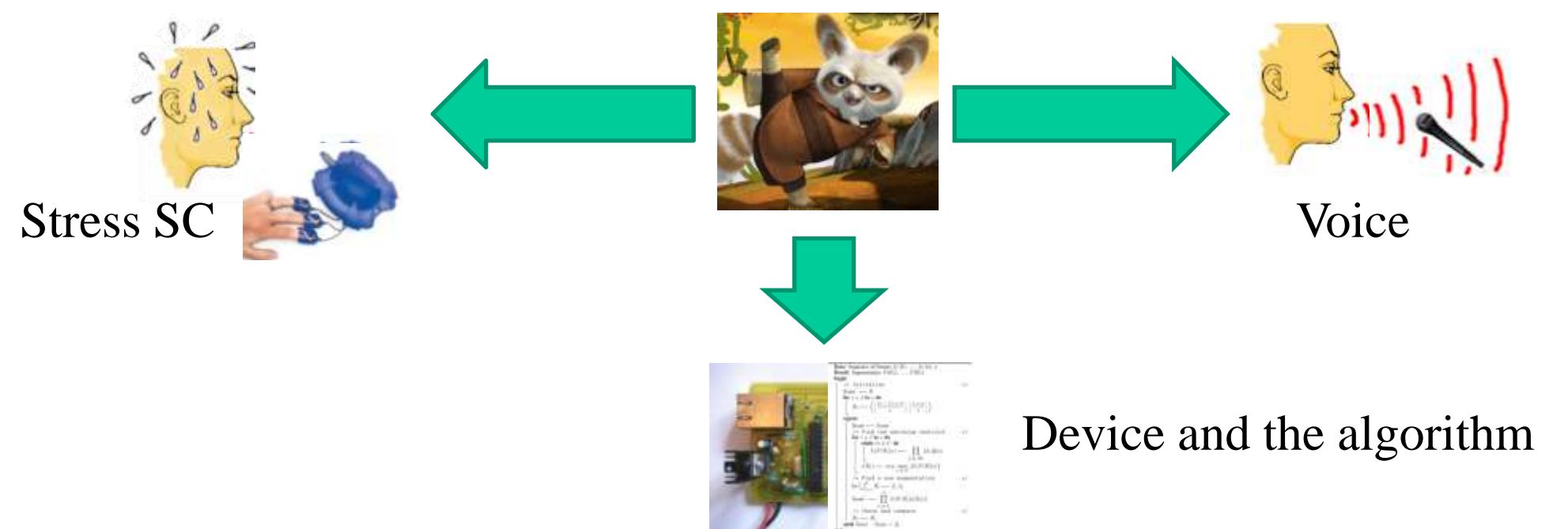Change in Skin Conductance of a Participant Under Stress

A B C D E F

A. Examiner leaves the room, leaving the subject alone
B. Subject sits in-front of a PC and is asked to type a few sentences
C. The core of the experiment begins when the PC shuts off as the subject is typing a letter
D. As a result, subject succumbs to stress
E. Examiner enters the room
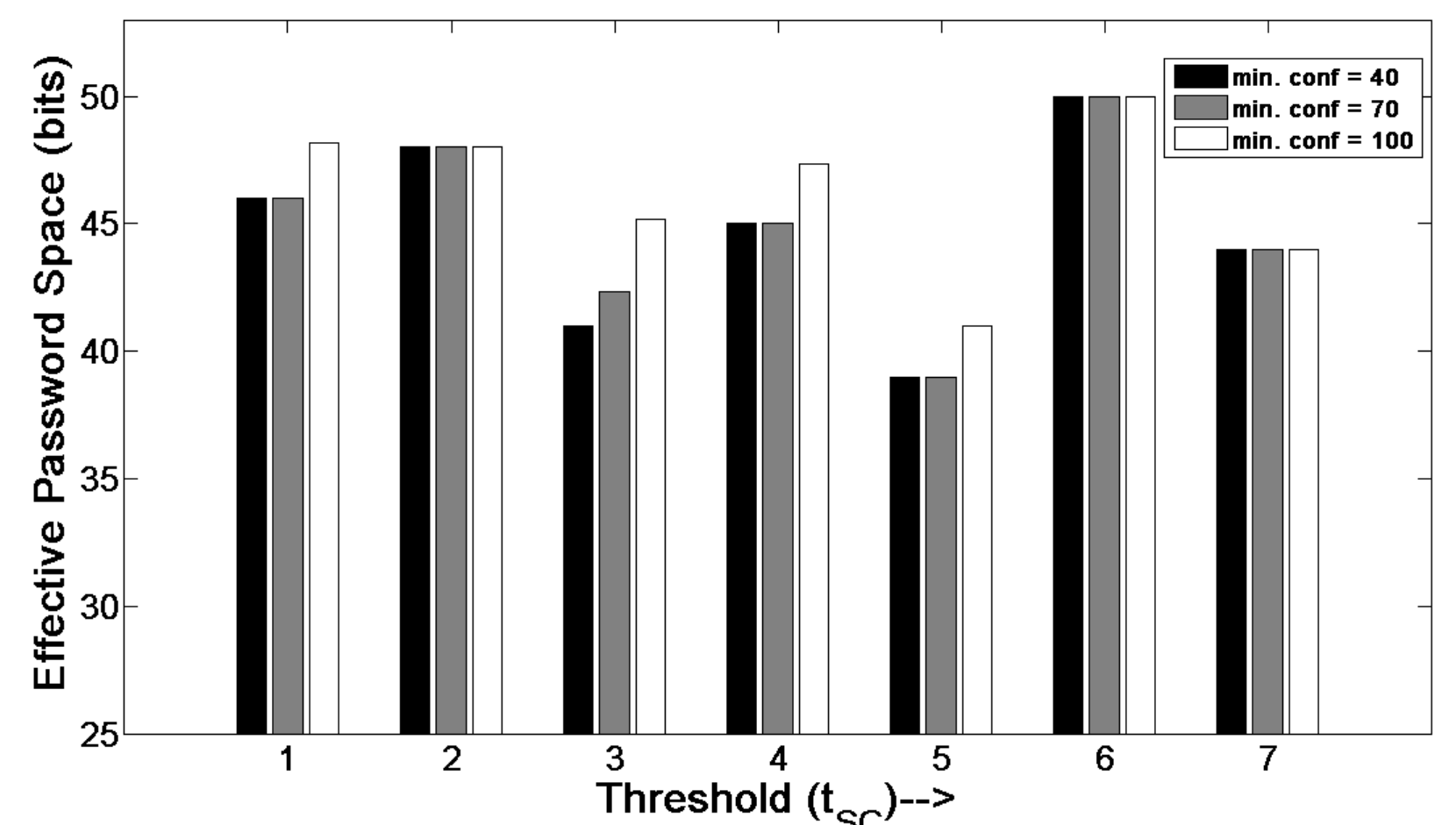F. And, falsely accused the subject for inappropriate handling of PC and corresponding data loss

False -ve when Normal Users try to generate keys

False Negative

k=1.25, k=1.375, k=1.5, k=1.625, k=1.75, k=1.875
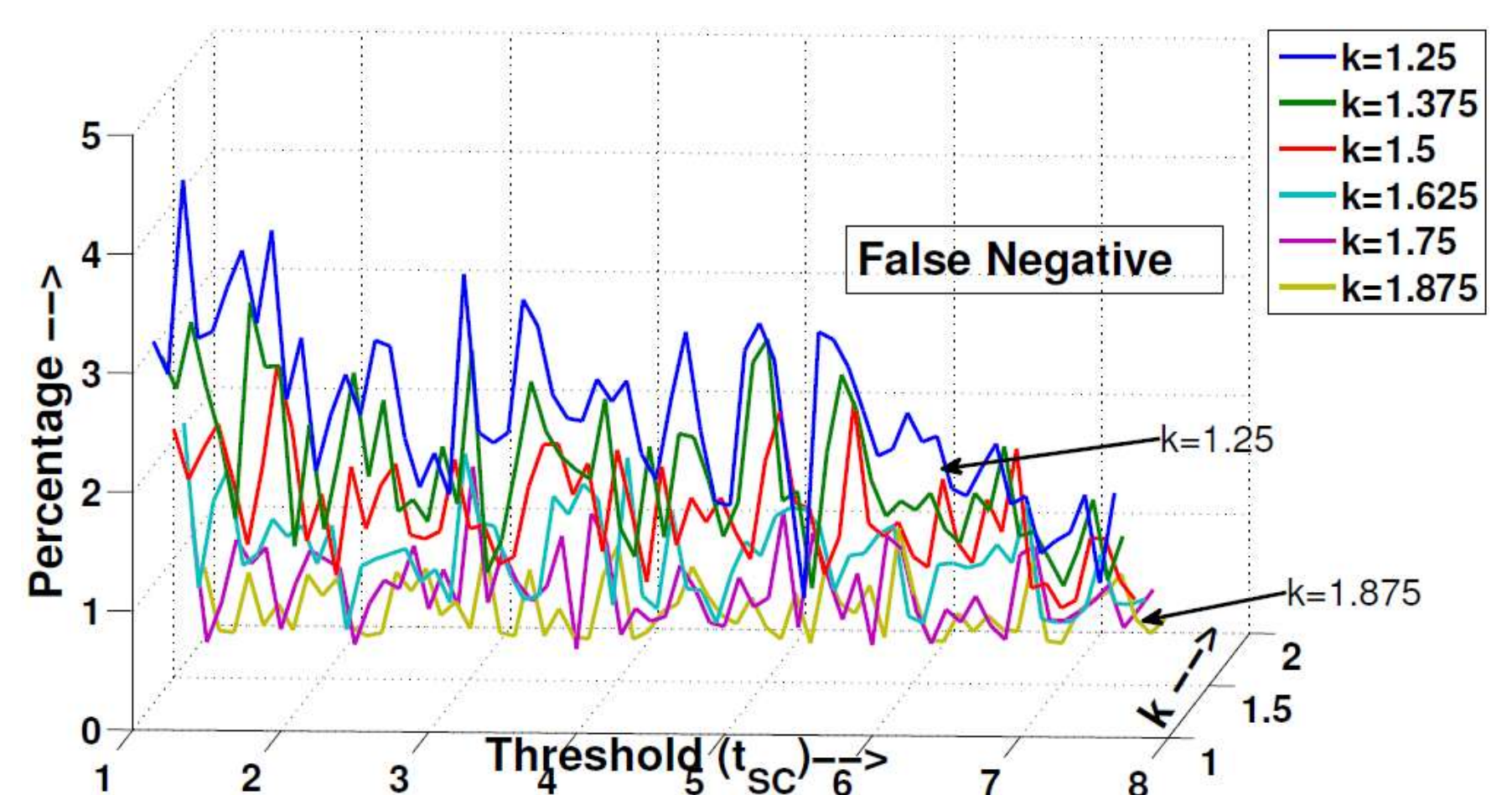
False +ve when Stressed Users try to generate keys

False Positive

k=1.25, k=1.375, k=1.5, k=1.625, k=1.75, k=1.875