aLeak: Privacy Leakage through Context-Free Wearable Side-Channel

Yang Liu, Zhenjiang Li

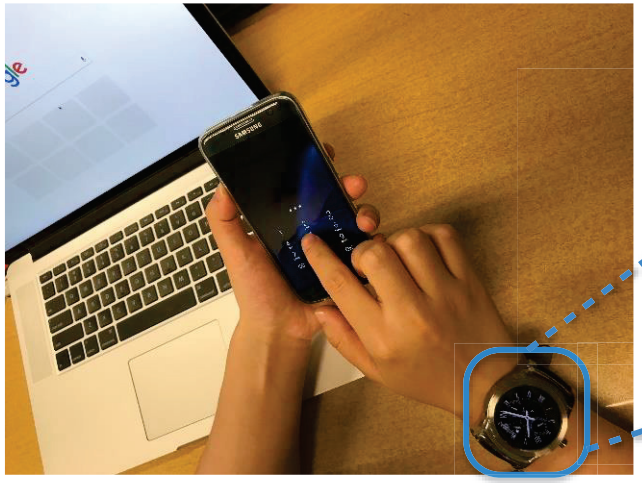
Department of Computer Science

City University of Hong Kong

CityU
香港城市大學
City University of Hong Kong

One day…

Gyro.

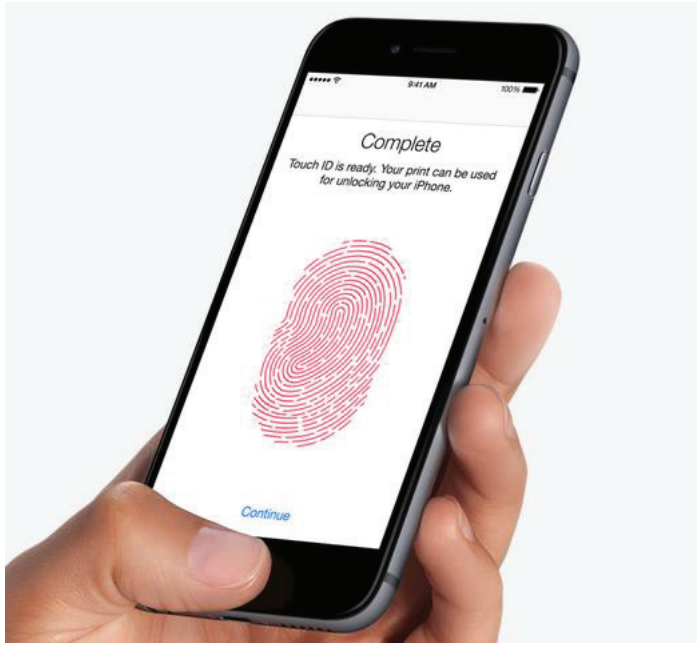


Acc.

CityU
香港城市大學
City University of Hong Kong

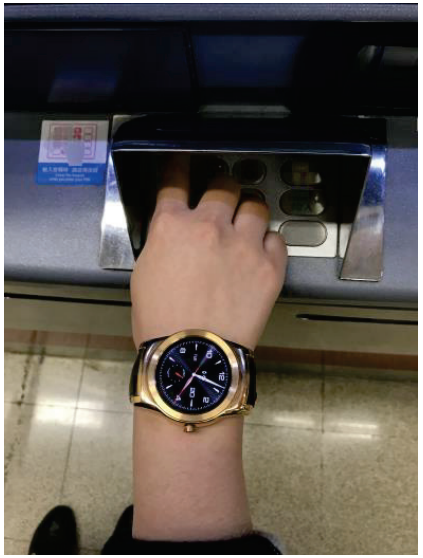
Any countermeasure?

Touch ID



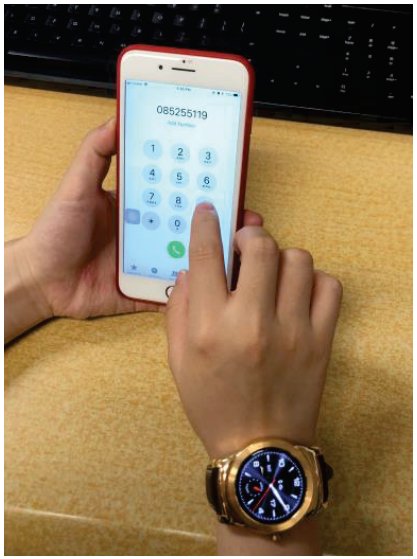
Face ID

But…

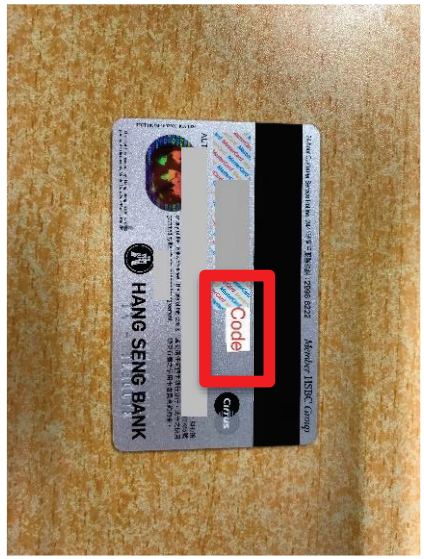


ATM or POS

Door entrance



Telephone



Secure code

Explicitly typing cannot be avoided

CityU
香港城市大學
City University of Hong Kong

Existing works

[ASIA CCS'16]

[CCS'15]

[MobiCom'15]

- **Horizontal keypad plane**
- **Known keyboard layout**
- **Fixed "Enter" button**

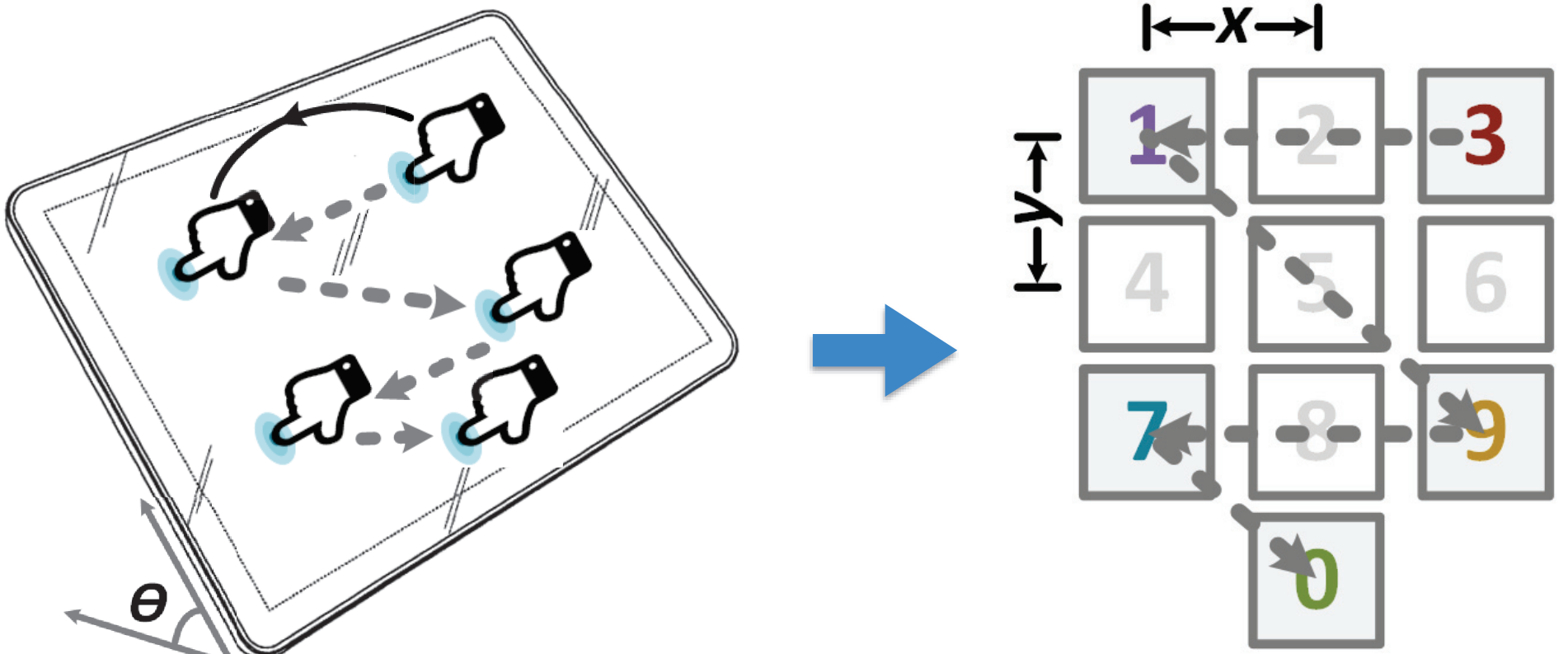
Context-free

?

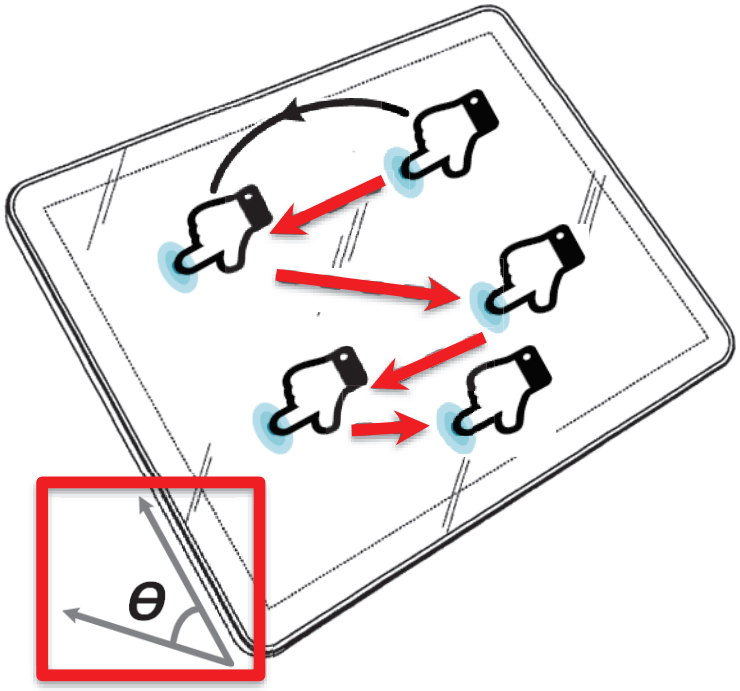
Arbitrary attitude

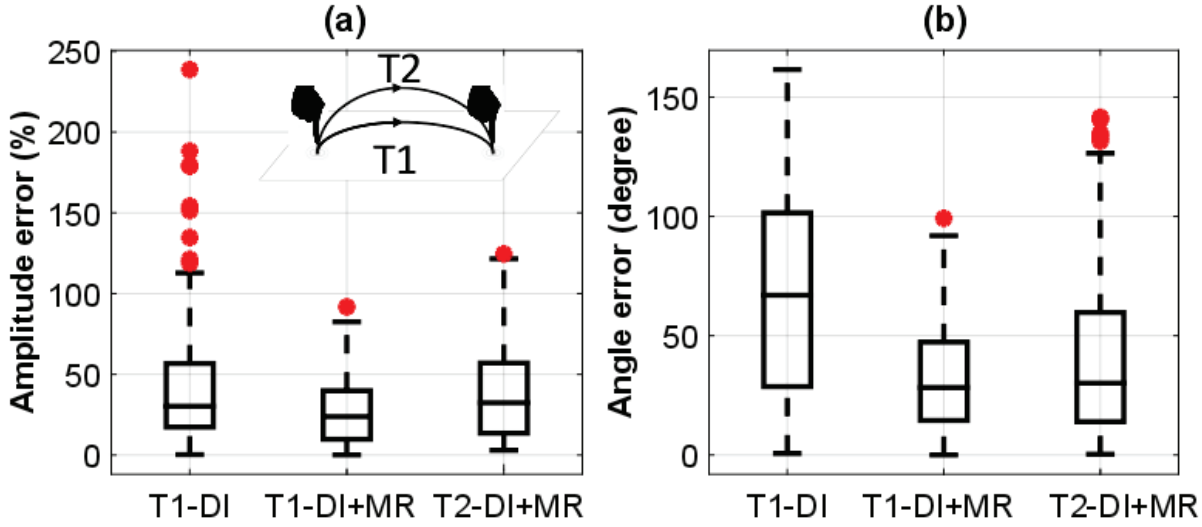
Unknown keyboard size

Attack process



Challenge-I: motion recovery





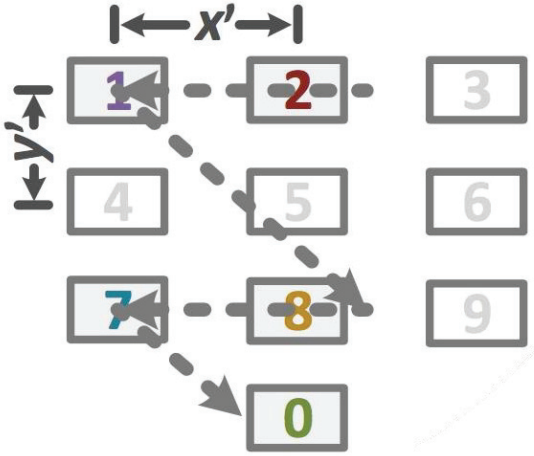
Cannot reliably reconstruct

Challenge-II: Unknown keyboard

x: 21	x: 15	x: 14	x: 21
y: 21	y: 14	y: 10	y: 20

Range of x: 19 ~ 91 (mm)

Range of y: 19 ~ 97 (mm)

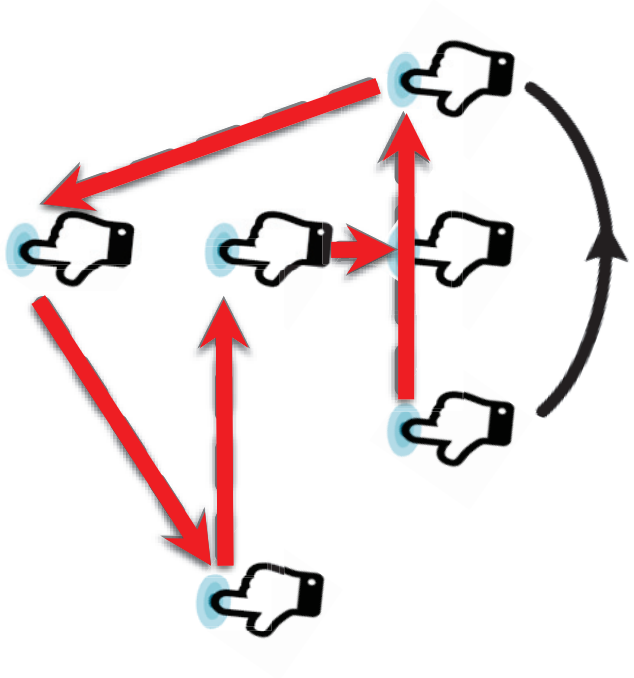


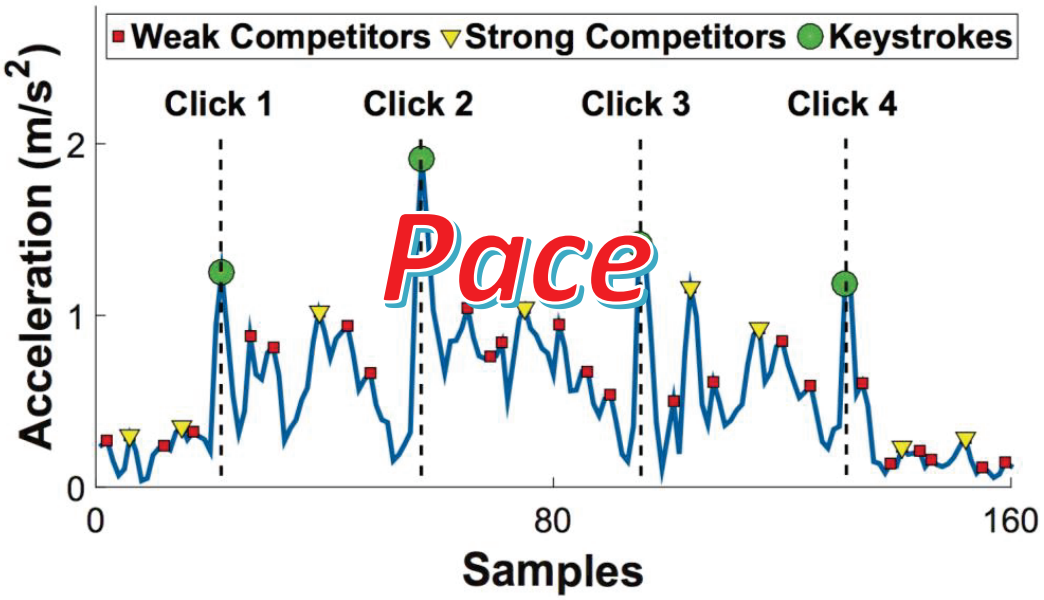
Correct result: 31970

Wrong result: 12780

System Design

Motion recovery: segmentation

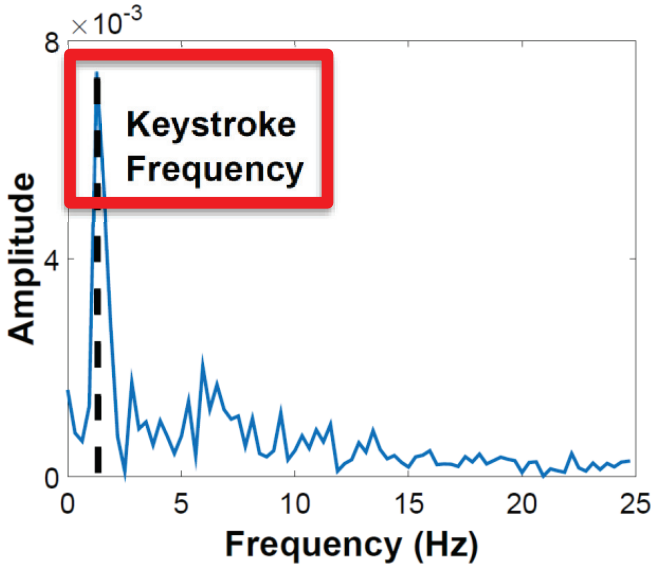




Motion data

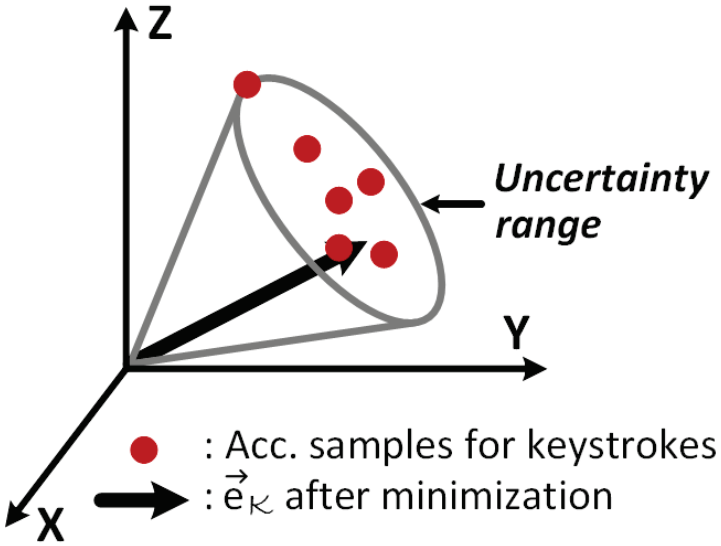
Segment

Displacement vectors



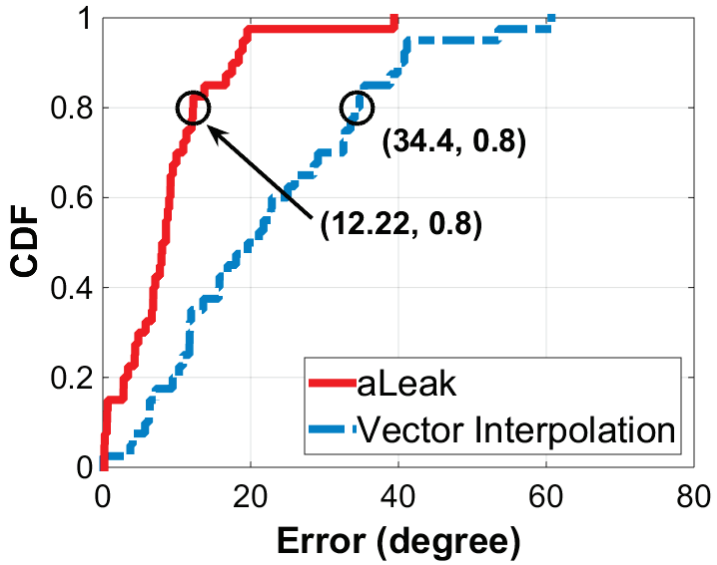
$$t_{pace} = 1/f_{type}$$

Motion recovery: plane reconstruction



Keystroke is perpendicular to the keypad plane

$$max_{\vec{e}_K \in cone} \sum_l ||g(s_j, \vec{e}_K)||_2$$



No error accumulation

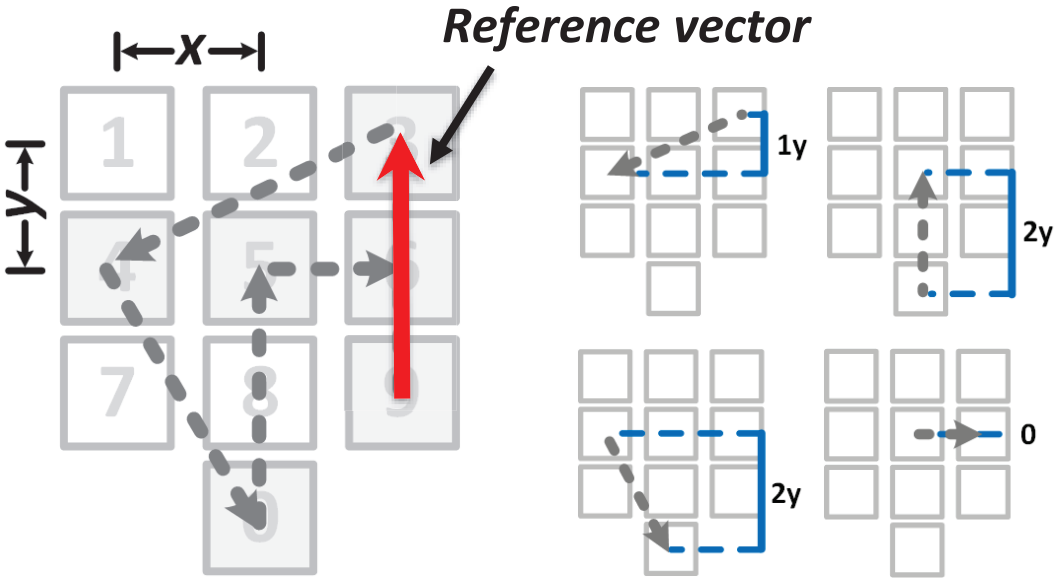
Now

Derived keypad plane

Moving trajectory on the plane

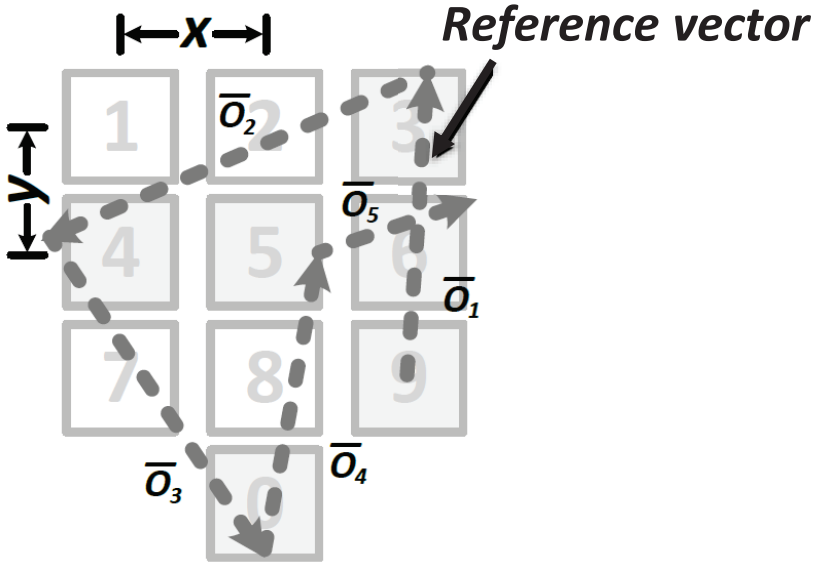
CityU
香港城市大學
City University of Hong Kong

Keyboard size derivation



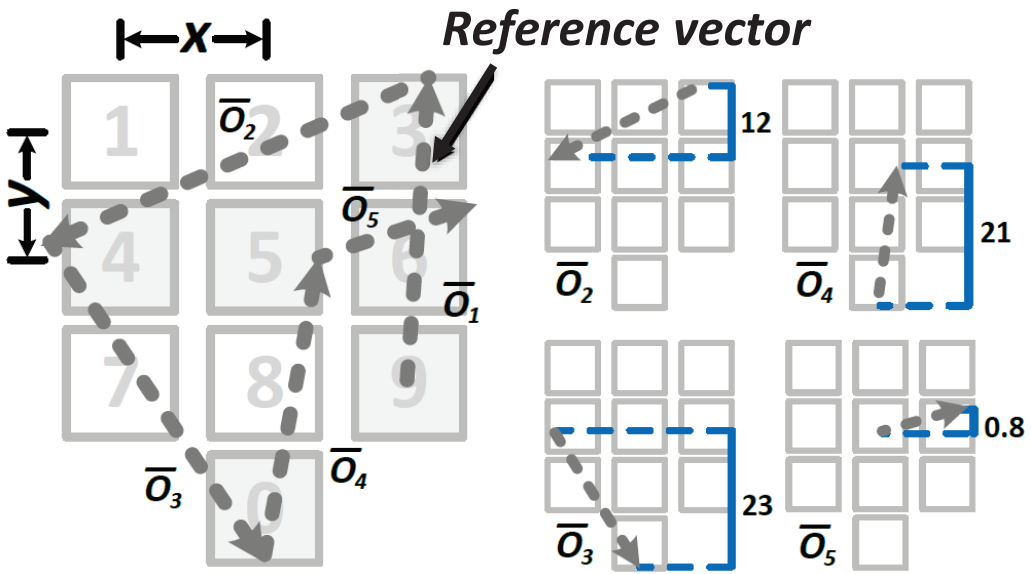
Key observation:

Integral multiples of x and y



Errors in trajectory

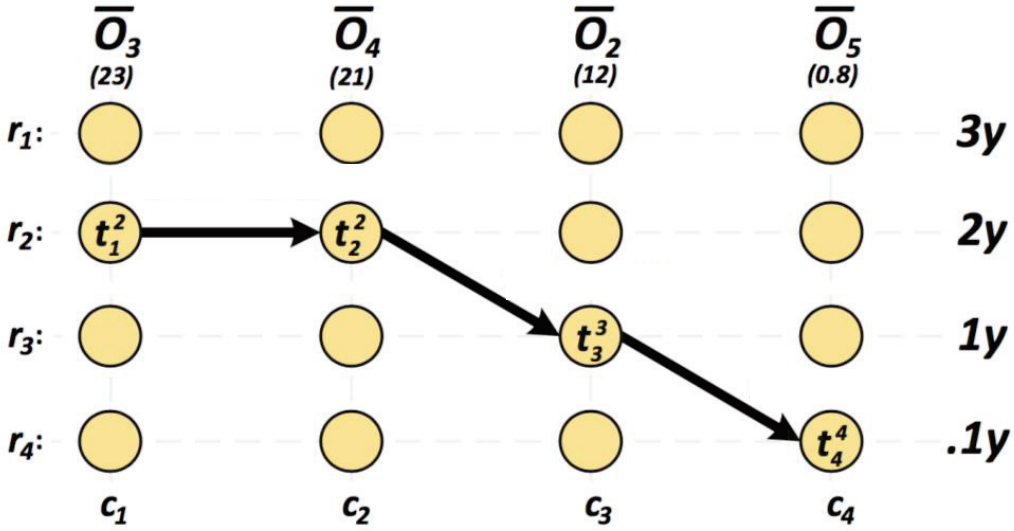
Keyboard size derivation



Our solution:

Projected lengths ➡ **constraints**

Search with a best match

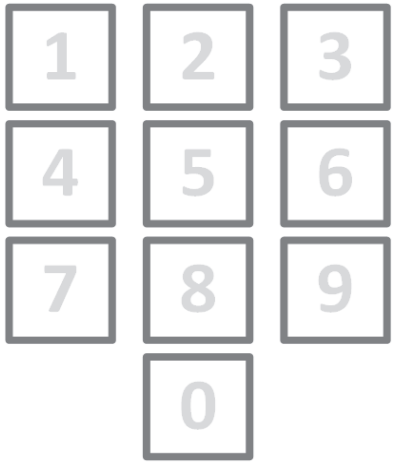


$$w(t_j^i, t_{j+1}^{i'}) = \left| \frac{len(c_{j+1})}{len(c_j)} - \frac{len(r_{i'})}{len(r_i)} \right|$$

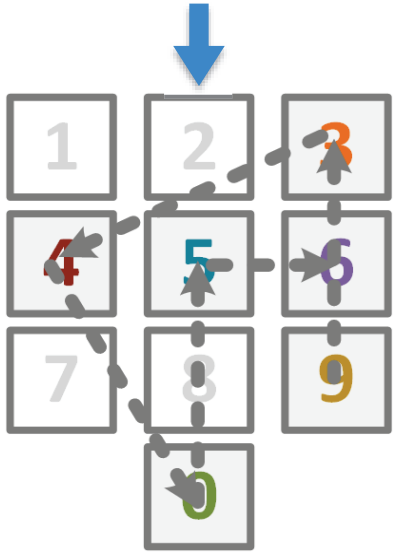
$$0.09 = \left| \frac{21}{23} - \frac{2y}{2y} \right|$$

Typed information inference

Moving trajectory



Keyboard



Inference result

- **Position of reference vector**
- **Computation overload reduction**
- **Handling “enter” cases**

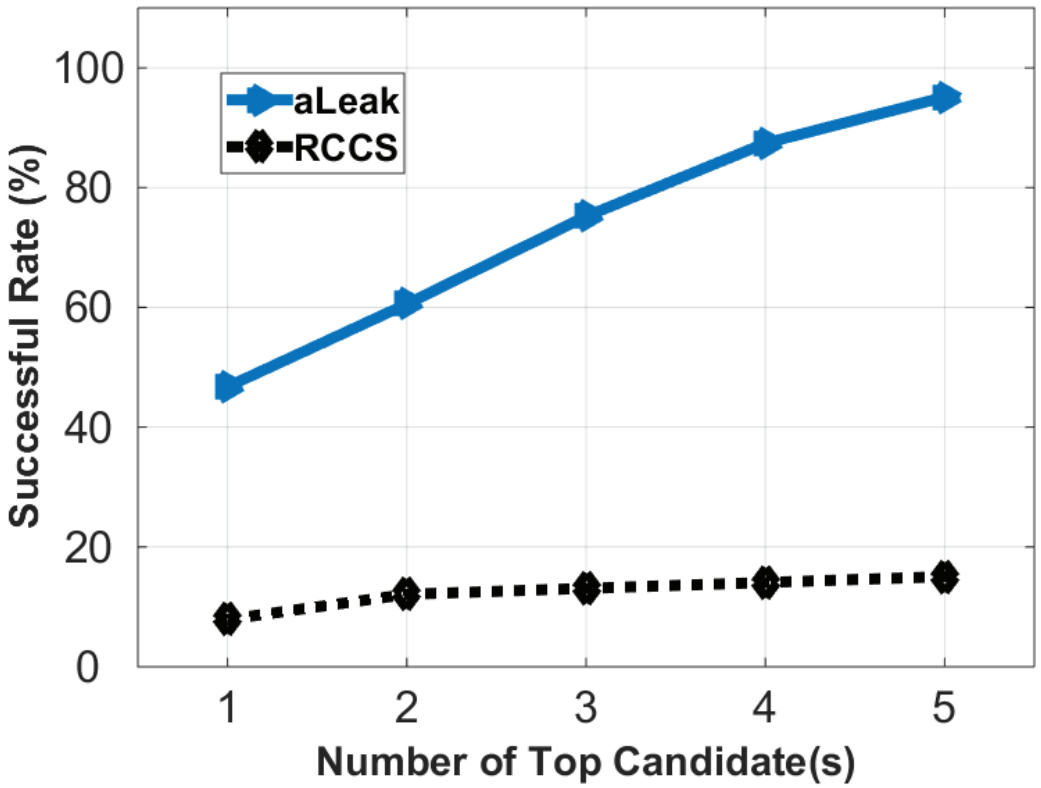
Evaluation

Experiments setup

- **LG W150**
- **4 common types of keyboards**
- **More than 300 rounds with 5 users**
- **Compared with [ASIA CCS'16]**

Evaluation results

- **Overall Performance**



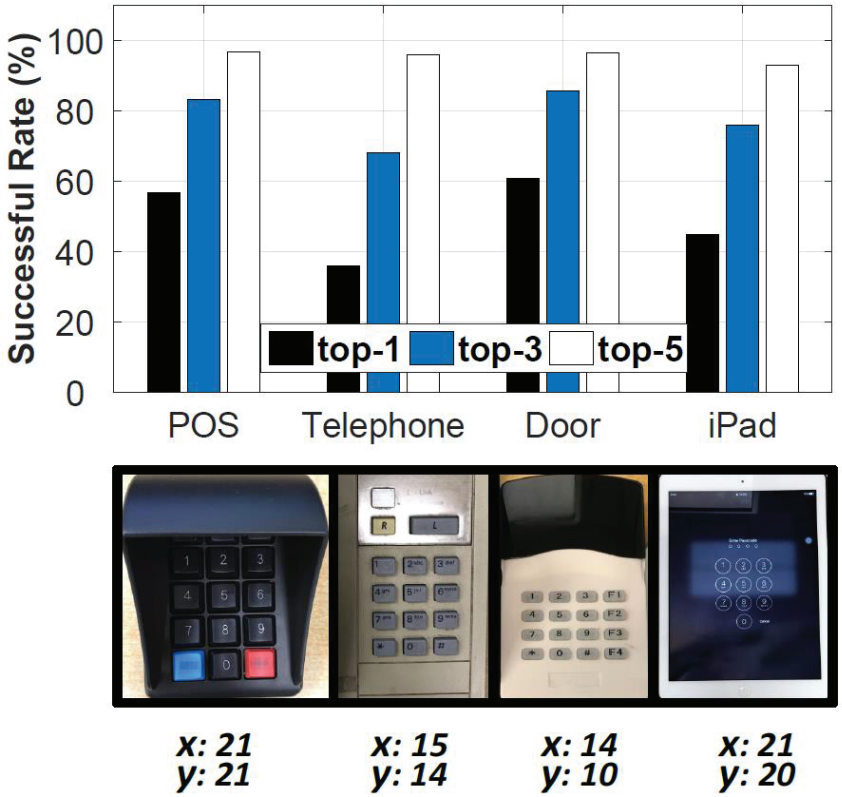
Keypad posture: 0 ~ 90°

top-1: 45%

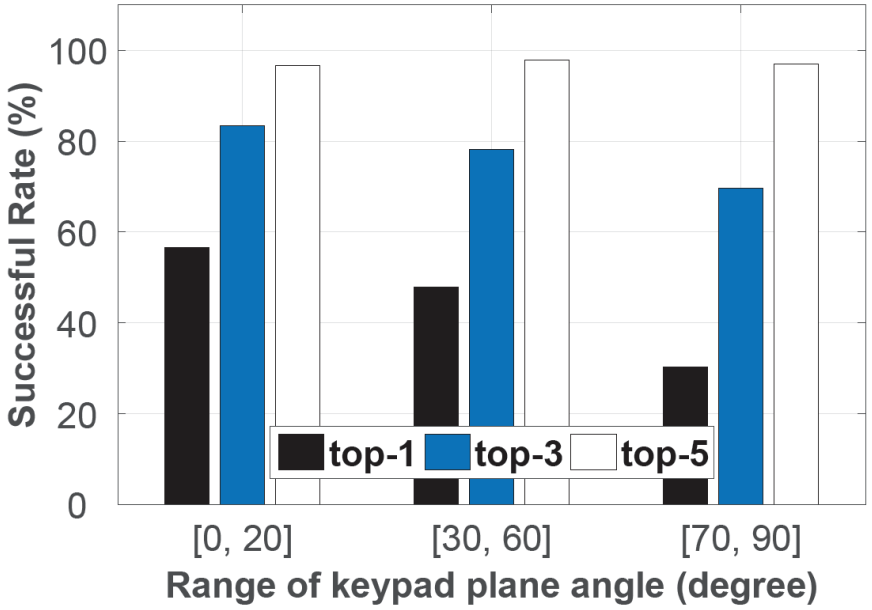
top-5: 94%

Evaluation results

- **Different keyboards**



- **Different keypad postures**

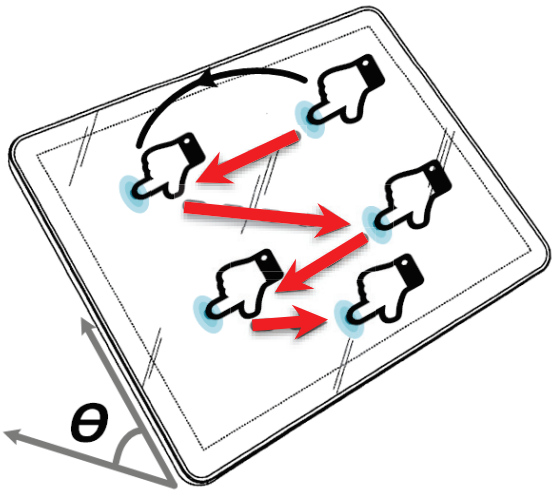


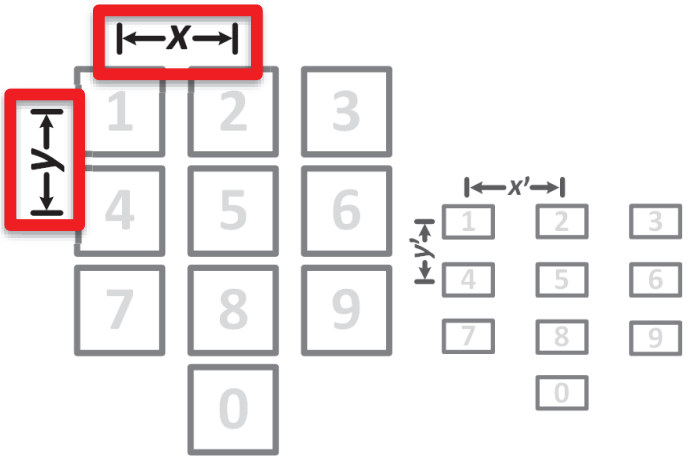
Conclusion 1,2,3

1. **Side-channel attack is possible in context-free scenarios**

2. **Challenges**
   - **2.1 Inaccurate motion recovery**
   - **2.2 Unknown keyboard size**

3. **Techniques**





CityU
香港城市大學
City University of Hong Kong

Q&A

aLeak: Privacy Leakage through Context-Free Wearable Side-Channel

Yang Liu, Zhenjiang Li

Department of Computer Science

City University of Hong Kong