SlidePIN: Slide-based PIN Entry Mechanism on a Smartphone

Huiping Sun,

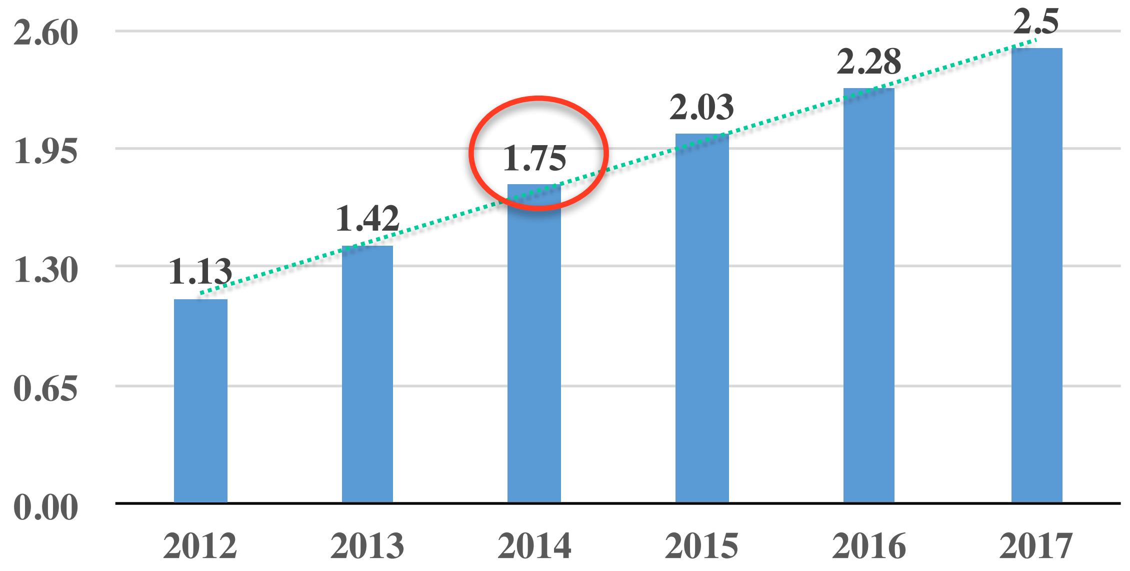
Shuaiying Guo, Ke Wang, Nan Qin, Zhong Chen

School of Software & Microelectronics

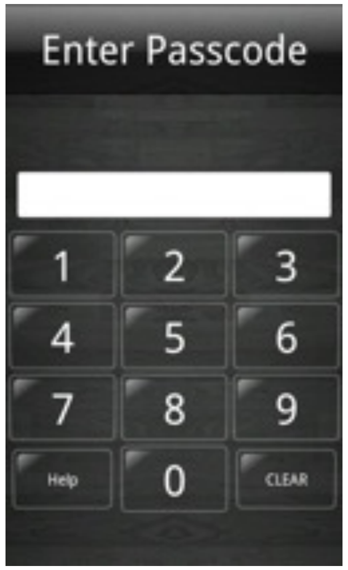
Peking University, Beijing, China

Background

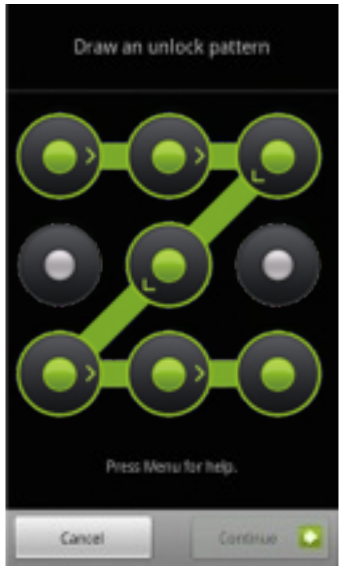
www.eMarketer.com



4 digits PIN



PatternLock



No

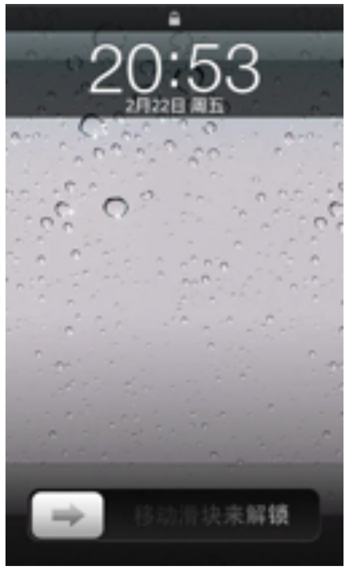


Photo Audio Video
SMS Call Email
Payment Location
SNS Blog IM
… …

Shoulder surfing attack

http://www.mireview.com/blog/wp-content/uploads/2013/03/timthumb.jpg

Existing Solutions

Computing burden

Memory burden

Indirect Entry Mechanism

Human-computable challenge-response

Challenge

Keypad layout

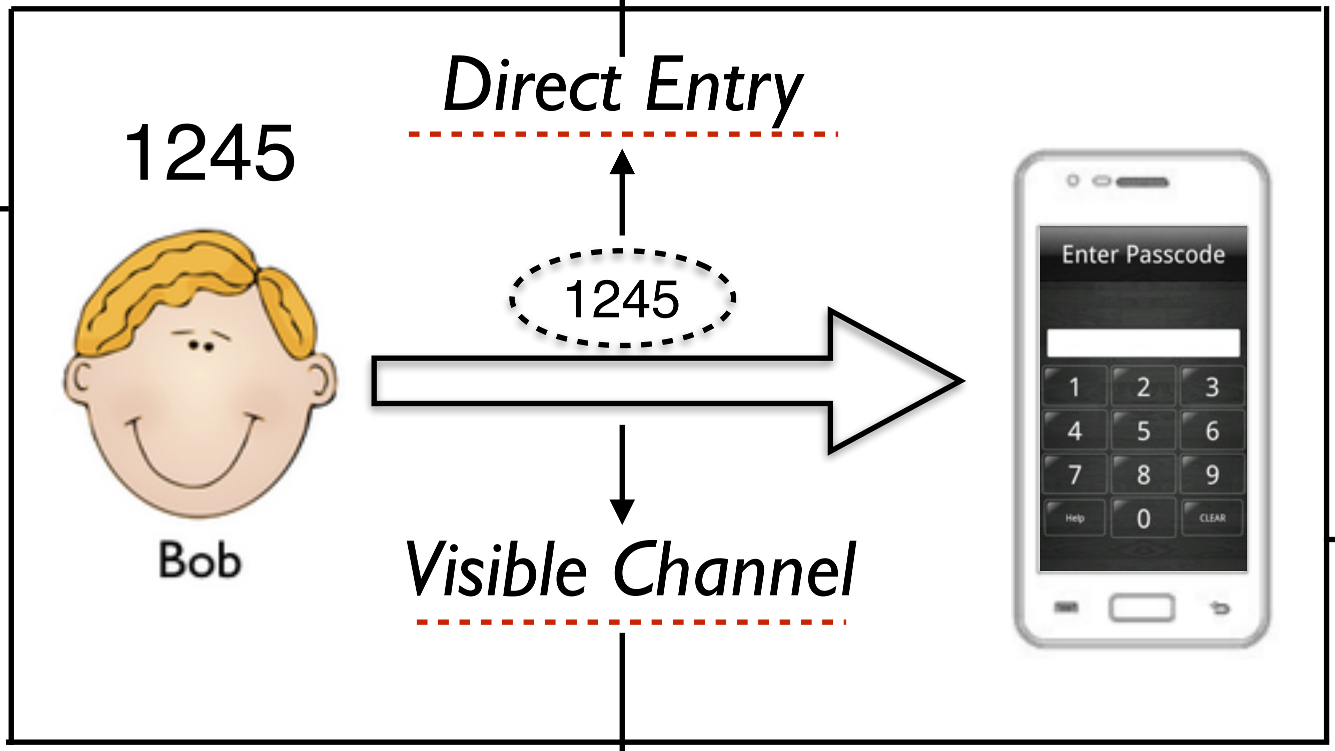
Additional factors

☆ *Colors*

☆ *Symbols*

☆ *Directions*

… …



… …

☆ *Physical block*

☆ *Eye tracking*

☆ *Tactile sensor*

☆ *Pressure sensor*

☆ *Vibration sensor*

☆ *Back-of-Device interface*

Special human-computer Interface

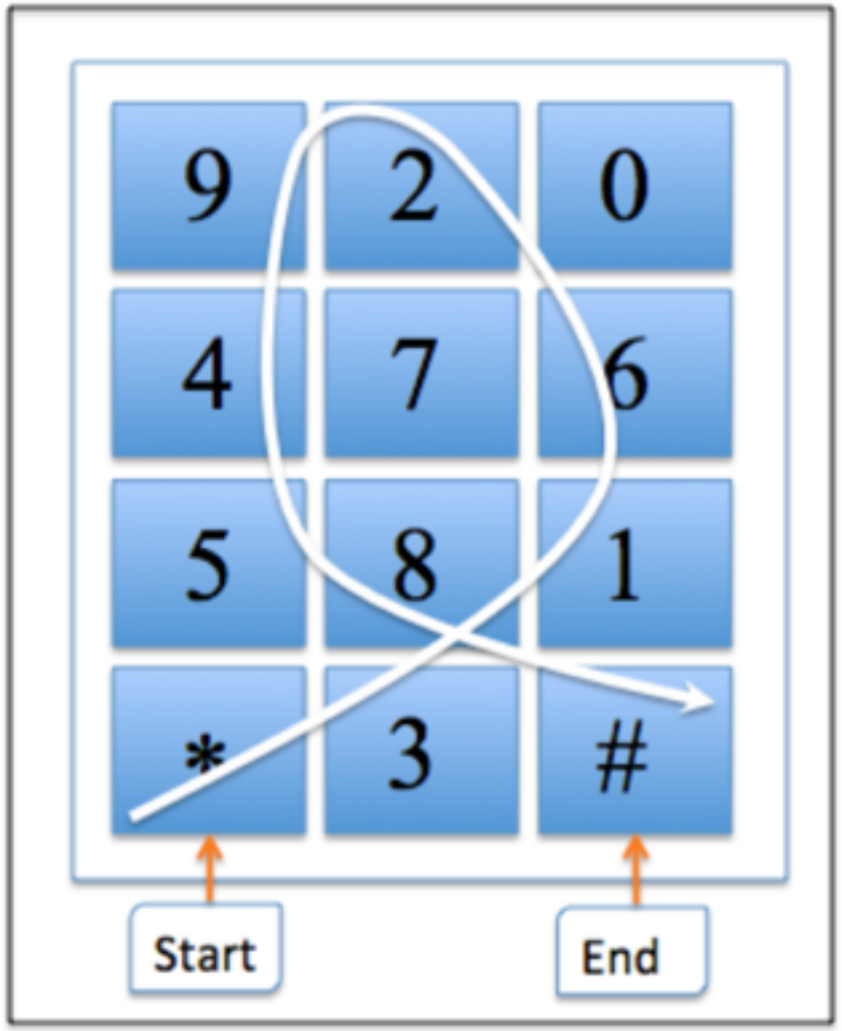
Invisible Entry Mechanism

Hardware support

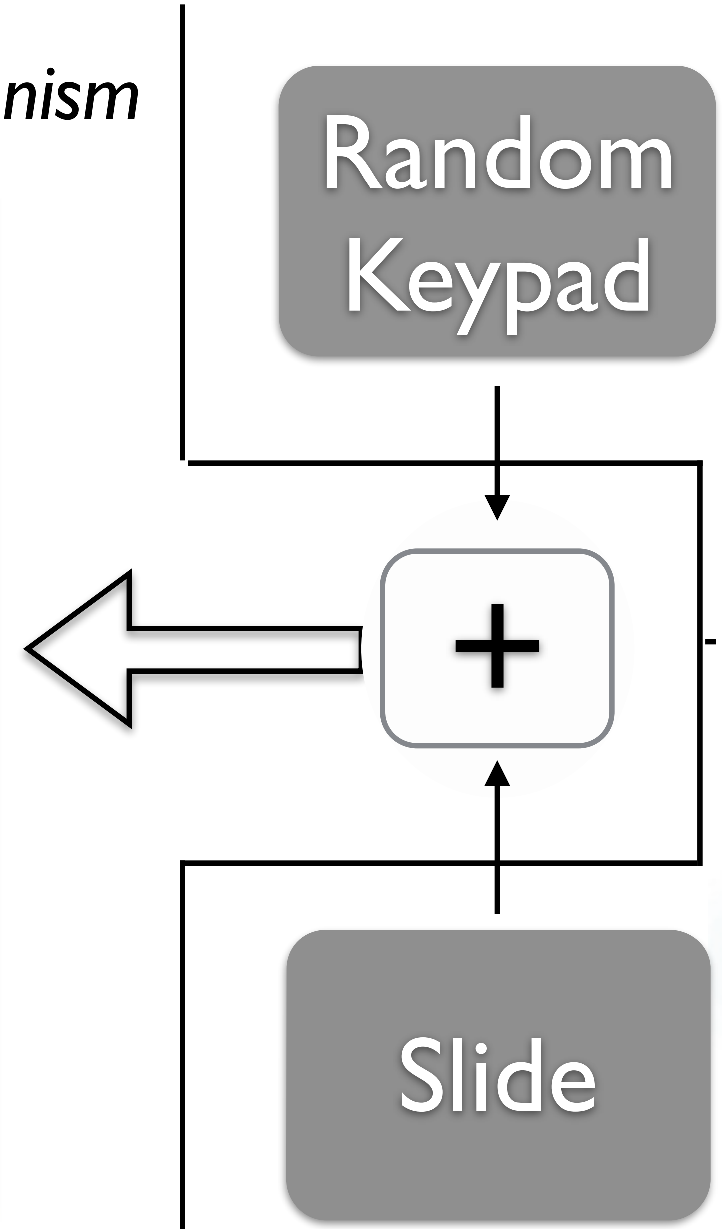
Deployment costs

SlidePIN Concepts

Slide-based PIN Entry Mechanism



PIN	1245
SlidePIN	*381629458#



Input with random numeric keypad is more secure

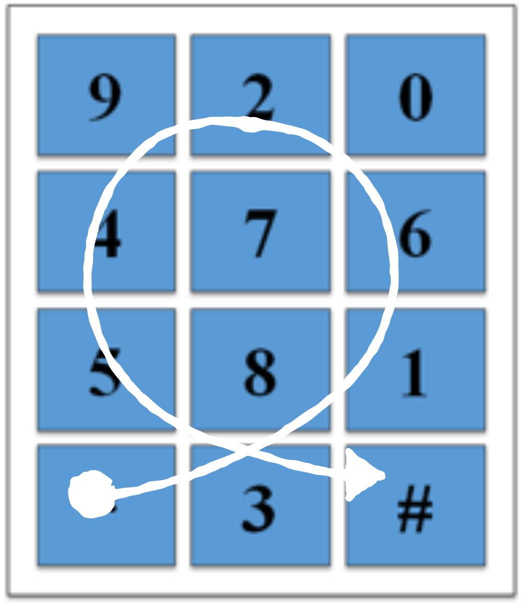
Word-Gesture Keyboard

Slide input is faster

Slide input is more secure

Model Design

PIN: 1245

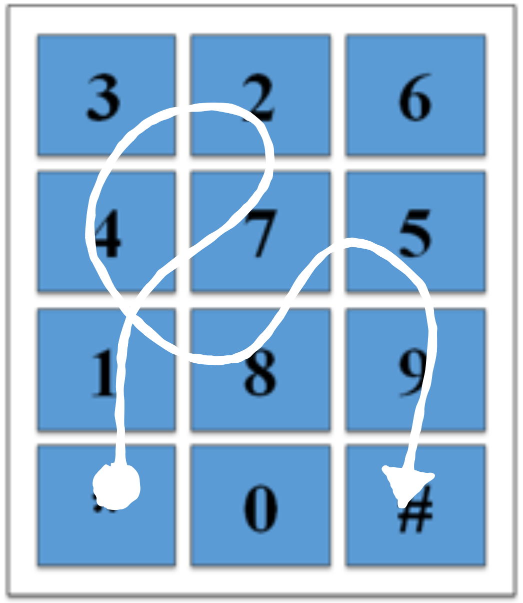


Layout 1

Trajectory 1

Sequence 1

*381629458#



Layout 2

Trajectory 2

Sequence 2

*1472341859#

Slide Map Function

$F\ (\ PIN, Layout\ ) \rightarrow Sequence$

Attack Function

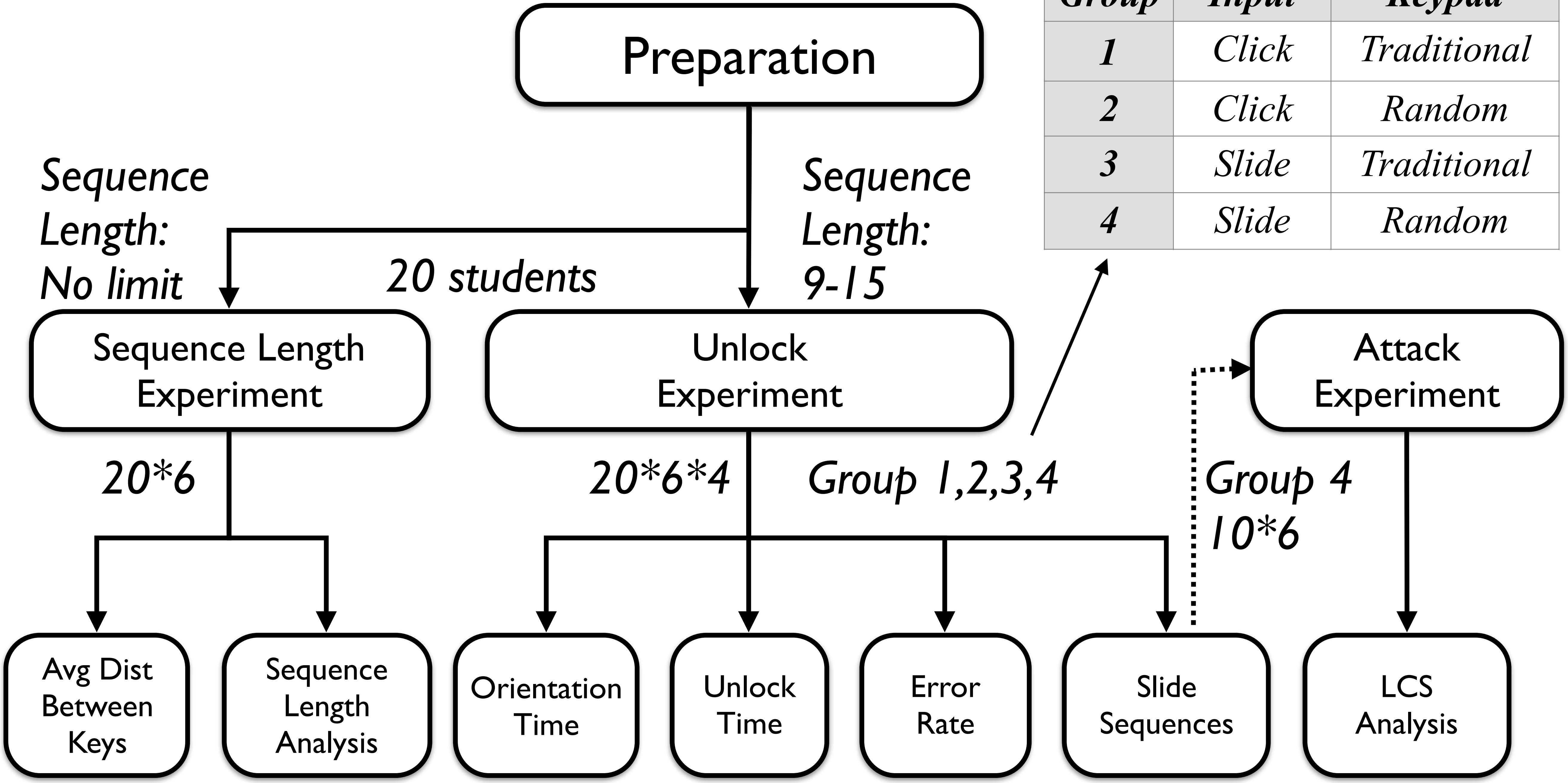
One-Time

$F^{-1}(\ Sequence\ 1\ ) \rightarrow PIN$

Multi-Time

$F^{-1}(\ Sequence\ 1,\ Sequence\ 2,\ \ldots\ \ldots\ Sequence\ n) \rightarrow PIN$

Experiment Design



Preparation

Sequence Length: No limit

20 students

Sequence Length: 9-15

Sequence Length Experiment

Unlock Experiment

Attack Experiment

*20*6*

*20*6*4*

Group 1,2,3,4

Group 4
*10*6*

Avg Dist Between Keys

Sequence Length Analysis

Orientation Time

Unlock Time

Error Rate

Slide Sequences

LCS Analysis

Group	***Input***	***Keypad***
1	*Click*	*Traditional*
2	*Click*	*Random*
3	*Slide*	*Traditional*
4	*Slide*	*Random*

Sequence Length Analysis

Too long

* 0123456789 0123456789 0123456789 0123456789 #

Why

*3816279450#

*381629450#

Too short

*31629450#

How

20 students
** 6 times*

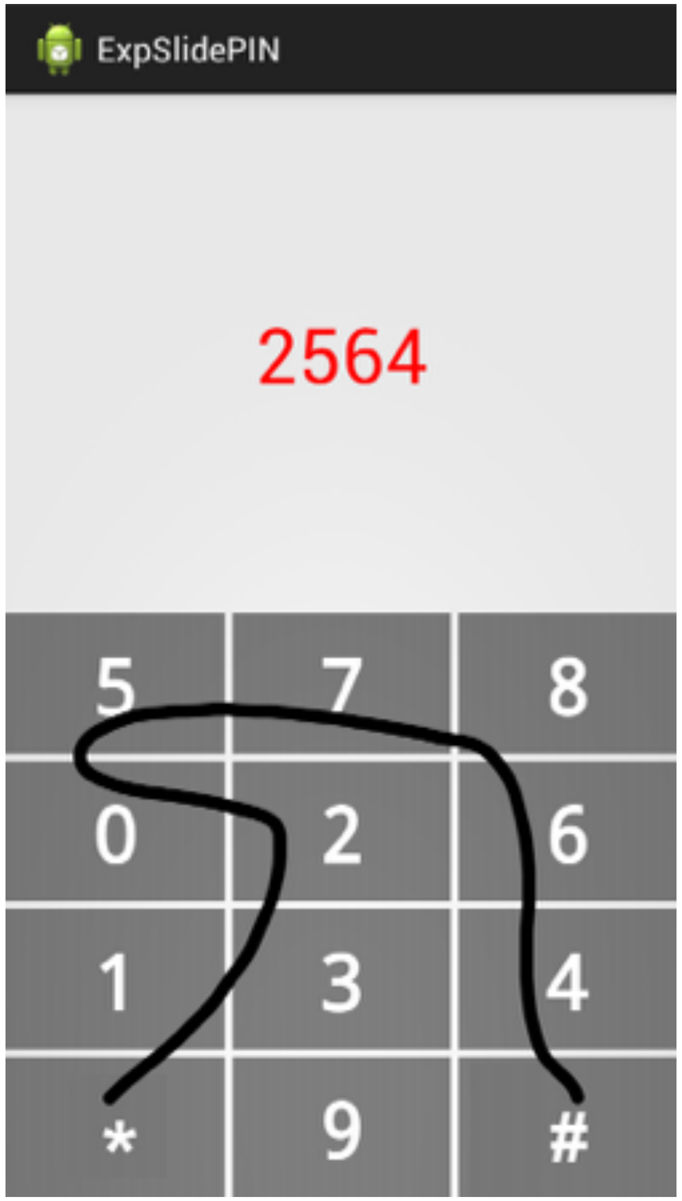
A	B	A
C	D	C
C	D	C
A	B	A

(a)

A	1.03	2.24
1.11	2.08	3.03
2.25	2.84	4.00
3.33	3.83	4.88

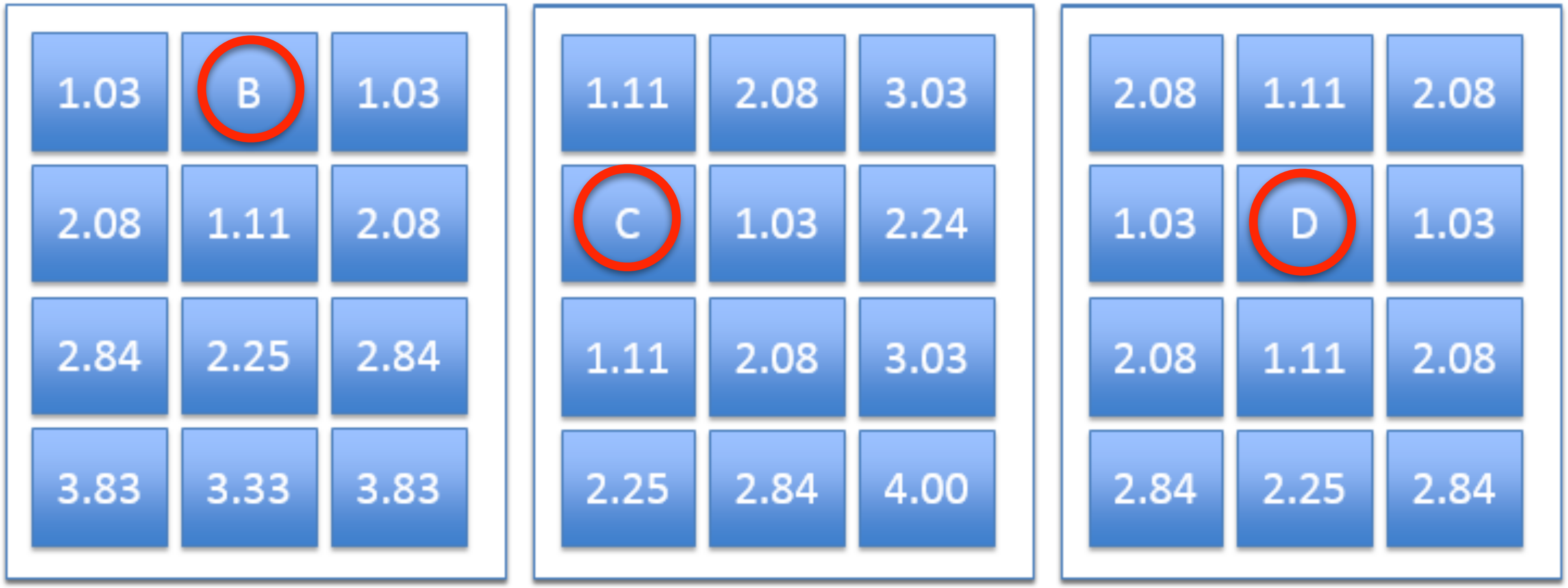
(b)

Estimate of Distance between Keys



$$D(A)=(1.03+2.24+1.11+2.08+3.03+2.25+2.84+4.00+3.33+3.83+4.88)\ /11 \approx 2.78$$

Sequence Length Analysis



1.03	B	1.03
2.08	1.11	2.08
2.84	2.25	2.84
3.83	3.33	3.83

(a)

1.11	2.08	3.03
C	1.03	2.24
1.11	2.08	3.03
2.25	2.84	4.00

(b)

2.08	1.11	2.08
1.03	D	1.03
2.08	1.11	2.08
2.84	2.25	2.84

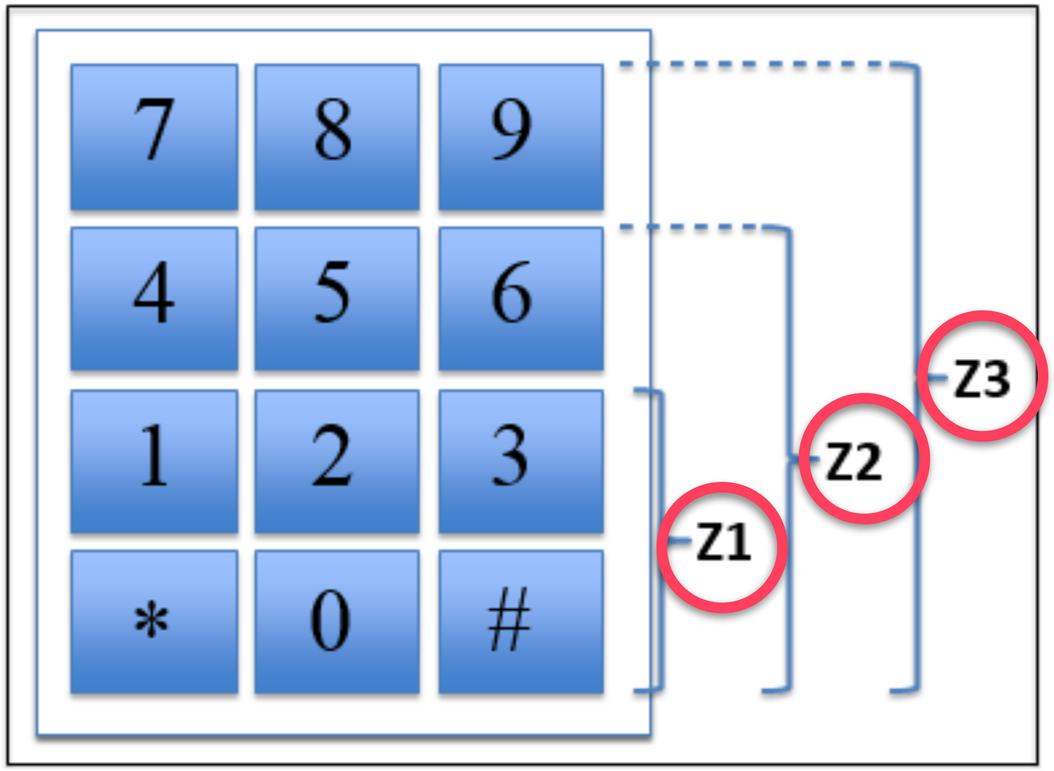
(c)

$D(B) = 2.38$

$D(C) = 2.25$

$D(D) = 1.87$

$Davg = (D(A)*2+D(B)*2) +D(C)*4+D(D)*2) / 10 \approx 2.31$



$P(Z3) = 1$ $D(Z3) = \boxed{11.55}$

$P(Z2) = 1/6$ $D(Z2) = 10.82$

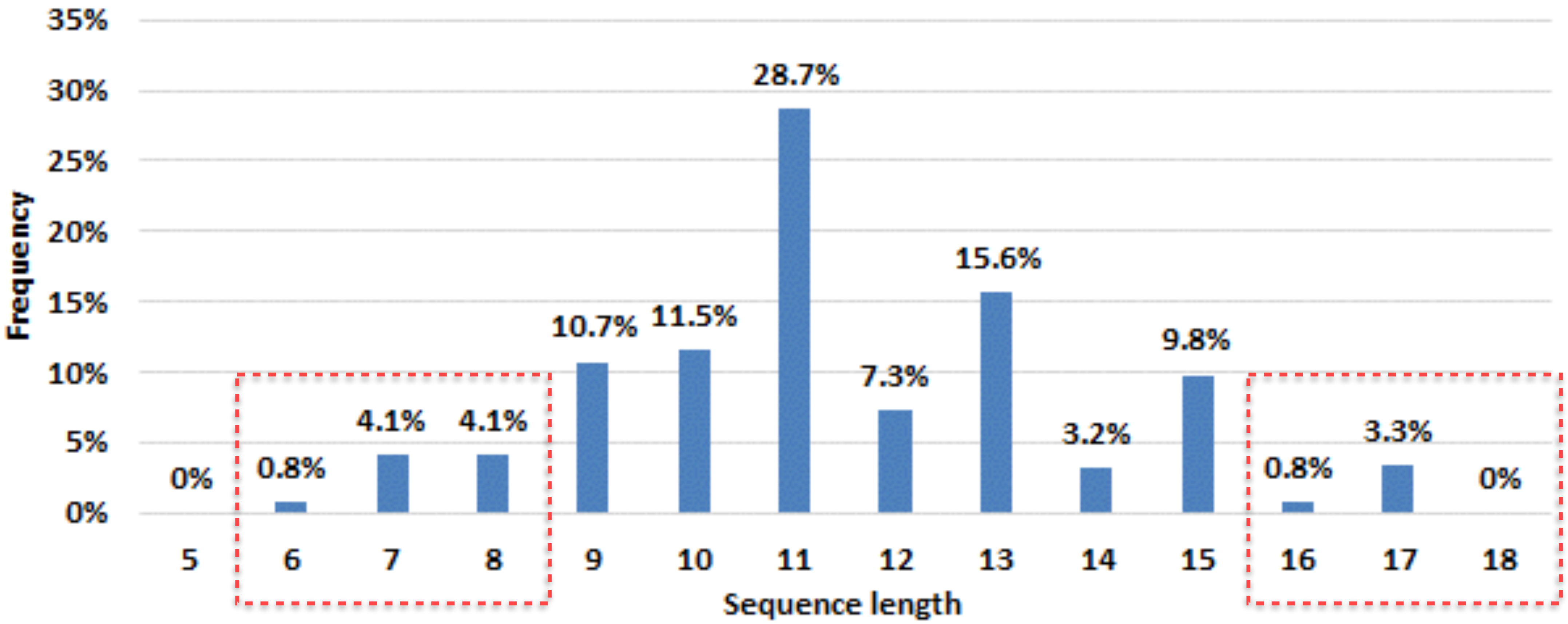
$P(Z1) = 1/200$ $D(Z1) = \boxed{8.08}$

$8.08 * 1.87 \approx \boxed{15.11}$

9 - 15

Sequence Length Analysis

- *Estimate of Sequence Length*
  - ✳ *Mean value of sequence length: 11.55 vs 11.46*
  - ✳ *Lower threshold of sequence length: 9*
  - ✳ *Upper threshold of sequence length: 15*



Security Analysis

- *Shoulder surfing attack*

One-Time

Sequence Length	*9*	*10*	*11*	*12*	*13*	*14*	*15*
PIN	*126*	*210*	*330*	*495*	*715*	*1001*	*1365*

Multi-Time

Times	*u1*	*u2*	*u3*	*u4*	*u5*	*u6*	*u7*	*u8*	*u9*	*u10*
2	*6*	*6*	*6*	*6*	*7*	*6*	*6*	*7*	*6*	*4*
3	*5*	*5*	*4*	*4*	*4*	*4*	*4*	*5*	*4*	
4	*4*	*4*						*4*		

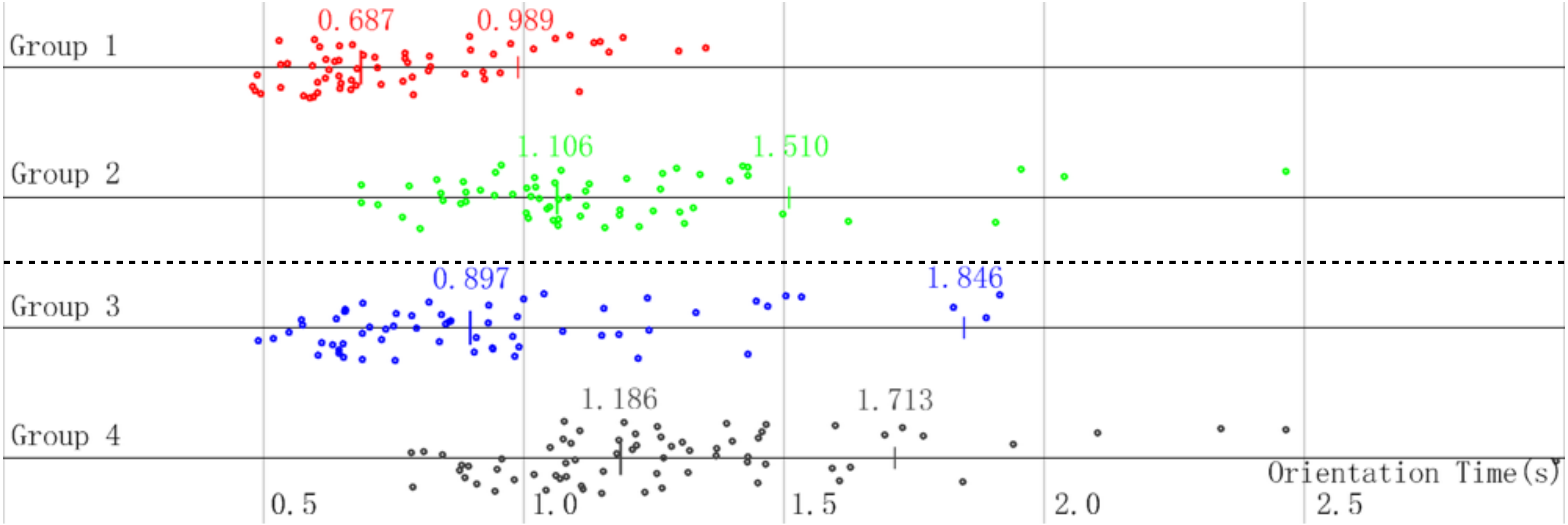
- *Guessing attack*
  - ✳ *Brute force attack*
  - ✳ *Dictionary attack*

- *Replay attack*
  - ✳ *Random numeric keypad*

Usability Analysis

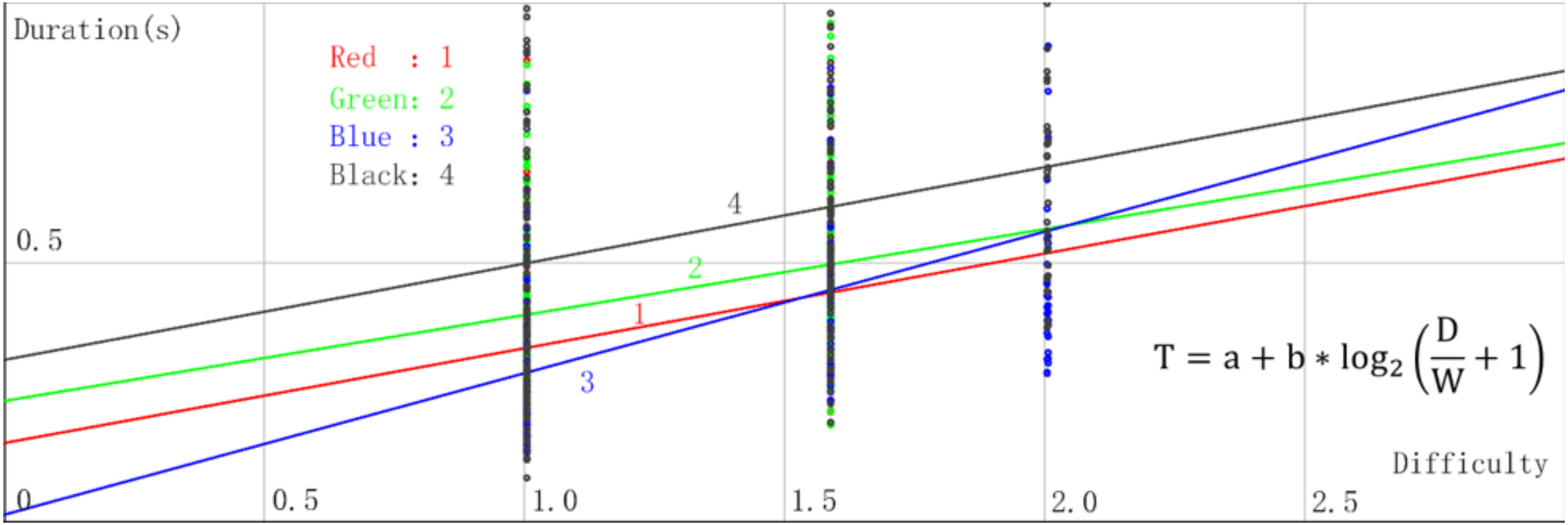
- *Orientation time*

Groups	*Average*	*Standard Deviation*	*Threshold Value*
1	*0.687*	*0.133*	*0.989*
2	*1.064*	*0.199*	*1.510*
3	*0.798*	*0.293*	*1.846*
4	*1.186*	*0.225*	*1.713*



Usability Analysis

- *Unlock time*
  - ✳ *Sliding is faster*
  - ✳ *Input sequence become longer*
  - ✳ *Random number keypad increases unlock time*



$$T = a + b * \log_2\left(\frac{D}{W} + 1\right)$$

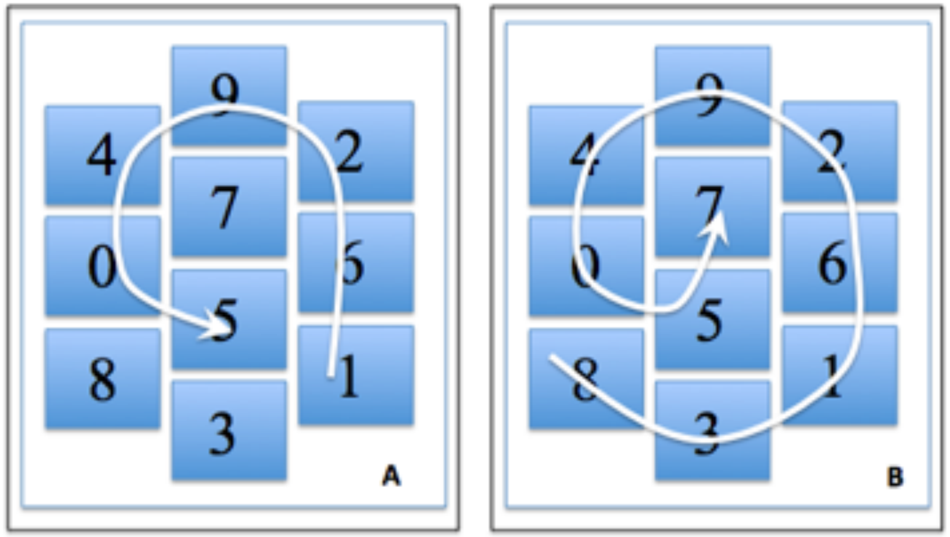
Usability Analysis

- Error rate
  - ✳ *Sequence length limit*
  - ✳ *Start point and end point*
  - ✳ *No familiar enough*

Groups	*Error Rate*
1	*1.67%*
2	*3.33%*
3	*7.69%*
4	*13.04%*

- Cost of learning
  - ✳ *SlidePIN is build based on 4-digits PIN*
  - ✳ *SlidePIN is easy to use*
  - ✳ *SlidePIN is interesting to use*

Discussion

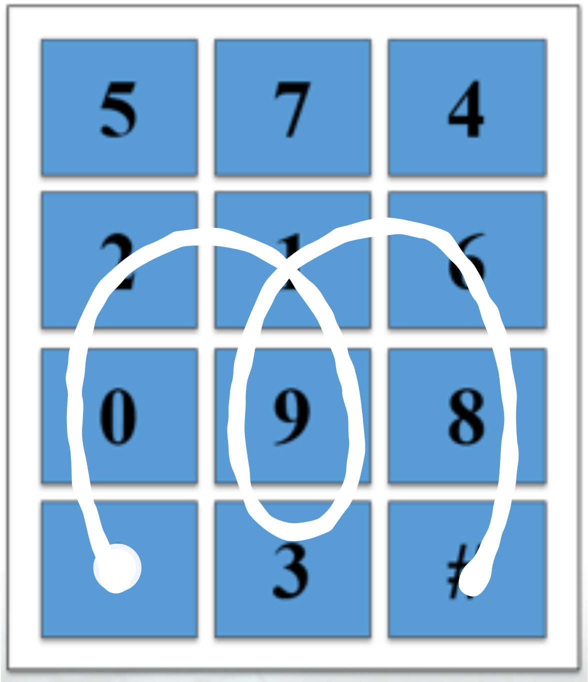


PIN: 1245

1: Fixed start point and end point

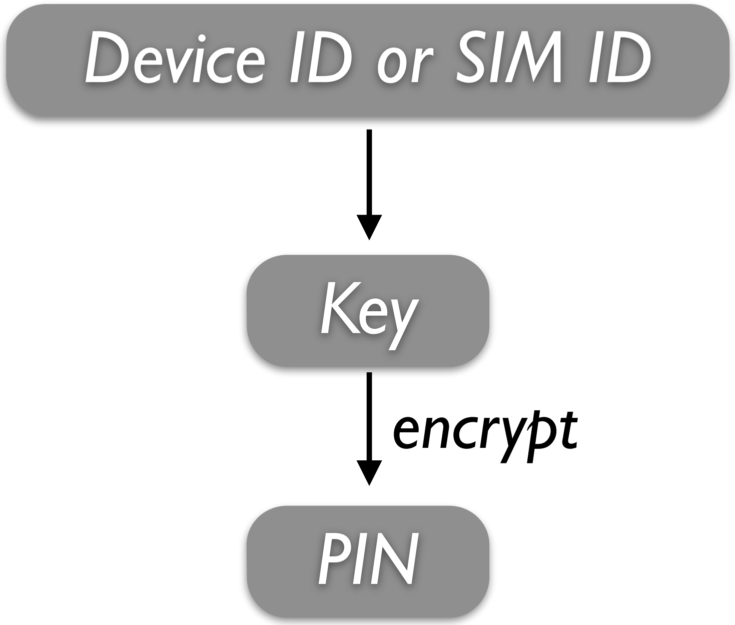
PIN: 2118

*021939168#



2: Same adjacent Digits

3: PIN storage


Device ID or SIM ID

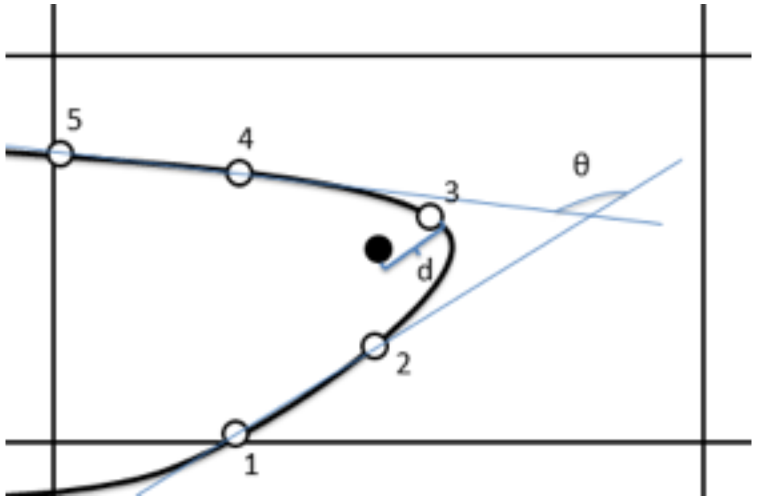
Key

encrypt

PIN

4: Smudge attack

5: Attack based on Features



Conclusion

- *SlidePIN performs better than 4-digits PIN against shoulder surfing attack.*
- *At the same time, SlidePIN has acceptable usability.*