口令

北京大学 软件与微电子学院
School of Software and Microelectronics, Peking University

Huiping Sun(孙惠平)
sunhp@ss.pku.edu.cn

Password

Human Computation回顾

1 概念	2 算法	3 例子	4 CAPTCHA
• 计算历史 • 定义 • 相关概念 • 人工智能	• 算法描述 • 算法组成 • 算法正确性 • 参与动机	• ESP • Citizen科学 • Amazon Turk • 众包	• 定义和历史 • 文本类型 • 技术和攻击 • 其余类型

Why Information Is Hard

- Abstract
- Introduction
- Network Externalities
- Competitive Applications and Corporate Warfare
- Information Warfare - Offense and Defense
- Distinguishing Good from Bad
- Conclusions

ATM DDOS

Microsoft Philosophy

Passport

Bug TPM

Common Criteria

Network Externalities

Asymmetric Information

Moral Hazard

Adverse Selection

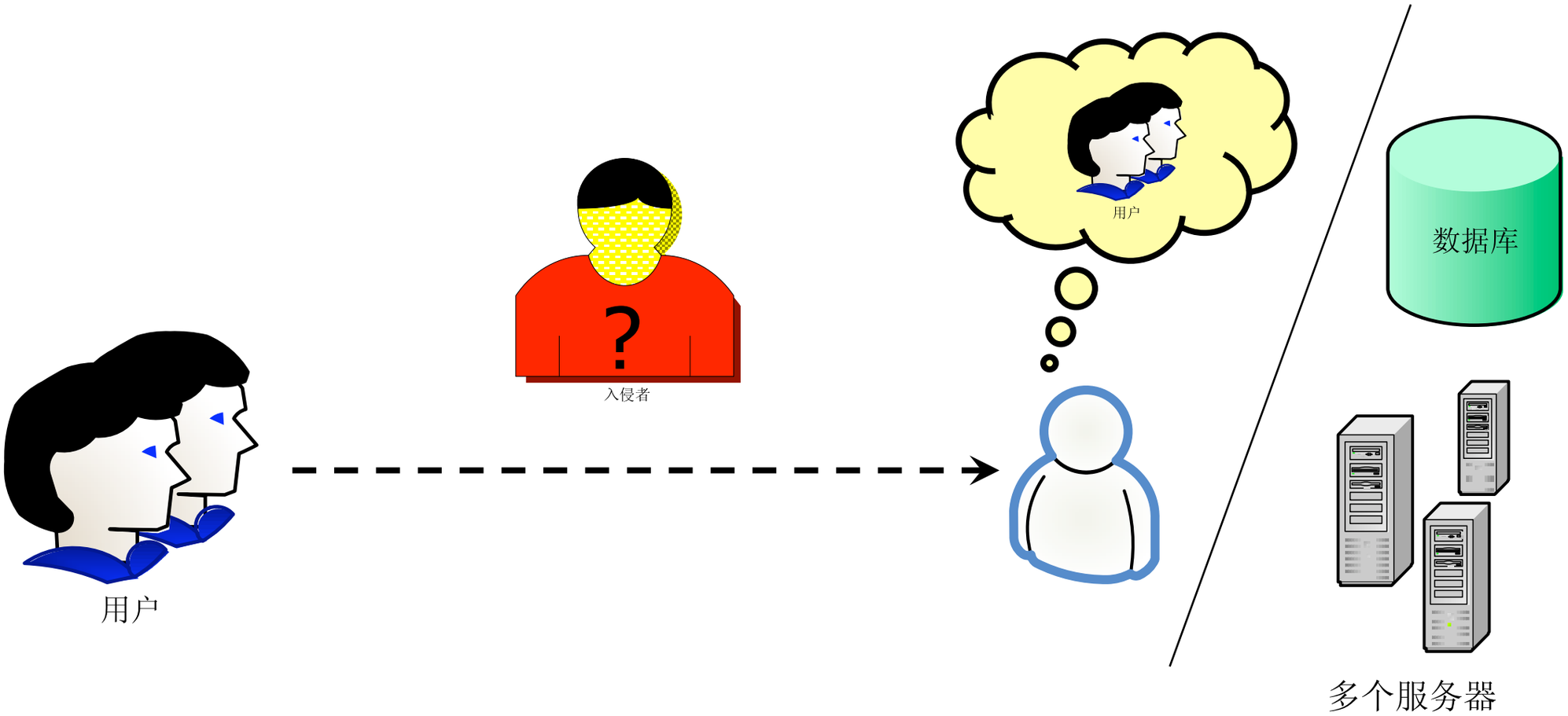
Liability Dumping

Tragedy of the Commons

身份认证

Password

身份认证



身份认证因子

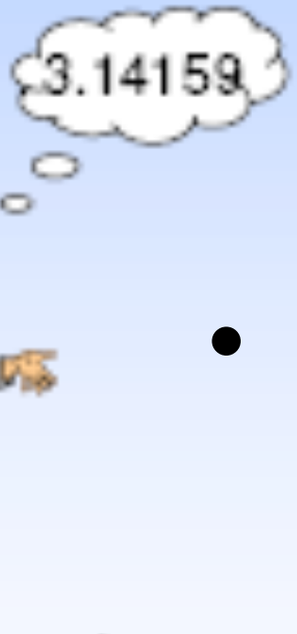
Security Level

- Something you have
  - OTP
  - Smart Card
  - USB Token
  - Mobile Phone

Something you have

- Something you are /can do
  - Fingerprint
  - Voice

Something you are



Something you know

- Something you know
  - Password
  - Image
  - Answer

Method

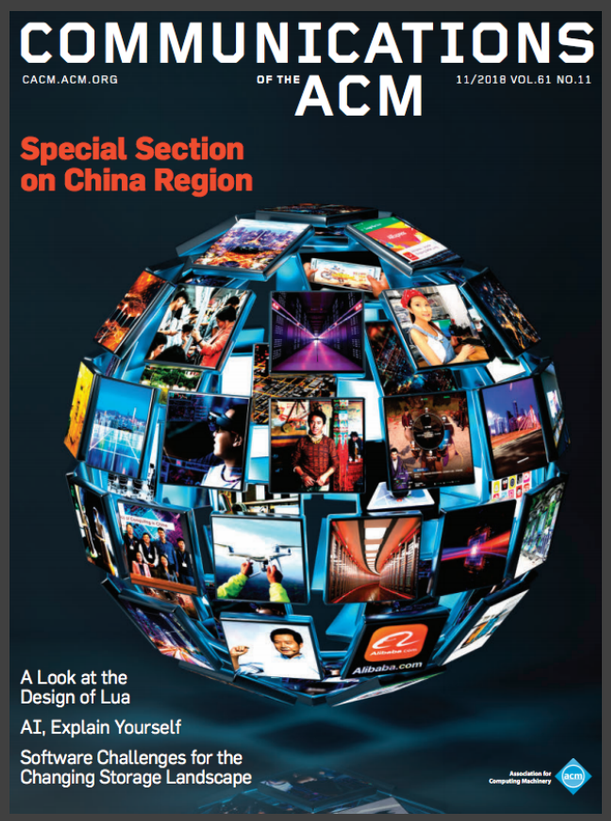
Password is Imperfect


Theory on passwords has lagged practice, where large providers use back-end smarts to survive with imperfect technology.

BY JOSEPH BONNEAU, CORMAC HERLEY, PAUL C. VAN OORSCHOT, AND FRANK STAJANO

Passwords and the Evolution of Imperfect Authentication

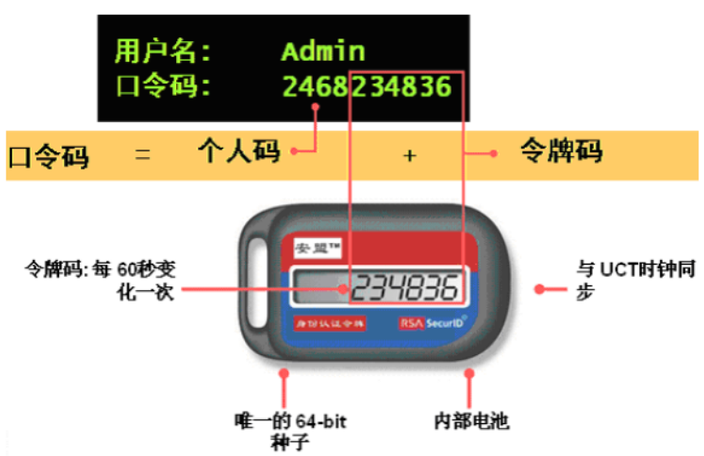
https://cacm.acm.org/



But ... ...

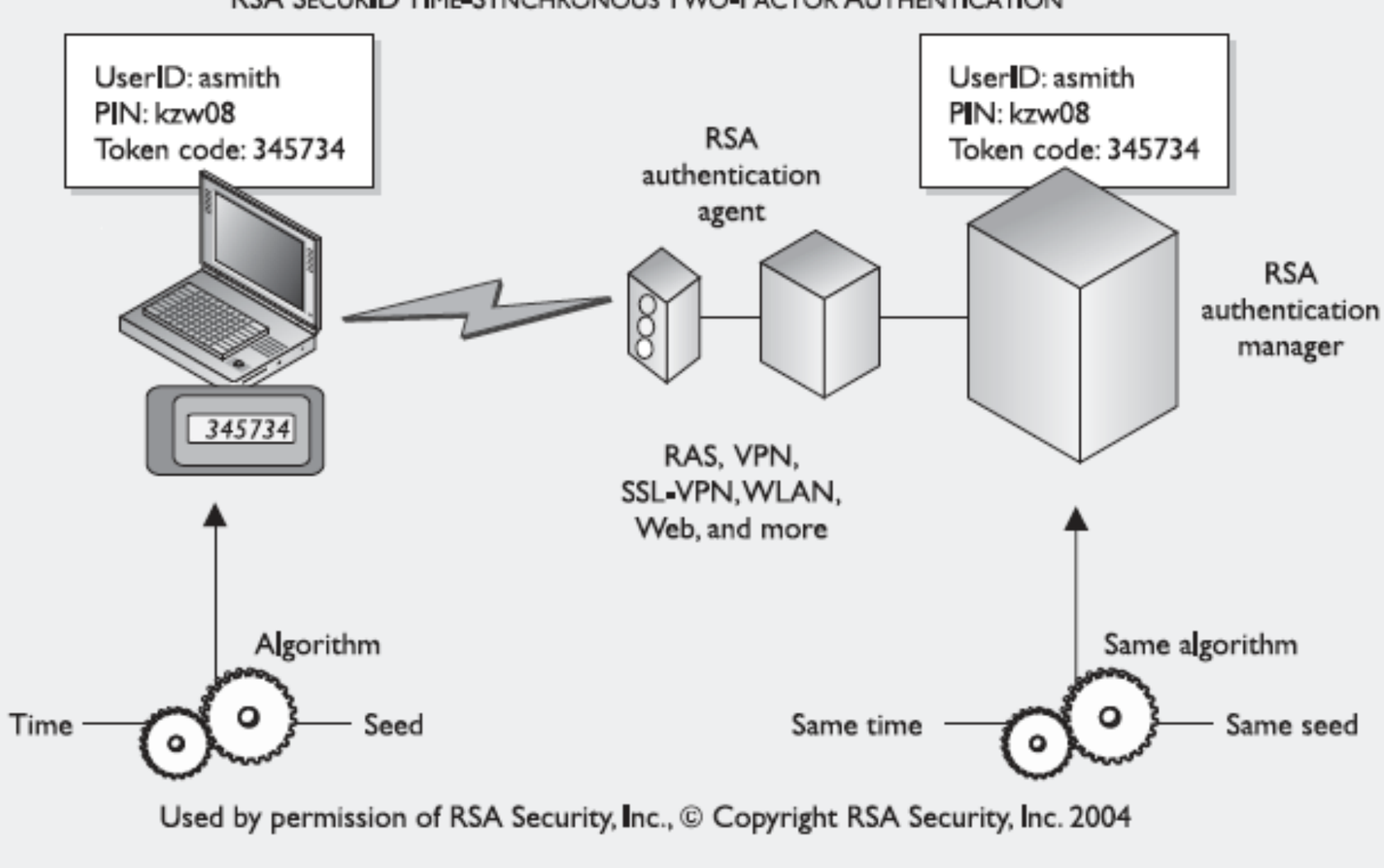
OTP: One Time Password

一次性(动态)口令。是由电子令牌(Token)等手持终端设备生成的，根据某种加密算法，产生的随某一个不断变化的参数(例如时间，事件等)不停地、没有重复变化的一种口令。



SecureID

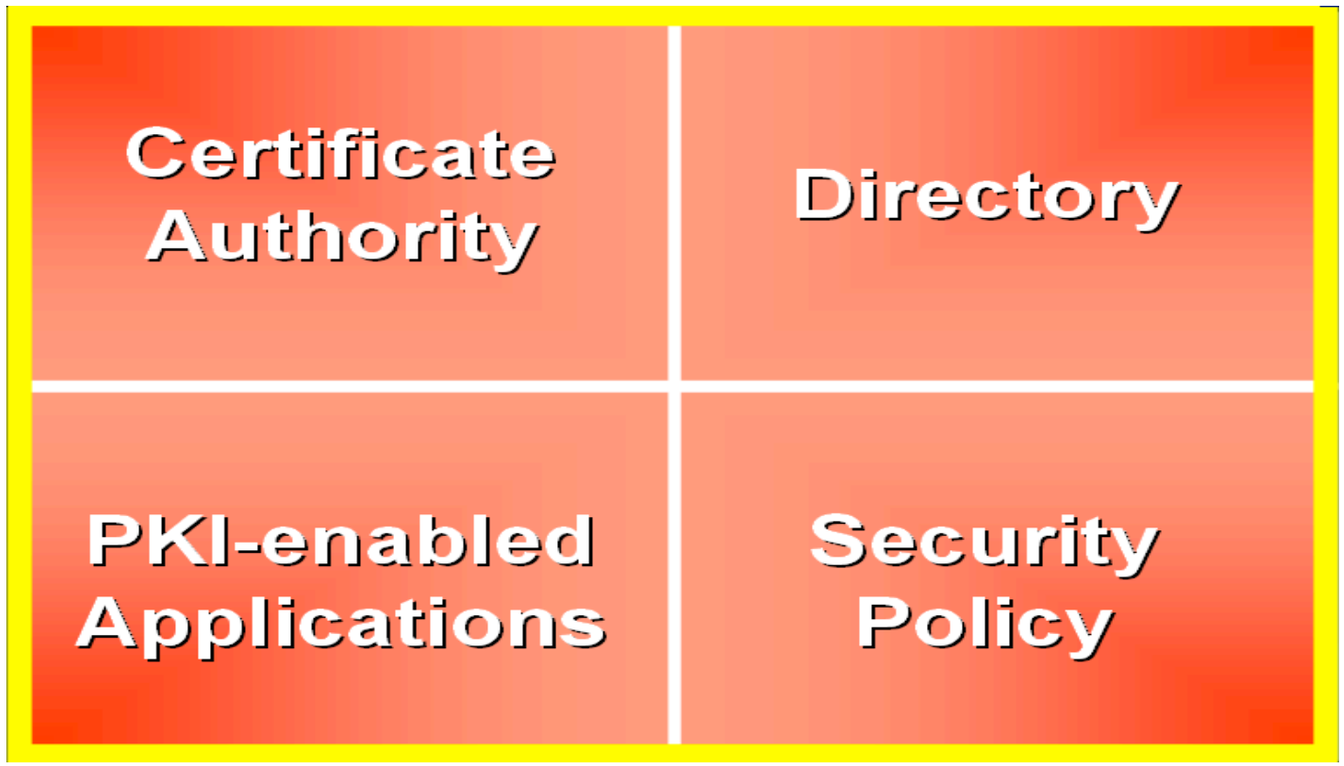
SecureID, from RSA Security, Inc., is one of the most widely used time-based tokens. One version of the product generates the one-time password by using a mathematical function on the time, date, and ID of the token card. Another version of the product requires a PIN to be entered into the token device.



PKC & PKI

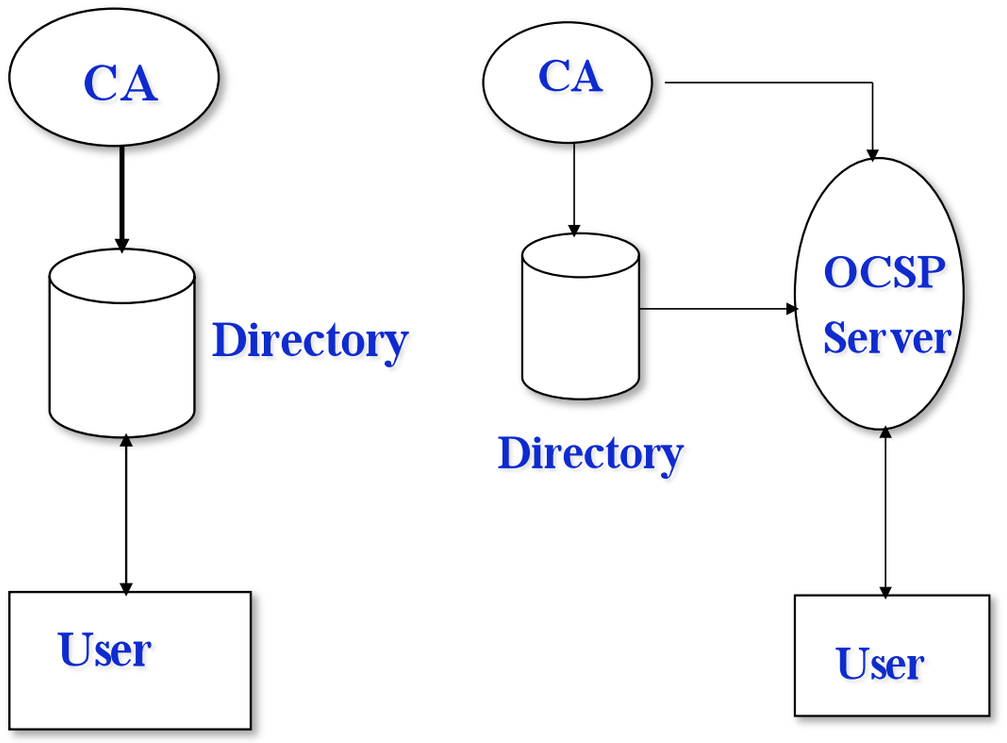
- 一系列基于公钥密码学之上，用来创建、管理、存储、分布和作废证书的软件、硬件、人员、策略和过程的集合。

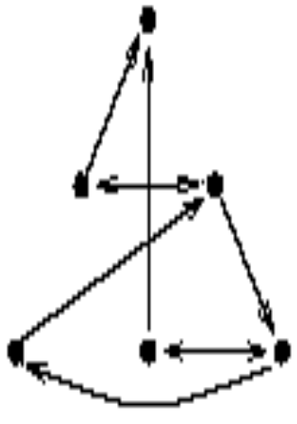
- 基础：公钥密码学 ***mid-1990s***
- 动作：创建、管理、存储、分布和作废证书
- 包含：软件、硬件、人员、策略和过程
- 目的：表示和管理信任关系

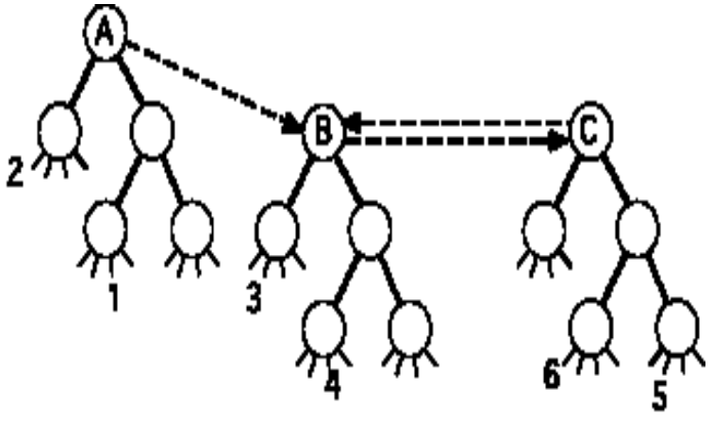


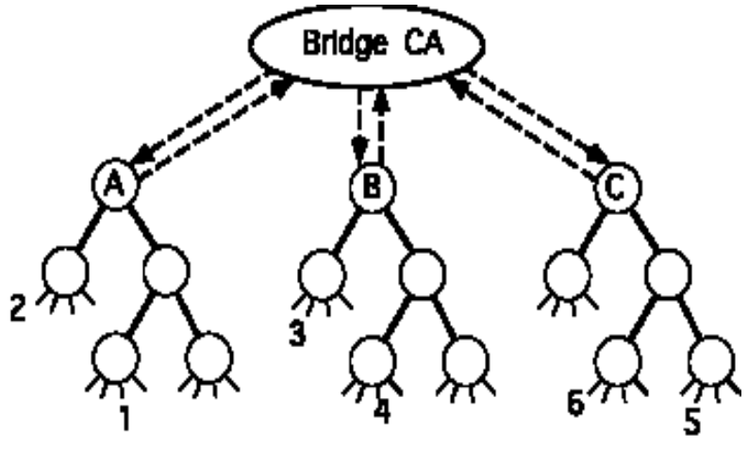
PKC & PKI

- 需要预先知道对方的公钥、需要在线服务器的支持
- 引入证书、引入可信第三方
- 密钥管理、证书管理
- 信任问题、规模问题
- 性能问题、互联互通问题



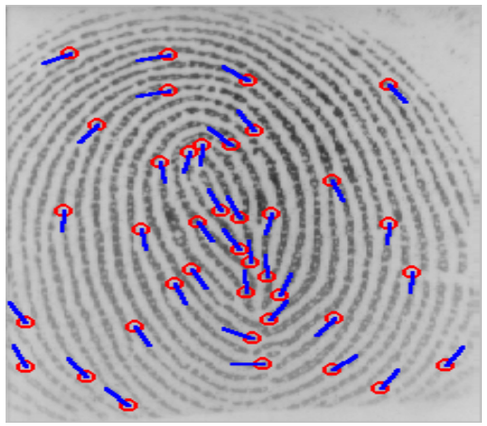


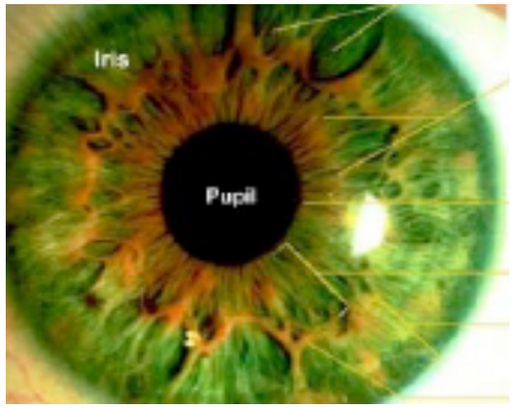


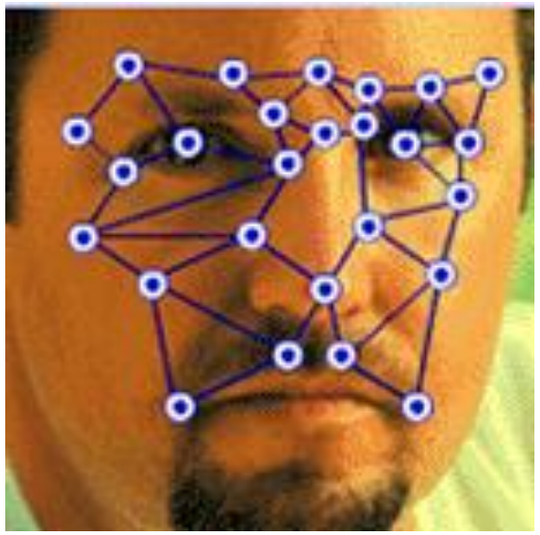


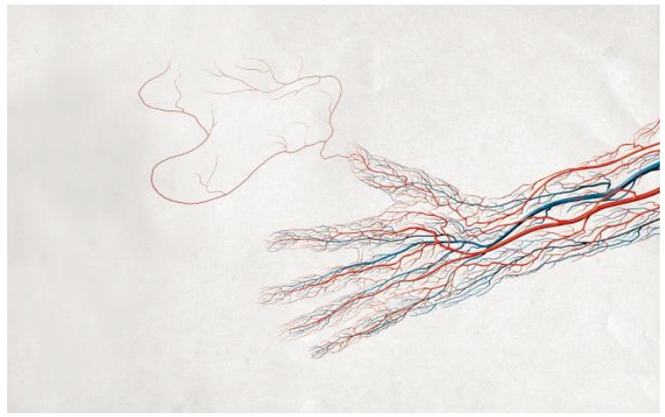
Password

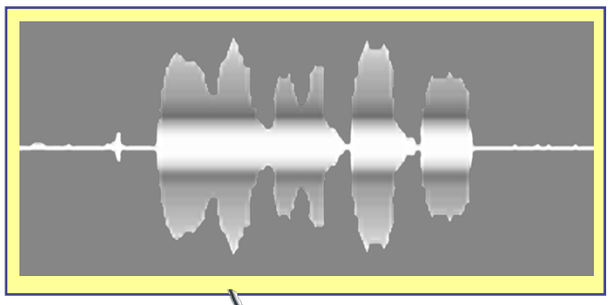
Biometrics

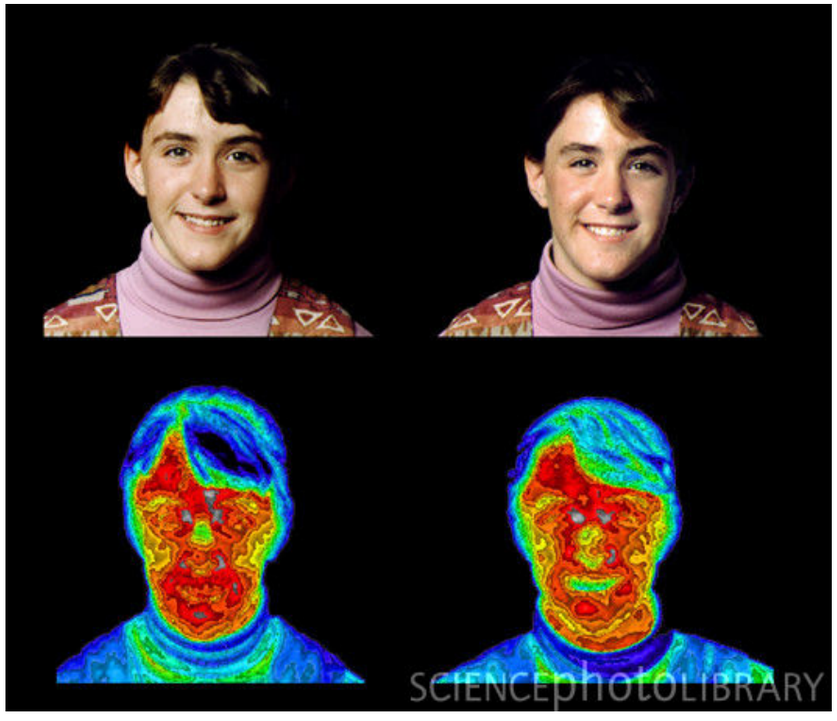


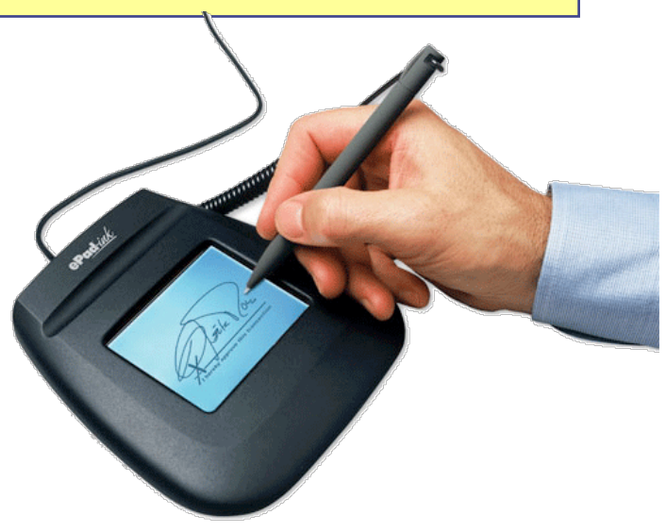












攻击指纹

Chaos Computer Club

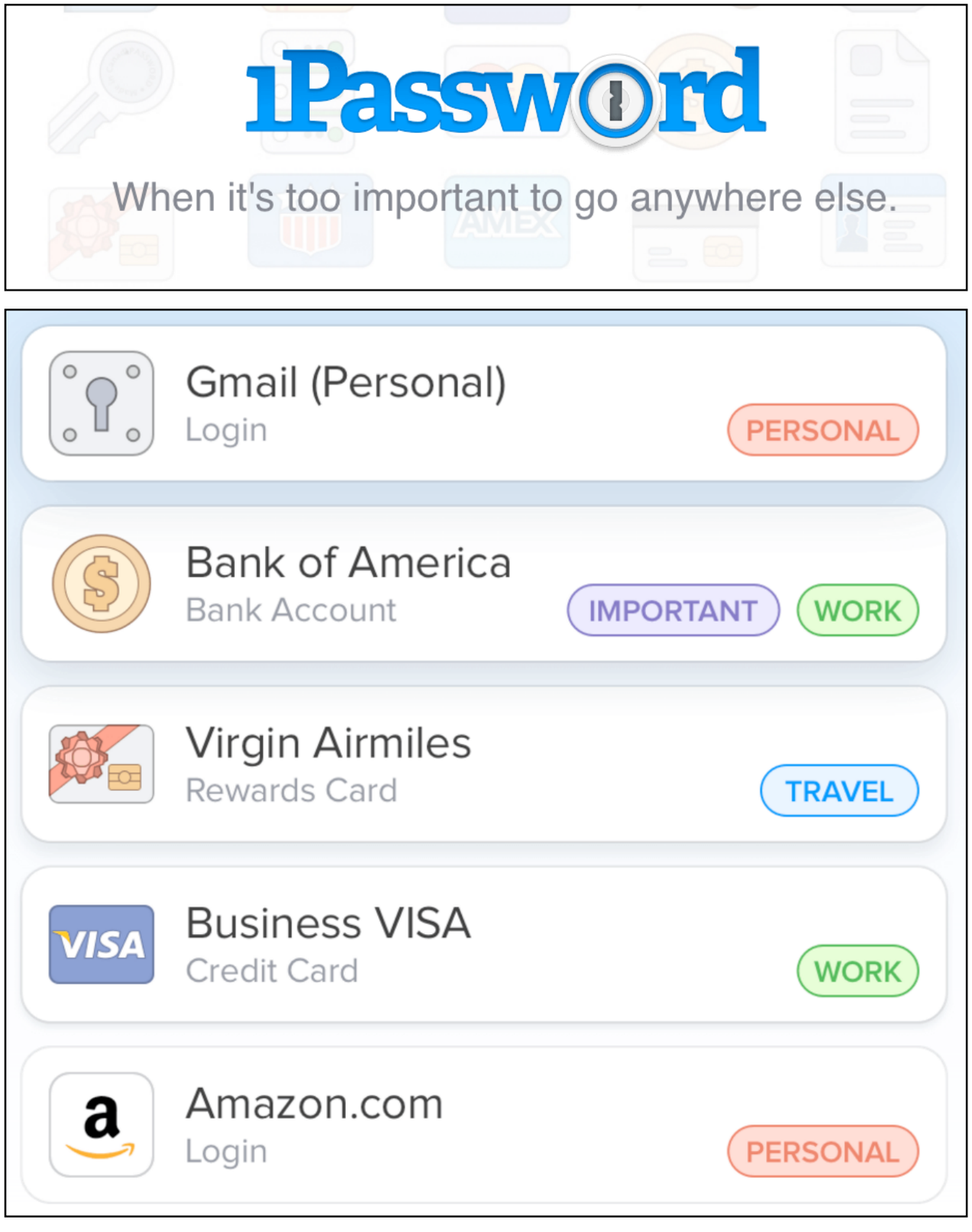
尽管存在大量的其余选择

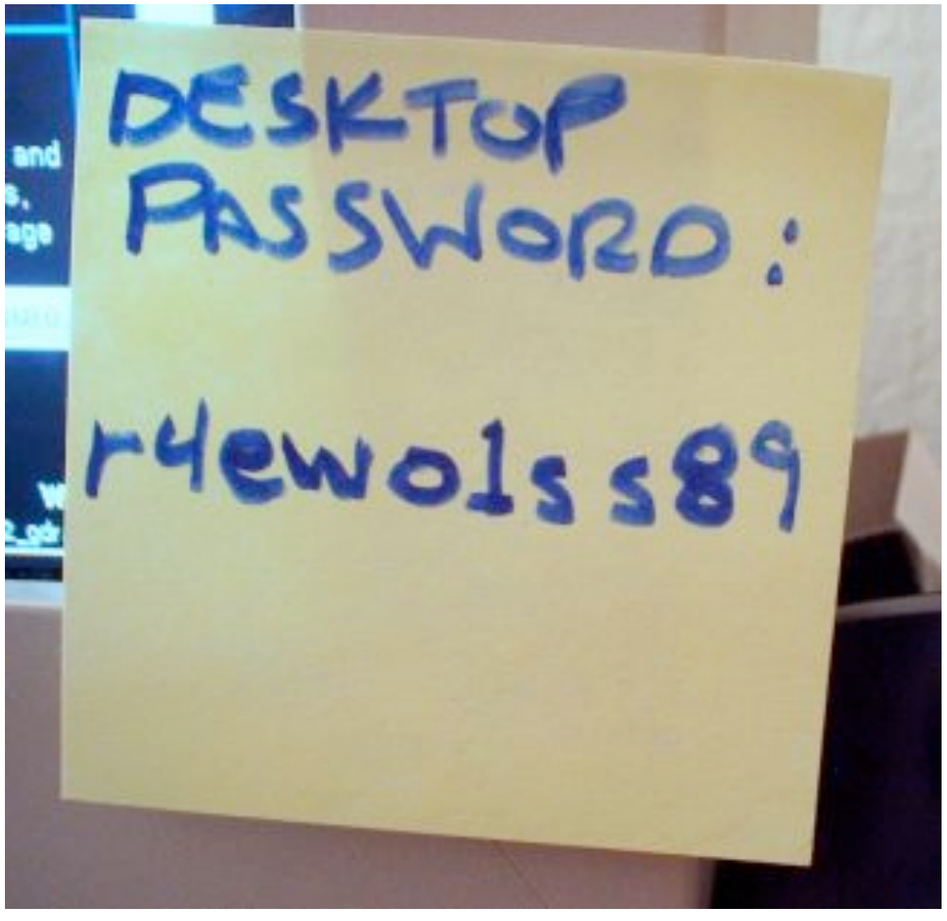
文本口令

依然是最常用的认证机制

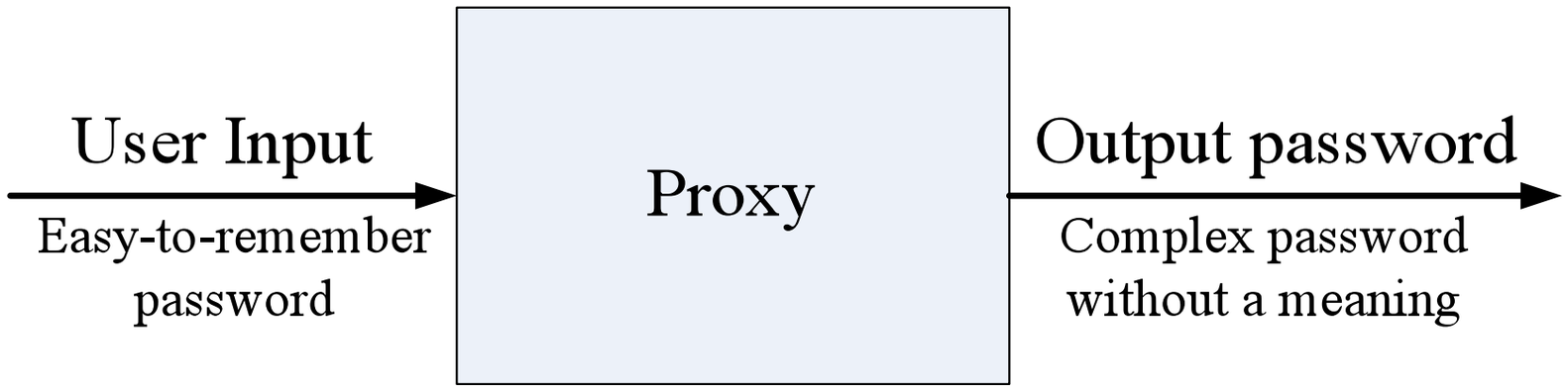
Password

口令管理





口令管理



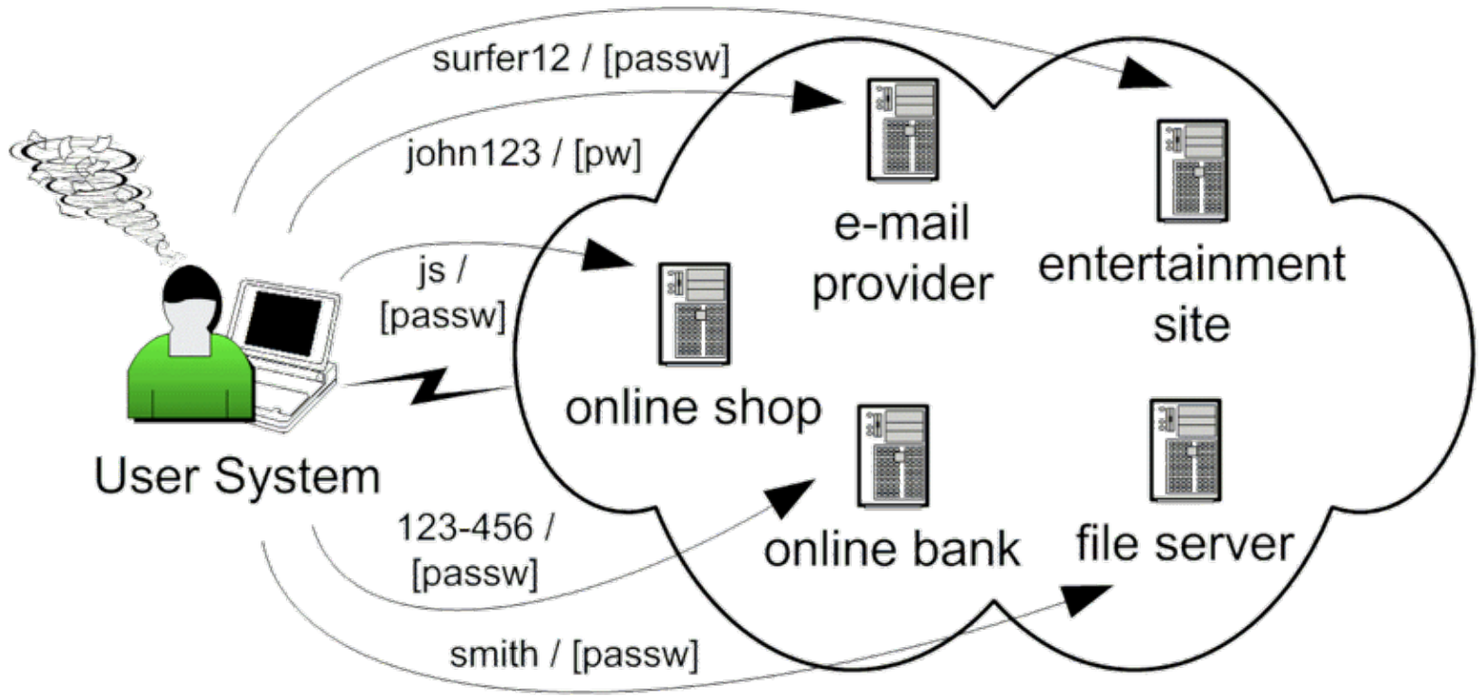
pu'r'du'e'c's 1仆人毒蛾醋酸 2仆人 3朴 4普 5扑	普熱毒蛾參賽
pu'ren'du'e'cu'suan 1仆人毒蛾醋酸 2仆人 3朴 4普 5扑	僕人毒蛾醋酸
p'r'd'e'cu'suan 1仆人毒蛾醋酸 2骗人 3旁人 4派人 5平日	疲軟的醋酸

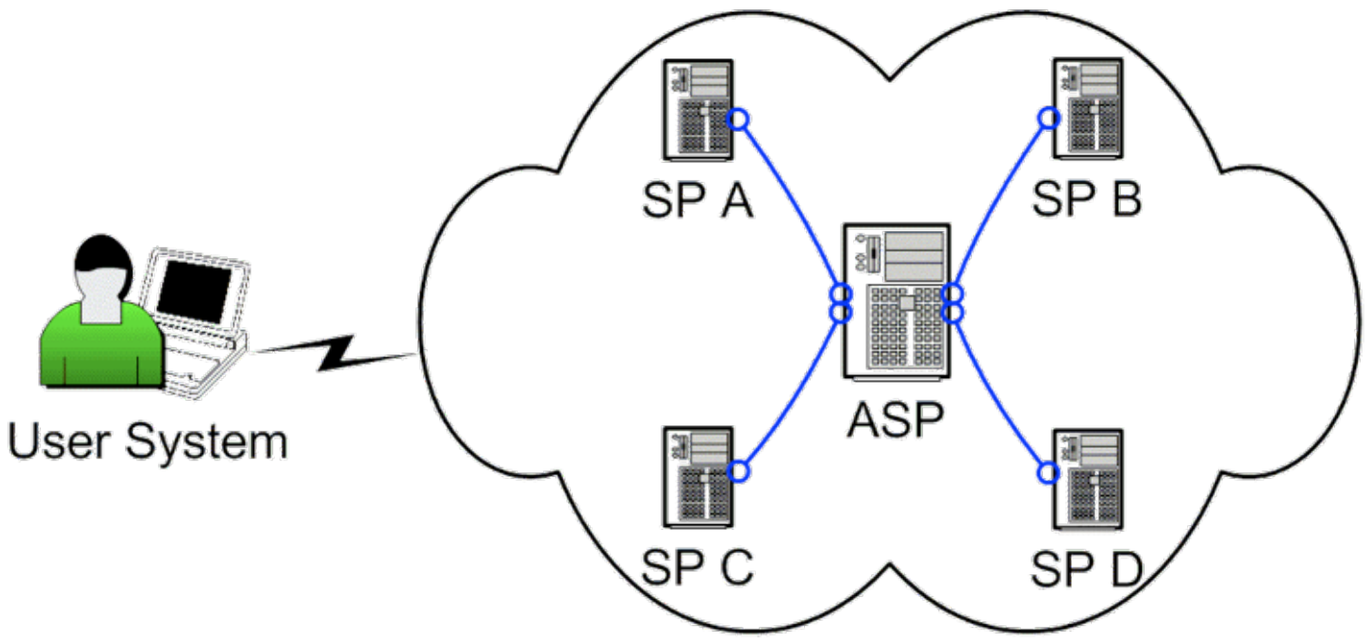
1a 2a
1b 2b
1c 2c

- ***Single password to all resources, One Password For Everything***

facebook

OpenID

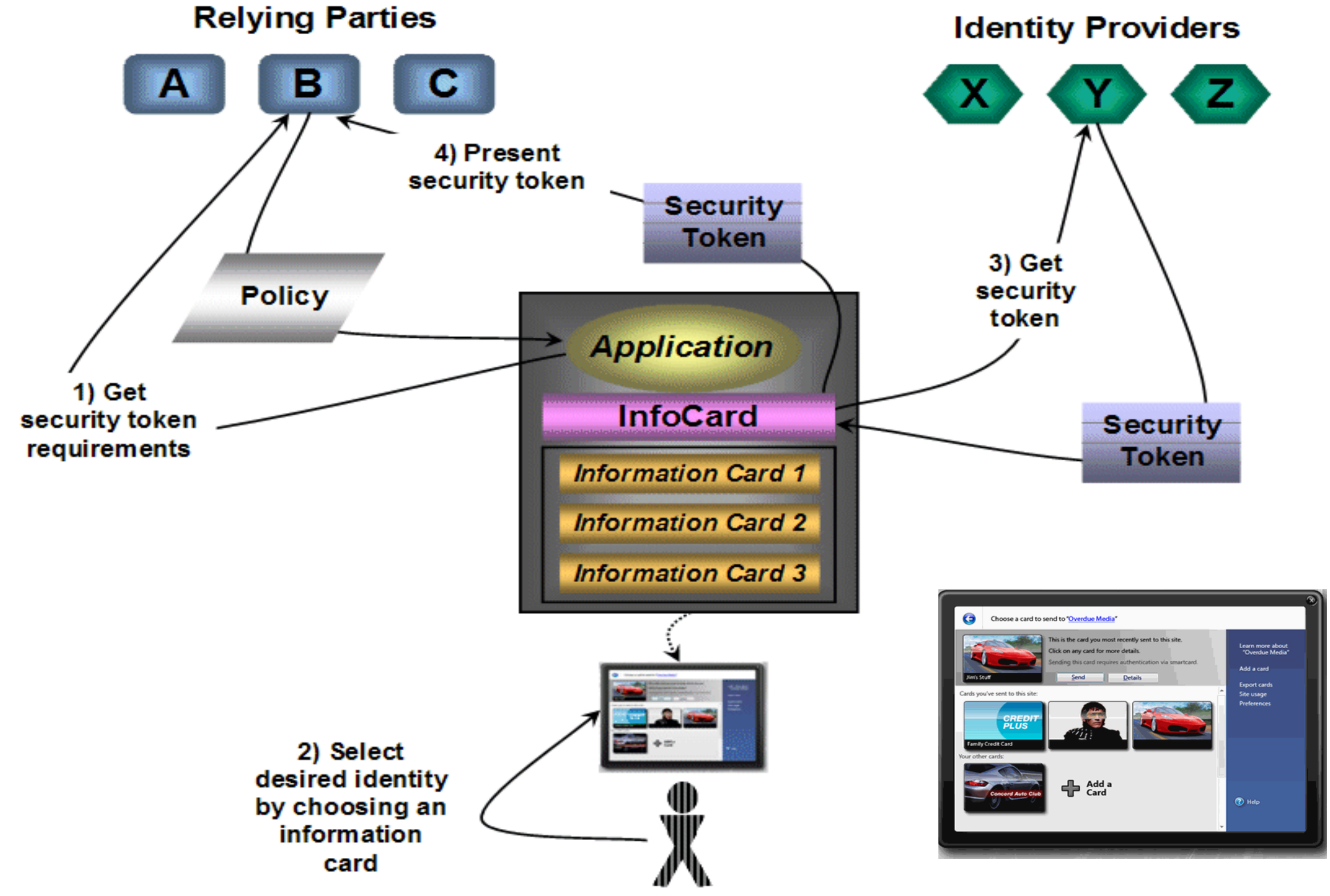




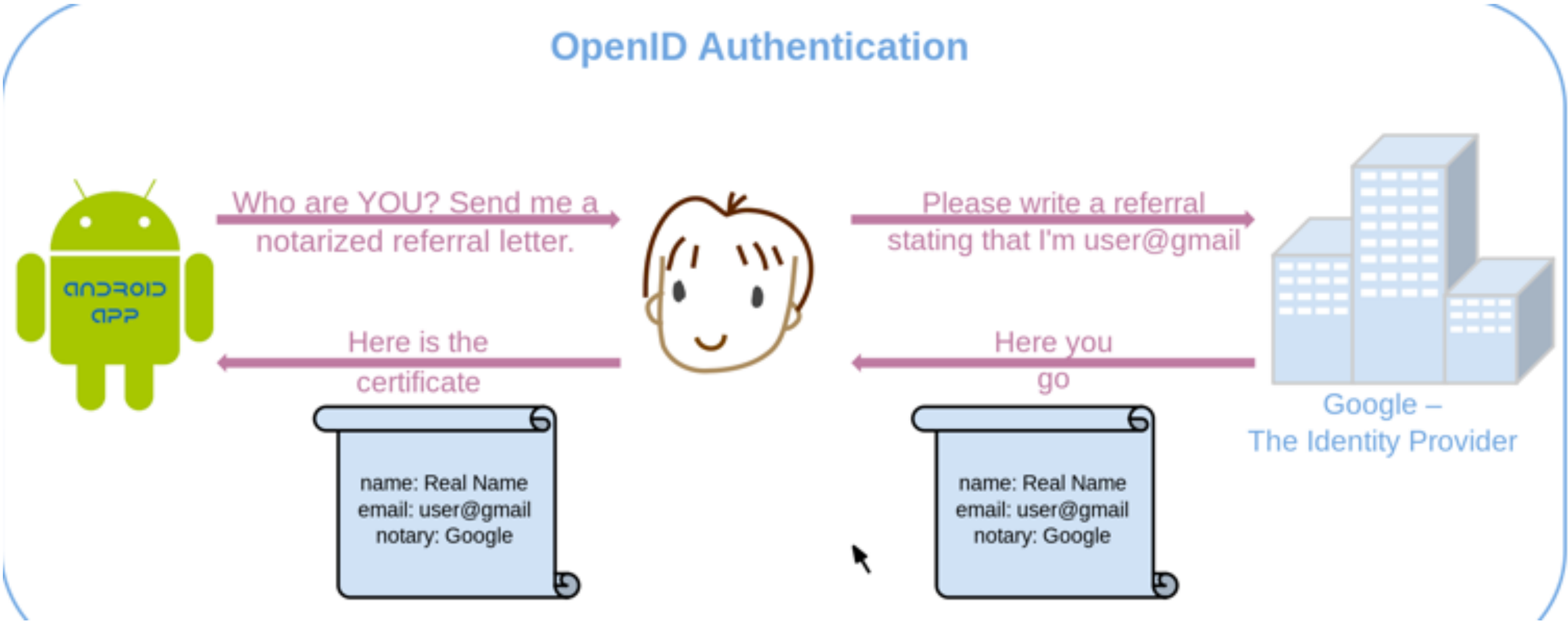
应用集成 性能瓶颈

单点失败 灵活性

Password CardSpace



OpenID



OpenID

轻量级IDM、基于URI

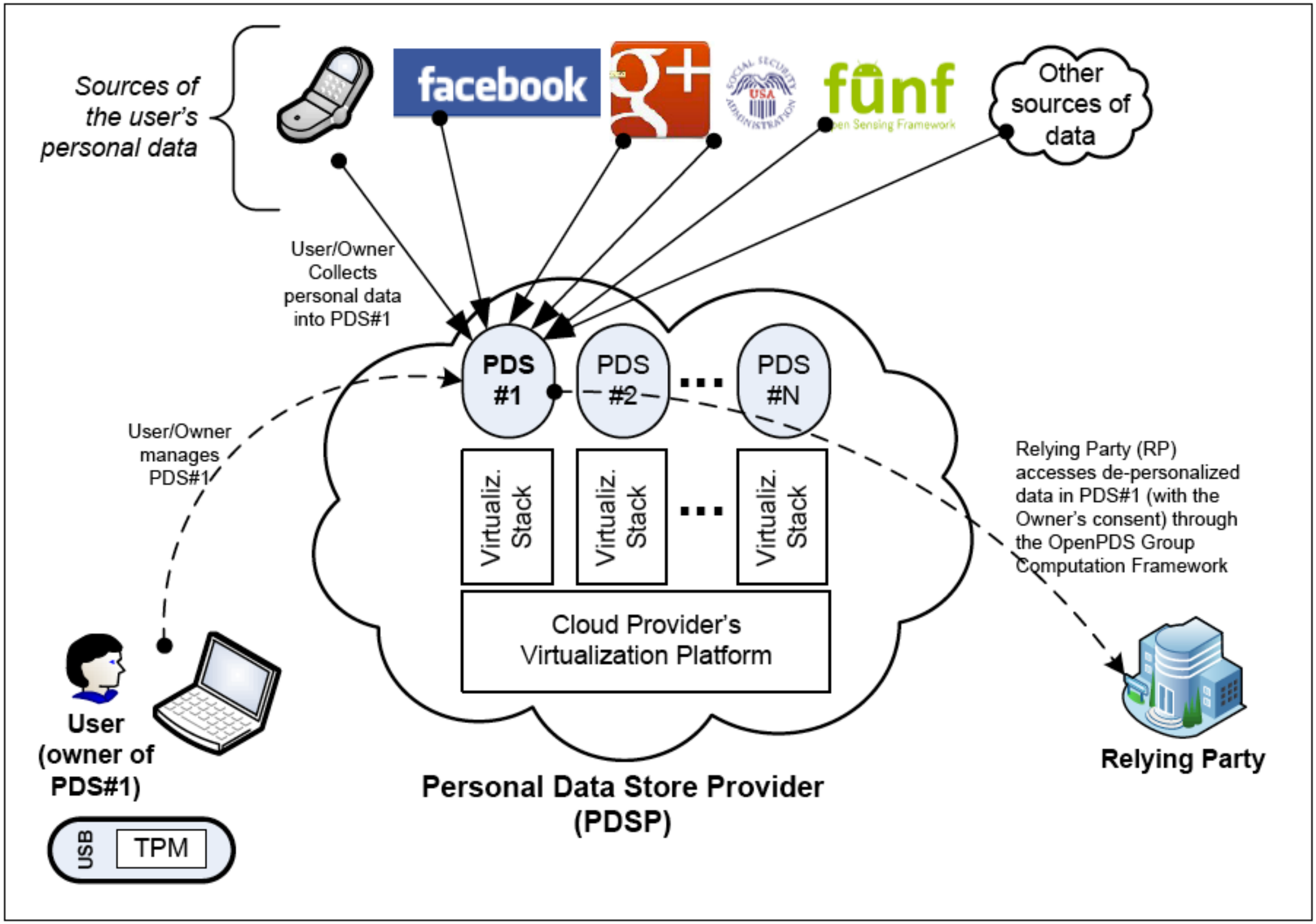
OAuth

- OAuth是一个开放标准，允许用户让第三方应用访问该用户在某一个网站上存储的私密的资源（如照片、视频、联系人列表），而无须将用户名和密码提供给第三方应用
- Oauth允许用户提供一个令牌，而不是用户名和密码来访问他们存放在特定服务提供者的数据。每一个令牌授权一个特定的网站
- 是OpenID的一个补充

视频编辑网站可以在
接下来的2个小时内
访问我一个目录中的视频

Dropbox
Facebook
Flickr
Google
Instagram
LinkedIn
Microsoft
QQ
PayPal
Salesforce
Sina Weibp
Twitter
Yahoo

OpenPDS


Sources of the user's personal data
facebook
funf
Other sources of data
User/Owner Collects personal data into PDS#1
PDS #1
PDS #2
PDS #N
Virtualiz. Stack
Virtualiz. Stack
Virtualiz. Stack
Cloud Provider's Virtualization Platform
User/Owner manages PDS#1
Relying Party (RP) accesses de-personalized data in PDS#1 (with the Owner's consent) through the OpenPDS Group Computation Framework
User (owner of PDS#1)
USB
TPM
Relying Party
Personal Data Store Provider (PDSP)

Web Authentication as Classification

新的口令模型

- *2000s:* 基于风险的模型，口令作为一个*signal*
- 其余*signal*：*Ip*地址、地理位置、浏览器信息、*cookies*、登录时间、口令输入方式和特征、申请资源
- 认证的结果不是一个*0/1*，而是一个估计值

- *Continual authentication*
- *Multilevel authentication*
- *Progressive authentication*

- *winner-take-all*
- *two sided market*

- 错误接受率 *vs* 错误拒绝率
- 训练数据的获取
- 更多的用户数据，隐私
- 用户的困惑和抱怨
- 共享口令

防止口令泄露

Password Leakage

口令泄漏

CSDN 全球最大中文IT社区 600w 2011

LinkedIn 600w 2012

EVERNOTE 5000w 2013

网易 NetEase www.163.com 过亿 2015

myspace.com a place for friends 4.27亿 2016

Traditional Salt Hash

Username	PassSalt	HashPwd
Username1	PassSalt1	HashPwd1
username2	PassSalt2	HashPwd2
.....	.....	.....
Username(i)	PassSalt(i)	HashPwd(i)
.....	.....	.....
Username(n)	PassSalt(n)	HashPwd(n)

字典攻击

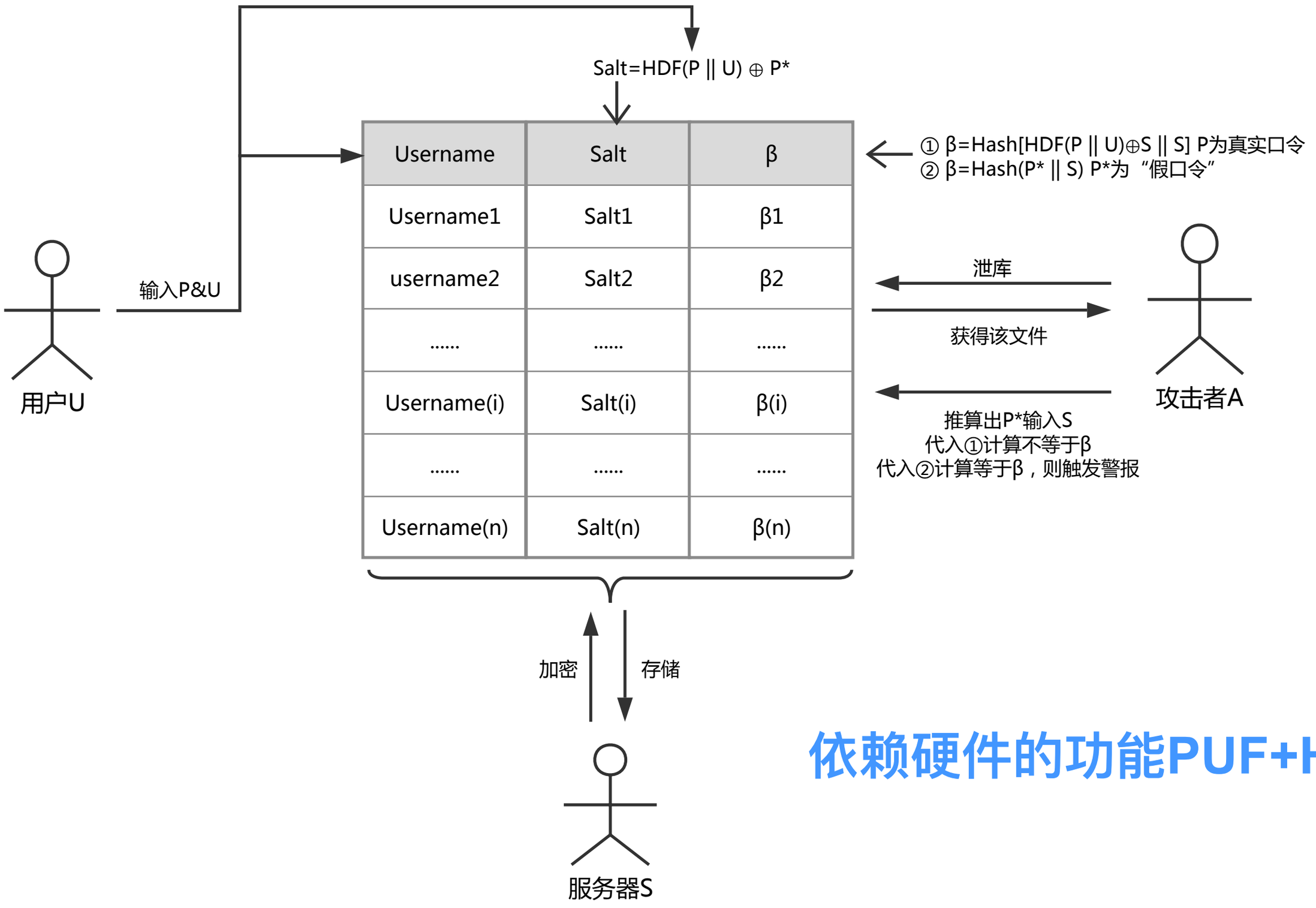
Index	Plain Text		Hash	Index
7210	Effluvium	→ Hash →	er4345dg	7210
7211	Effort	→	e1qqw3	7211
7212	Effusive	→	edf234	7212
7213	Eft	→	jkl244	7213
7214	egalitarian	→	fgt24	7214

Jdoe:345[illegible]16:24:Cathy Roe:/home/croe:/bin/csh
Stewart:edf234[illegible]16:24:Mark Stewart:/home/stewart:/bin/csh
Andy:wer345t:16:24:Andy O Ram:/home/andy:/bin/csh

password1	abc123	myspace1	password
Blink182	**qwerty1**	fuckyou	123abc
baseball1	football1	123456	soccer
monkey1	liverpool1	princess1	**jordan23**
slipknot1	superman1	iloveyou1	**monkey**

Password Leakage

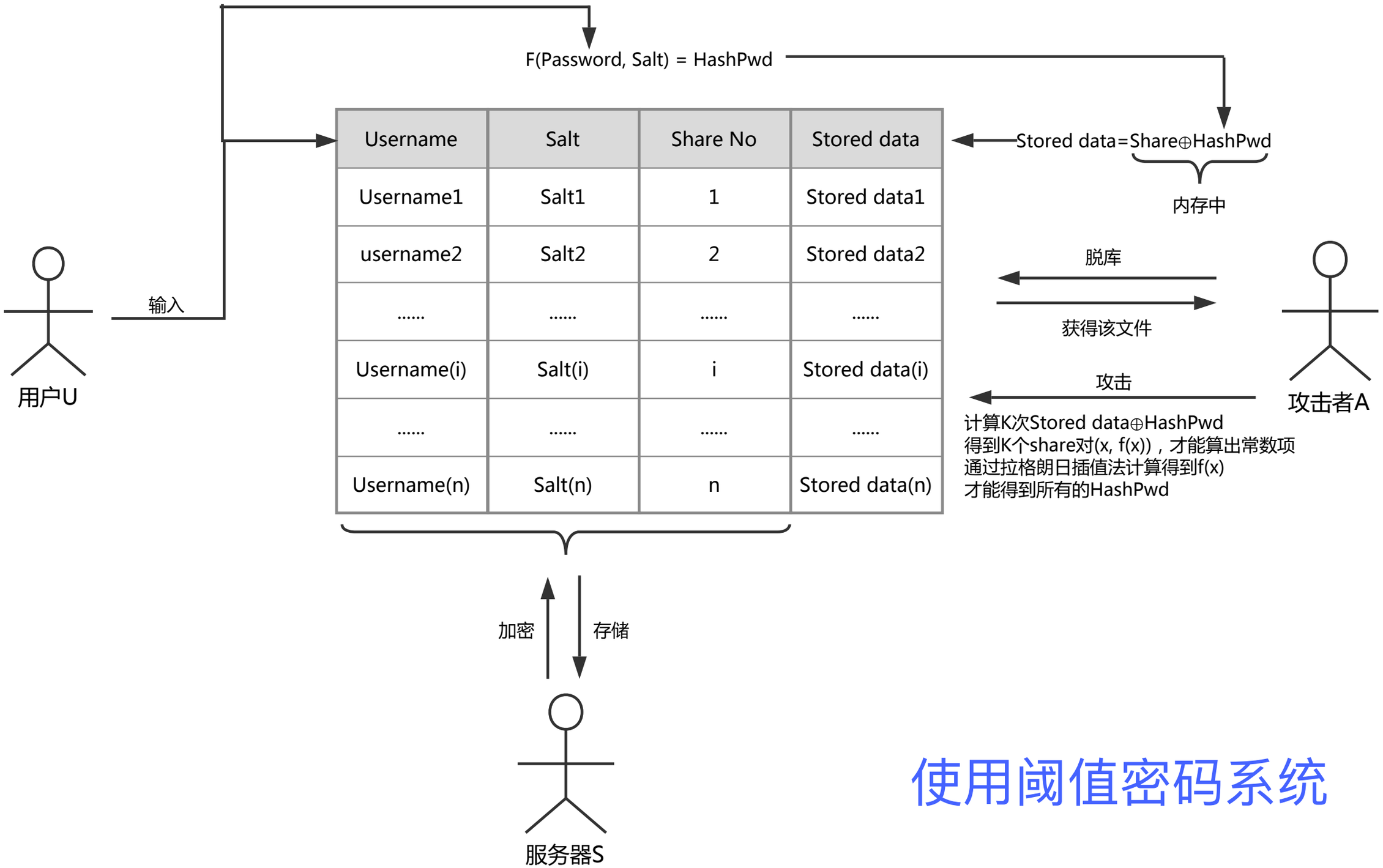
ErsatzPasswords



依赖硬件的功能PUF+HSM

Password Leakage

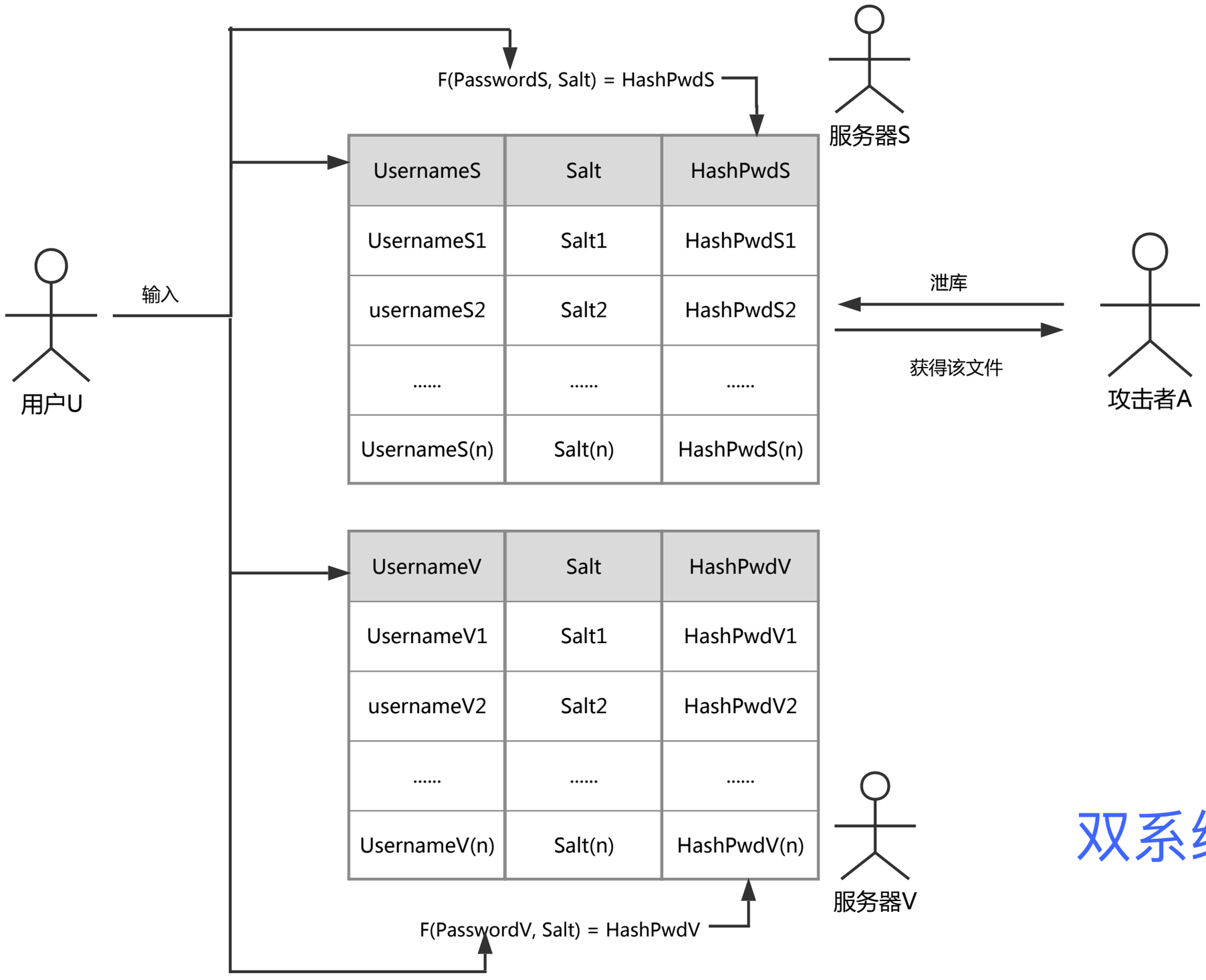
PolyPassHash



使用阈值密码系统

Password Leakage

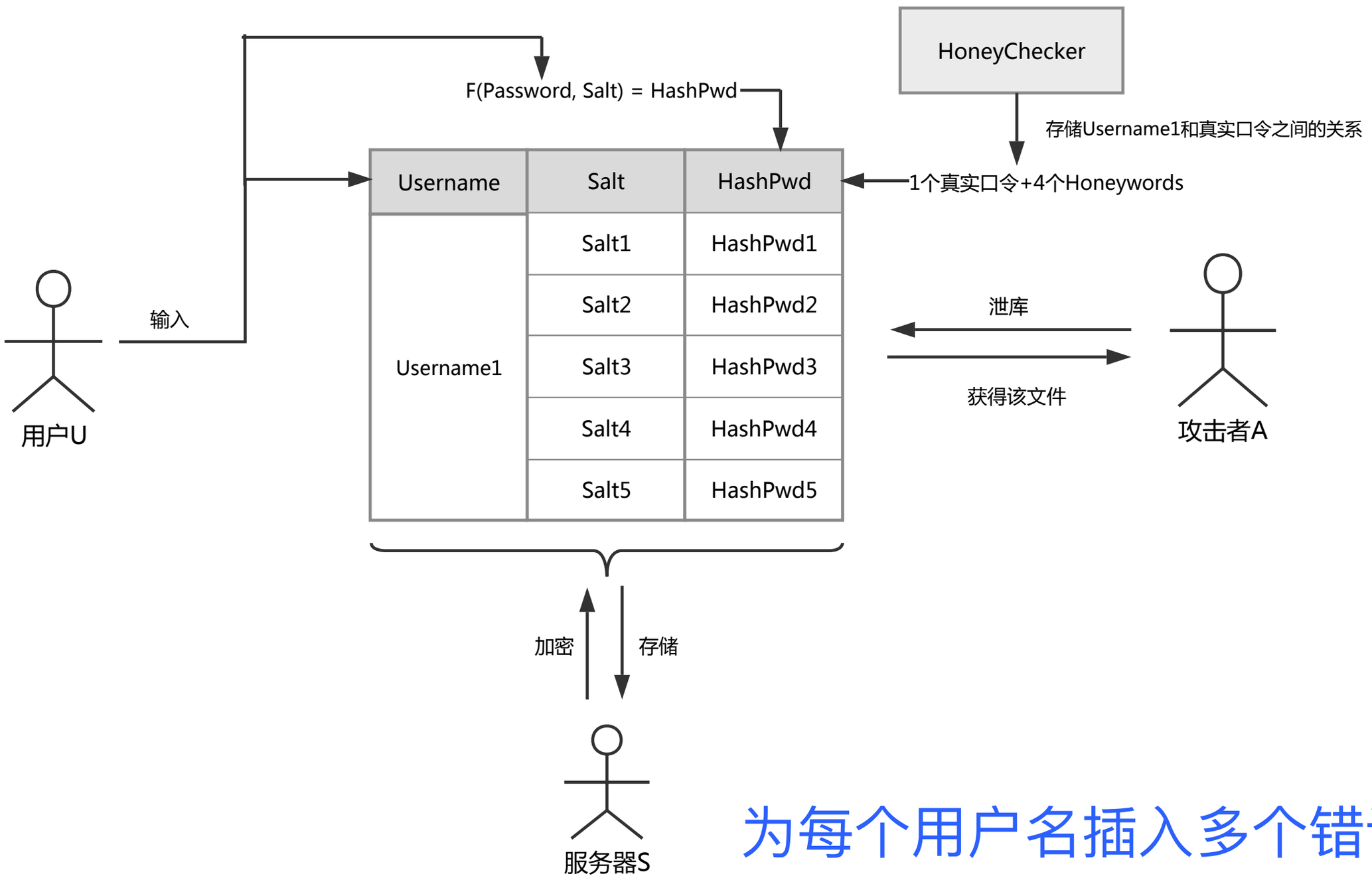
SAuth



双系统双口令认证

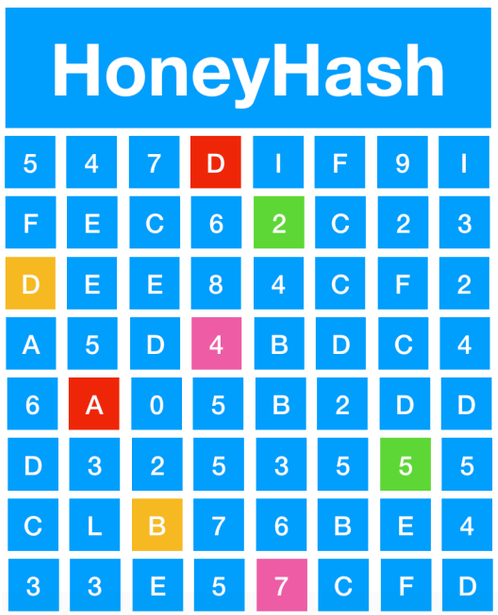
Password Leakage

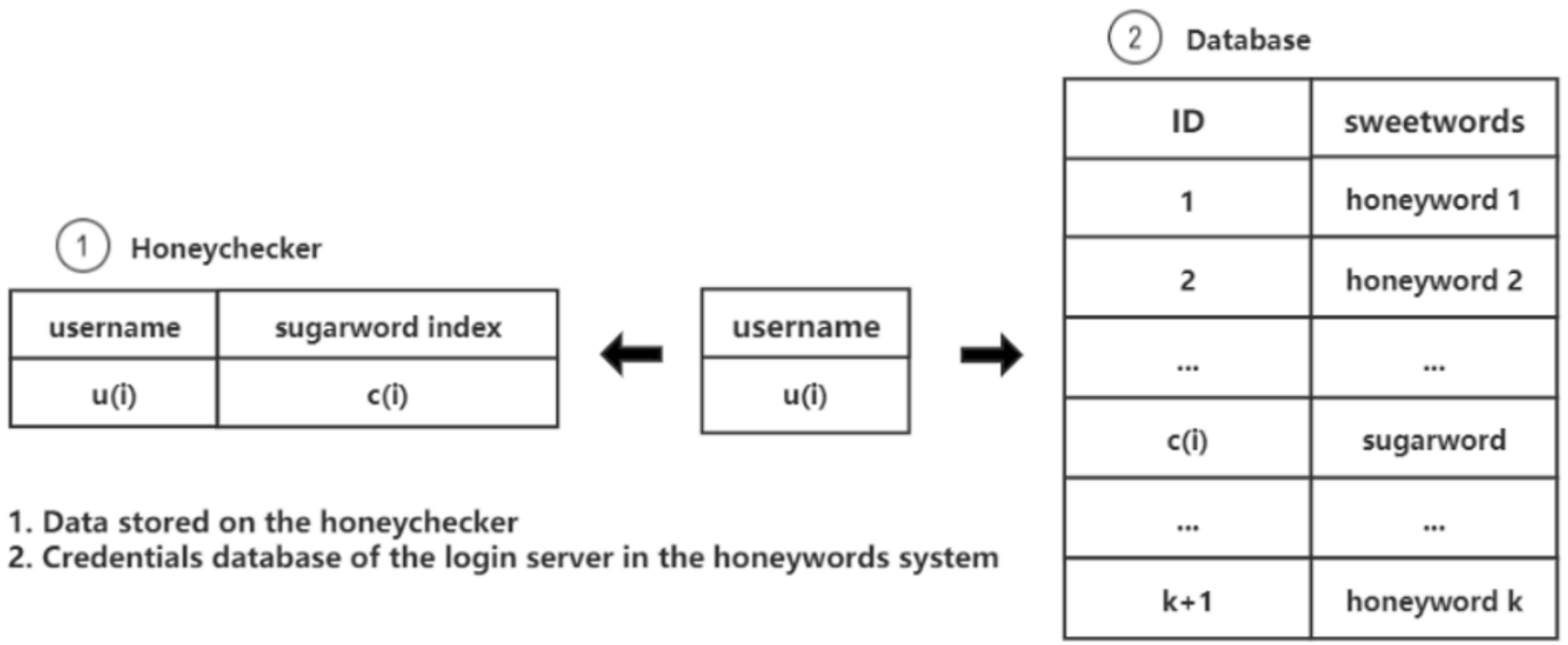
Honeywords



为每个用户名插入多个错误的口令

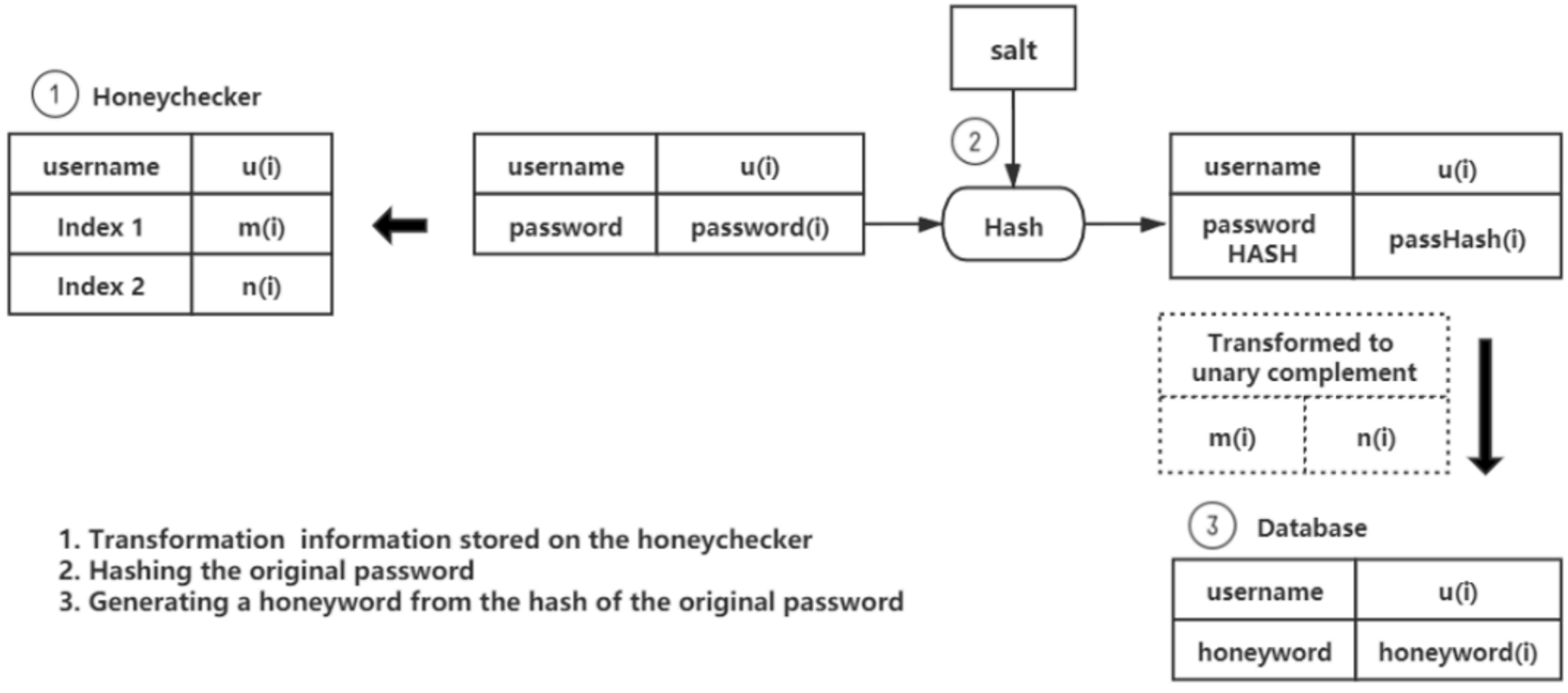
HoneyHash





https://nordsec2020.on.liu.se/

The 25th Nordic Conference on Secure IT Systems (Nordsec 2020)



SlidePIN:

Slide-based PIN Entry Mechanism on Smartphones

背景

www.eMarketer.com

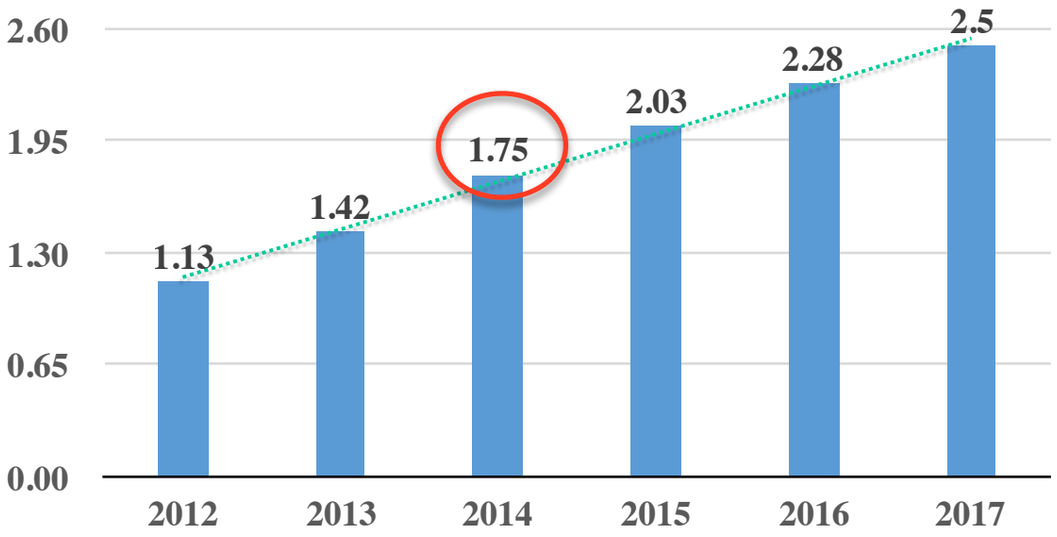
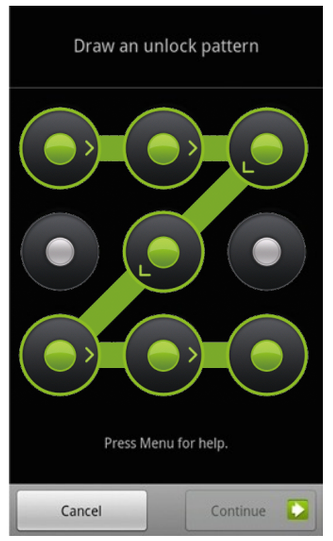


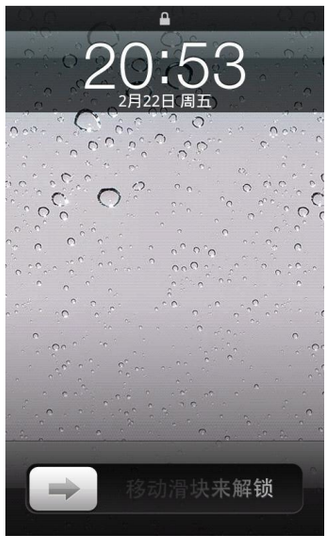
Photo Audio Video
SMS Call Emai
l
Payment Location
SNS Blog IM
… …

4 digits PIN

PatternLock

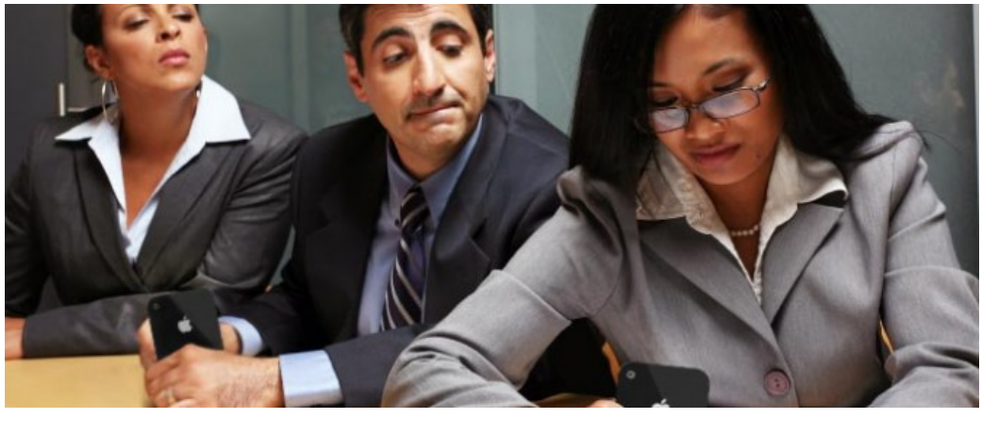


No



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

Shoulder surfing attack



什么是肩窥攻击

- 肩窥攻击（Shoulder Surfing）也称为窥视攻击，是一种利用直接观察就可以得到所需要信息的攻击技术，是社会工程的一种，对于基于知识的身份认证机制有着非常大的威胁，特别对于文本密码、图形密码和隐私问题这三个最主要的认证机制。

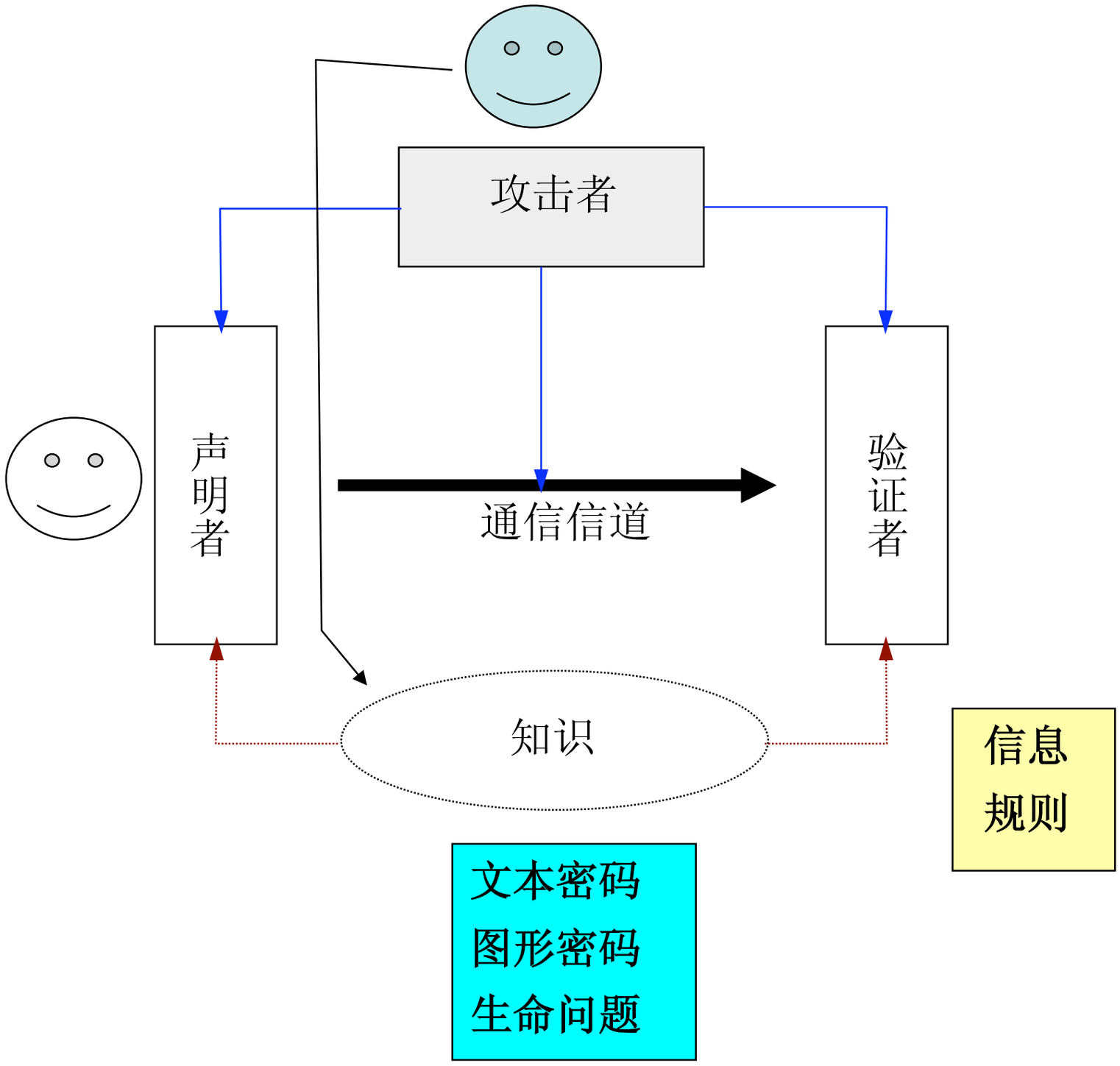
- 肩窥攻击一般发生在相对临近的环境中，特别是在比较拥挤的地方，在这种环境中攻击者可以很容易的看见临近的一些人所填写的标单、在ATM机器上录入的PIN、在公用电话上使用的电话卡、在屏幕上显示得各种信息等。当然在摄像头、望远镜、录像机等设备的支持下，肩窥也能发生在非常远的距离。

- 肩窥攻击基本上有四种形式：临近偷看、使用设备、声学跟踪、电磁泄露。

- 该类攻击被人提及已有20多年的历史，但一直没有引起足够的重视，现有的相关研究和论文还不太多。但是随着移动网络和移动计算的发展，越来越得到了重视。

SlidePIN

肩窥攻击产生原因



相关工作

Computing burden

Memory burden

Indirect Entry

Human-computable challenge-response

Challenge ← *Keypad layout*

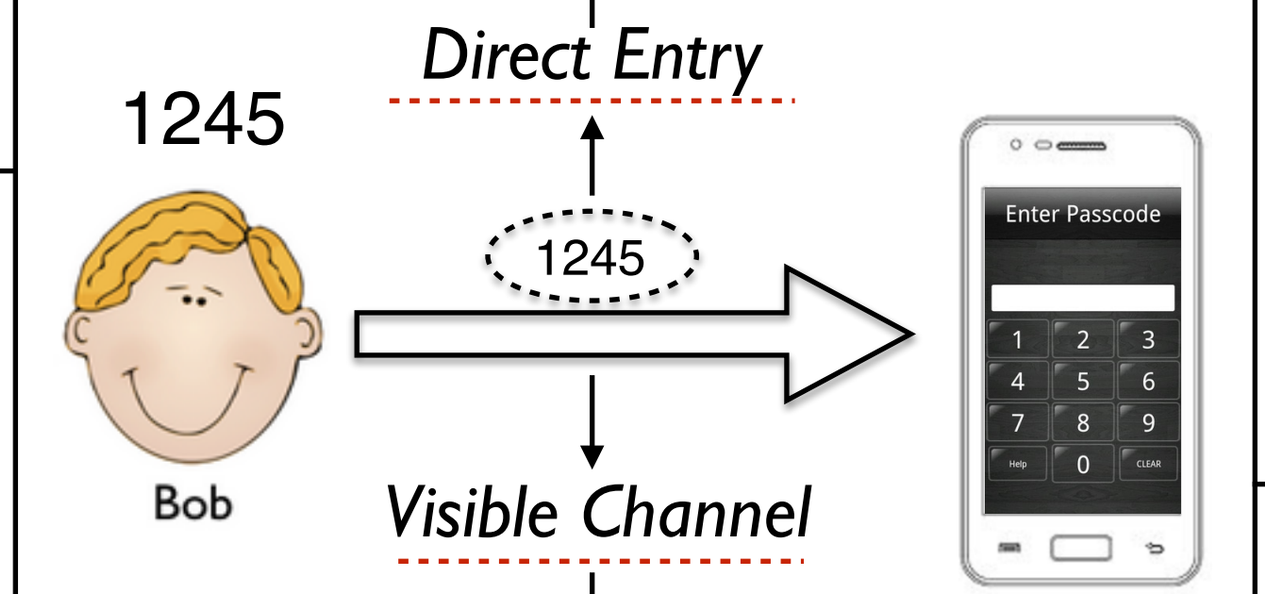
← *Additional factors*

☆ *Colors*

☆ *Symbols*

☆ *Directions*

… …



… …

☆ *Physical block*

☆ *Eye tracking*

☆ *Tactile sensor*

☆ *Pressure sensor*

☆ *Vibration sensor*

☆ *Back-of-Device interface*

Special human-computer Interface

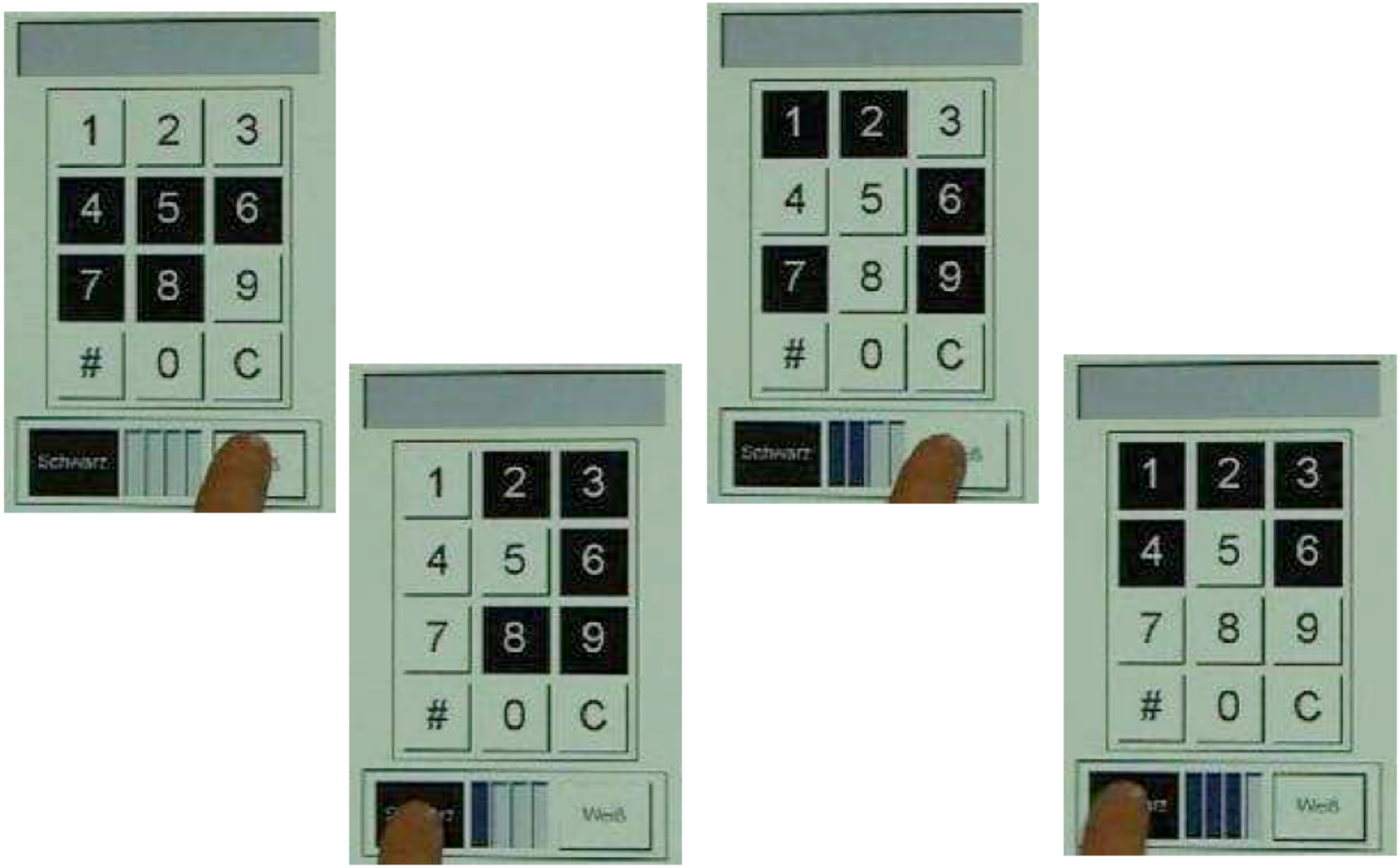
Invisible Entry

Hardware support

Deployment costs

SlidePIN

PINEntry



A PINEntry Method Resilient Against Shoulder Surfing@ CCS 2004

ColorPIN

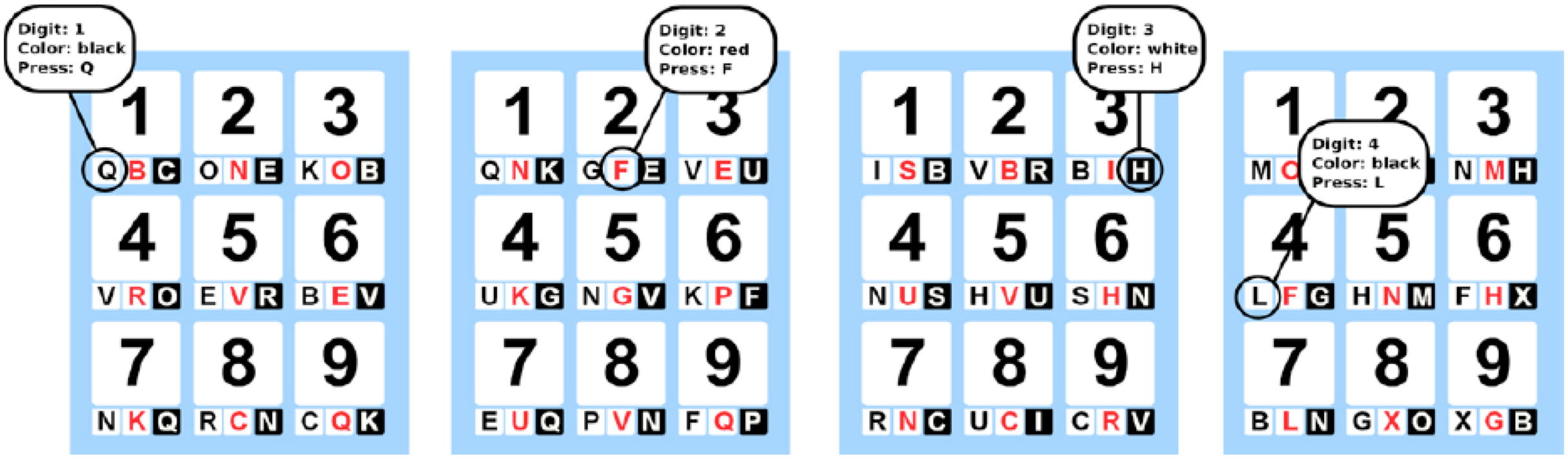


Figure 1: Exemplary PIN entry with ColorPIN. To input the PIN 1(black) 2(red) 3(white) 4(black) the user inputs the letters "QFHL". After each key press, letter assignment changes randomly.

SlidePIN

BoD AuthE

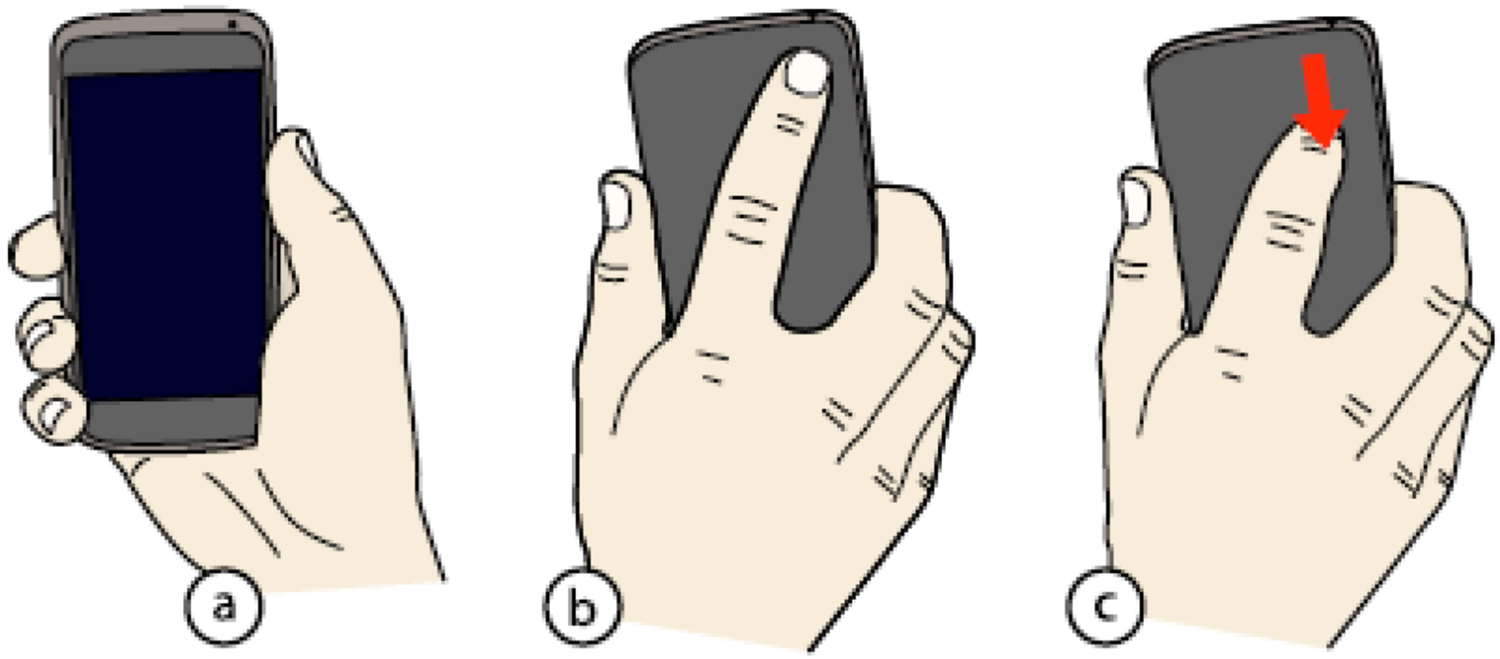
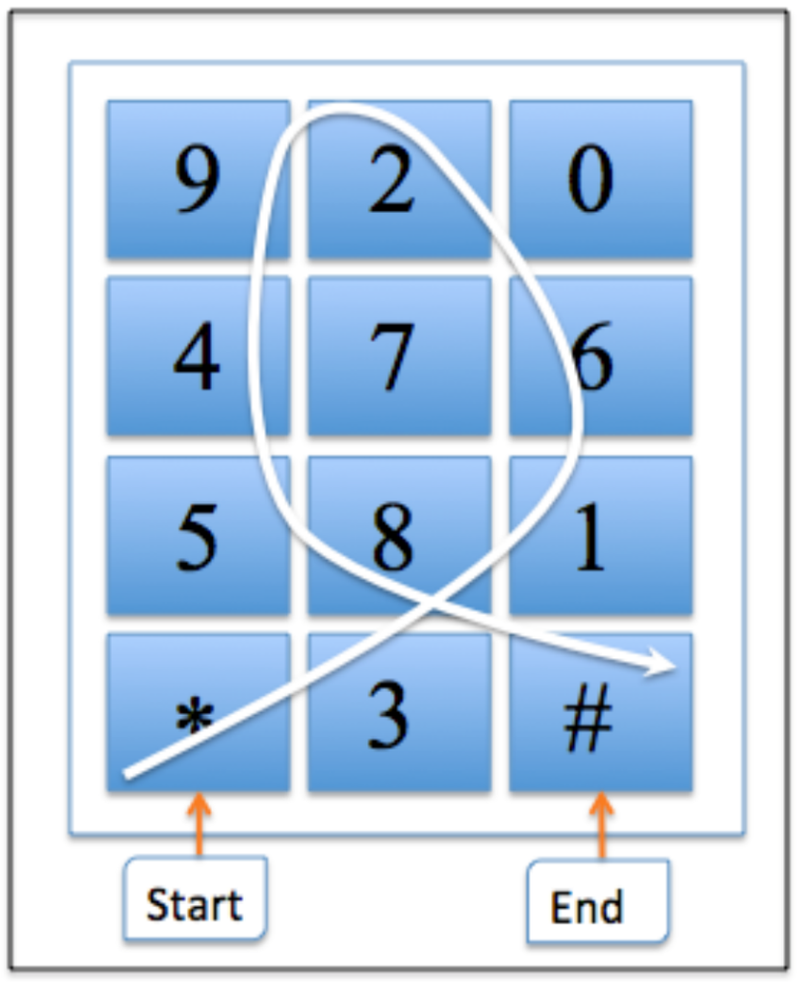


Figure 1. BoD (Back-of-Device) Shapes authentication concept. a) Typical hand posture when using one-handed input for authentication. b) The user authenticates by performing a row of simple shapes on the back. c) Example of a user performing a single-stroke shape ("Down").

Back-of-Device Authentication on Smartphones @ CHI 2013

SlidePIN概念

Slide-based PIN Entry Mechanism



Random

Slide

Input with random numeric keypad is more secure

Word-Gesture Keyboard

PIN 1245

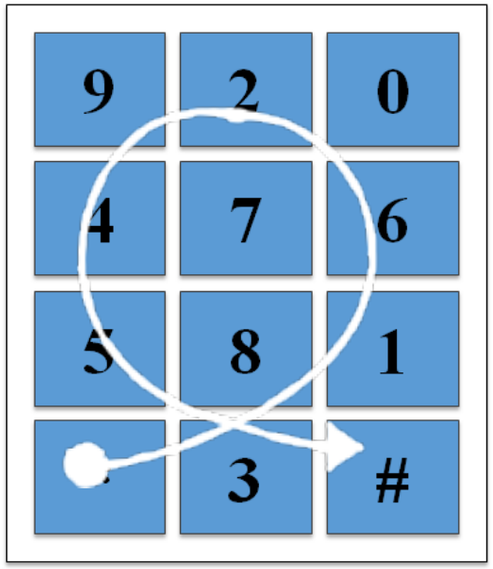
SlidePIN *381629458#

Slide input is faster

Slide input is more secure

模型分析

PIN: 1245

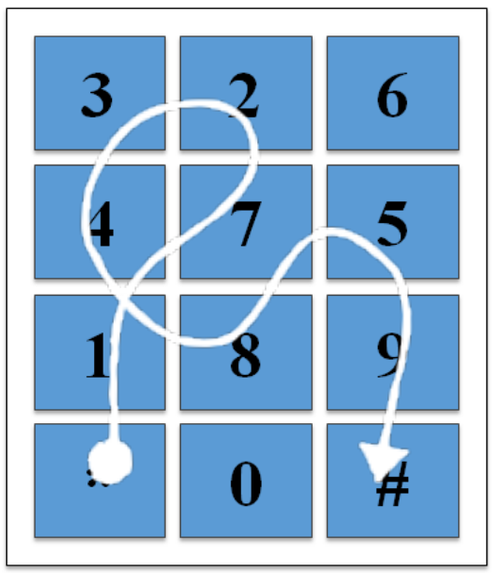


Layout 1

Trajectory 1

Sequence 1

*381629458#



Layout 2

Trajectory 2

Sequence 2

*147234185 9#

Slide Map Function

F (PIN, Layout) → Sequence

Attack Function

One-Time

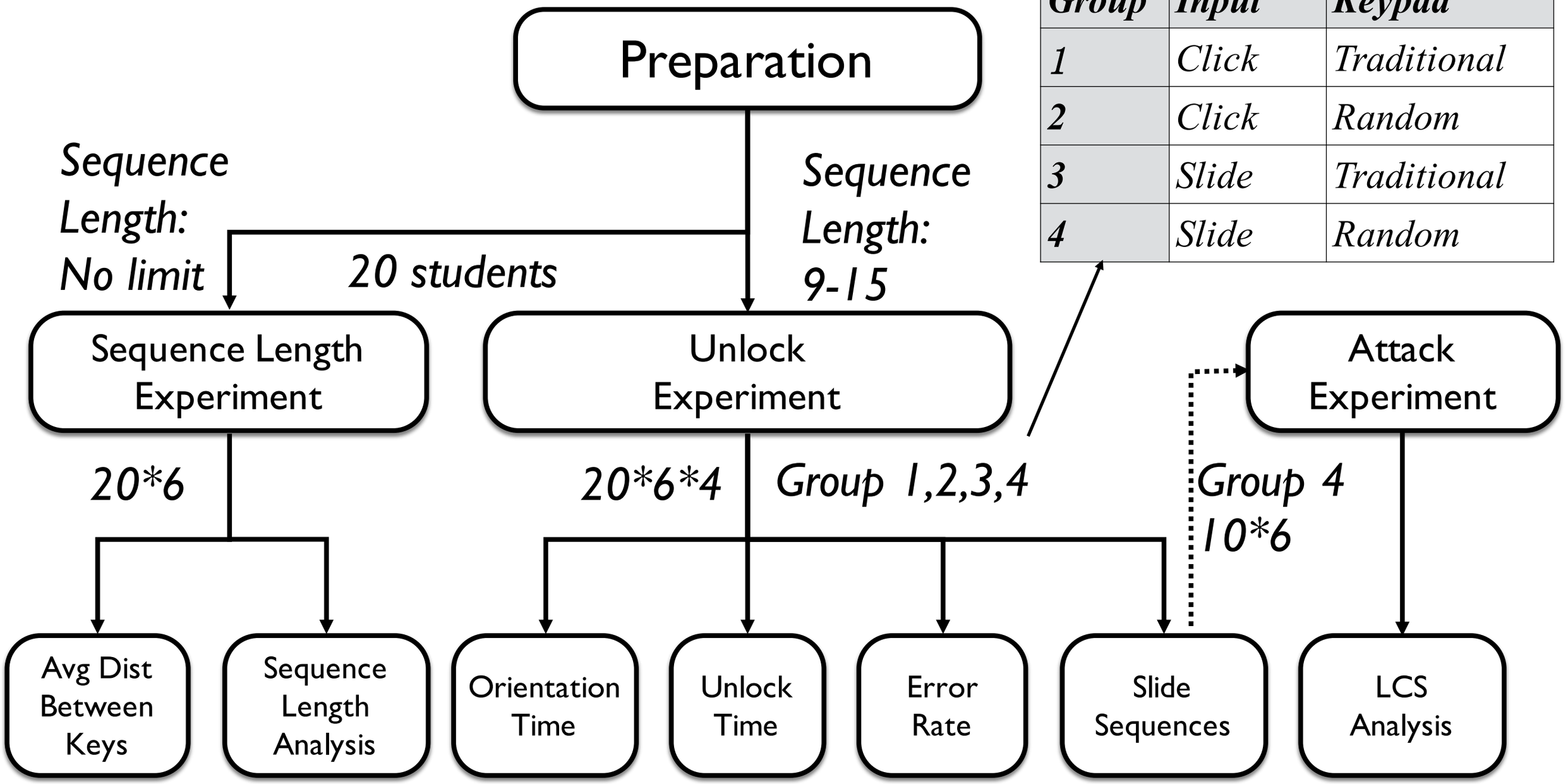
F^{-1}(Sequence 1) → PIN

Multi-Time

F^{-1}(Sequence 1,
Sequence 2,
… …
Sequence n) → PIN

实验设计

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



SlidePIN

序列长度分析

Too long * 0123456789 0123456789 0123456789 0123456789 #

Too short *31629450#

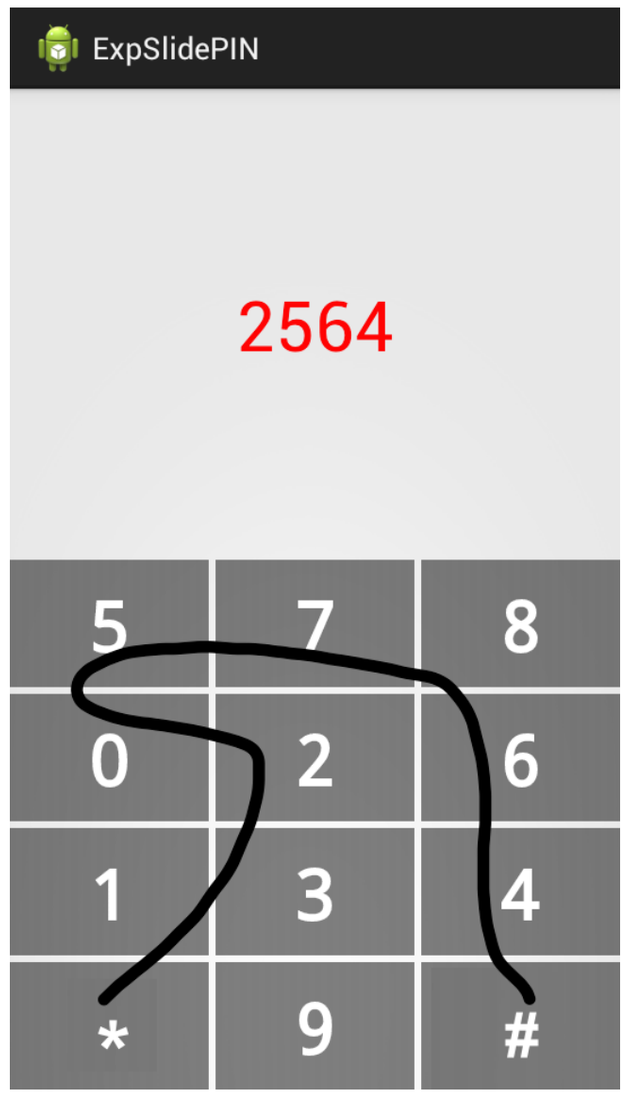
Why

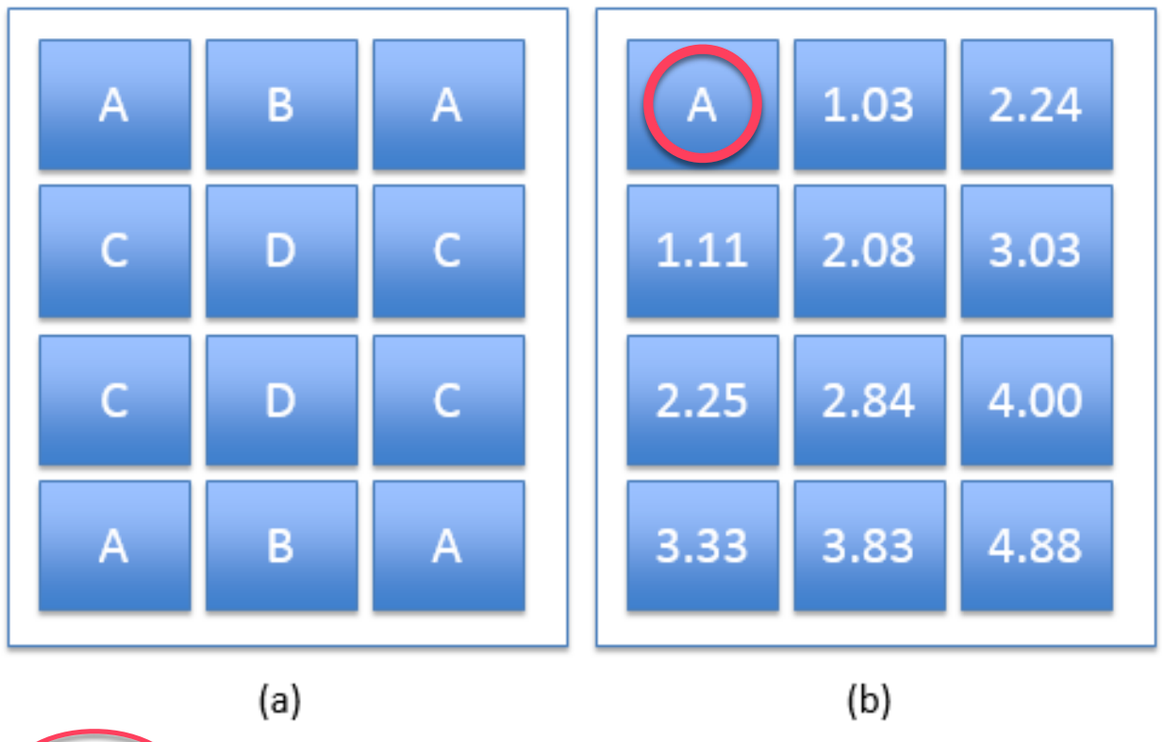
*3816279450#

*381629450#

How

20 students
** 6 times*





Estimate of Distance between Keys

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

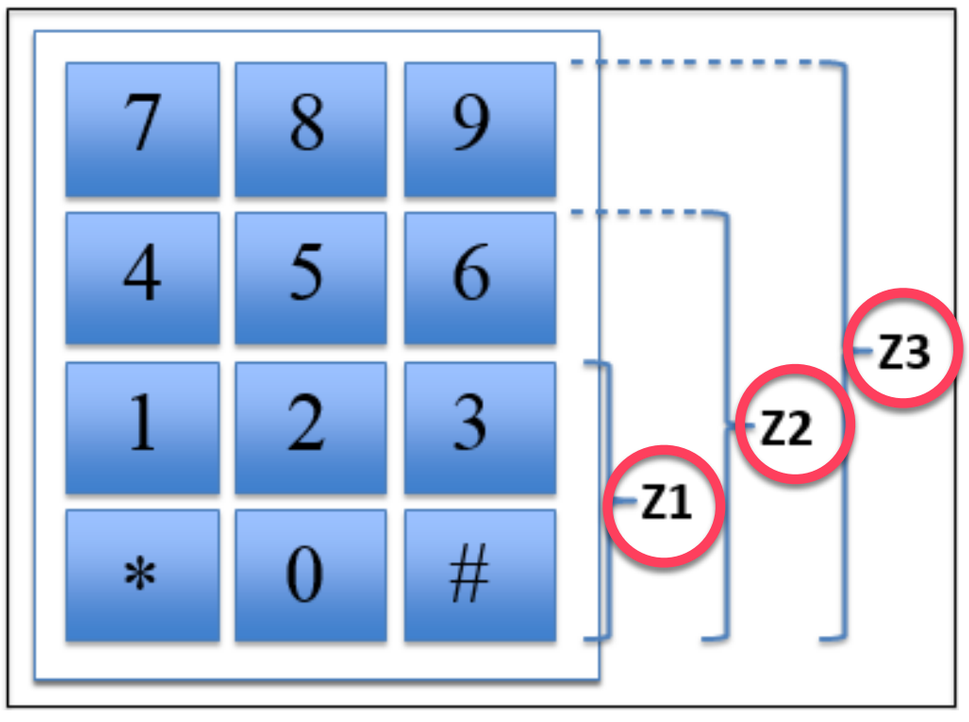
序列长度分析

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 ≈ 2.31*



P(Z3) = 1 *D(Z3) = 11.55*

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

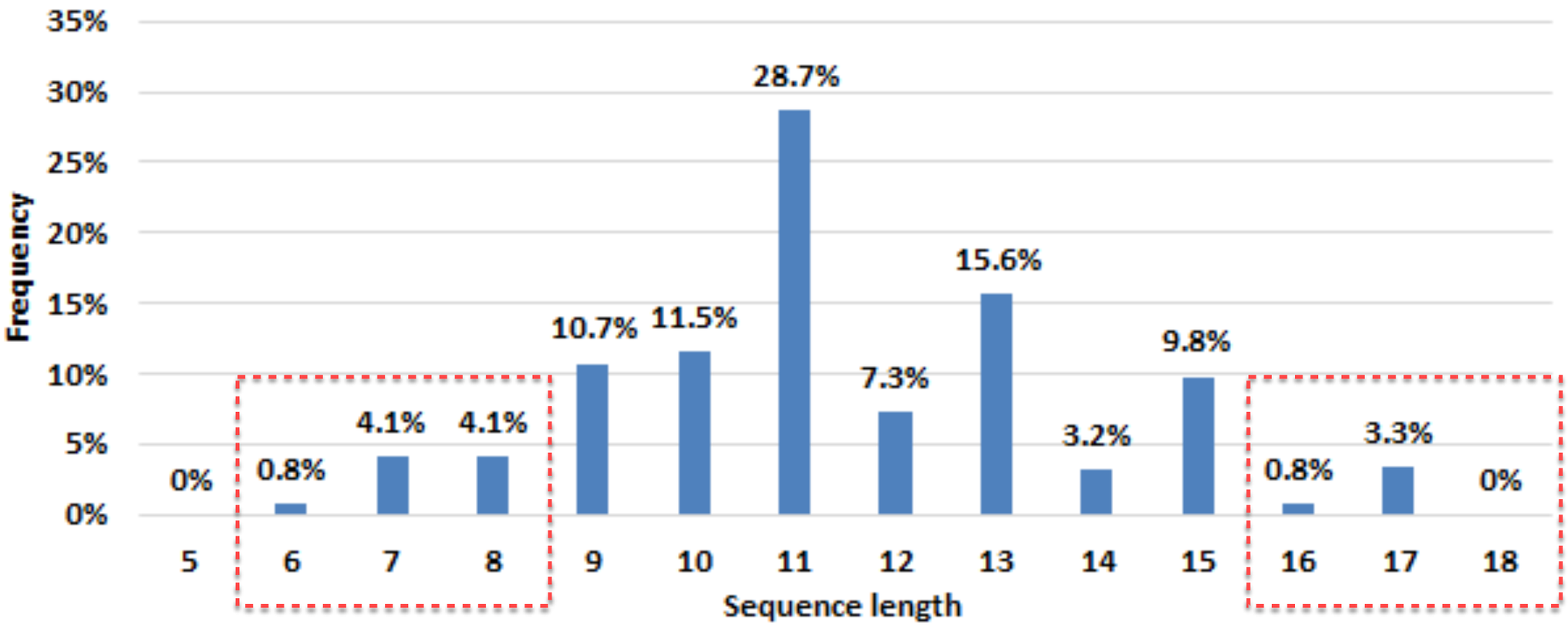
P(Z1) = 1/200 *D(Z1) = 8.08*

*8.08 * 1.87 ≈ 15.11*

9 - 15

序列长度分析

- *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*



安全性分析

- *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*		

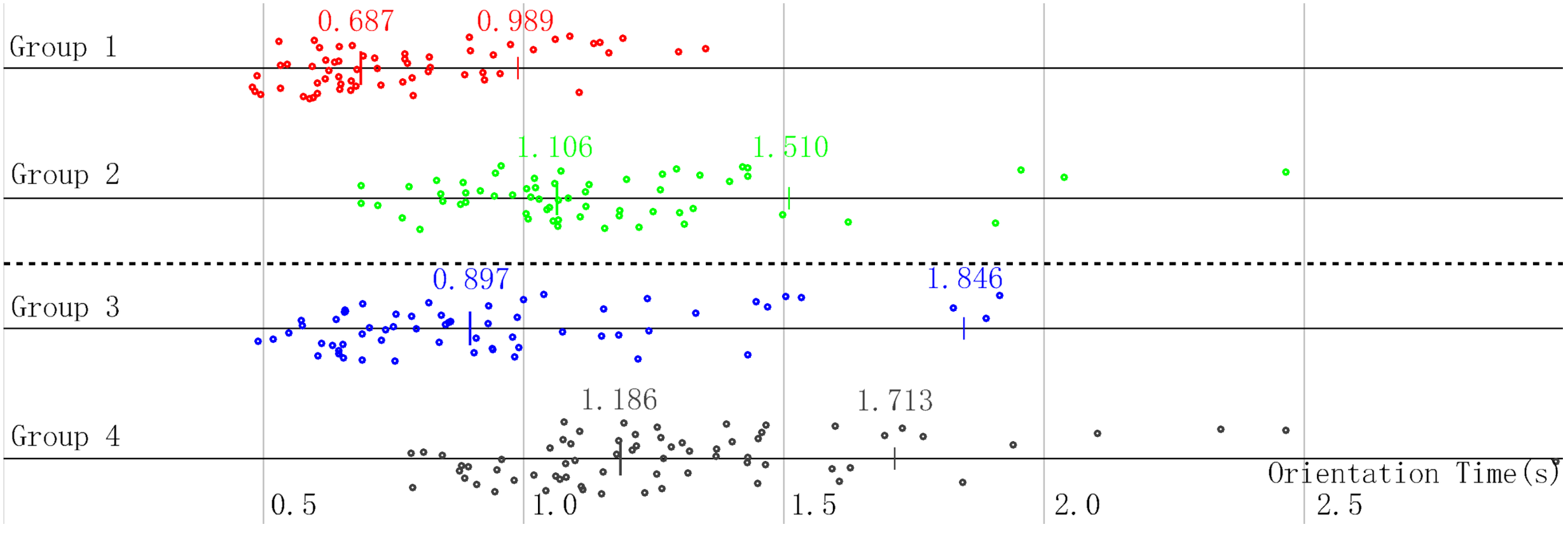
- *Guessing attack*
  - ✴ *Brute force attack*
  - ✴ *Dictionary attack*

- *Replay attack*
  - ✴ *Random numeric keypad*

可用性分析

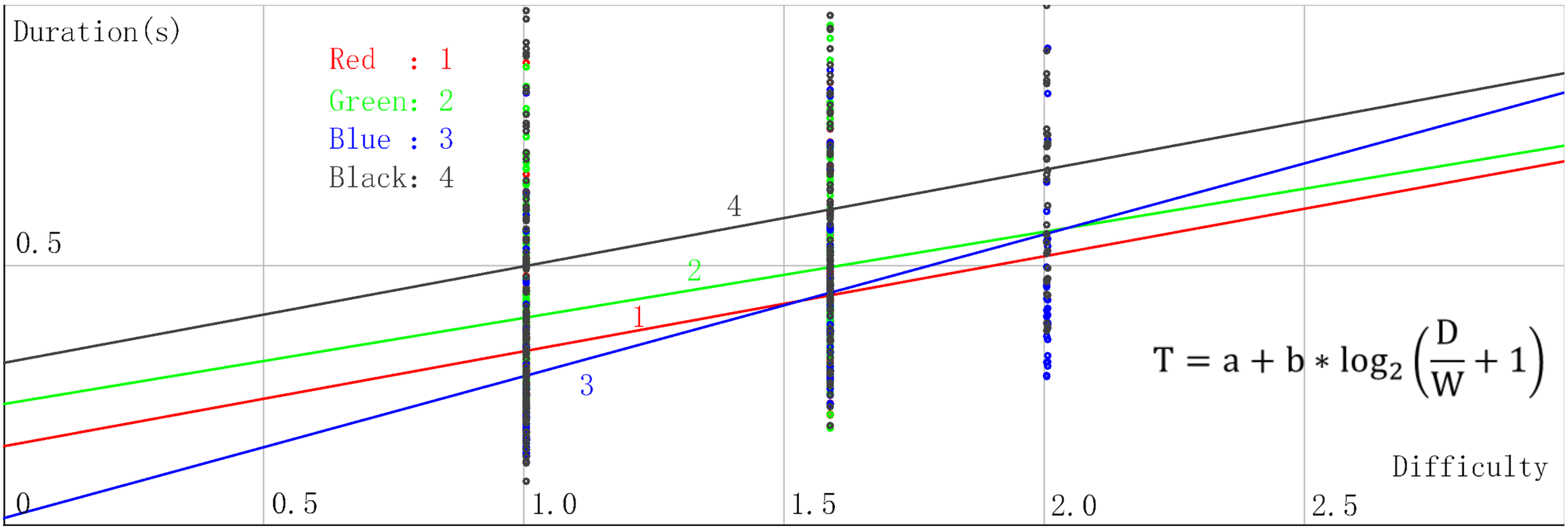
- *Orientation time*

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*



可用性分析

- *Unlock time*
  - ✴ *Sliding is faster*
  - ✴ *Input sequences become longer*
  - ✴ *Random number keypad increases unlock time*



可用性分析

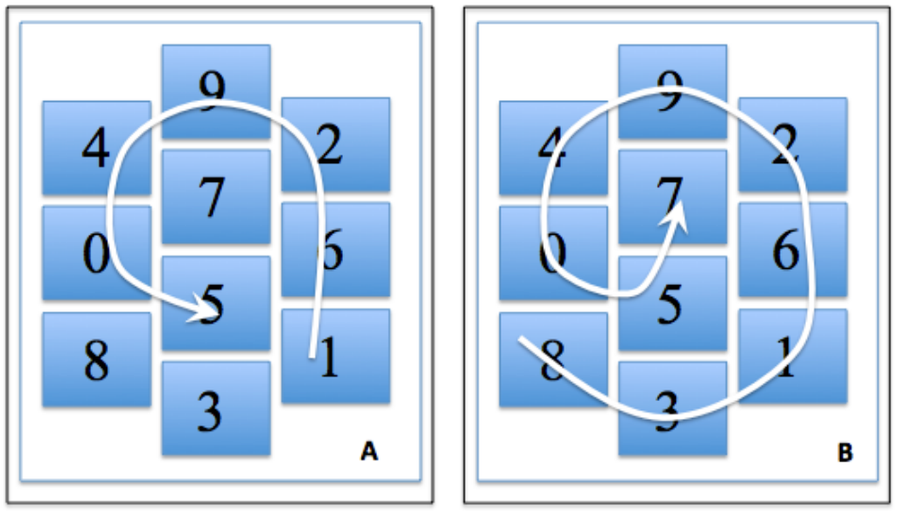
- Error rate
  - ✴ *Sequence length limit*
  - ✴ *Start point and end point*
  - ✴ *Not familiar enough*

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

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

SlidePIN

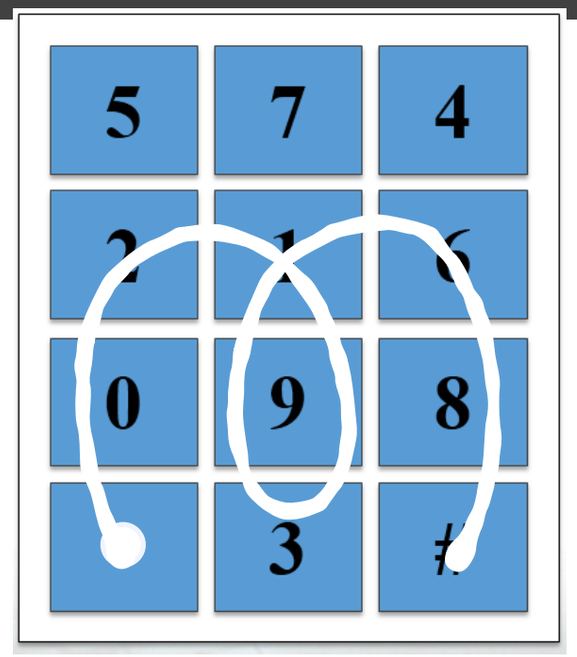
讨论



PIN: 1245

PIN: 2118

*021939168#



1: Fixed start point and end point

2: Same adjacent Digits

3: PIN storage

Device ID or SIM ID

↓

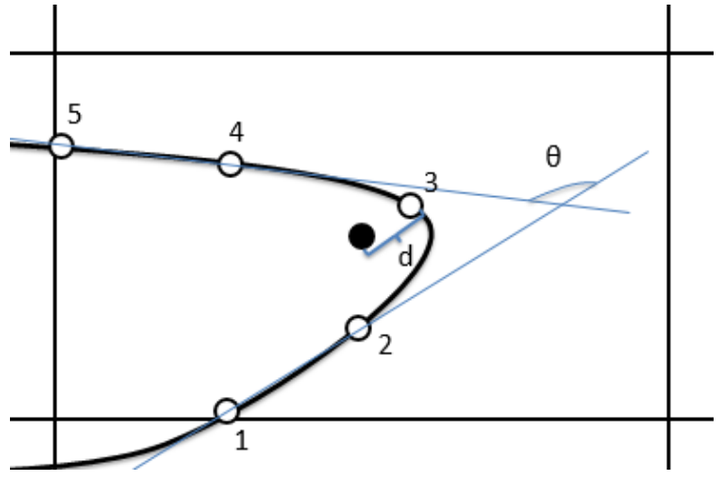
Key

↓ encrypt

PIN

4: Smudge attack

5: Attack based on Features

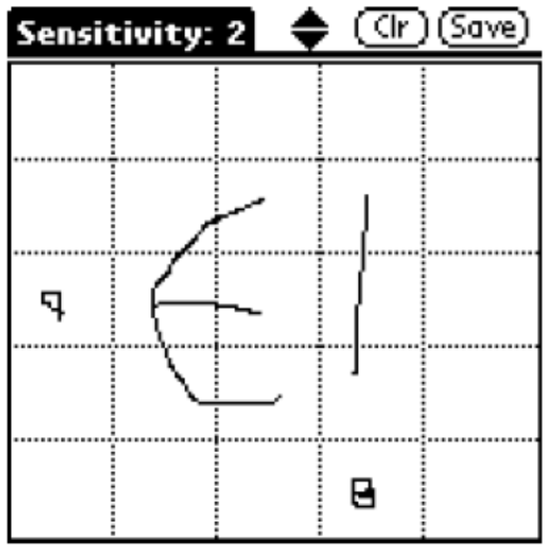


图形口令

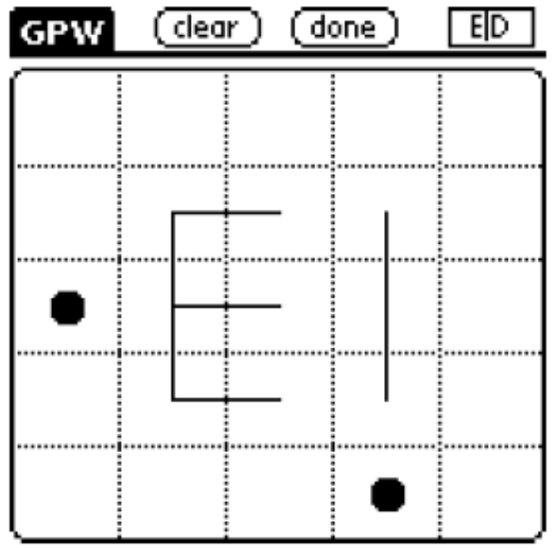
回忆、识别、线索回忆

DAS: Draw-A-Secret

对称图像
很少笔画
中心放置

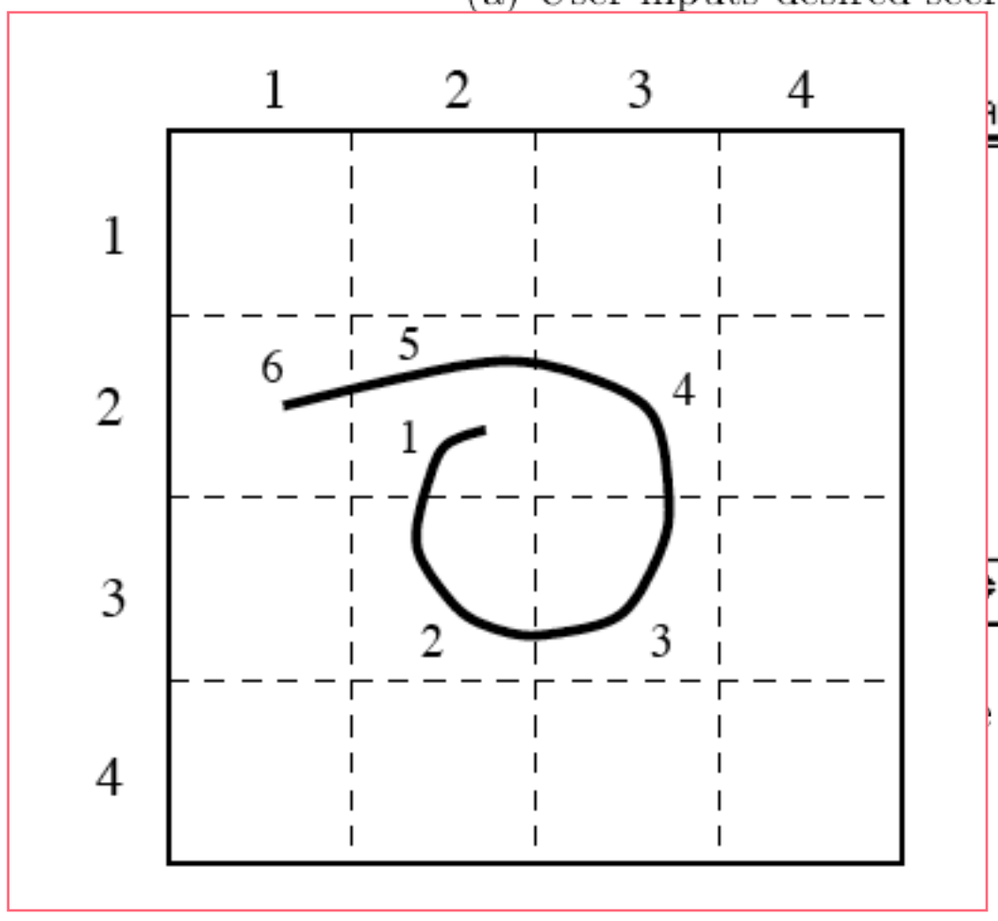


(a) User inputs desired secret

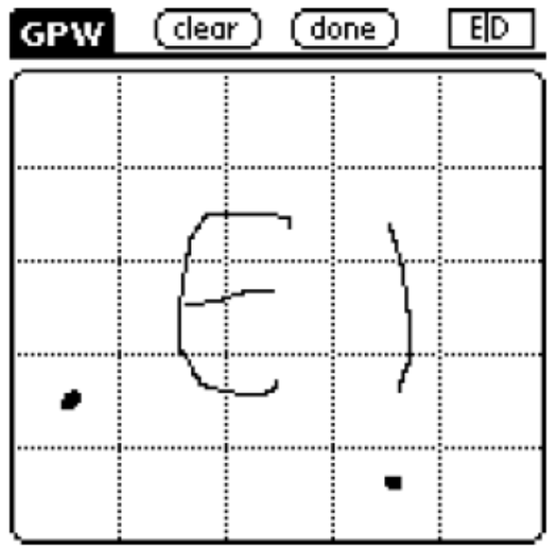


(b) Internal representation

(c) Raw bit string



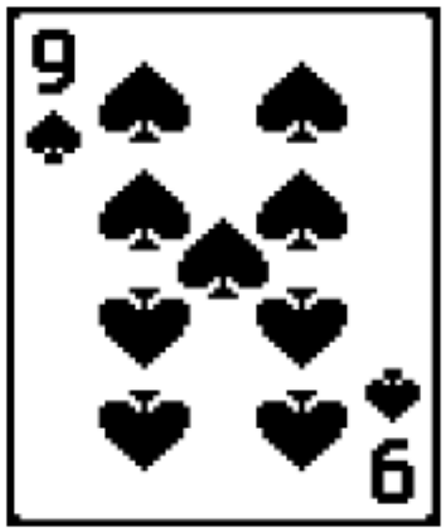
(d) Re-entry of (correct) secret

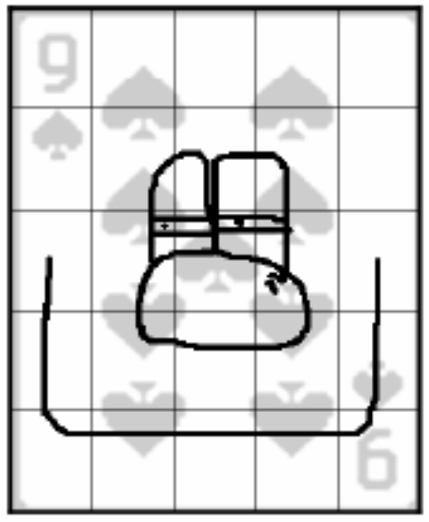


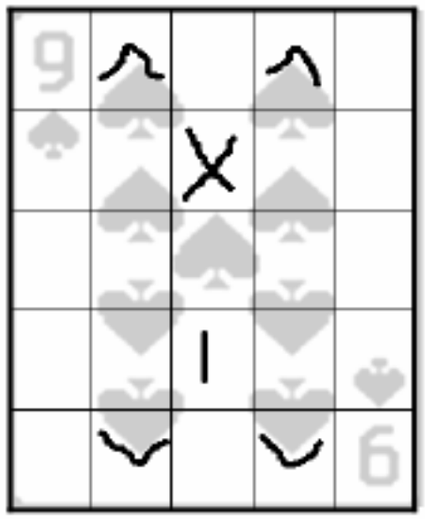
(e) Re-entry of (incorrect) secret

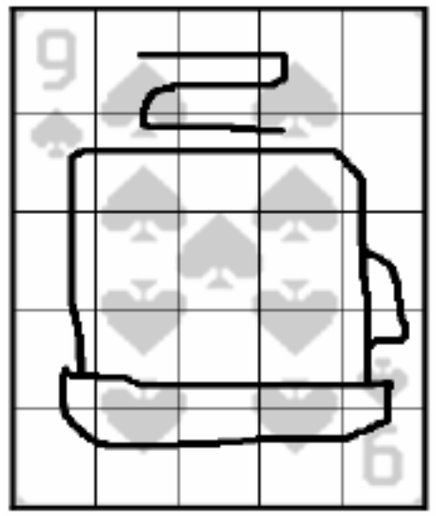
(f) Authorization failed

BDAS: Background DAS

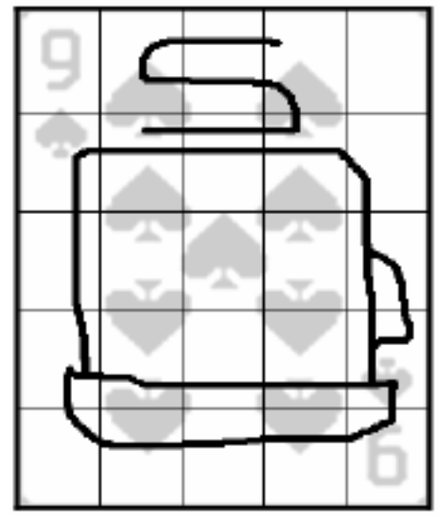




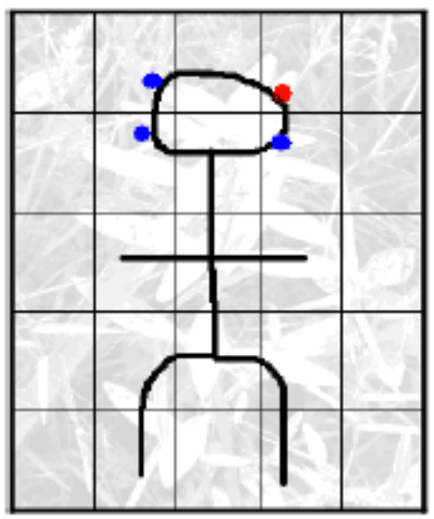


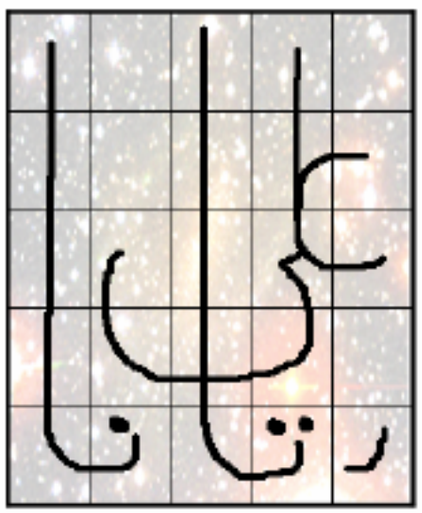


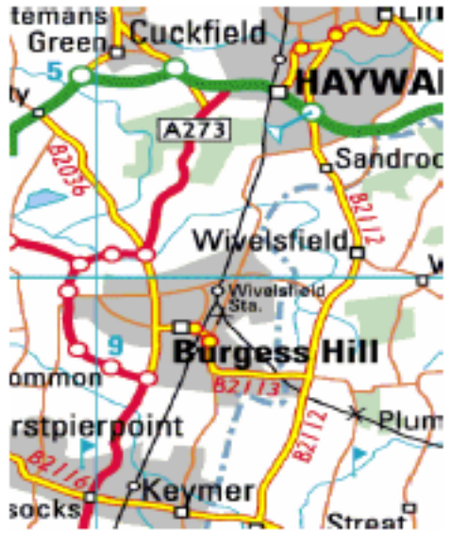
(a)



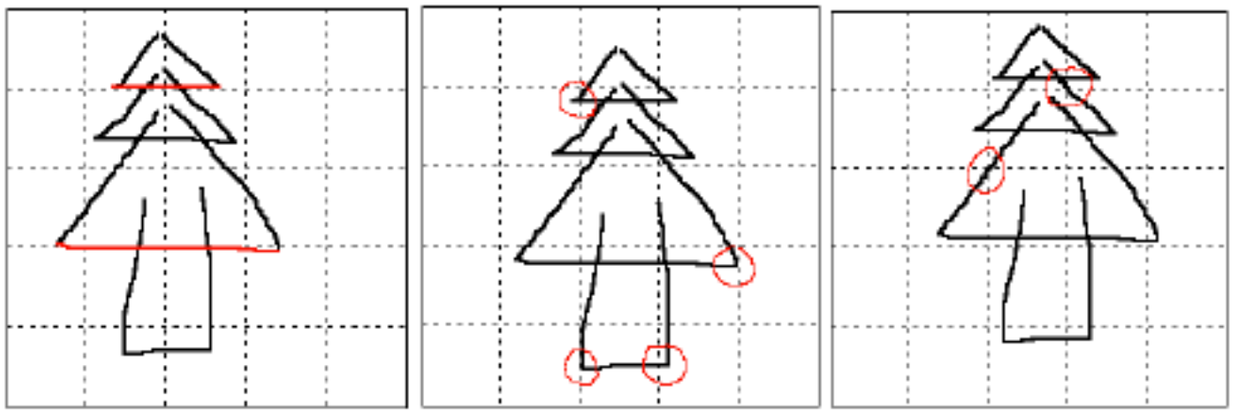
(b)





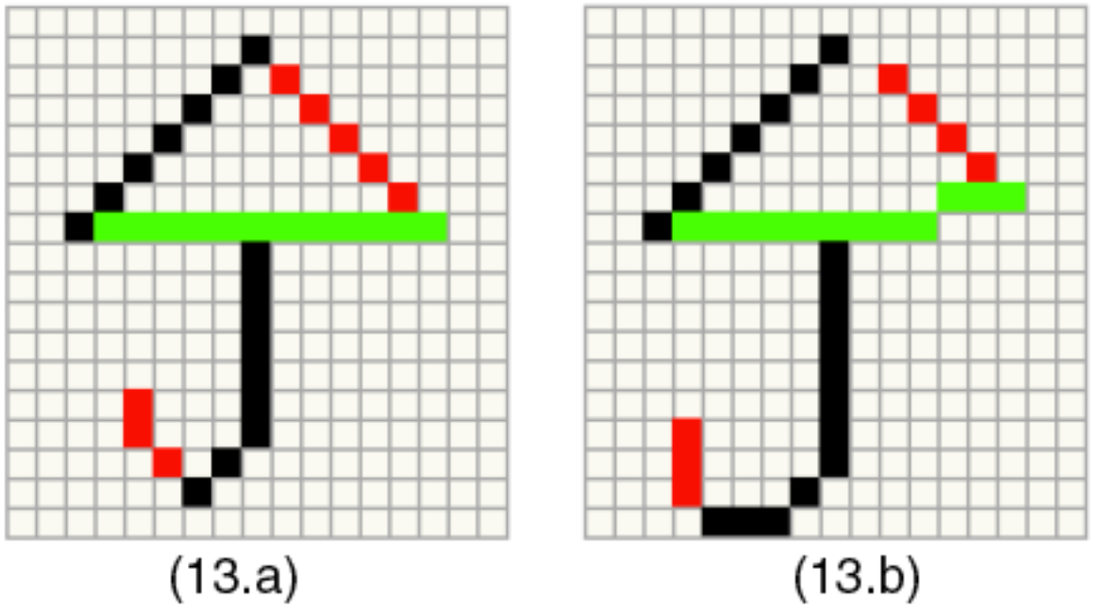


YAGP: Yet Another Graphical Password



(3.a) (3.b) (3.c)

Figure 3. Examples of rule violations in DAS. (a) Lines near grid line. (b) Endpoints near grid line. (c) Strokes near cell corner.



(13.a) (13.b)

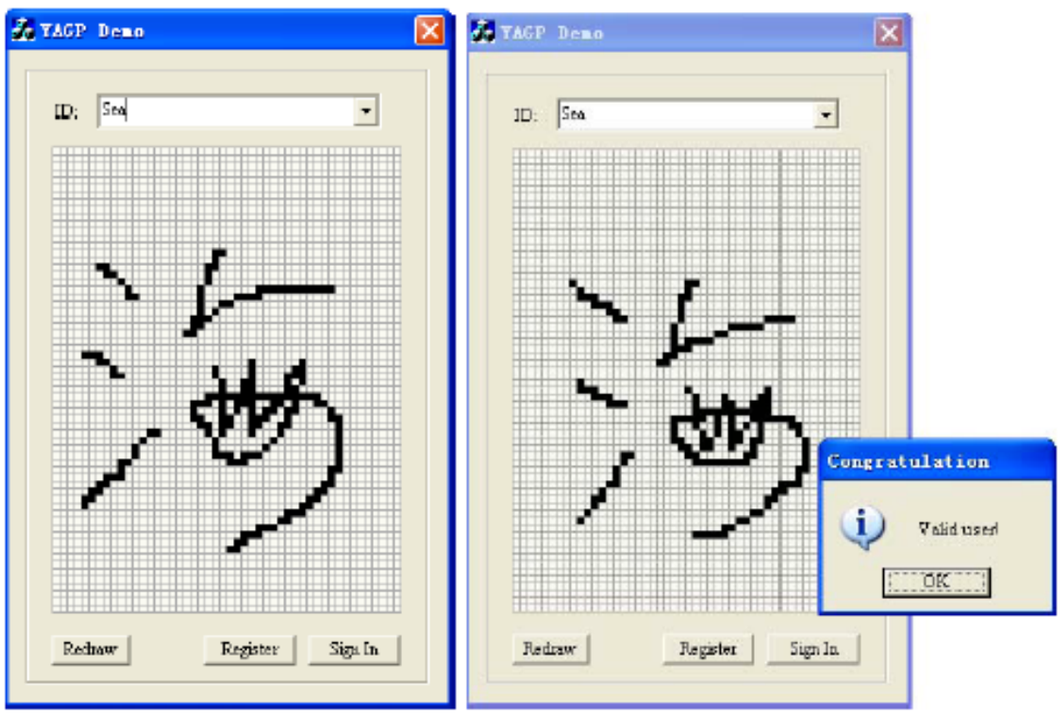
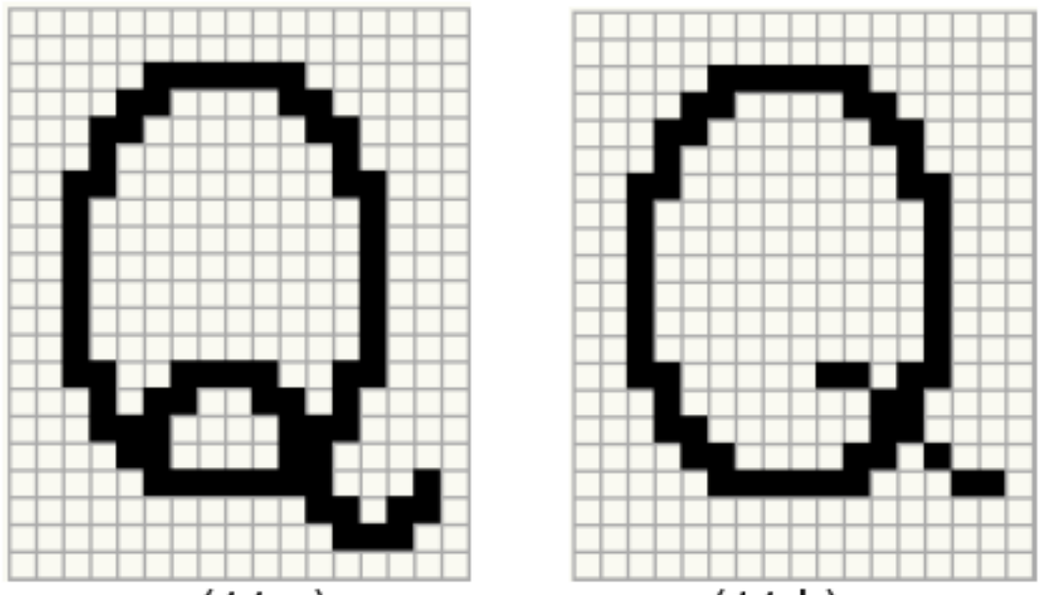
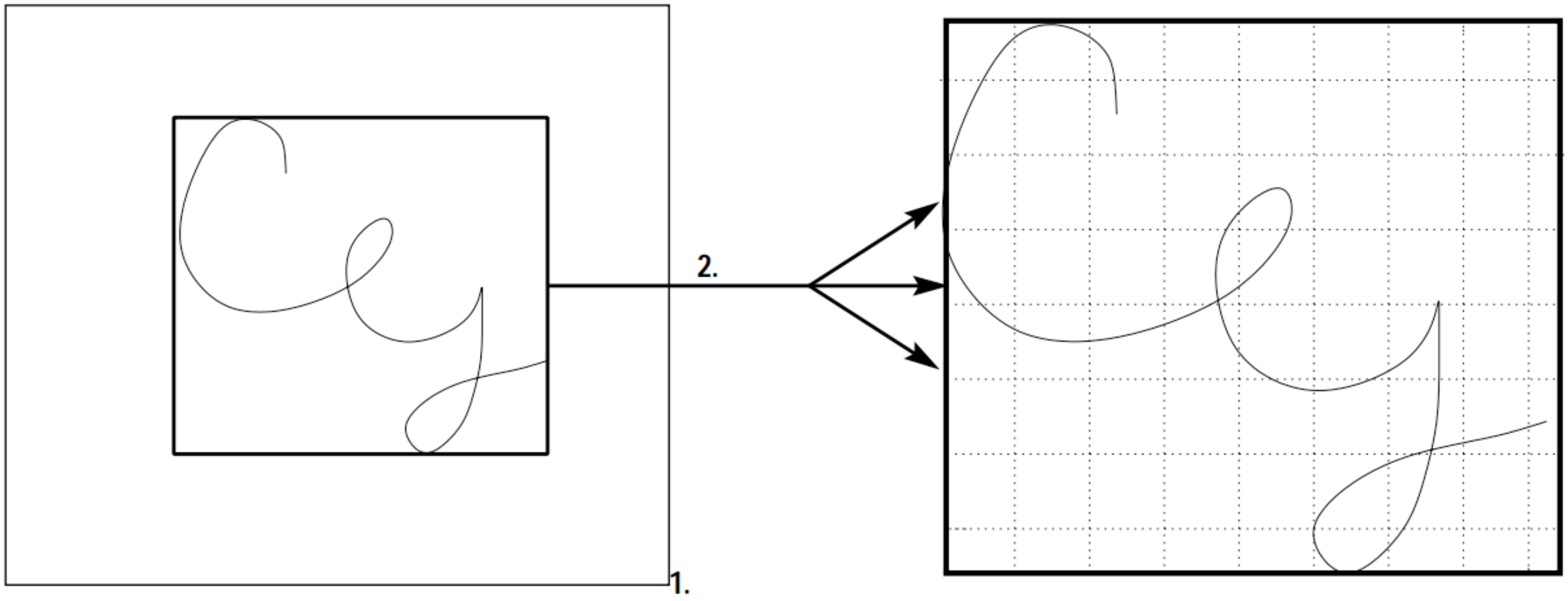


Figure 15. The YAGP system Interface (48×64 density grid).



(11.a) (11.b)

Passdoodle



1. Read mouse input
2. Scale and stretch doodle to grid
3. Analyze against stored user data
   - Compare against distribution grid
   - Measure variance of points accross distribution grid
   - Compare instantaneous speed
4. If tests confirm identify of user, authenticate, if not repeat analysis agianst other stored users.

Figure 1: An Example of a Passdoodle

PassShapes

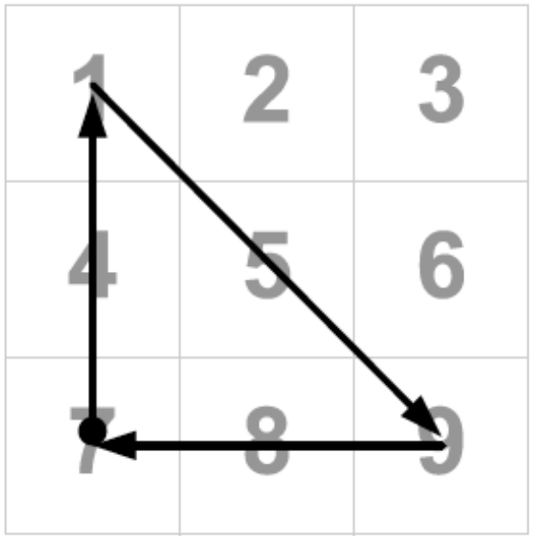


Figure 6: PassShapes and users' associations

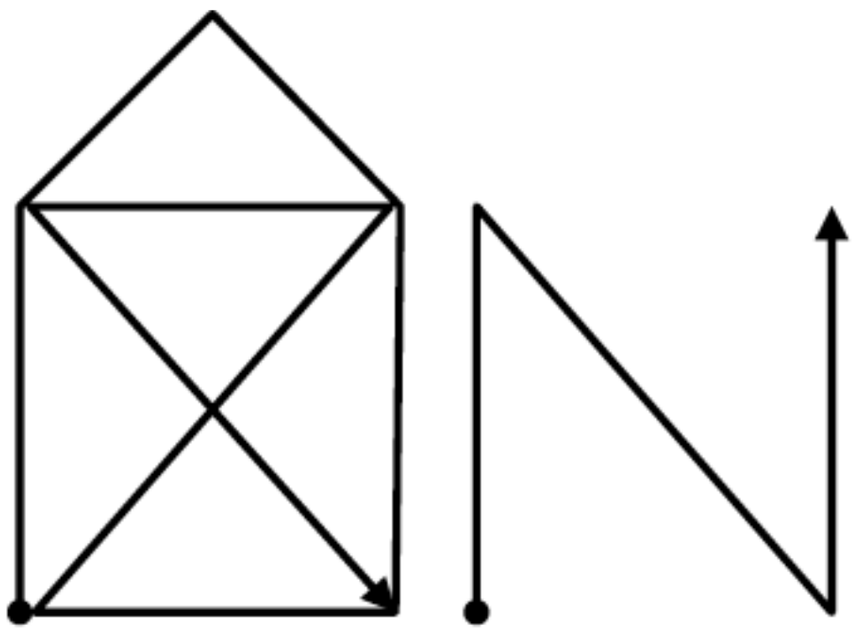
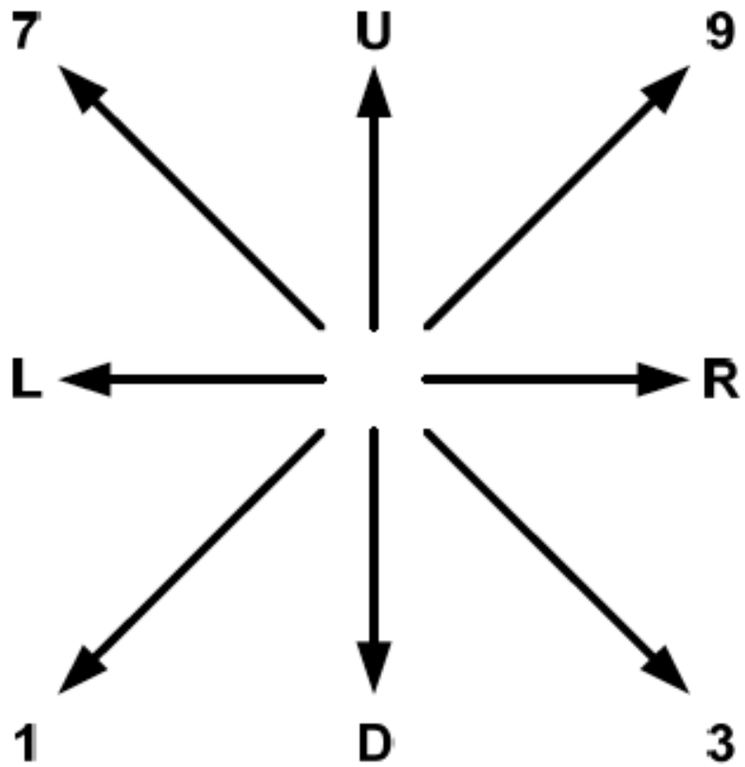


Figure 3: An example PassShape with the internal representation U93DL9L3XU3U



PassFaces

Figure 6 Passfaces™ [Passfaces 2006]

- recognise images from decoy images
- face、random art、everyday objects、icons
- challenge-response
- system side security
- 图像来源：自己 vs 系统
- 注册时间：3-5分钟
- decoy的选择
- 口令空间

Story

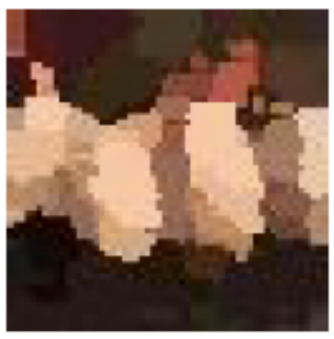
Figure 7 Story scheme [Davis et al. 2004]

- 图像之间有序
- 口令空间更大
- 记忆有负担

Use your Illusion

可用性干扰

马赛克去除技术



(a) People

(b) Shrimp dumplings

(c) Panda

(d) Battery

(a) Winnie the Pooh

(b) Wall Clock

Graphical Password

Passpoints

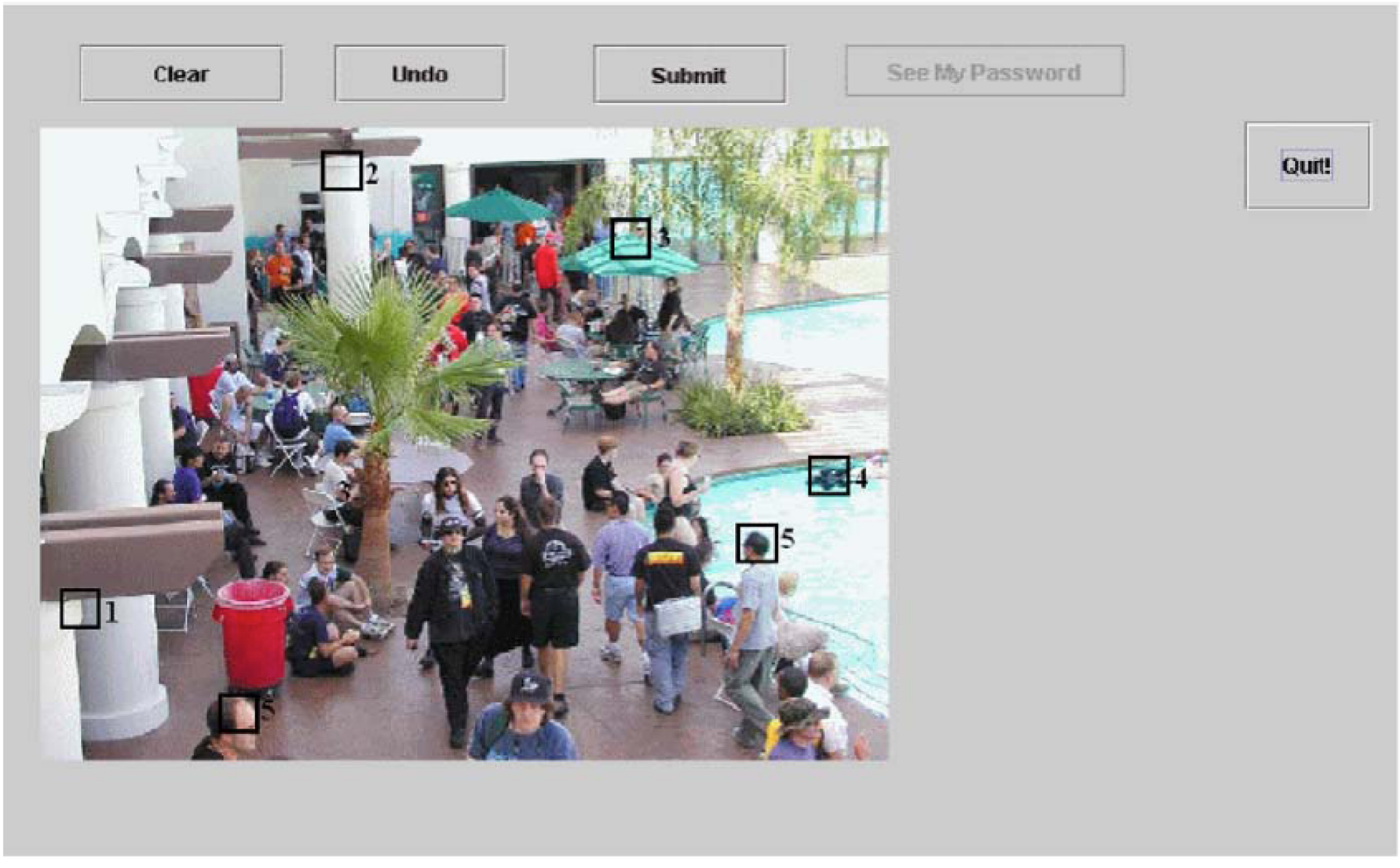


Fig. 2. Example of participant password with tolerance and click order displayed.

Figure 3 VisKey [Sfr 2006]

- 图像中的位置是秘密
- 点击输入
- 需要工具来注册
- 注册： 171秒
- login： 19秒
- 14*14像素容忍度

热点攻击

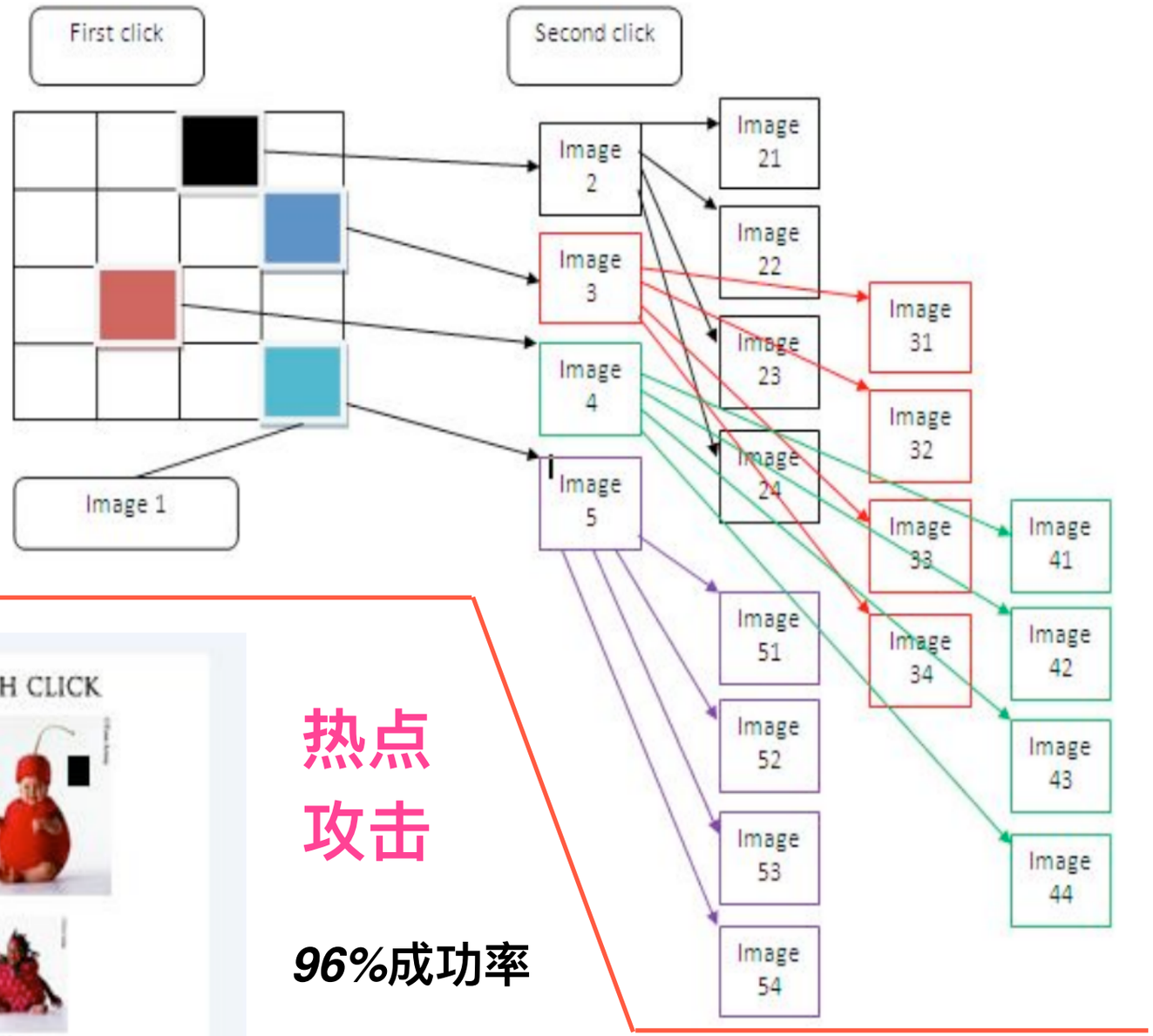
多个口令

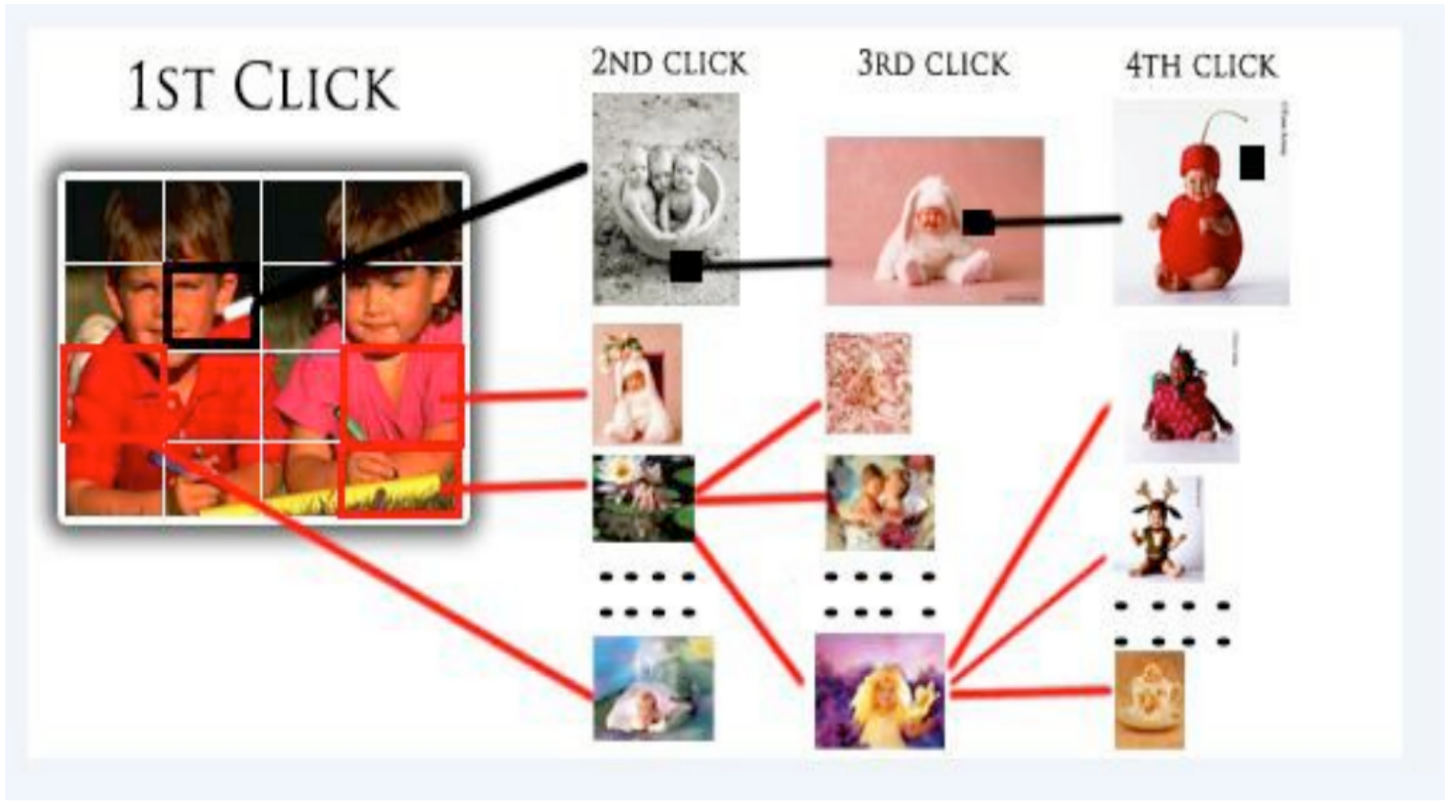
一对多

Graphical Password

CCP: Cued Click Points

- 一对一线索
- **implicit feedback**
- 避免简单模式





热点攻击

*96%*成功率

- 注册：25秒
- Login：7秒

Graphical Password

PCCP: Persuasive CCP

- viewport
- 随机化
- 避免hotspots
- 创建：50秒
- Login：8秒

图形口令评价

可用性 vs. 安全性

用户 & 环境

- 专家
- 频繁使用用户
- 不频繁使用用户
- 特殊群体

- 使用设备

➡手机、PAD、PC

➡网络、屏幕、

- 使用环境

➡高风险

➡低风险

任务

- **口令初始化**
  - ➡用户自己产生 vs 系统自动产生
  - ➡口令可预测 vs 训练时间 vs 口令重用
- **Login**
  - ➡成功率、错误率
  - ➡记忆测量、记忆干扰
- **口令改变和重置**
  - ➡不容易通信、临时的非图形口令

安全

- 猜测攻击
  - ➡在线：延迟、次数、锁定
  - ➡离线：hash、salting、
  - ➡图形口令：checker
  - ➡暴力攻击：彩虹表
  - ➡字典攻击：face、hotspot
- 俘获攻击
  - ➡肩窥攻击
  - ➡交叉攻击
  - ➡污渍攻击
  - ➡个性化攻击

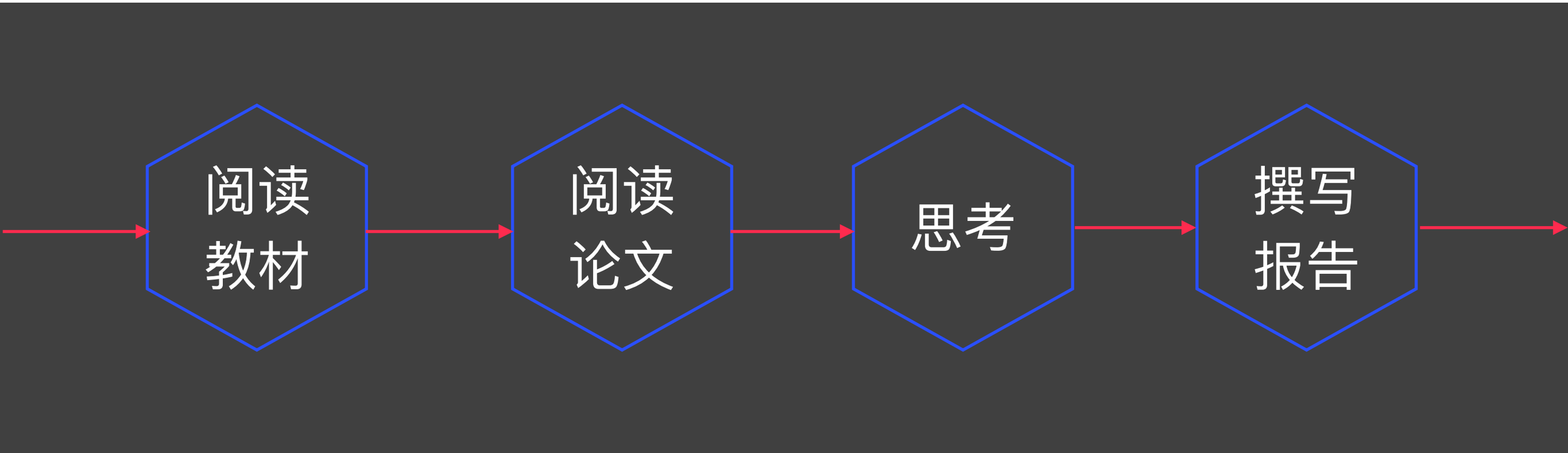
Methodology of Evaluation

评估方法

- 专家评估 vs 用户实验 vs 实际使用
- 使用文本口令作为参照
- lab study vs field study
- 问卷、访谈
- 实验人数
- 多个session
- 基于Web：Amazon Mechanical Turk
- IRB：伦理审查
- 盲试

提问时间！

课后作业



Homework

课后作业

要求阅读如下文章，写阅读报告

Double Patterns: A Usable Solution to Increase the Security of Android Unlock Patterns*

Timothy J. Forman
U.S. Naval Academy
tforman37@gmail.com

Adam J. Aviv
The George Washington University
aaviv@gwu.edu

ACSAC'2020

https://www.acsac.org

检索一篇该论文相关的2018以后的论文，简单阅读

1、文章概述
2、主要收获
3、存在疑问
4、所思所感
5、一篇论文

周日晚上12点前提交

论文报告

- 论文分享
  - ➡ 11月4日开始
  - ➡ 每次课20分钟，4位同学分享，每人5分钟
  - ➡ 要求3张ppt，每张最好一张图，字要少
  - ➡ 同学们每个人打分，打分规则和网站课上通知
  - ➡ 论文可以是上周完成论文，也可以是其余论文
  - ➡ 报告时间不能超时，到点结束

谢谢！

Huiping Sun

sunhp@ss.pku.edu.cn

https://huipingsun.github.io