

# 基于Emoji的身份验证

黄瑞瑶、许泽昊、郭知娇、刘亚楠

# 汇报内容

- Emoji身份验证的研究现状
- 类似4PIN的emoji安全性分析
- 基于EmojiStory的emoji身份验证

# Emoji口令的研究现状

- 针对屏幕锁的移动认证方式

基于知识的身份验证机制（Android手机上的PIN、密码（password）和解锁模式）

生物特征认证方法（指纹识别（苹果的TouchID）和人脸识别（主要用在Android设备上））

- 使用表情符号（emoji）进行身份认证

积极的用户体验：能够在书面文本中表达情绪、情感和细微差别。

强记忆性：表情符号密码可以通过构建故事（类似于记忆短语），有助于提高记忆能力。

理论密码空间高：在安全性方面，大量可用的表情符号（目前超过1200）导致理论密码空间很大。

## 使用表情符号（emoji）->身份认证

- 需求

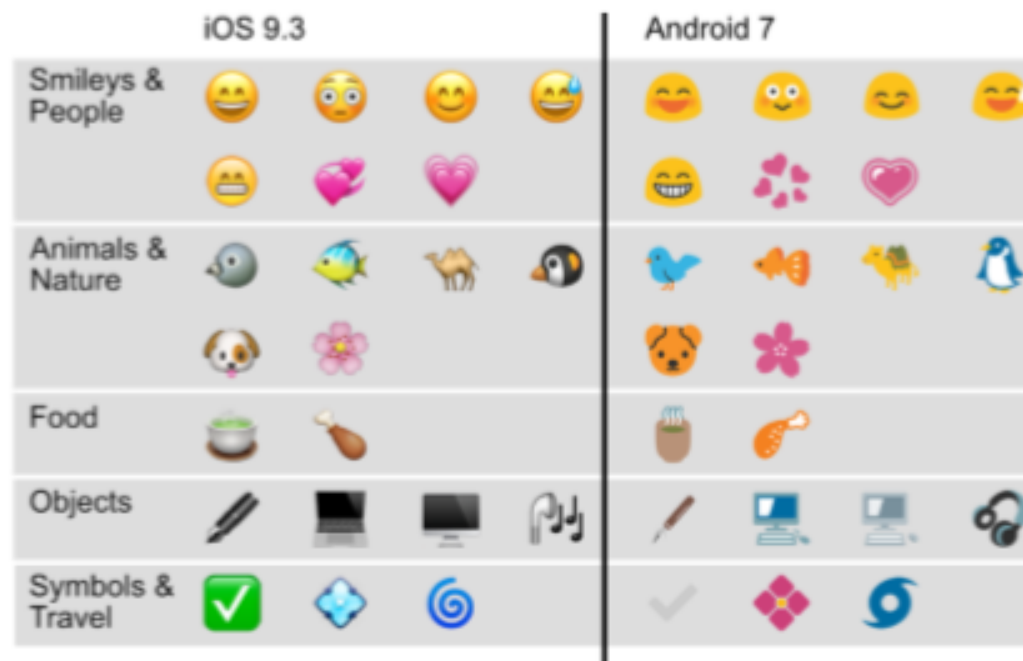
短时间登录：移动环境中的身份验证时间应尽量短暂，即不能超过PIN登录时间

用户选择弹性：提出了一种基于图标的计算机身份验证方案。密码输入的用户界面显示了来自15个不同类别的图标（类似于表情符号）。

绘制不同类别的可用图标是为了减少热点问题

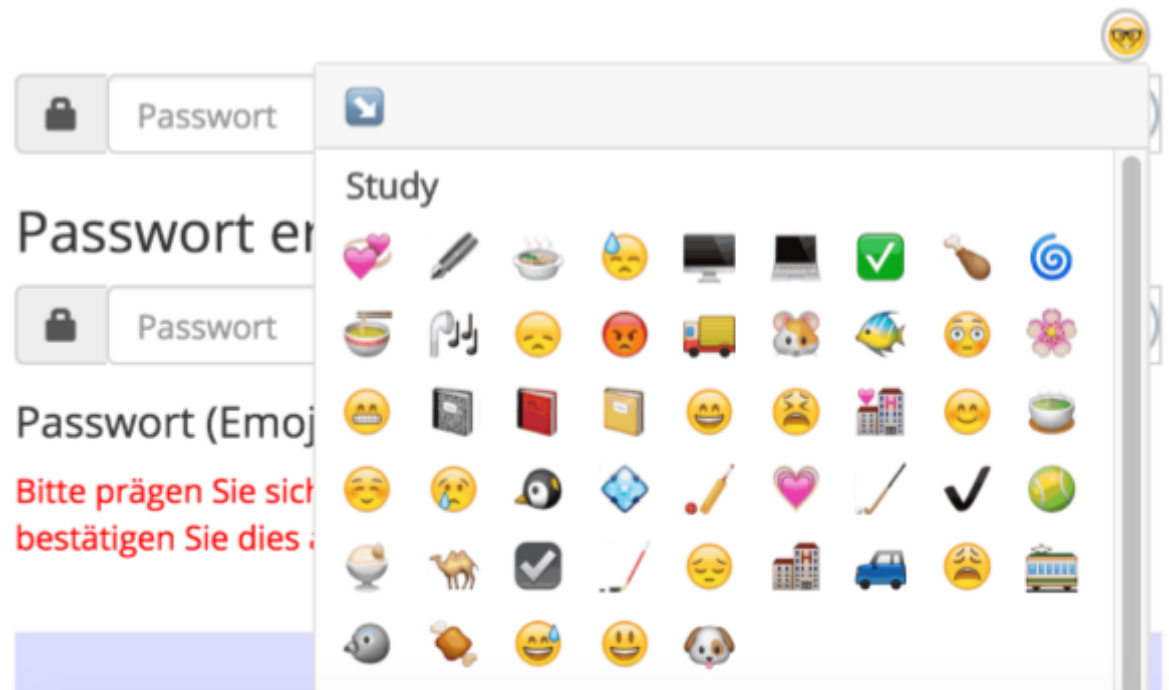
- 现实挑战

在不同的平台上，可能会安装不同的表情符号字体，因此表情符号在不同的设备和操作系统上看起来可能不同。这给实现带来了许多挑战。






# Emoji Picker

从图形用户界面中选择可用的emojis（n=50）。右上角的按钮会显示对话框。每次都会对顺序进行更新





Das Passwort muss:

- mindestens 1 Emoji beinhalten,
- und eine Mindestlänge von 8 zusätzlichen Zeichen aufweisen (8/8).

Passwort erneut eingeben:

Passwort (Emojis):

Bitte prägen Sie sich Ihr Passwort mithilfe dieser Klartextausgabe ein und bestätigen Sie dies anschließend, indem Sie das Häkchen setzen:

My  isNotA 

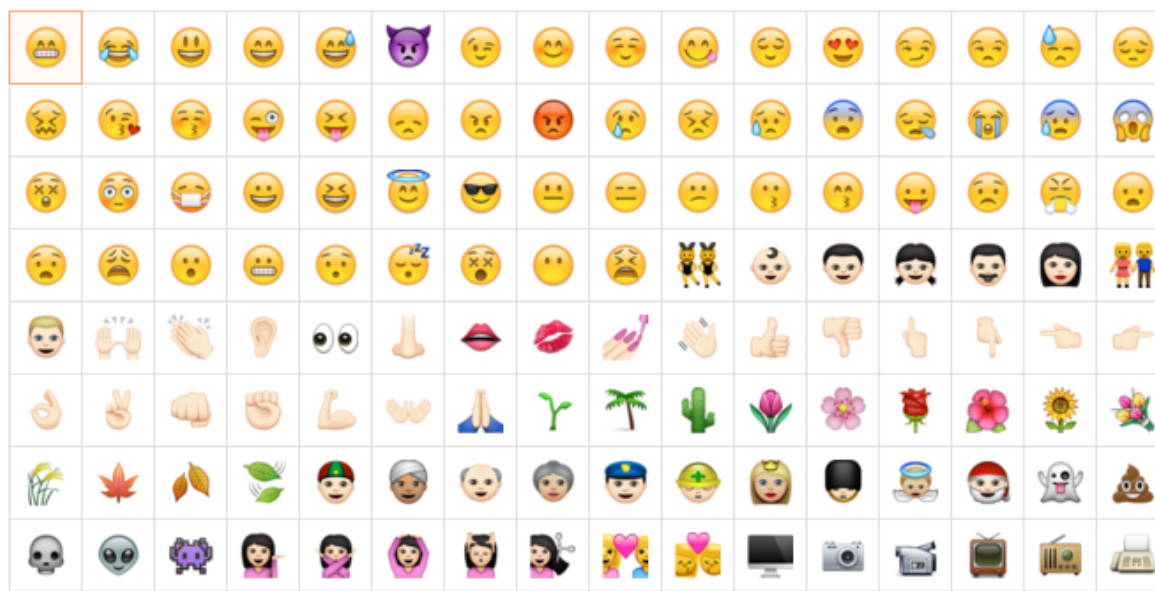
## 密码选择用户界面

绿色文本：具有实时反馈的策略通知用户已经满足哪些标准。需要重新输入密码才能排除错误。

红色文本：要求用户确认他们已经记住了他们的密码。

## 使用emoji进行身份认证的优势

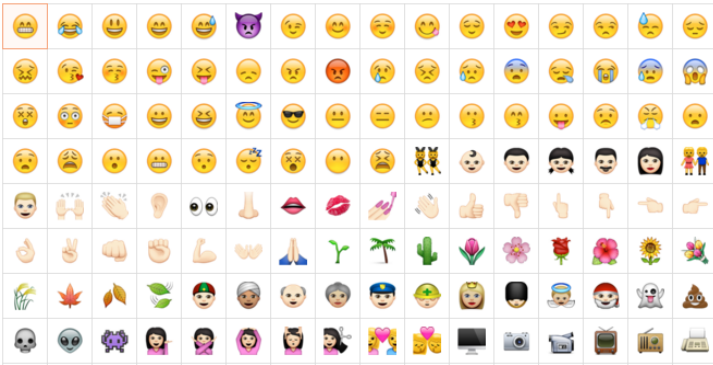
- 提供了基于文本的交流的方法，使人们能够在书面文本中表达情绪和情感。即使没有文字，表情符号也能传达意义。一个可以表达喜悦或幸福，一个悲伤的脸悲伤或忧伤。
- 无论表情符号的数量有多大，理论上的密码空间都会随着每个表情符号的增加而增加。
- 与字母数字密码相比，图形更容易记住。表情符号密码可以利用小故事。构建故事(类似于记忆短语)有助于提高记忆能力。
- 在安全性方面，大量可用的表情符号(目前超过1200)导致理论密码空间很大。



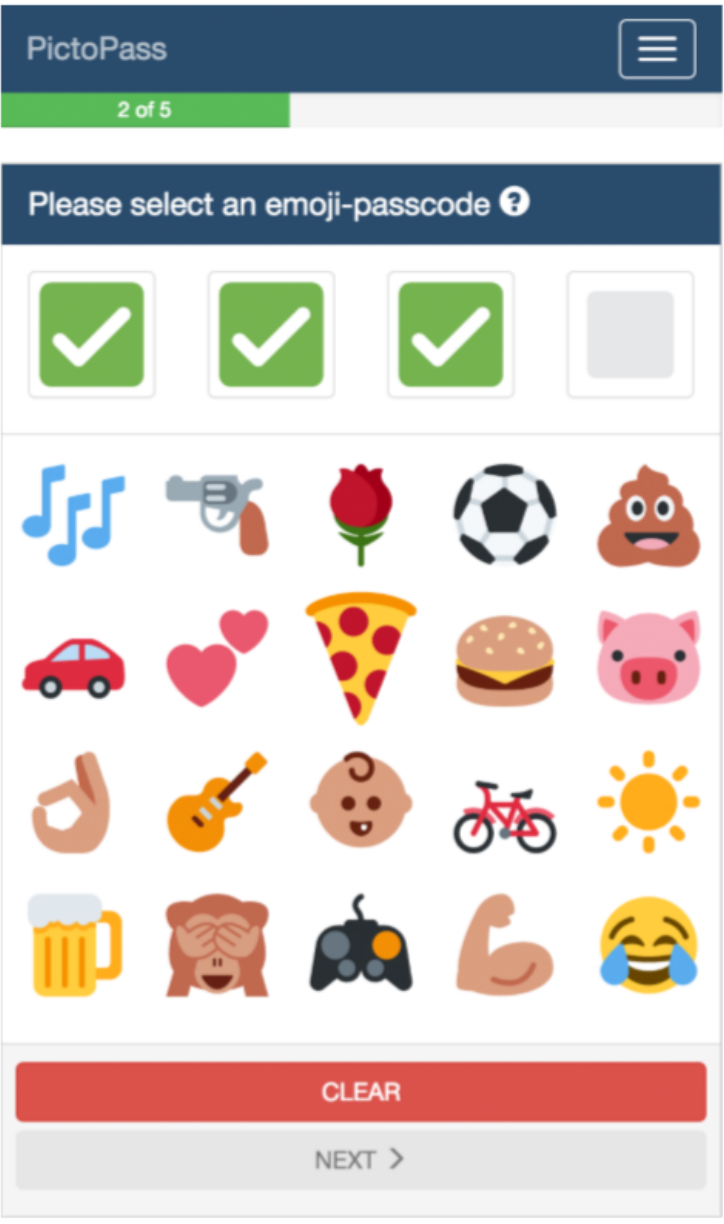
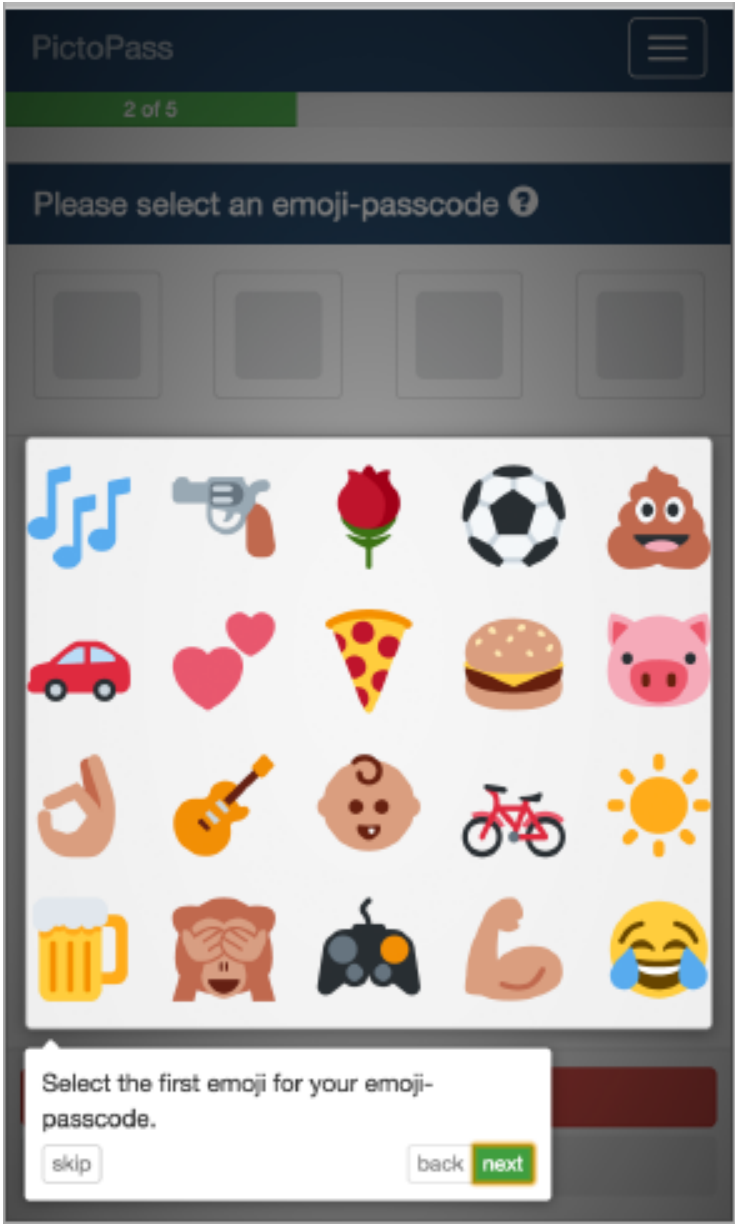


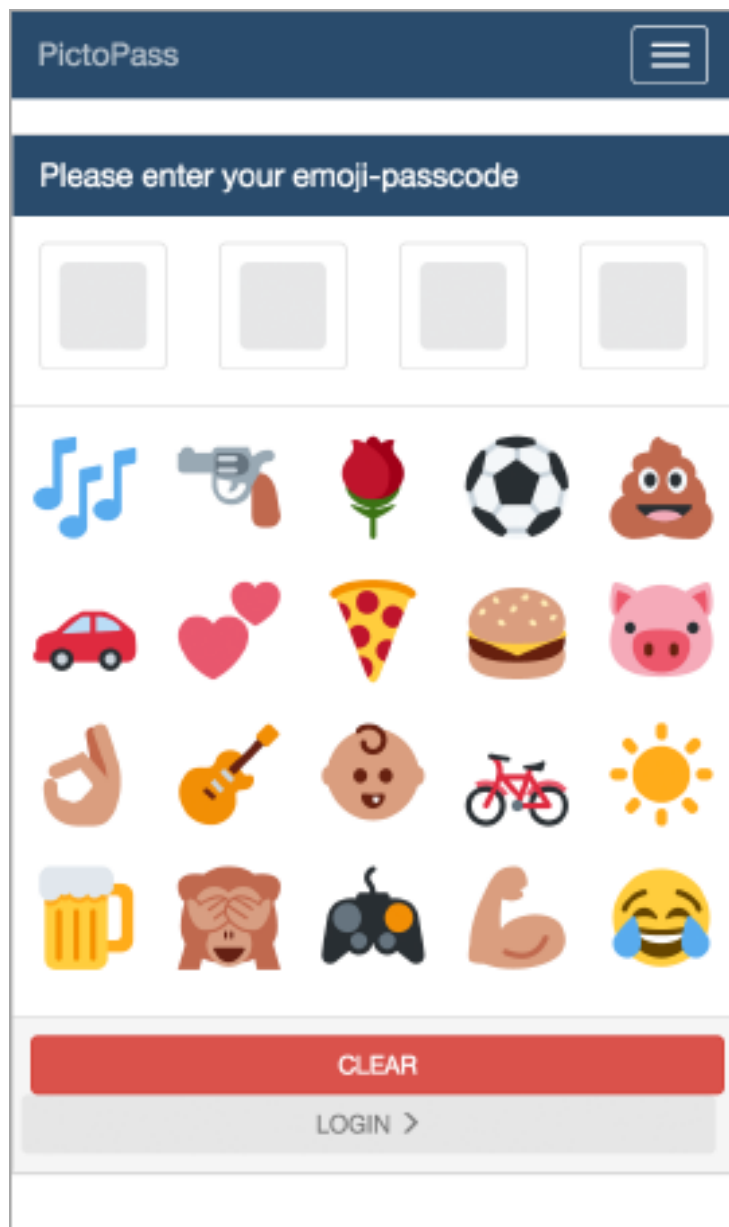
## Emoji身份验证的可用性

- 移动平台中的身份验证时间应尽量短暂，即不能超过PIN登录时间。为表情符号固定键盘位置是更好的，因为固定位置会导致登录时间更短。
- 要输入密码，用户需要知道他们已经输入了多少位数的密码。此外，提供按下按钮的反馈的方法是可取的，因为它允许用户注意错误，并在必要时纠正它们。



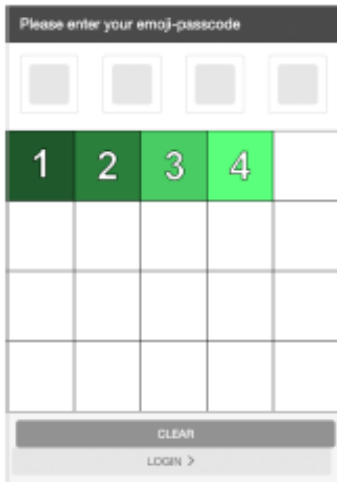
# 类似4PIN的emoji安全性分析



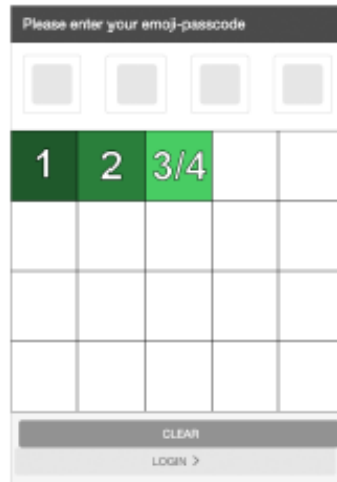


## 优点

- 1) 表情符号直观容易记忆;
- 2) 口令空间比PIN大;
- 3) 适合触摸屏使用;
- 4) 更好的抵抗猜测攻击的能力。



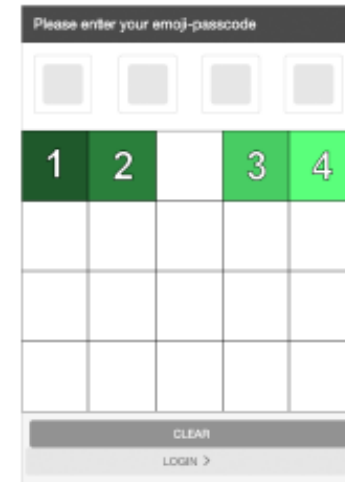
(a) Position 1



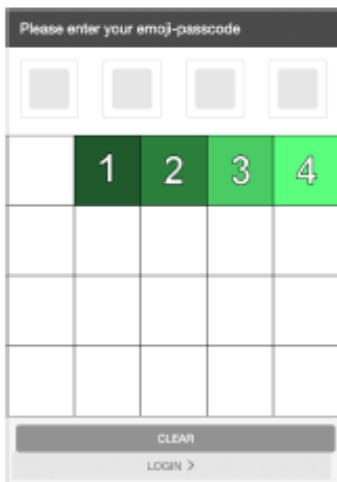
(b) Position 2



(c) Position 3



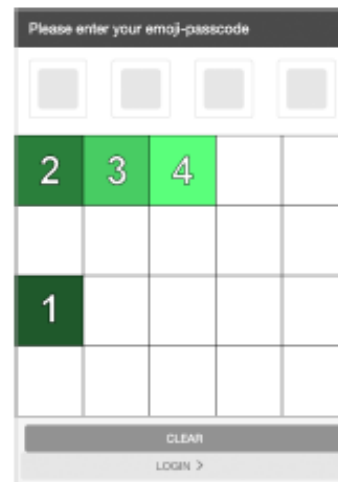
(d) Position 4



(e) Position 5



(f) Position 6

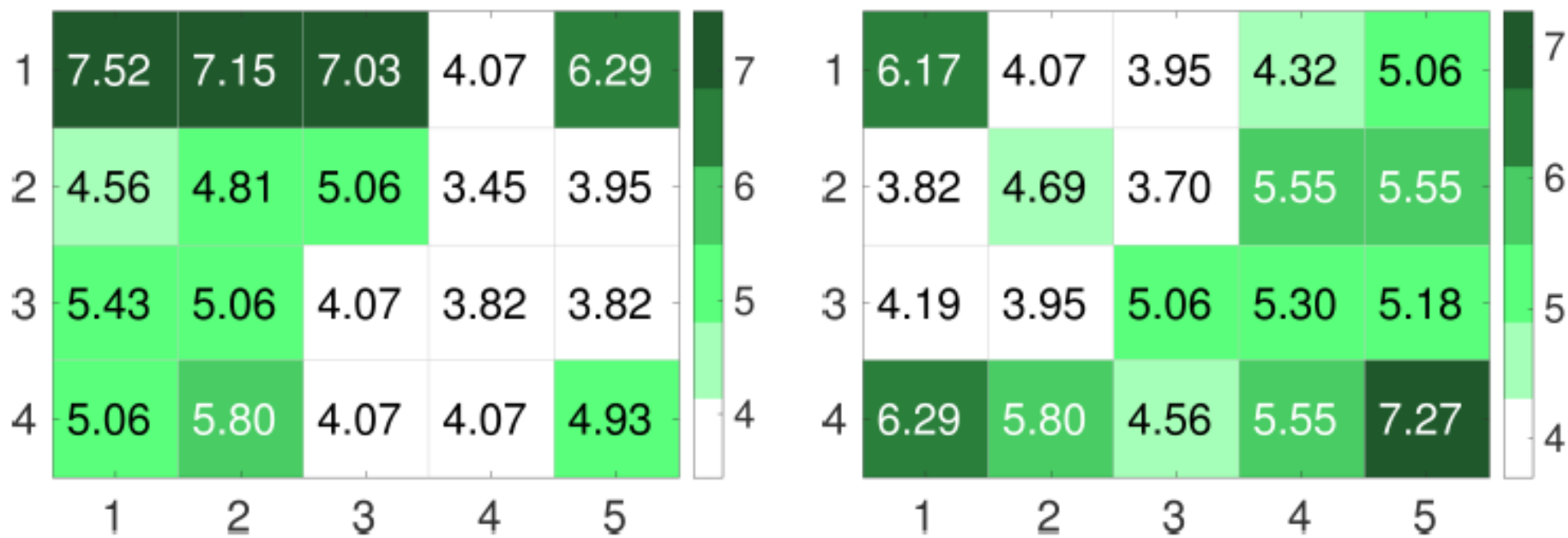


(g) Position 7

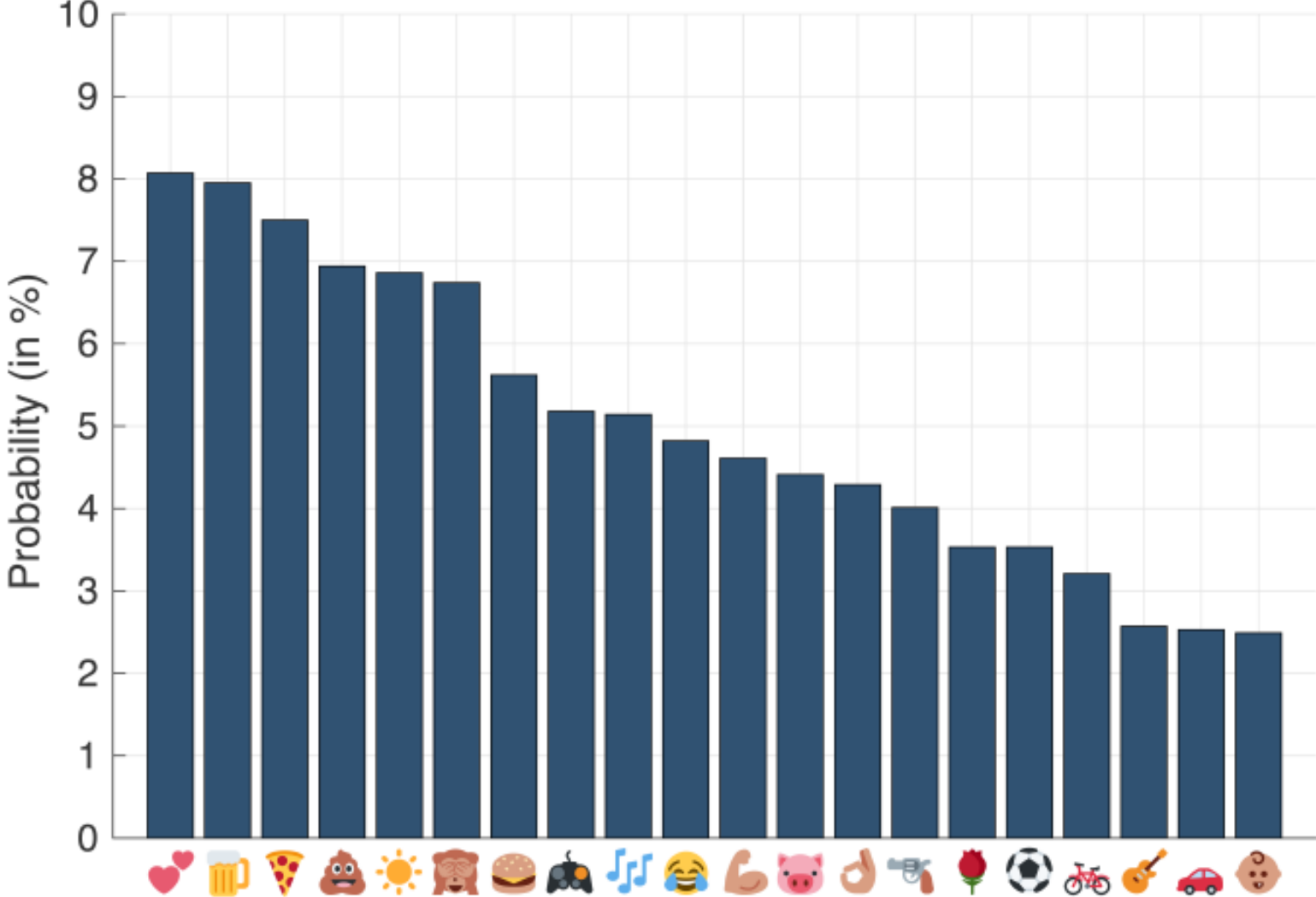


(h) Position 8

## 图形选择的开始位置和结束位置分析























# 图形选择频率分析





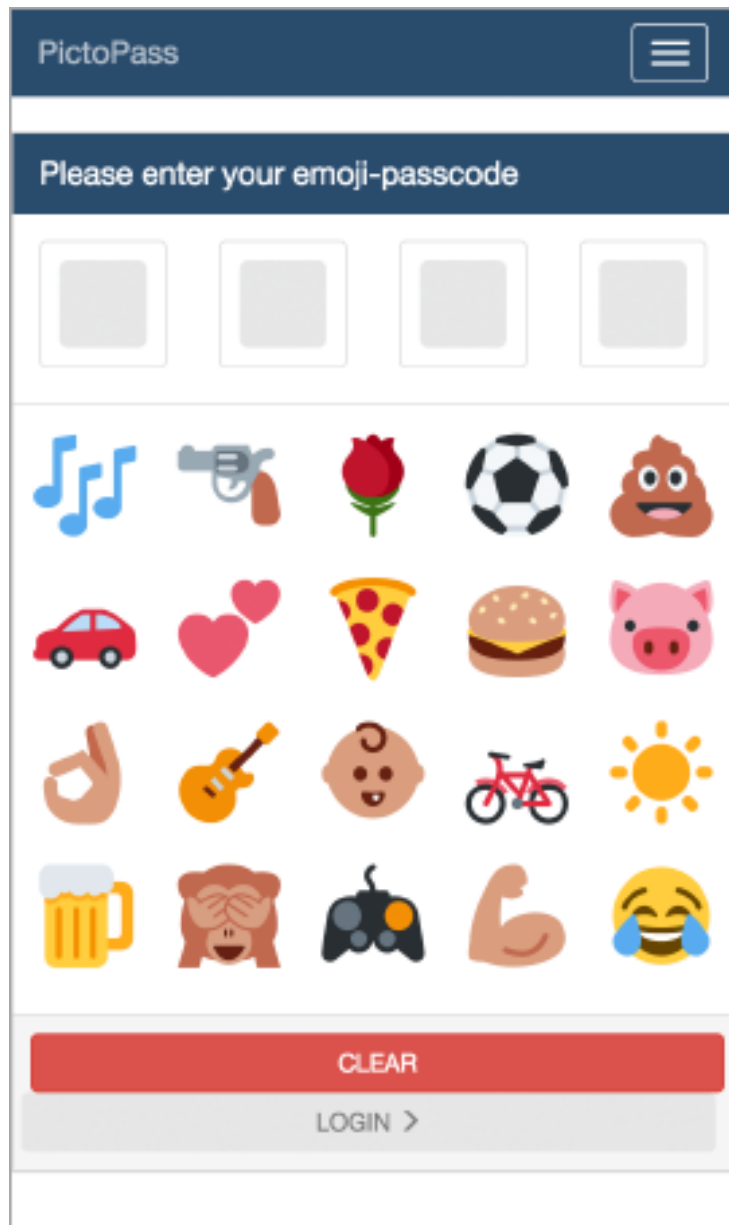


## 参与者最有可能选择的密码分析

Occ.	P1	P2	P3	P4	Prob.
4					0.64 %
3					0.48 %
2					0.32 %
2					0.32 %
2					0.32 %

passwd	count
123456789	235029
12345678	212766
11111111	76348
dearbook	46052
00000000	34953
123123123	20010
1234567890	17794
88888888	15033
111111111	6995
147258369	5966
aaaaaaaa	5890
987654321	5555
1111111111	5145
66666666	5026
a123456789	4686
11223344	4096
1qaz2wsx	3969
password	3654
xiazhili	3649
789456123	3611

!(*!!	!(()!!@
!(()!!!^	!(!@)(cloud
!((%)*)(QWtxd	!(!@)6125dou
!((%!((%	!()jian20
!((%)	!((^)^@@123123
!((!)*	!(@0709yxw
!((!())%	!(*03230225tian
!((	!()HB1990128
!(&^)^!(	!()0803
!(&^!!@&	!()@)@@@



## 缺点

- 1) 基于位置的攻击模型（左上开始右下结束）；
- 2) 基于内容的攻击（选择同类图标、A-B-A-B模式）具有感情倾向（图形选择频率），分布不均；
- 3) 肩窥攻击，弱密码等；
- 5) 混合猜测。

- 创造一个故事 (268)
- 使用他们生活中重要的东西 (234)
- 试图随机选择一个密码 (83) —— 不易记忆
- 重复我的生活 (54)
- 发短信时经常使用的表情符号 (44)
- 视觉模式：“A-B-A-B” (31) —— 位置攻击
- 网格内的位置 (19) —— 位置攻击
- 我最喜欢的表情符号 (17)
- 我觉得滑稽可笑的表情符号 (6)
- 相同颜色的表情符号 (3)
- 构建一个密码短语：“超级小猪便便” (3)
- 表情符号的第一个字母：“Baby, Ball, Beer, Burger” (3)

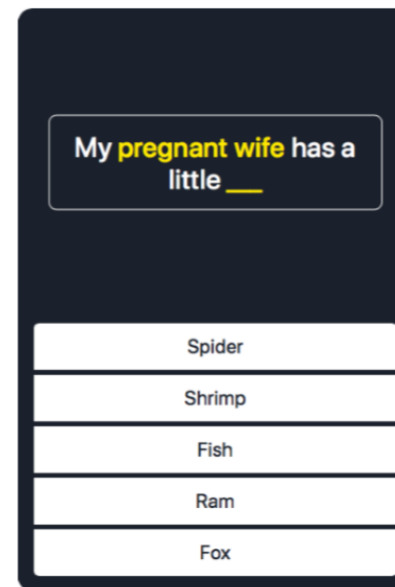
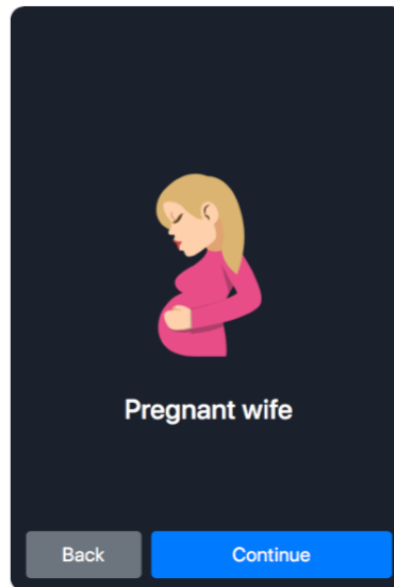
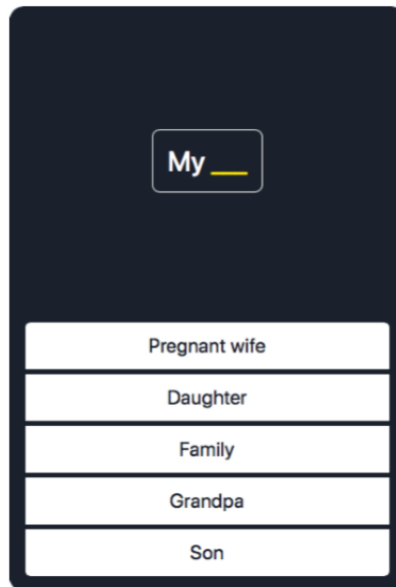
# 基于EmojiStory的身份验证

# Emoji Story

- 思路：基于故事生成口令。
  1. 在用户设置口令时加以限制，减小弱口令产生的可能性；
  2. 利用故事使口令变得容易记忆

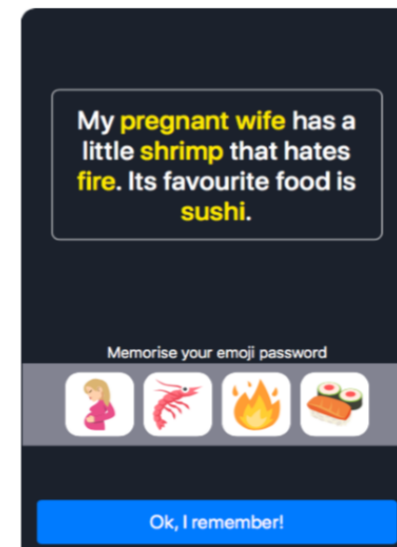
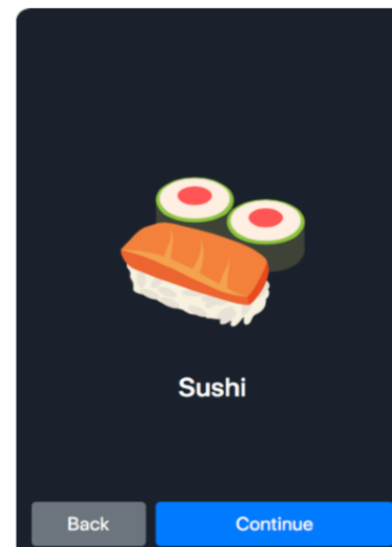
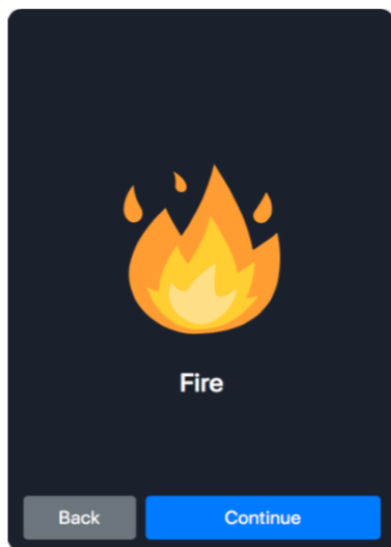
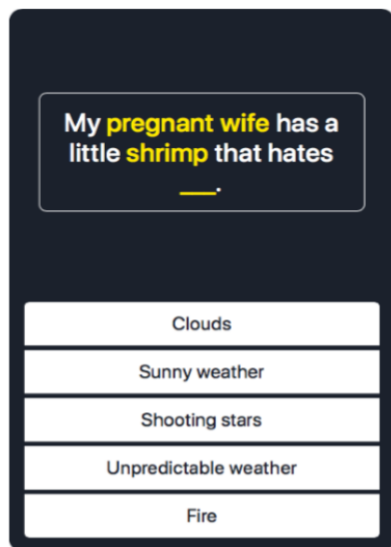
# 设置口令

- 设置包含4位emoji的口令。



# 设置口令

- 设置包含4位emoji的口令。





# 故事模板

- 随机选择故事

猜测攻击变得困难；  
故事帮助用户记忆口令。

- 故事模板创建的注意事项

同一个故事中emoji类别间  
避免关联；

所有故事中每个emoji类别  
的使用频率应尽可能平均。

- 故事模板缺陷

人工创造故事费时

The king of <country> owns a three-headed <animal> that eats <food> every day. This makes the king very <feeling>.

(a) Story 1

Jessica takes the <vehicle> to <country>. There she visits her <person>. Together, they are <activity>.

(b) Story 2

My <person> has a little <animal> that hates <weather>. Its favourite food is <food>.

(c) Story 3

The <animal> grew up <place>. After being kicked out of home, it decided to become the best <athlete> in the world. Today, it has won several <object 1>.

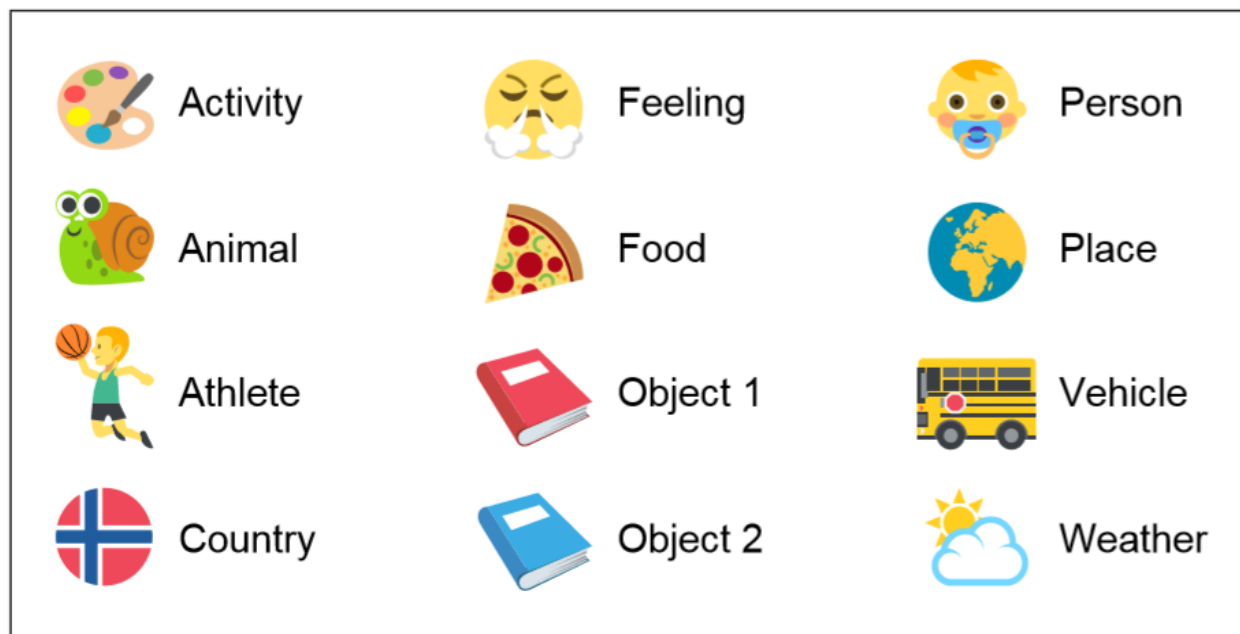
(d) Story 4

Collecting <object 2> from <country> that are made of <food> makes me feel <feeling>.

(e) Story 5

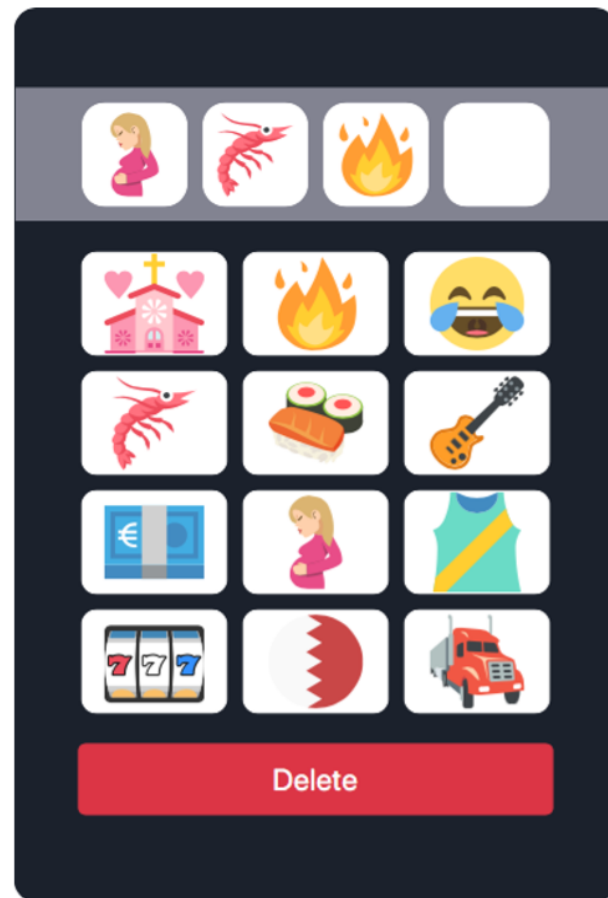
# Emoji分类

- 故事中的每个空格只能用预定义类别的emoji来填充。
- 每个类别下的emoji数量应尽可能平均。



# 登录键盘

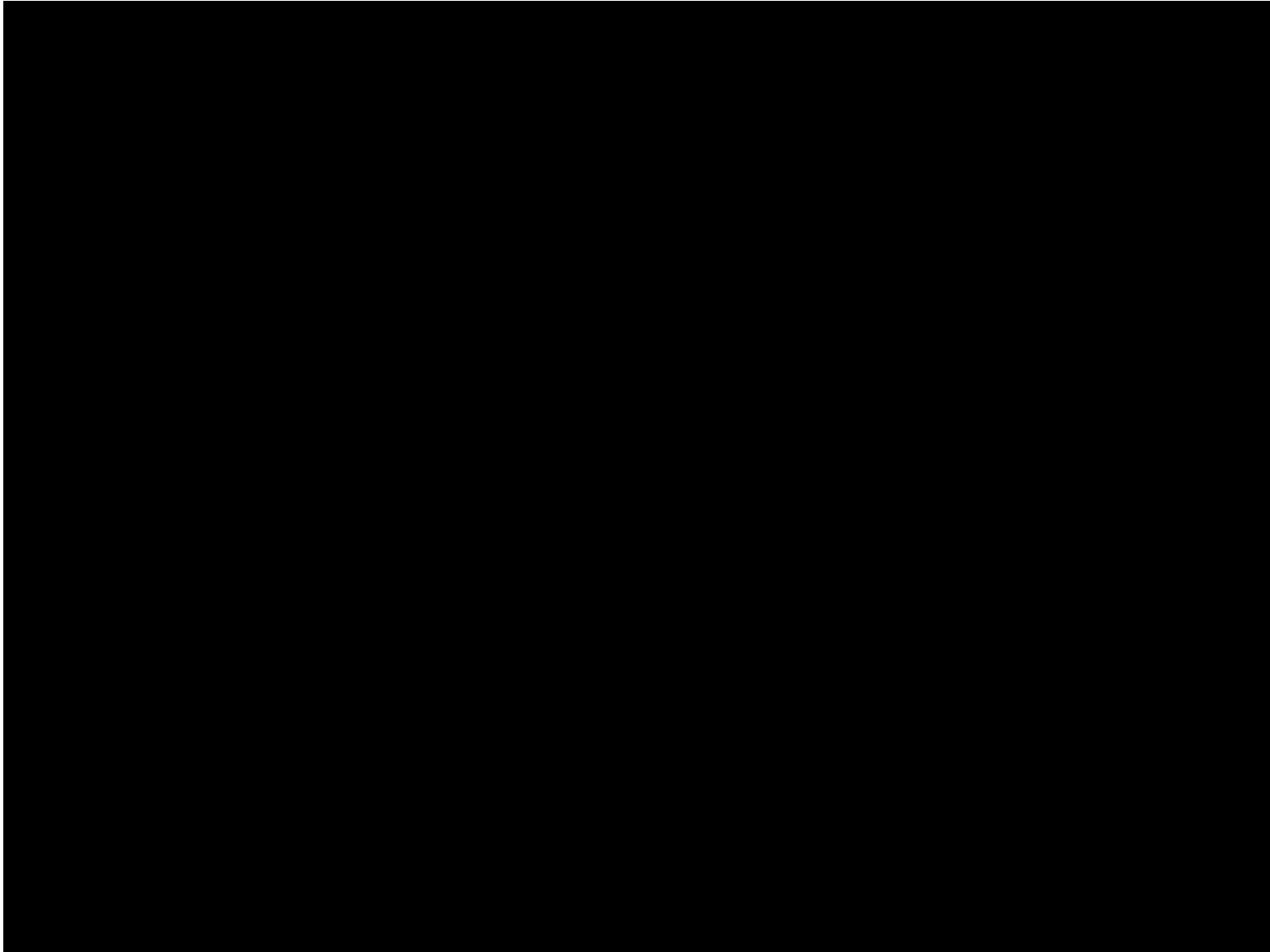
- 键盘内容不变，emoji位置改变
- 键盘内容包含不同类别的emoji，使得无法从键盘内容推测出故事内容。



# 方案评价

- 基于内容攻击  
故事模板：无同类图标、无固定模式、分布均匀
- 基于位置攻击  
登录键盘emoji随机排列
- **Brute-force**攻击  
 $16^4$
- 肩窥攻击  
抵御力较弱

Demo



谢谢！