Guessing human-chosen secrets

Joseph Bonneau
Security and Human Behavior
New York, NY, USA
June 4, 2012

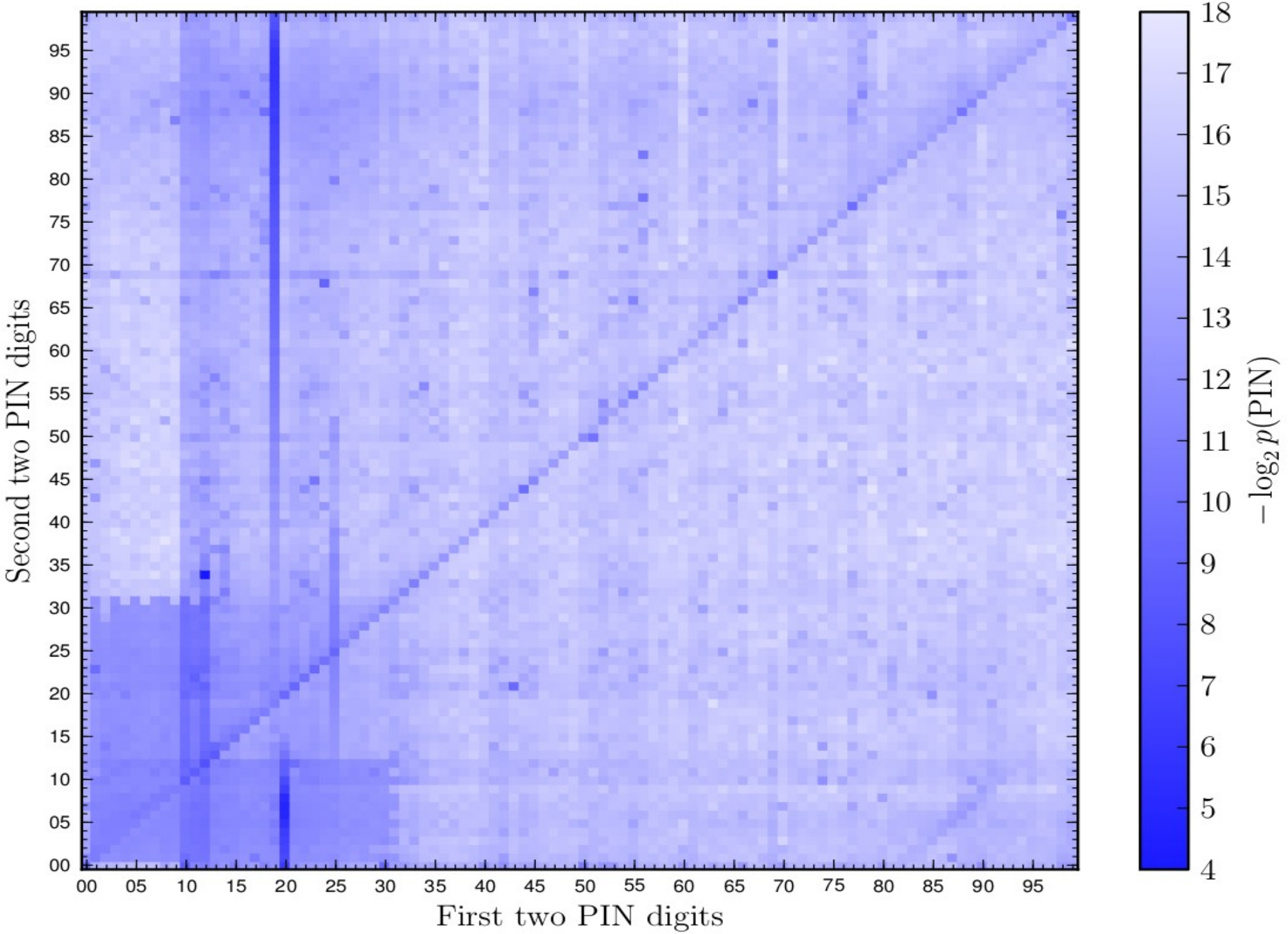
What's easier to guess?

- Passwords chosen by older or younger users?
- Passwords or random 9-digit numbers?
- PINs or mother's maiden name?

My PhD research

- **Measuring guessing difficulty empirically**
  - How do different user groups compare?
  - How do authentication schemes compare?

Case study #1: 4-digit PINs


Second two PIN digits
First two PIN digits
00 05 10 15 20 25 30 35 40 45 50 55 60 65 70 75 80 85 90 95
$-\log_2 p(\mathrm{PIN})$
4 5 6 7 8 9 10 11 12 13 14 15 16 17 18

Guessing a PIN with 6 guesses

- 2% chance of success against a random user
- **8%** given the user's birthday!

JESUS KEYS IN HIS PIN NUMBER

'Pin number' burglar used victims' cards

He struck as couple slept

GARRY WILLEY

A JUDGE laid down a pin number warning after he heard how a couple fell victim to a "cunning" career crook.

Serial offender Paul Miller - whose grim record carries 167 previous convictions - crept into the victim's North Tyneside home while they slept.

His haul included cash, laptops, a handbag and driving licence.

But Miller, 31, also pocketed two Barclays cards, Newcastle Crown Court heard. And within hours he was plundering £1,000 from an ATM on nearby Wallsend High Street when he guessed right the owner had used her date of birth as a pin. Jailing Miller for four and a half years, Judge Roger Thorn said: "If anybody is still using their date of birth as a pin they should learn a lesson from this case.

"You knew that by using the driving licence you could get the date of birth and having identified that you took a chance that the holder was using it as a pin. You were right."

The dead-of-night raid last summer has left the victims feeling paranoid in their own home, the court heard.

CONVICTED Miller

Miller, of Wilberforce Street, Wallsend, denied burglary and fraud but was convicted by a jury.

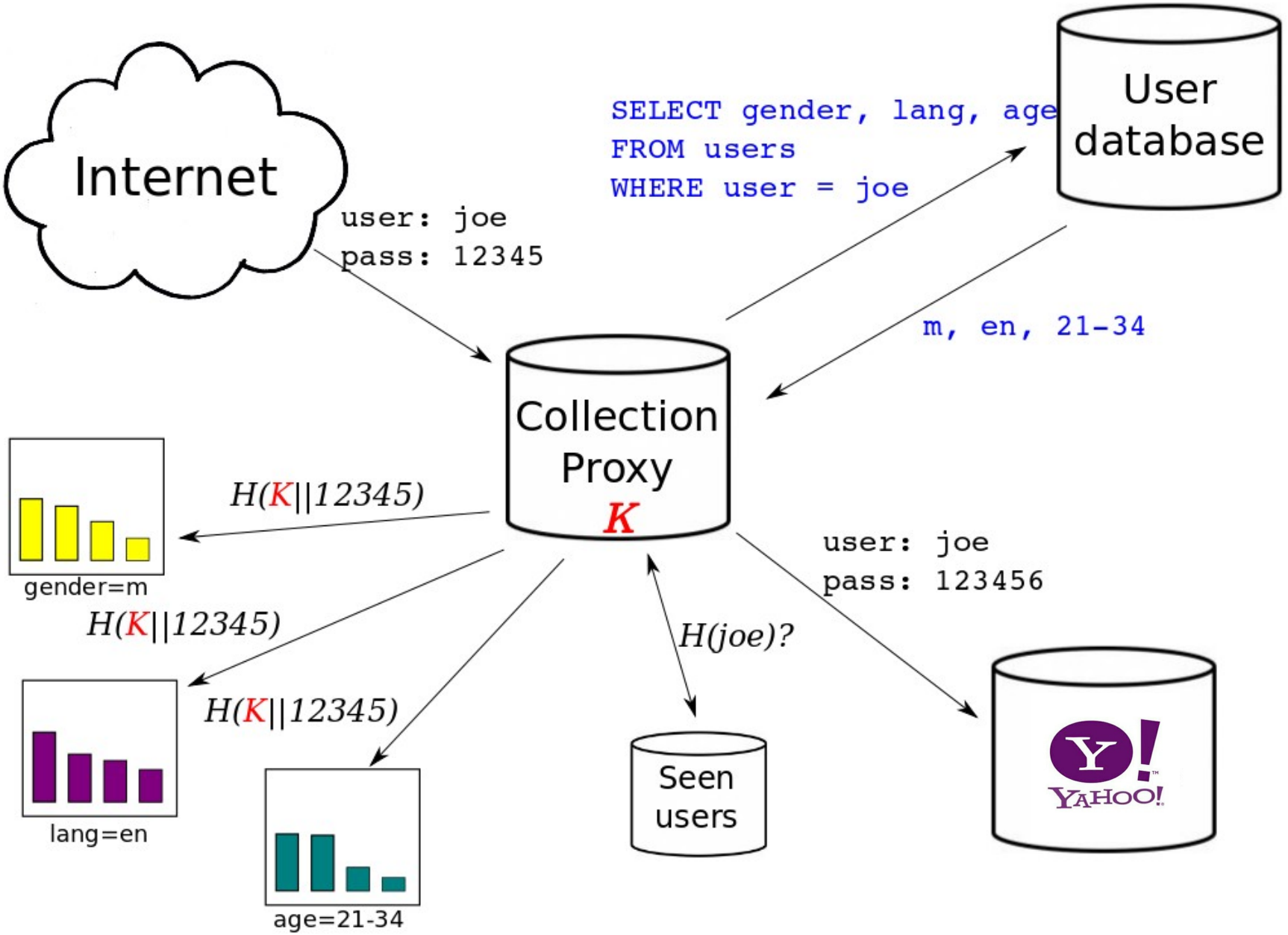
He slipped inside the house when he realised the front door was unlocked, prowling through rooms and rounding up property while the couple slept.

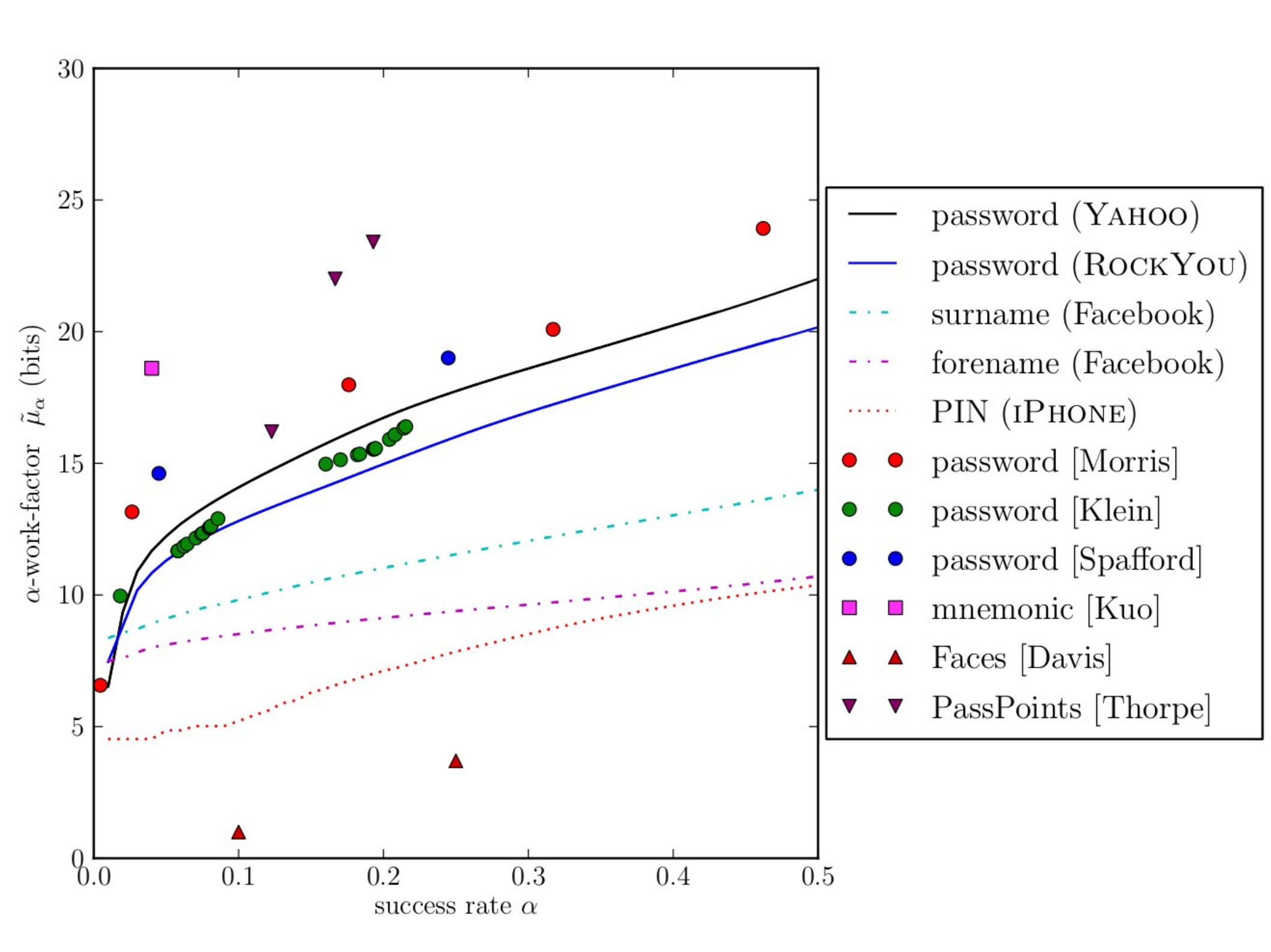
Miller was later captured on CCTV using the cards to withdraw batches of cash from the same ATM. A pre-sentence report said Miller - a heroin addict who first took drugs when he was 12- posed a risk of harm through potential confrontations with homeowners. His record includes offences of arson and robbery as well as 32 previous burglaries - nine targeting homes.

research in action...

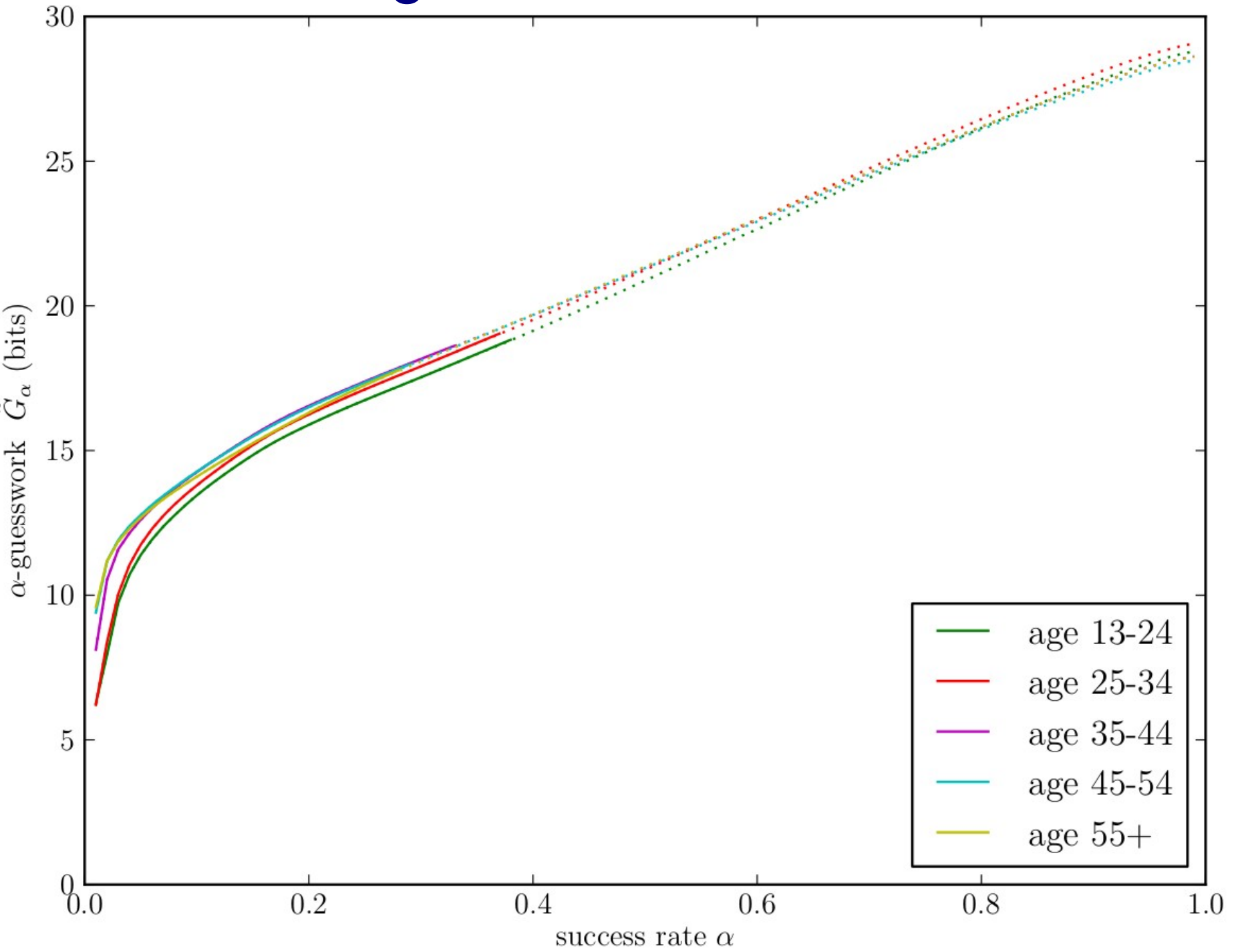
Case study #2: basic passwords

Password collection at Yahoo

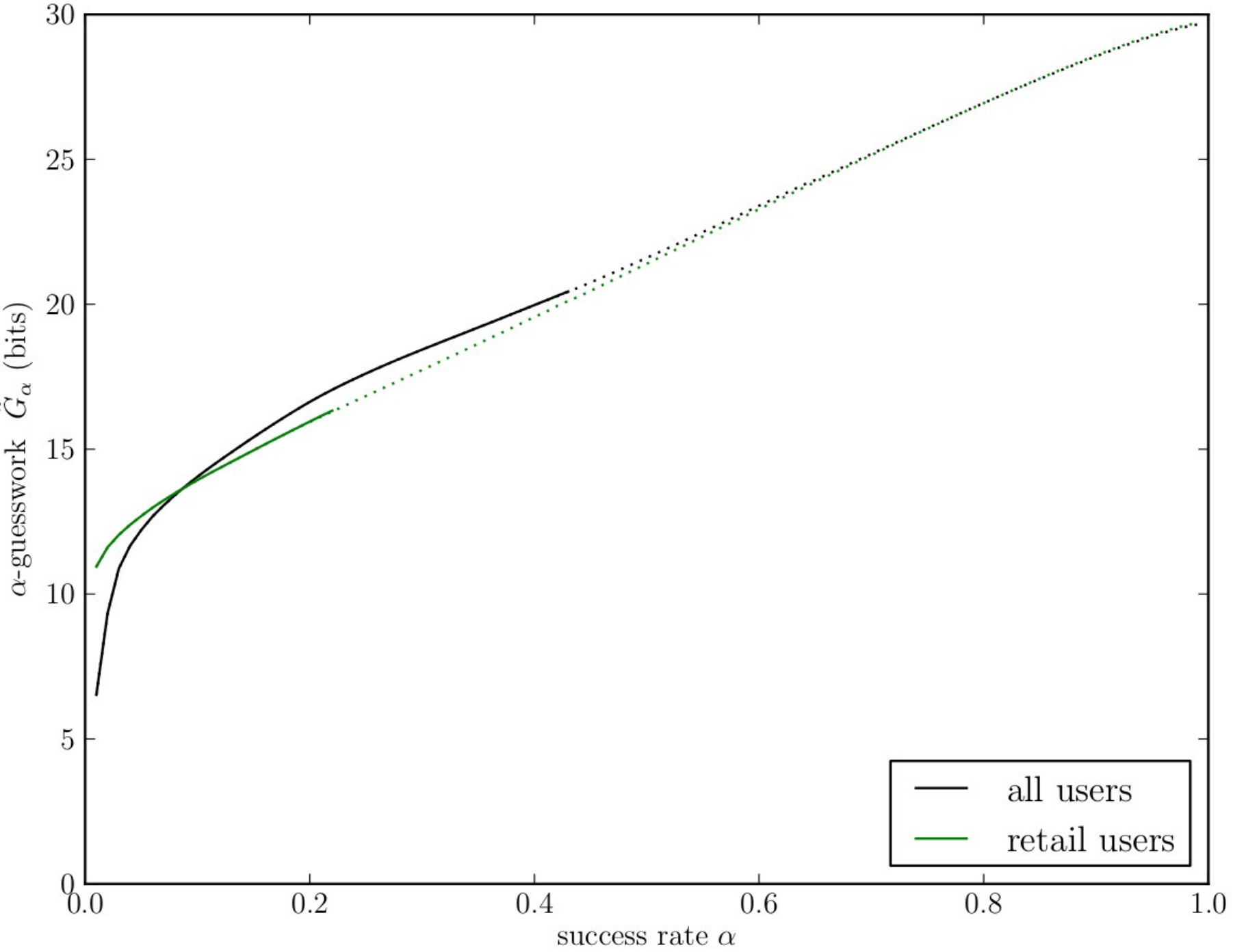



30
25
20
15
10
5
0
0.0
0.1
0.2
0.3
0.4
0.5
α-work-factor $\tilde{\mu}_\alpha$ (bits)
success rate α
password (YAHOO)
password (ROCKYOU)
surname (Facebook)
forename (Facebook)
PIN (IPHONE)
password [Morris]
password [Klein]
password [Spafford]
mnemonic [Kuo]
Faces [Davis]
PassPoints [Thorpe]

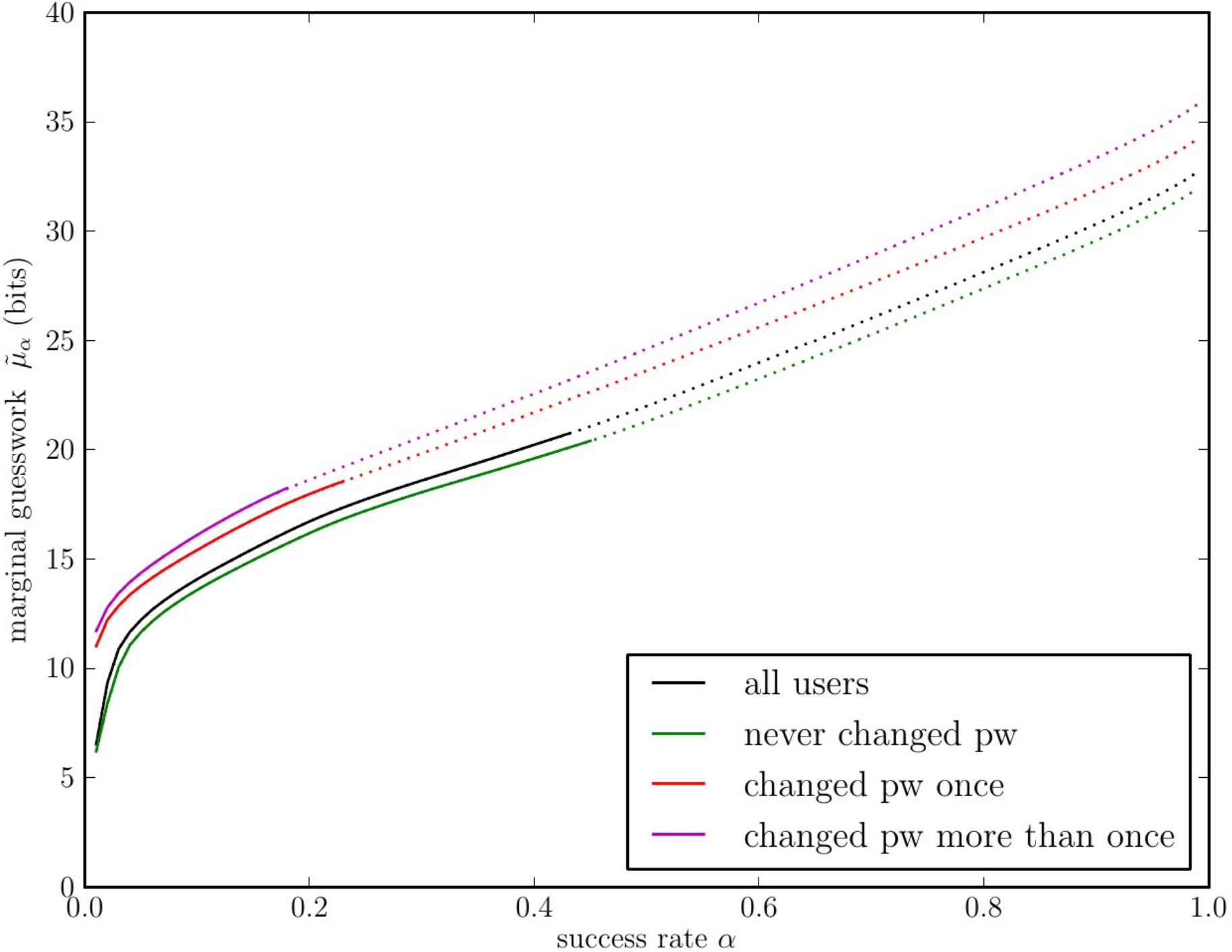
Age matters a little bit..



Financial motivation matters a little bit...

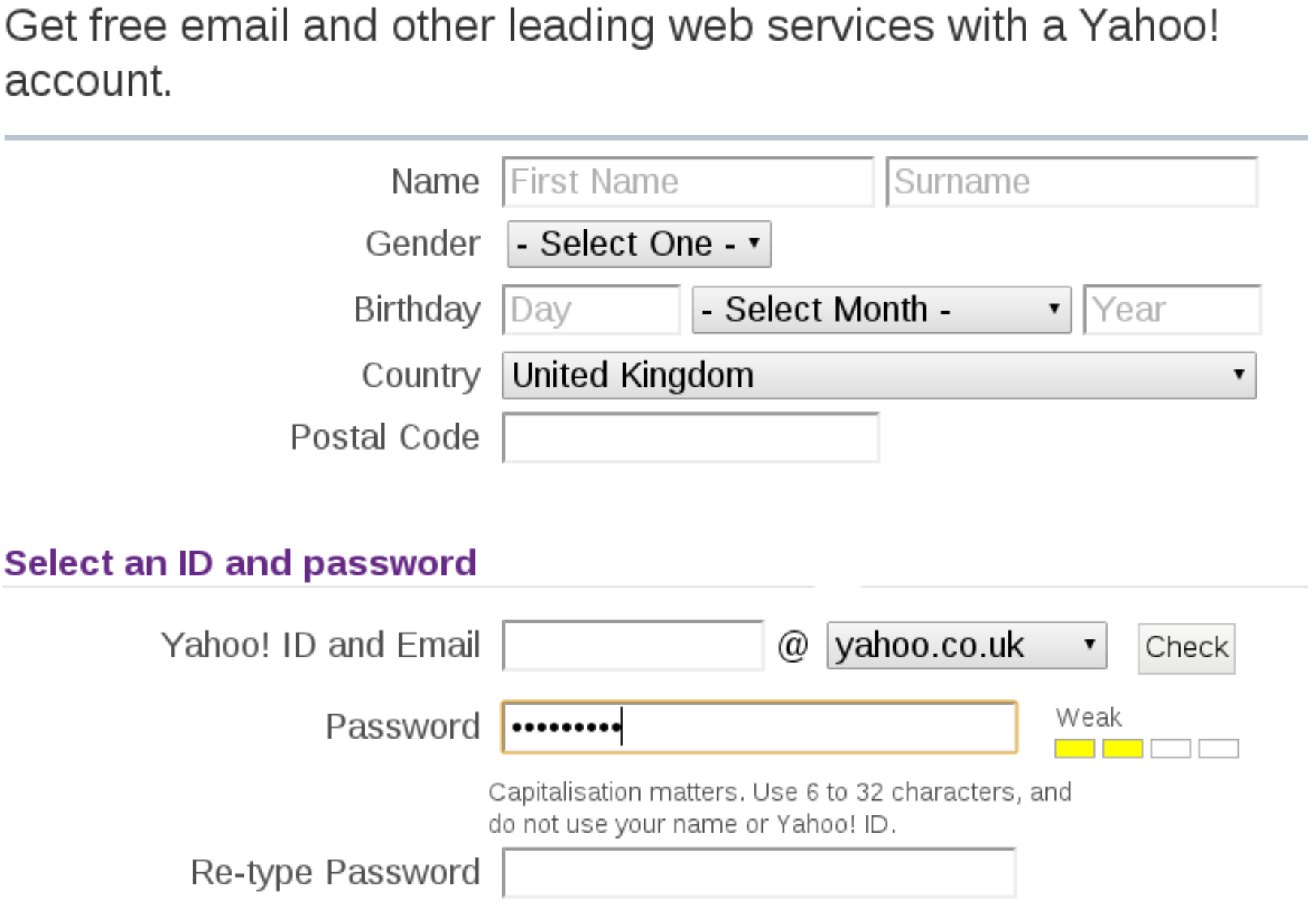


Security interest matters much more

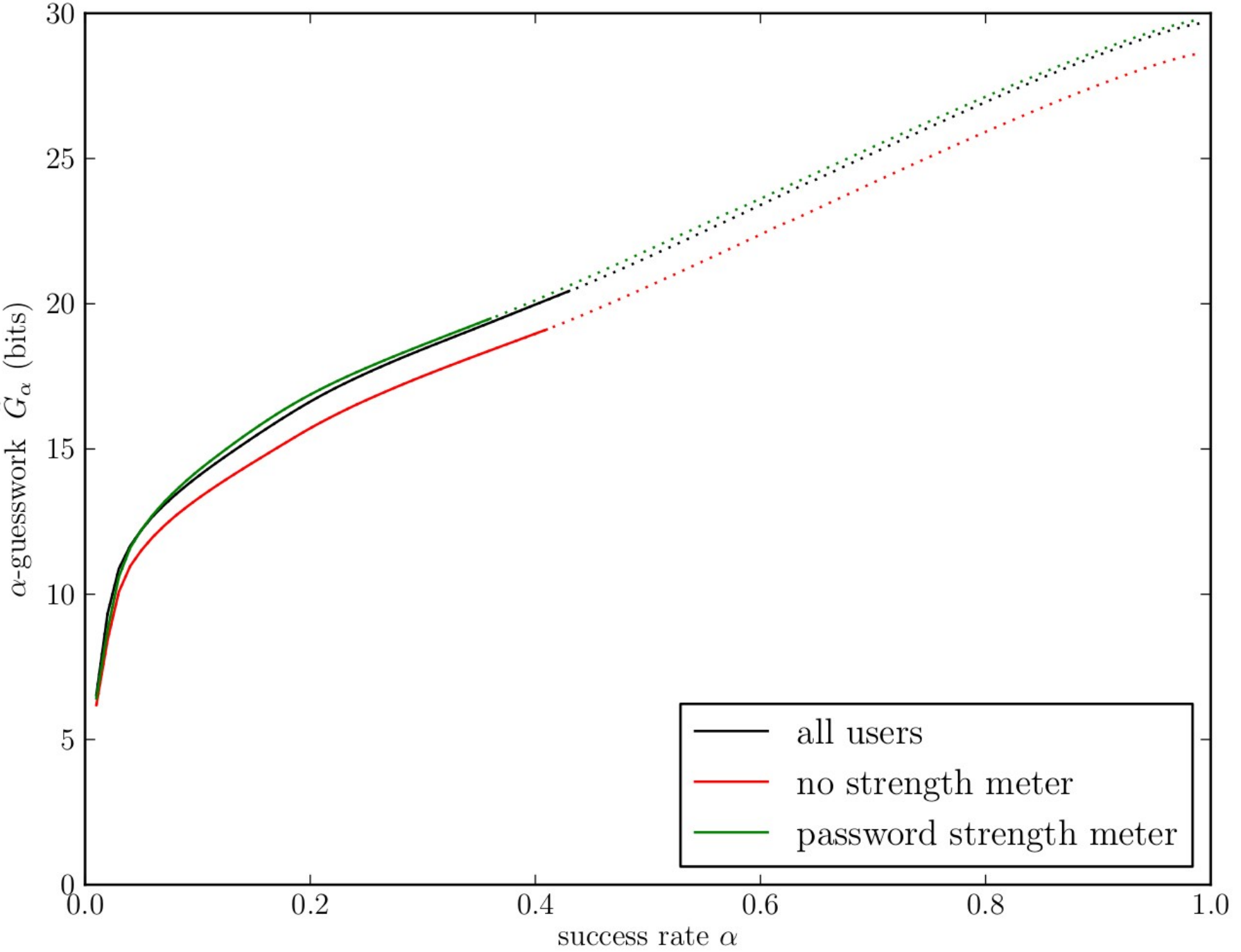


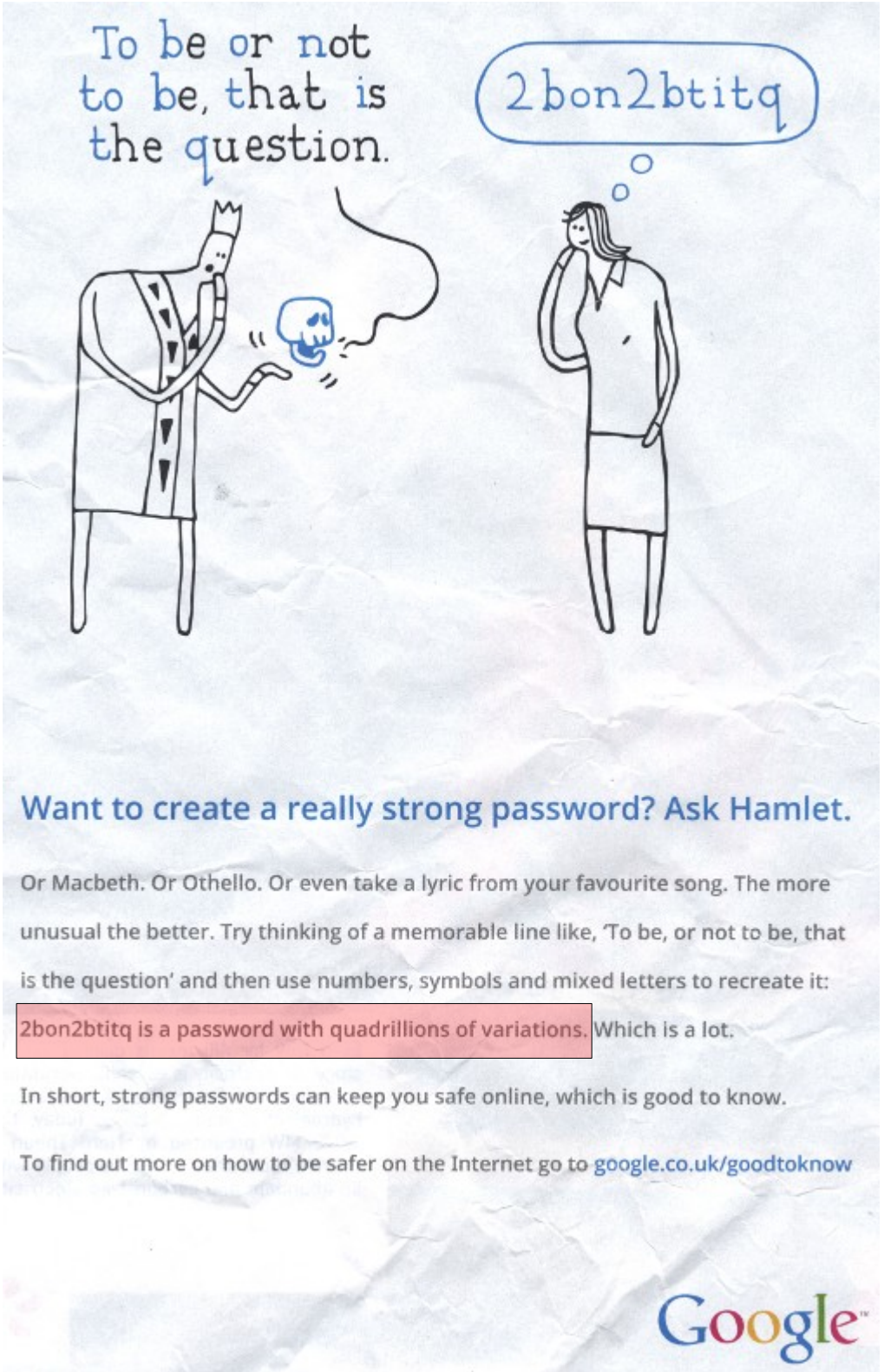
Case study #3: password advice

Password strength meter at Yahoo



Strength meter makes 1 bit of difference

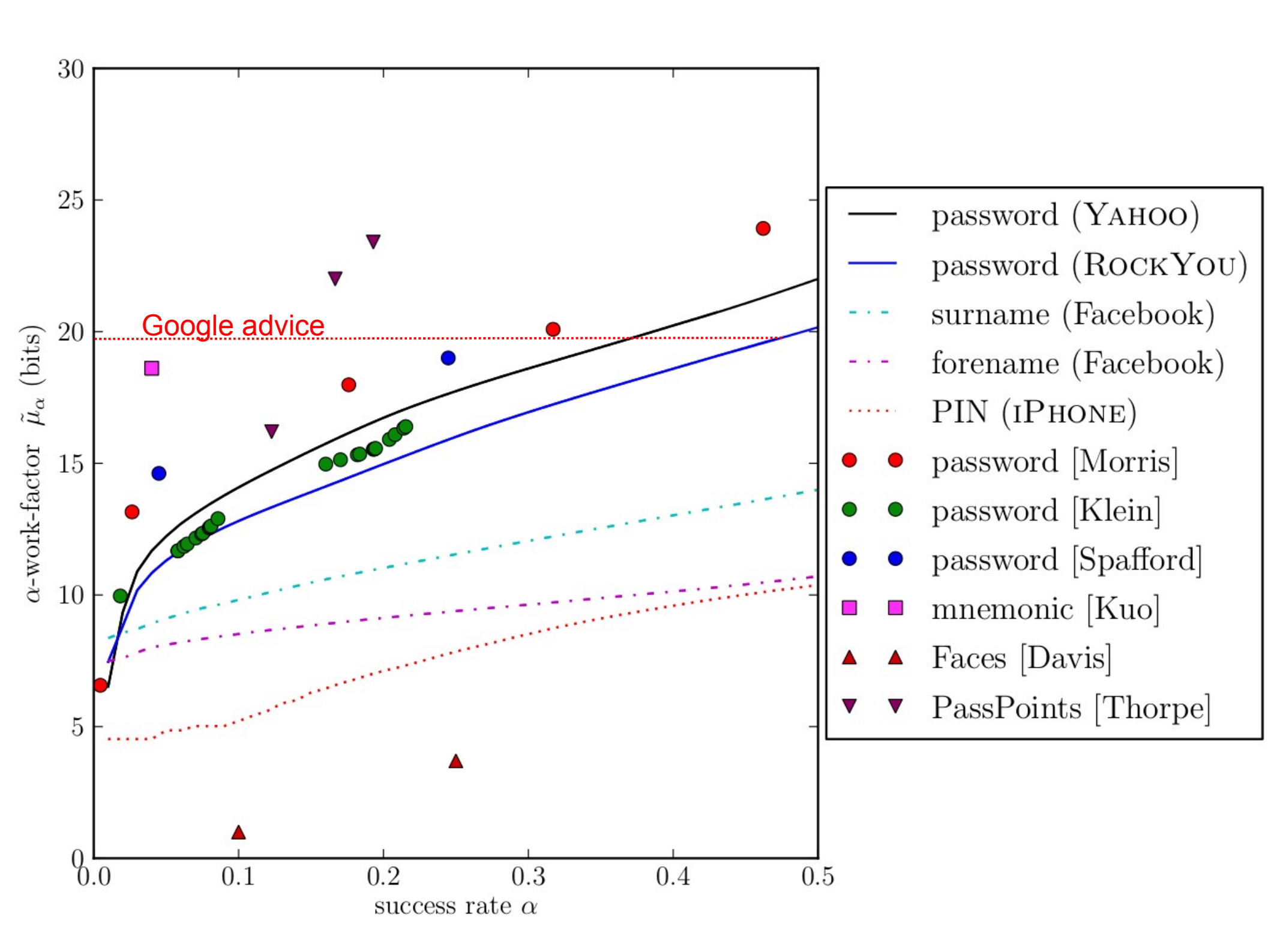


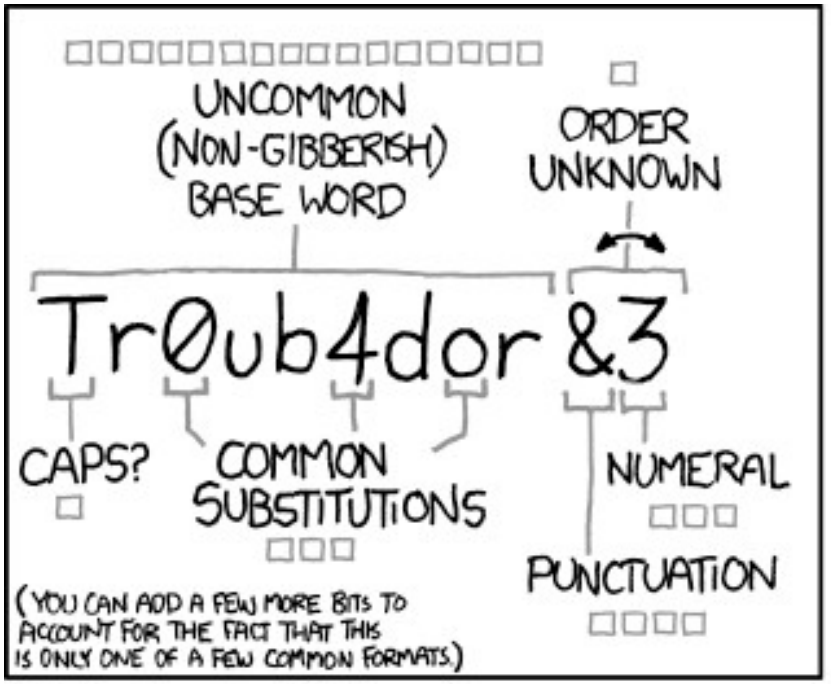


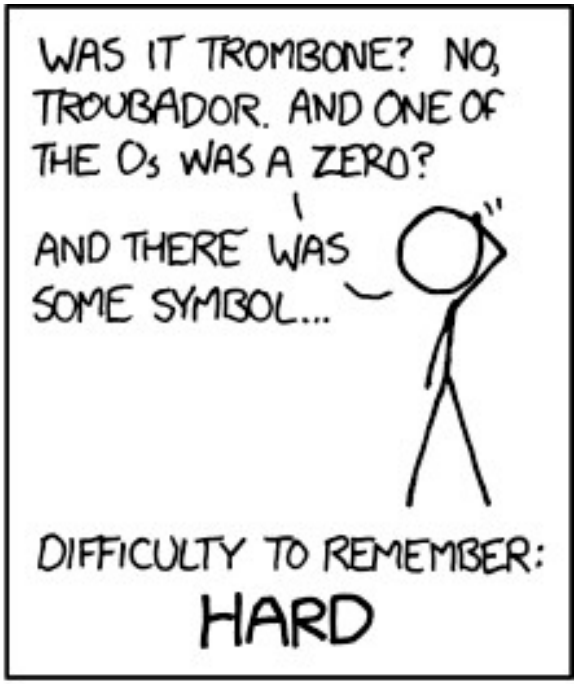
1 quadrillion variations

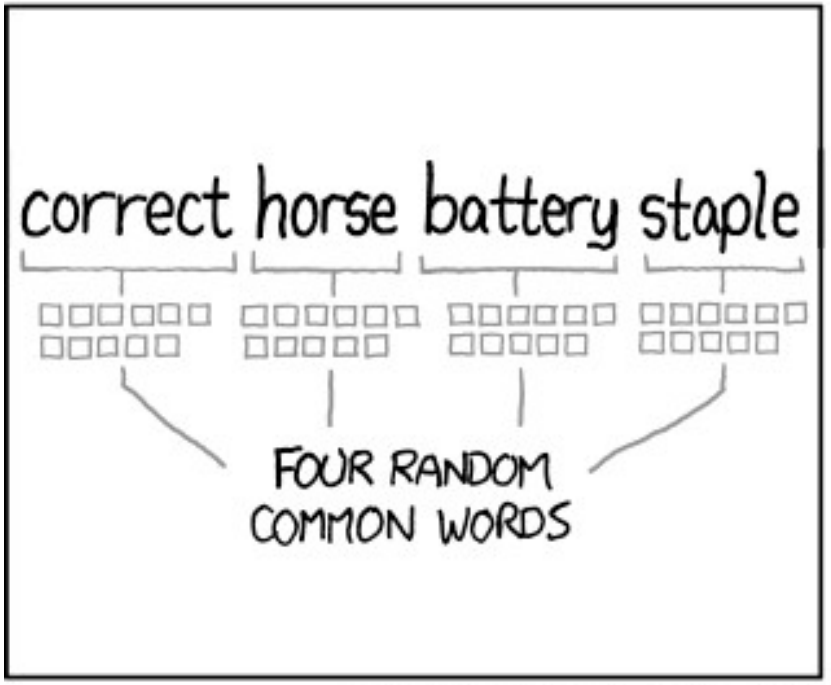
≈

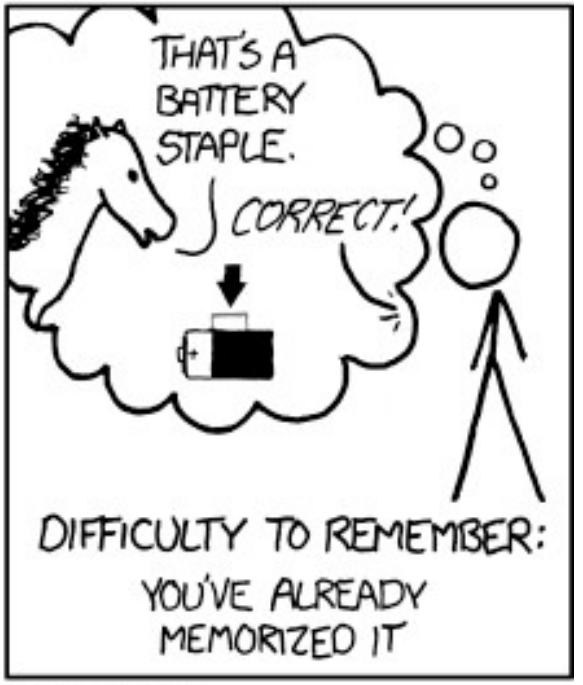
50 bits?


Google advice
α-work-factor $\tilde{\mu}_\alpha$ (bits)
success rate α
0
5
10
15
20
25
30
0.0
0.1
0.2
0.3
0.4
0.5
password (YAHOO)
password (ROCKYOU)
surname (Facebook)
forename (Facebook)
PIN (IPHONE)
password [Morris]
password [Klein]
password [Spafford]
mnemonic [Kuo]
Faces [Davis]
PassPoints [Thorpe]

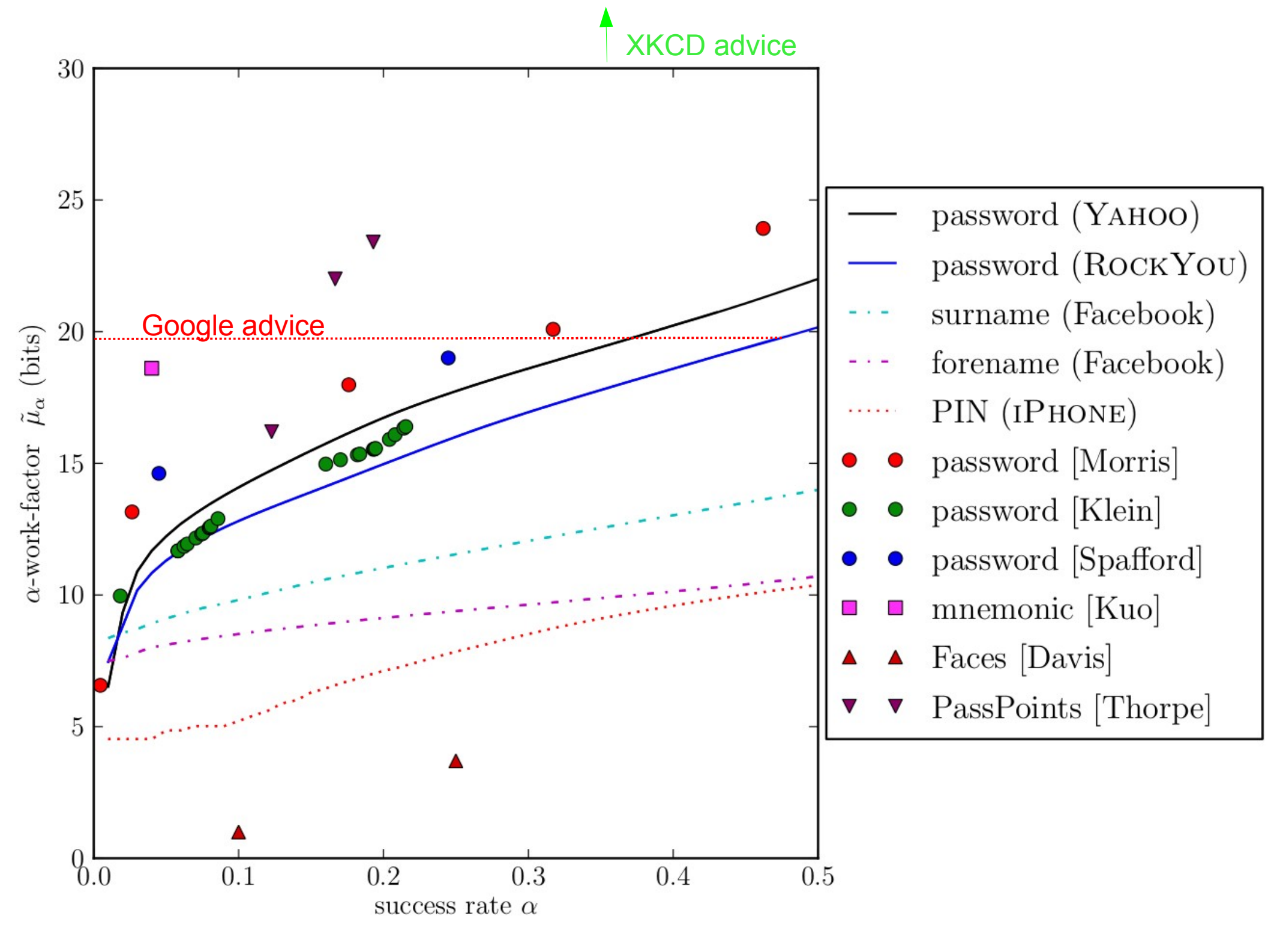


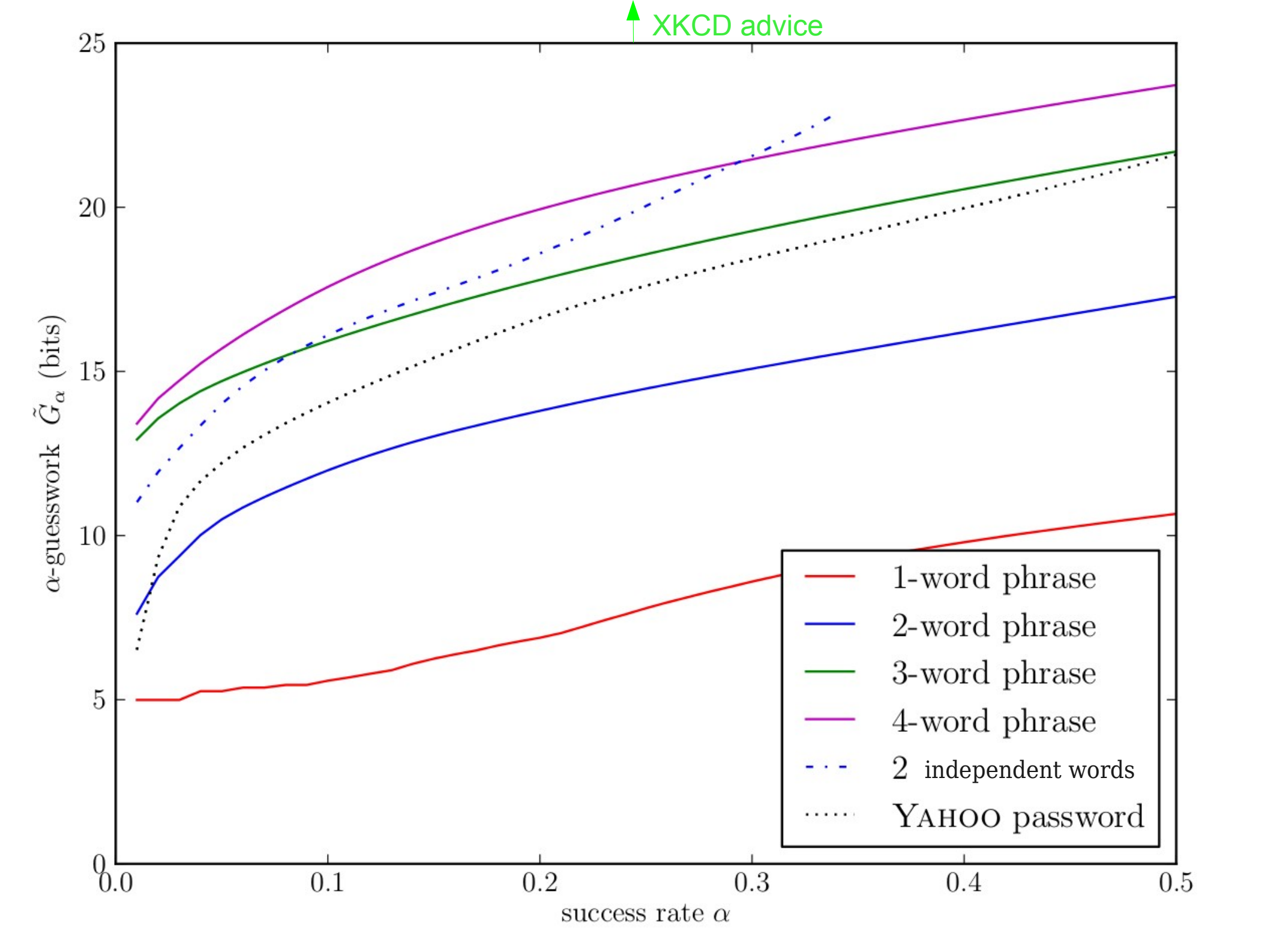






THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

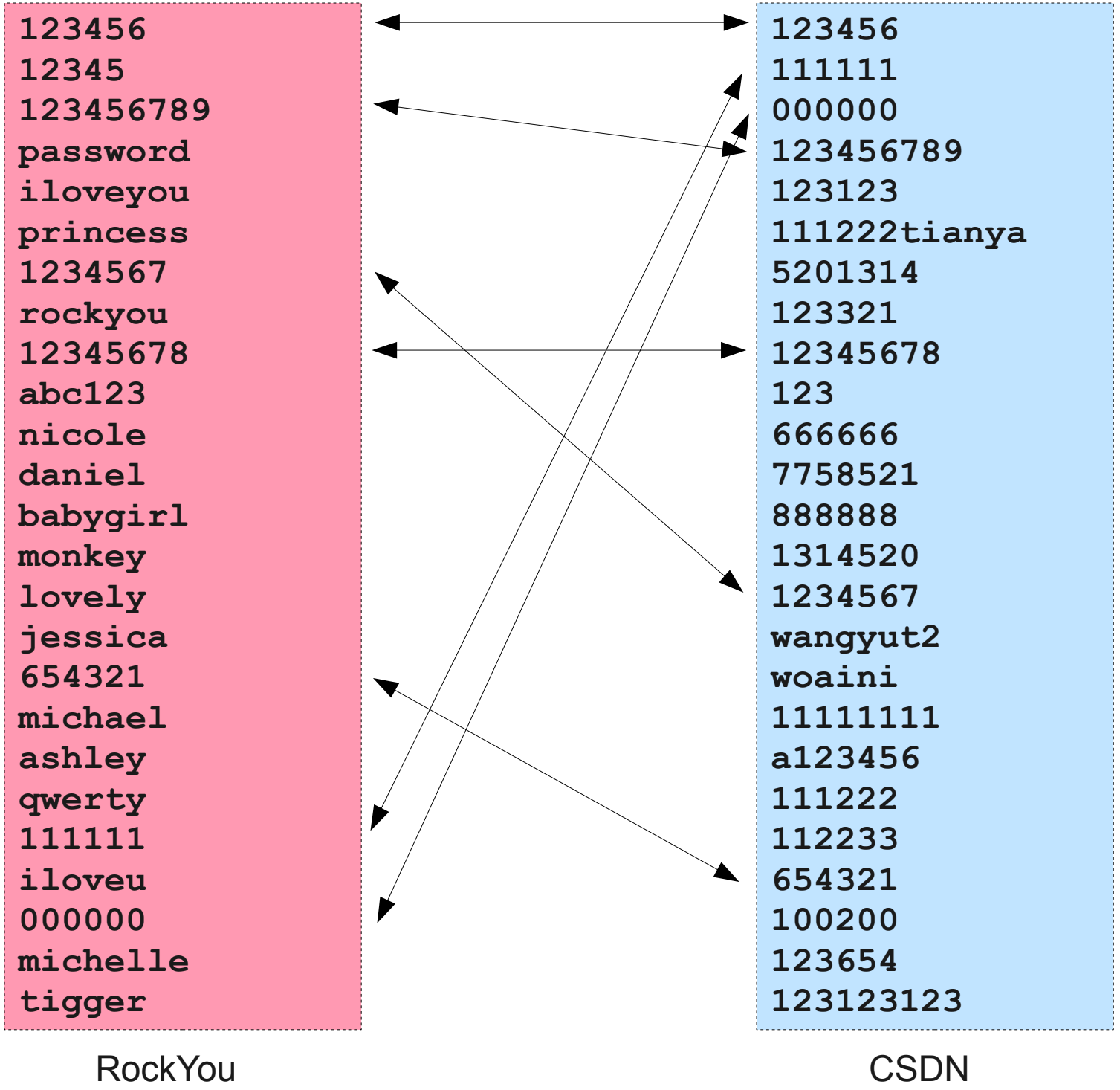

XKCD advice
Google advice
30
25
20
15
10
5
0
0.0
0.1
0.2
0.3
0.4
0.5
α-work-factor $\tilde{\mu}_\alpha$ (bits)
success rate α
password (YAHOO)
password (ROCKYOU)
surname (Facebook)
forename (Facebook)
PIN (IPHONE)
password [Morris]
password [Klein]
password [Spafford]
mnemonic [Kuo]
Faces [Davis]
PassPoints [Thorpe]

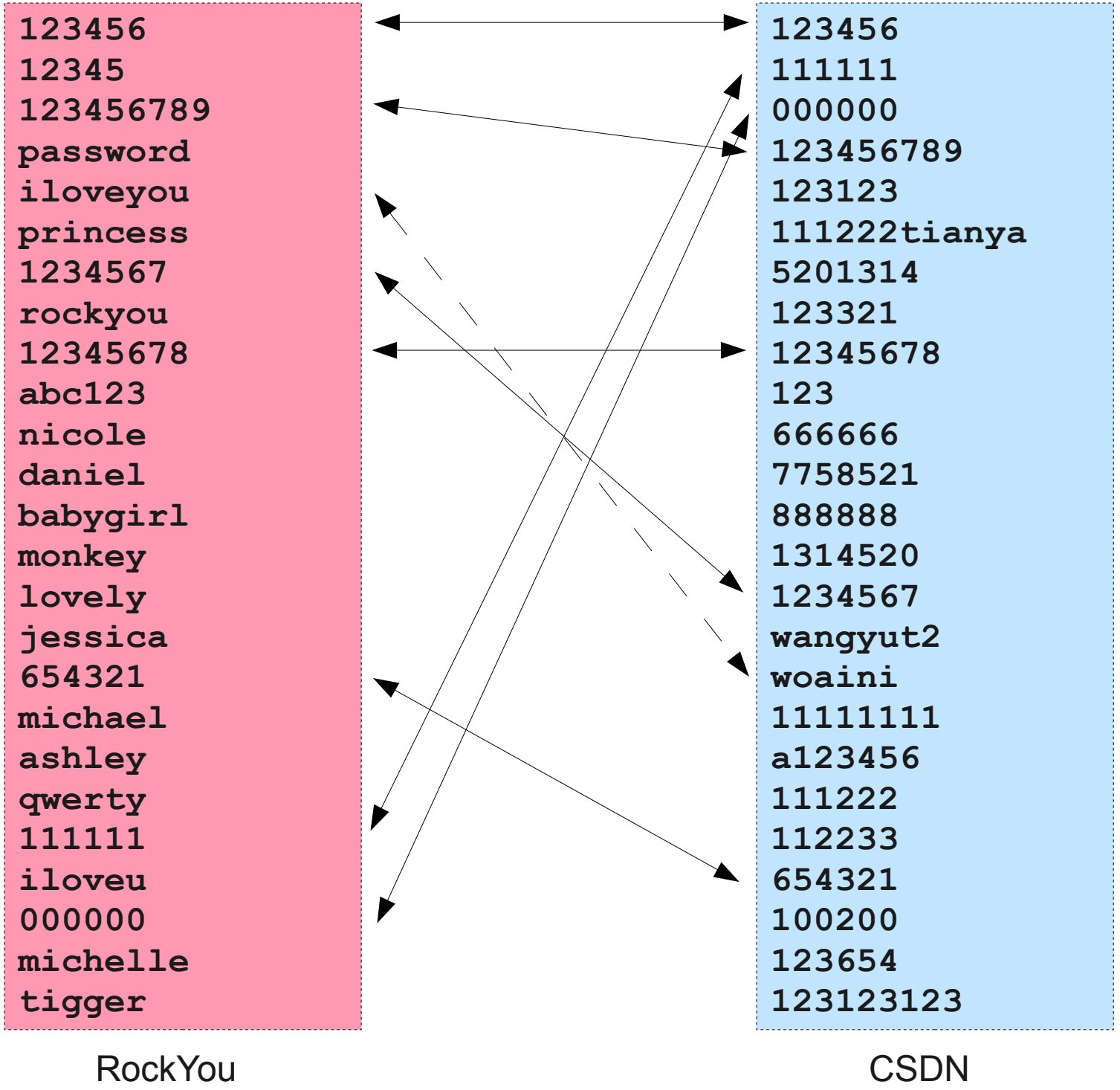

XKCD advice
25
20
15
10
5
0
0.0
0.1
0.2
0.3
0.4
0.5
α-guesswork $\tilde{G}_\alpha$ (bits)
success rate α
1-word phrase
2-word phrase
3-word phrase
4-word phrase
2 independent words
YAHOO password

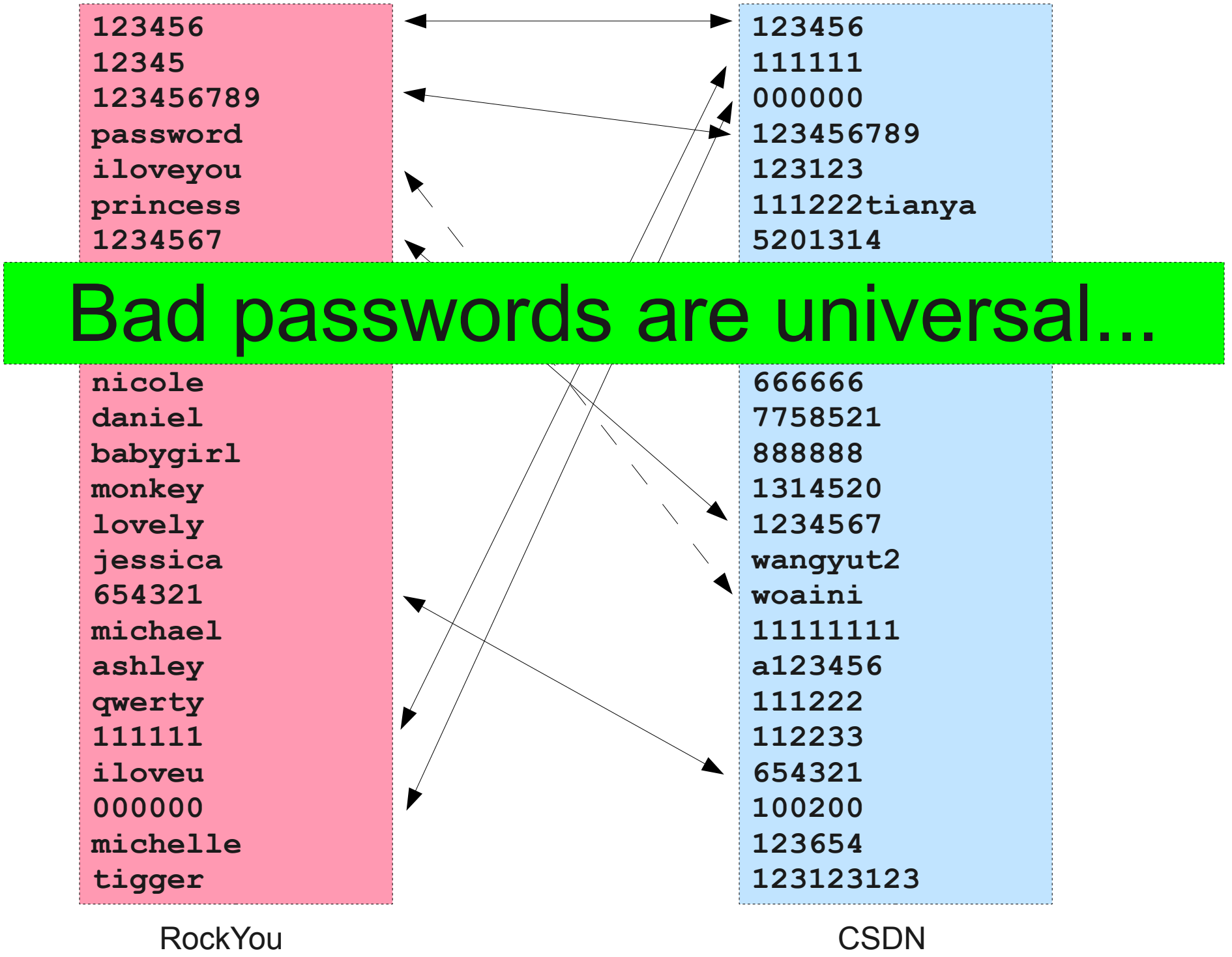
Case study #4: passwords and language

RockYou
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
michelle
tigger

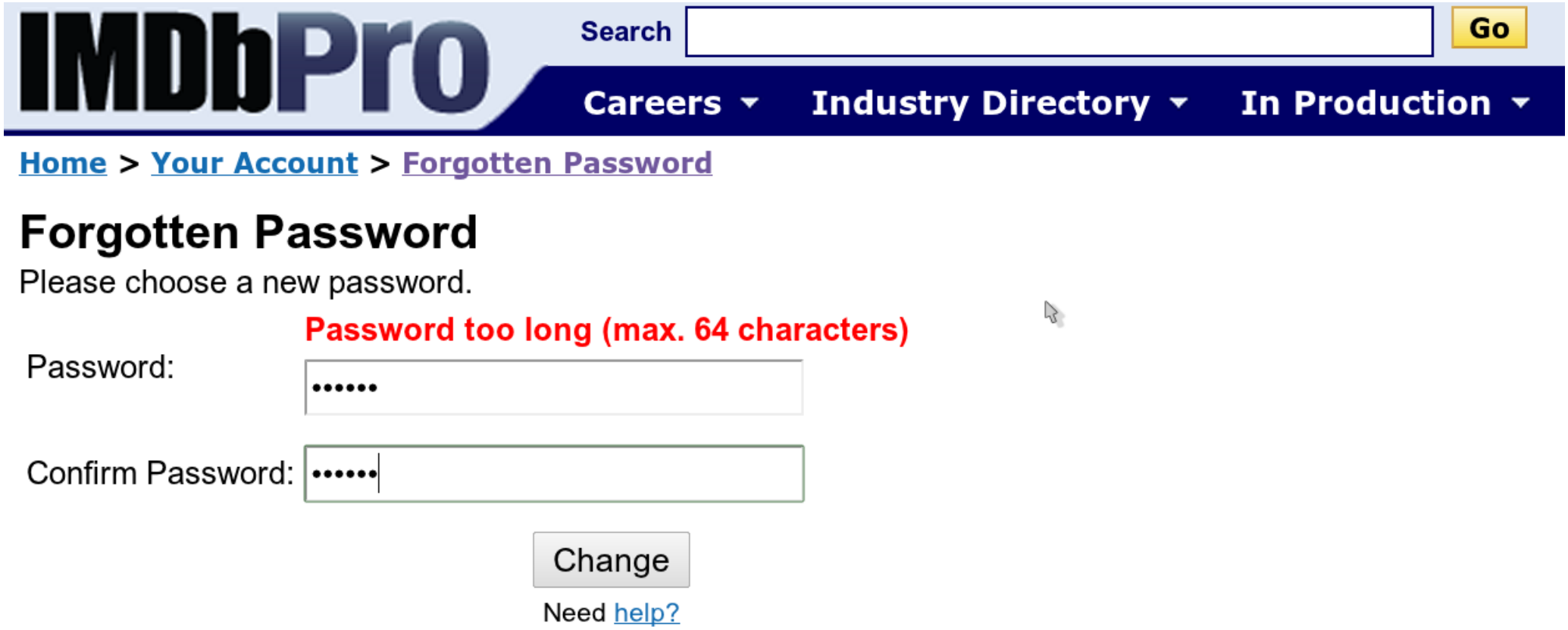
CSDN
123456
111111
000000
123456789
123123
111222tianya
5201314
123321
12345678
123
666666
7758521
888888
1314520
1234567
wangyut2
woaini
11111111
a123456
111222
112233
654321
100200
123654
123123123


123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
michelle
tigger
123456
111111
000000
123456789
123123
111222tianya
5201314
123321
12345678
123
666666
7758521
888888
1314520
1234567
wangyut2
woaini
11111111
a123456
111222
112233
654321
100200
123654
123123123
RockYou
CSDN


123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
michelle
tigger
123456
111111
000000
123456789
123123
111222tianya
5201314
123321
12345678
123
666666
7758521
888888
1314520
1234567
wangyut2
woaini
11111111
a123456
111222
112233
654321
100200
123654
123123123
RockYou
CSDN

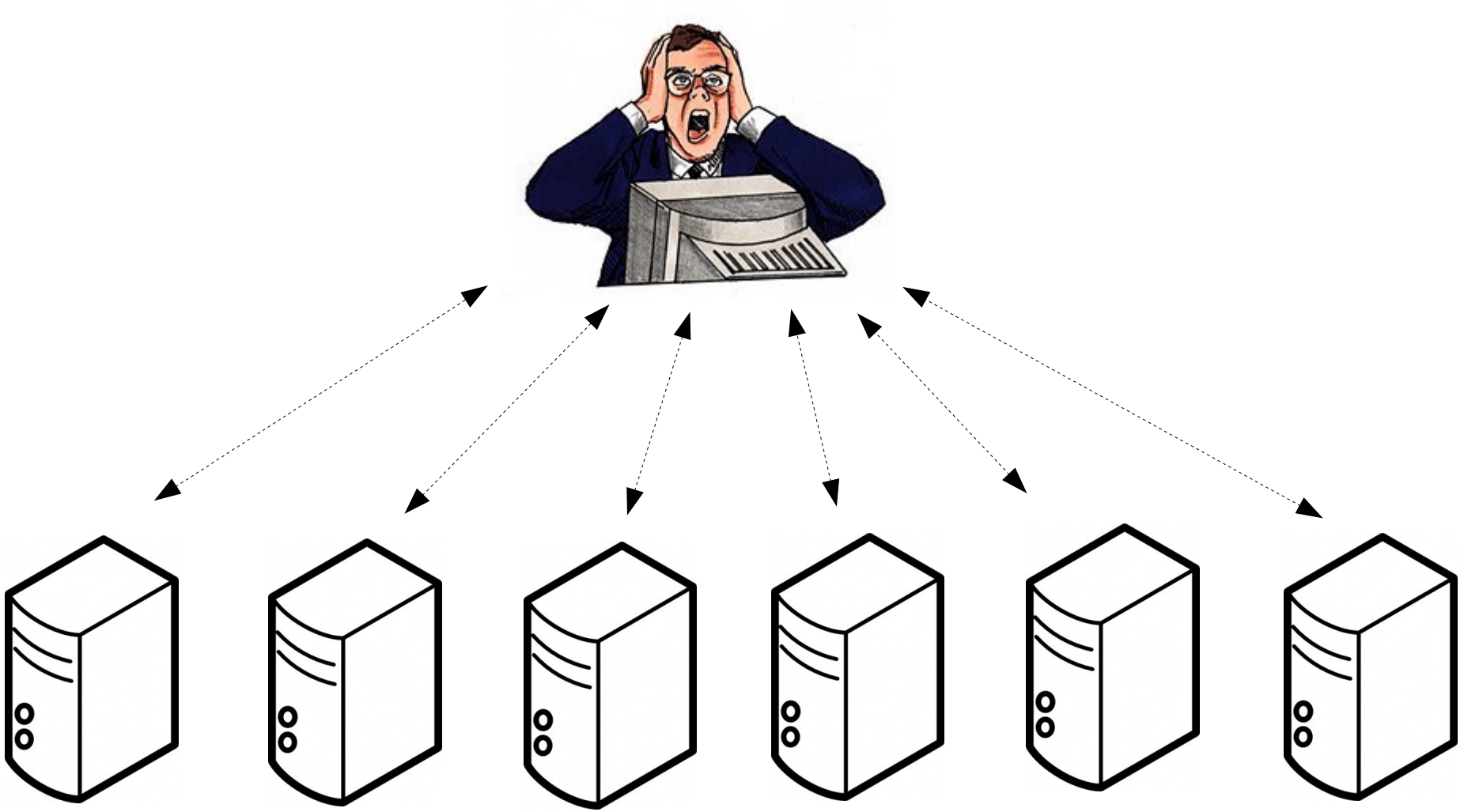

123456
12345
123456789
password
iloveyou
princess
1234567
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
michelle
tigger
123456
111111
000000
123456789
123123
111222tianya
5201314
666666
7758521
888888
1314520
1234567
wangyut2
woaini
11111111
a123456
111222
112233
654321
100200
123654
123123123
Bad passwords are universal...
RockYou
CSDN

Non-ASCII passwords poorly supported

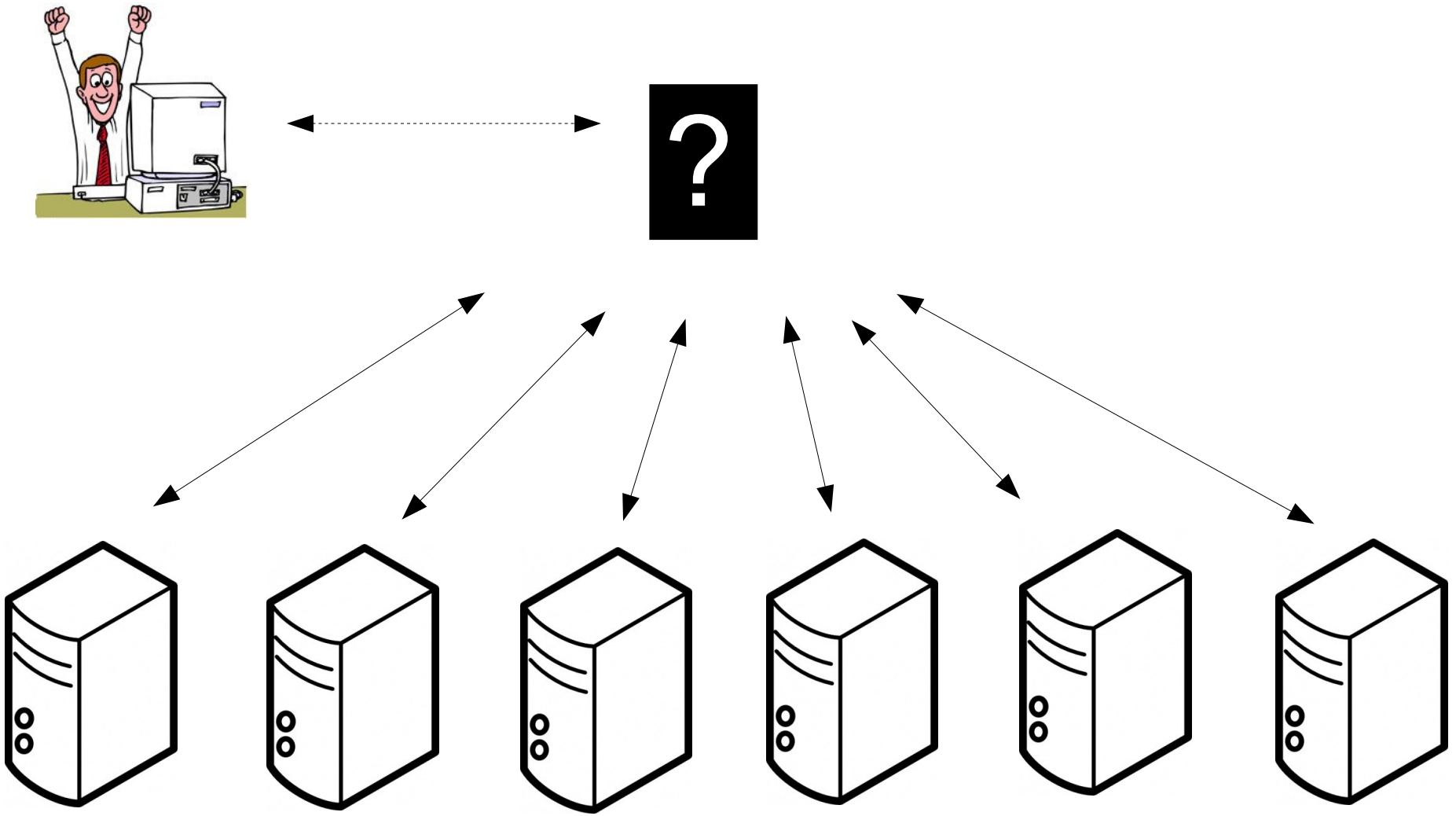


East Asian scripts disabled for passwords

Today's Internet identity layer



Tomorrow's Internet identity layer



Thanks to many collaborators ☺

Ross Anderson, Sören Preibusch, Frank Stajano, Ekaterina Shutova (Cambridge)

Elizabeth Zwicky, Henry Watts, Richard Clayton, Ram Marti, Clarence Chung, Christopher Harris (Yahoo!)

Paul van Oorschot (Carleton)

Cormac Herley (Microsoft Research)