Measuring Real-World Accuracies and Biases in Modeling Password Guessability

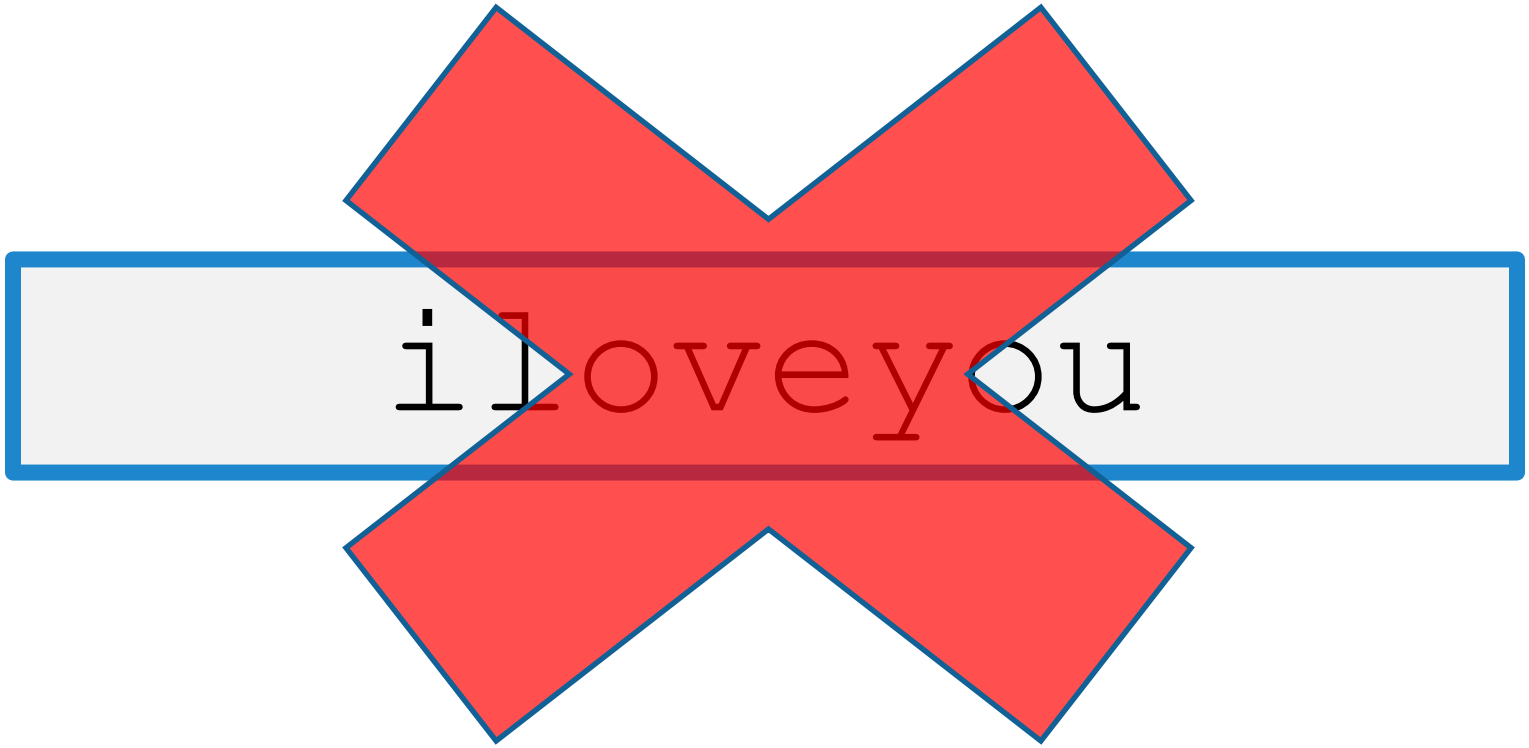
Blase Ur, Sean M. Segreti, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Saranga Komanduri, Darya Kurilova, Michelle L. Mazurek, William Melicher, Richard Shay

Carnegie Mellon

UNIVERSITY OF MARYLAND

How strong is a particular password?

iloveyou


iloveyou

n(c$JZX!zKc^bIAX^N

j@mesb0nd007!

Why Measure Password Strength?

Why Measure Password Strength?

- Eliminate bad passwords
  - Organizational password audits

Why Measure Password Strength?

- Eliminate bad passwords
  - Organizational password audits
- Help users make better passwords

Why Measure Password Strength?

- Eliminate bad passwords
  - Organizational password audits
- Help users make better passwords
  - Determine if interventions are effective

Why Measure Password Strength?

- Eliminate bad passwords
  - Organizational password audits
- Help users make better passwords
  - Determine if interventions are effective
  - Provide users feedback

Password-Strength Metrics

Password-Strength Metrics

- Statistical approaches
  - Traditionally: Shannon entropy
  - Recently: α-guesswork

Password-Strength Metrics

- Statistical approaches
  - Traditionally: Shannon entropy
  - Recently: α-guesswork
- Disadvantages for researchers
  - No per-password estimates
  - Huge sample required

Parameterized Guessability

- How many guesses a particular cracking algorithm with particular training data would take to guess a password

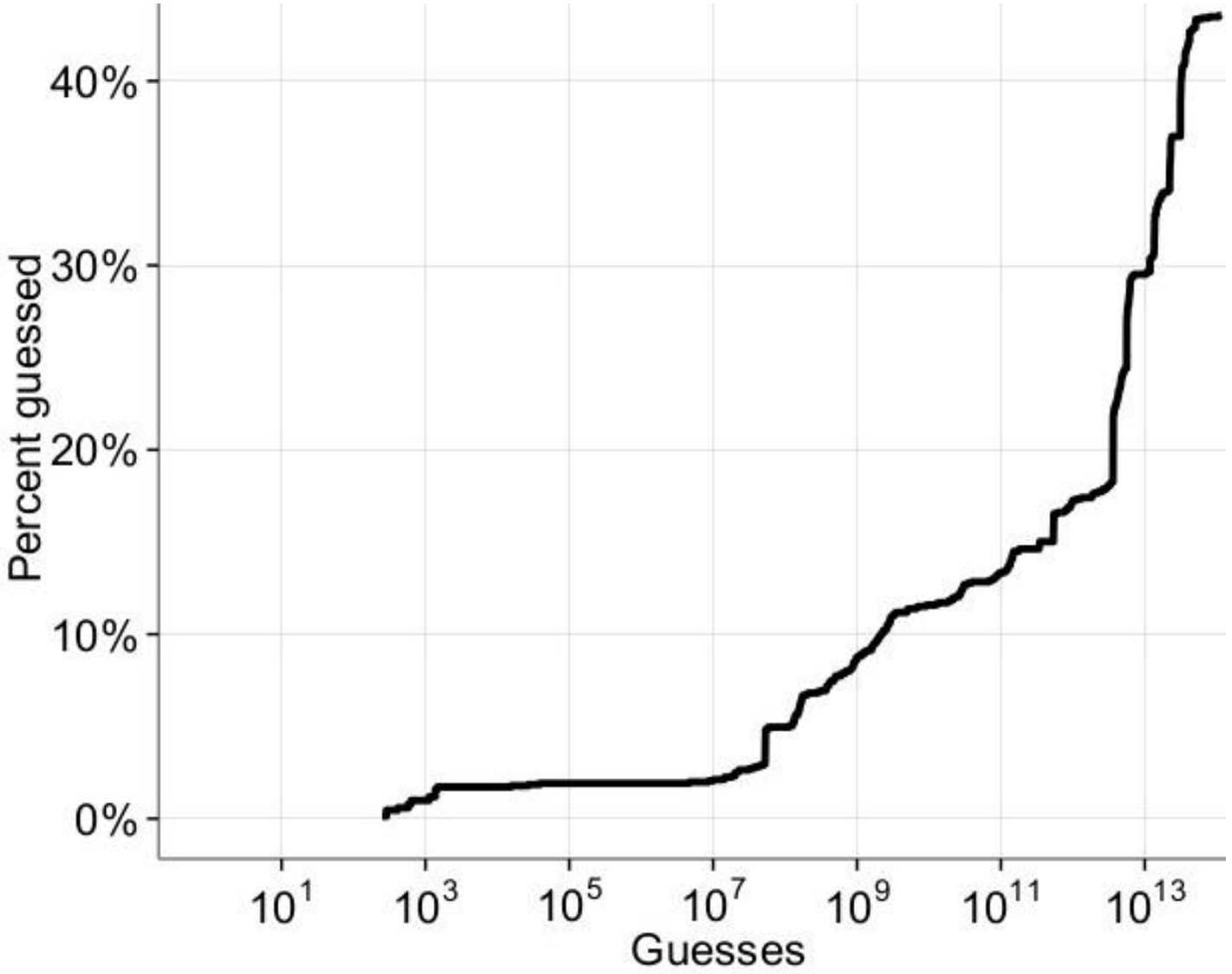
j@mesb0nd007!

Guess # 366,163,847,194

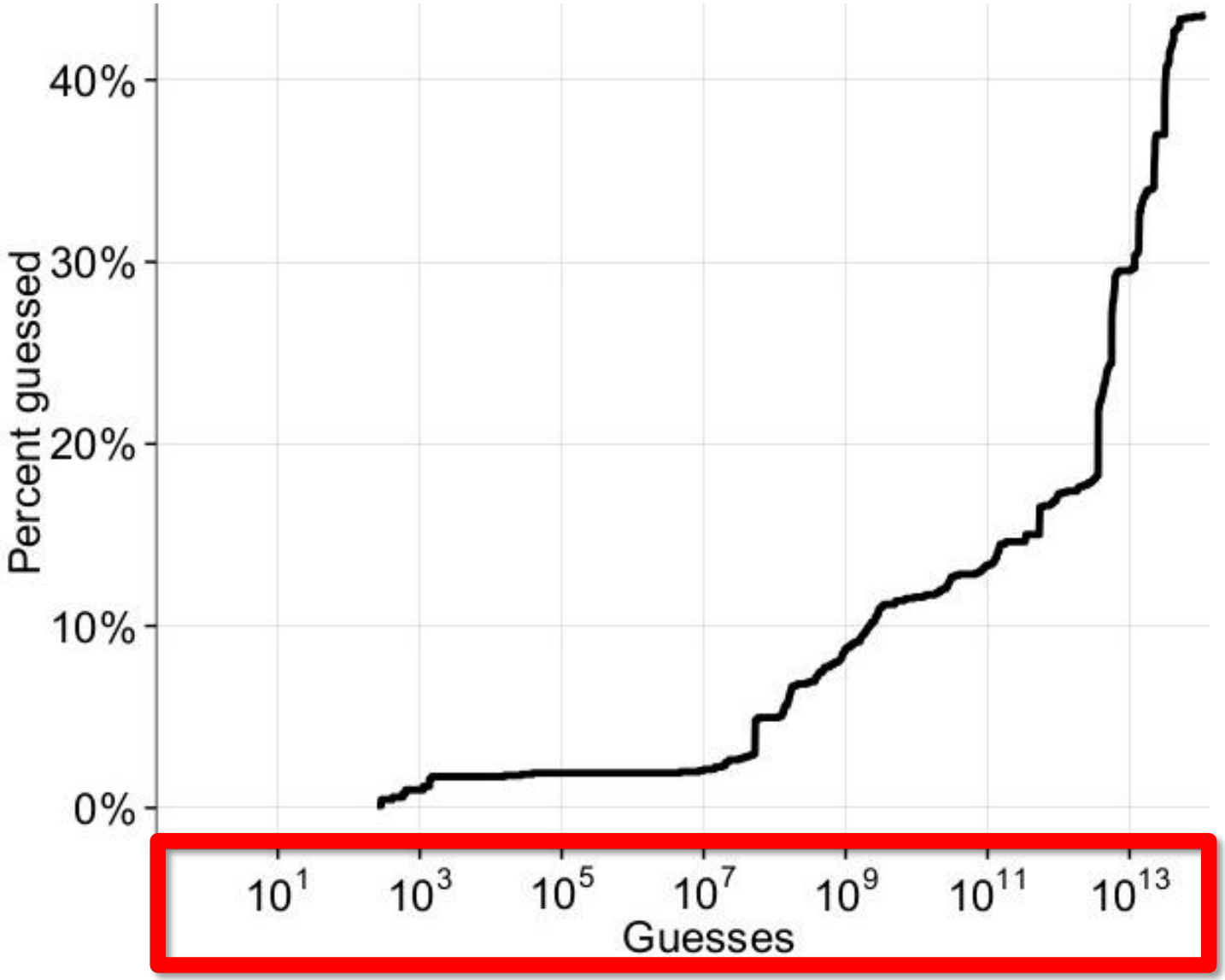
n(c$JZX!zKc^bIAX^N

Guess # past cutoff

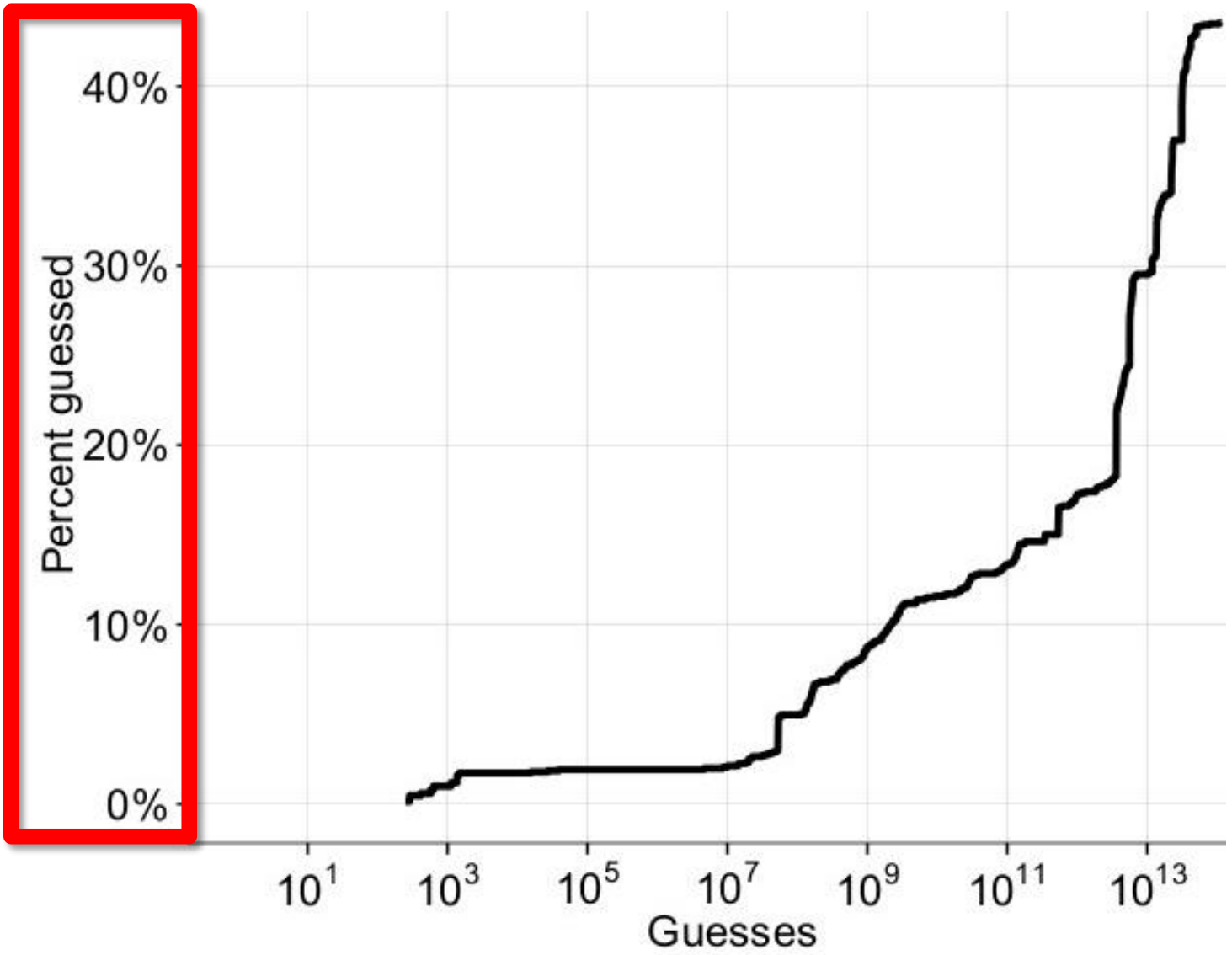
Guessability Plots



Guessability Plots



Guessability Plots

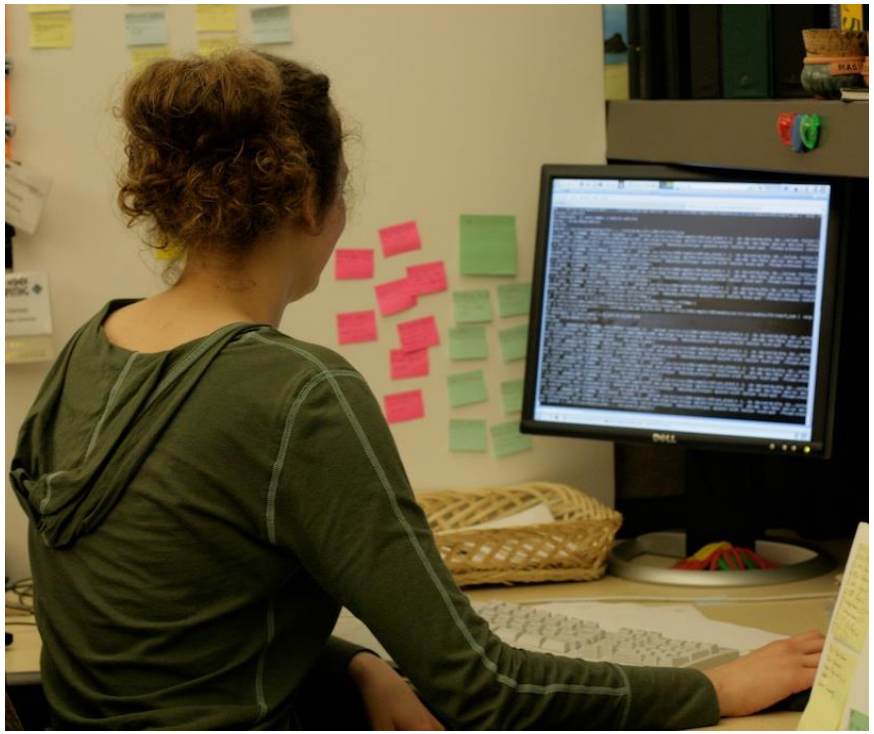


Advantages of Guessability

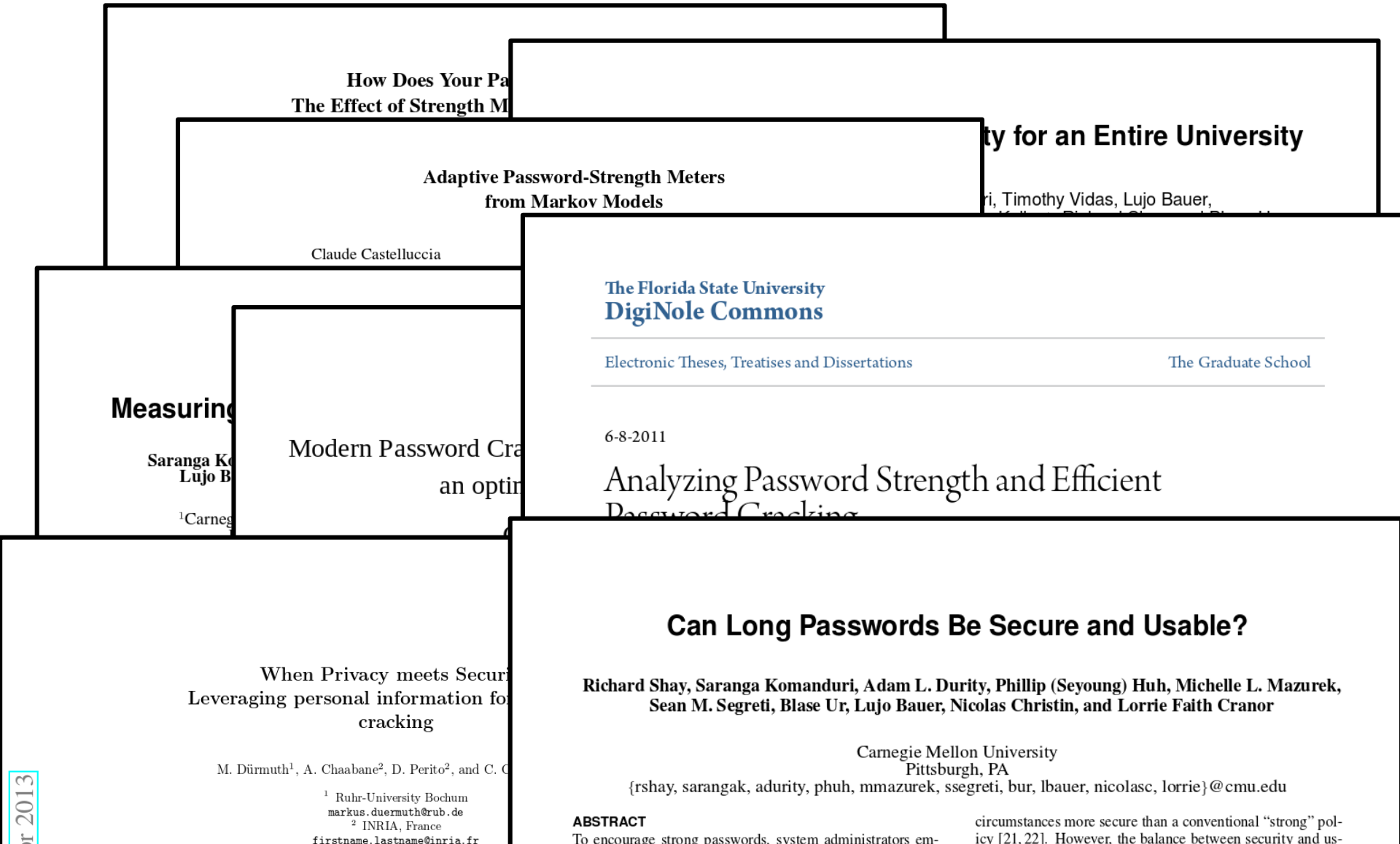
- Straightforward
- Models an attacker
- Per-password strength estimates

Guessability in Practice

Guessability in Practice



Single Cracking Approach



Default Configuration

Of Password
Measuring the Effect of Pas

Saranga Komanduri[1], Richard Shay[1], Pa

On The Ecological Validi

Sascha Fahl, Marian Harbach, Y
Usable Security and P
versity Ha
smith@

Improving Text Passwords Through Persuasion

Alain Forget[1,2], Sonia Chiasson[1,2], P.C. van Oorschot[1], Robert Biddle[2]
[1]School of Computer Science & [2]Human Oriented Technology Lab
Carleton University, Ottawa, Canada
{aforget, chiasson, paulv}@scs.carleton.ca, robert_biddle@carleton.ca

A Study of User Password Strategy for Multiple Accounts

S M Taiabul Haque
Department of CSE
University of Texas at
Arlington,TX USA 7
eresh03@gmail

Matthew Wright
Department of CSE

Shannon Scielzo
Department of Psychology

topic
pass-
study

ABSTRACT

Despite advances in biometrics
words remain the most common
tion in computer systems. User
levels for different passwords.
the degree of similarity among
rity levels of a user. We conduc
with 80 students from a publi
United States. We asked the su

The Tangled Web of Passw

Anupam Das*, Joseph Bonneau†, Matthew Caesar*, Nikita Boris
*University of Illinois at Urbana-Champaign
{das17, caesar, nikita}@illinois.edu

From *Very Weak* to *Very Strong*:
Analyzing Password-Strength Meters

Xavier de Carné de Carnavalet and Mohammad Mannan
Concordia Institute for Information Systems Engineering
Concordia University, Montreal, Canada

International Journal of Innovative Computing, Information and Control
Volume **9**, Number **2**, February **2013**

ICIC International ©2013 ISSN 1349-4198
pp. 821–839

PASSWORD CRACKING BASED ON LEARNED PATTERNS FROM DISCLOSED PASSWORDS

Hsien-Cheng Chou[1], Hung-Chang Lee[2], Hwan-Jeu Yu[1], Fei-Pei Lai[1,3]
Kuo-Hsuan Huang[4] and Chih-Wen Hsueh[1]

[1]Department of Computer Science and Information Engineering
[3]Graduate Institute of Biomedical Electronics and Bioinformatics
National Taiwan University
No. 1, Section 4, Roosevelt Road, Taipei 10617, Taiwan
{ d96922034; flai }@csie.ntu.edu.tw; ecpro@seed.net.tw

[2]Department of Information Management
Tamkang University
No. 151, Yingzhuan Road, Tamsui District, New Taipei City 25137, Taiwan

The Florida State University
DigiNole Commons

Electronic Theses, Treatises and Dissertations — The Graduate School

6-8-2011

Analyzing Password Strength and Efficient Password Cracking

Shiva Houshmand Yazdi
Florida State University

Questions About Guessability

Questions About Guessability

1) How does guessability used in research compare to an attack by professionals?

Questions About Guessability

1) How does guessability used in research compare to an attack by professionals?
2) Would substituting another cracking approach impact research results?

Approach

Approach

password iloveyou teamo123 …	Pa$$w0rd iLov3you! 1QaZ2W@x …	passwordpassword 1234567812345678 !1@2#3$4%5^6&7*8 …	pa$$word1234 12345678asDF !q1q!q1q!q1q …

4 password sets

5 password-cracking approaches

Four Password Sets

Four Password Sets

- **Basic** (3,062): 8+ characters

```
password
```

Four Password Sets

- **Basic** (3,062): 8+ characters

```
password
```

- **Complex** (3,000): 8+ characters, 4 classes

```
Pa$$w0rd
```

Four Password Sets

- **Basic** (3,062): 8+ characters

```
password
```

- **Complex** (3,000): 8+ characters, 4 classes

```
Pa$$w0rd
```

- **LongBasic** (2,054): 16+ characters

```
passwordpassword
```

Four Password Sets

- **Basic** (3,062): 8+ characters

```
password
```

- **Complex** (3,000): 8+ characters, 4 classes

```
Pa$$w0rd
```

- **LongBasic** (2,054): 16+ characters

```
passwordpassword
```

- **LongComplex** (990): 12+ characters, 3+ classes

```
pa$$word1234
```

Five Cracking Approaches

- John the Ripper
- Hashcat
- Markov models
- Probabilistic Context-Free Grammar
- Professionals

John the Ripper

- Guesses variants of input wordlist

John the Ripper

- Guesses variants of input wordlist
- Wordlist mode requires:
  - Wordlist (passwords and dictionary entries)
  - Mangling rules

John the Ripper

- Guesses variants of input wordlist
- Wordlist mode requires:
  - Wordlist (passwords and dictionary entries)
  - Mangling rules
- Speed: Fast

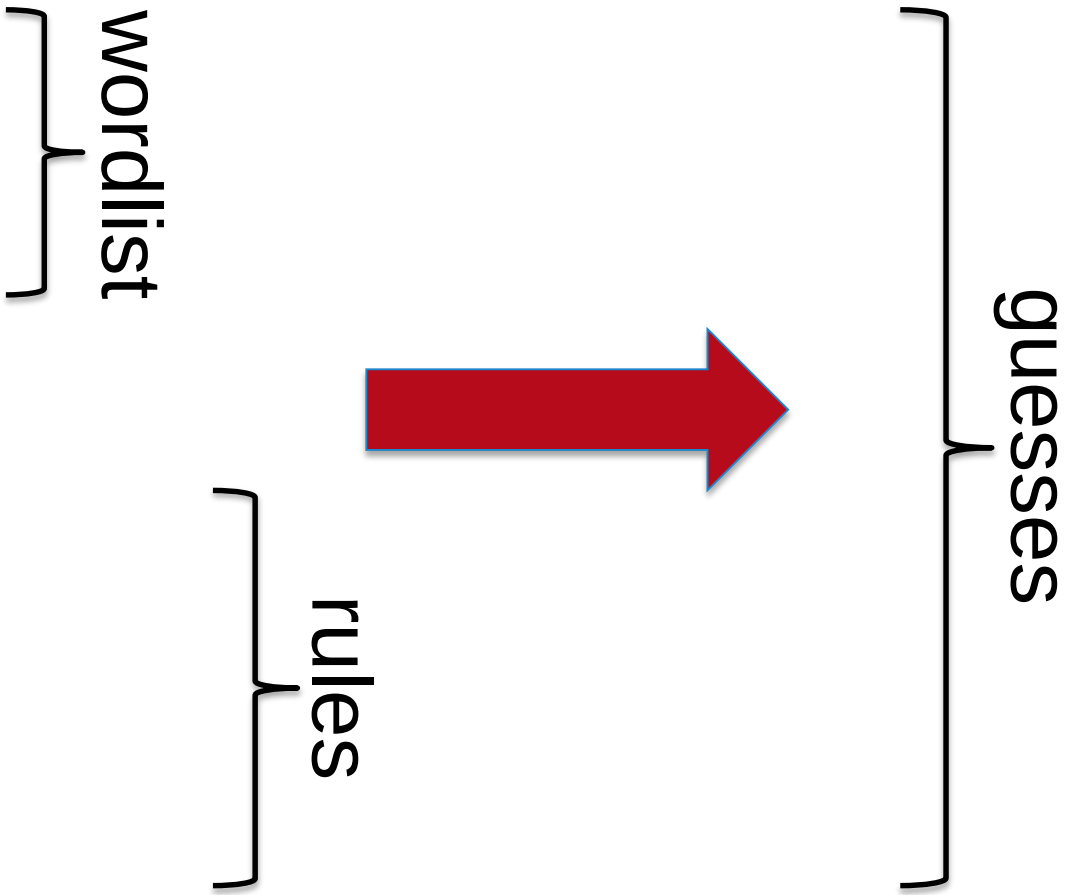
John the Ripper

- Guesses variants of input wordlist
- Wordlist mode requires:
  - Wordlist (passwords and dictionary entries)
  - Mangling rules
- Speed: Fast
  - 10^{13} guesses

John the Ripper

- Guesses variants of input wordlist
- Wordlist mode requires:
  - Wordlist (passwords and dictionary entries)
  - Mangling rules
- Speed: Fast
  - 10^{13} guesses
- “JTR”

John the Ripper



John the Ripper

usenix

security

wordlist

rules

guesses

John the Ripper

usenix

security

wordlist

[ ]

[add 1 at end]

[change e to 3]

rules

guesses

John the Ripper

usenix

security

wordlist

[ ]

[add 1 at end]

[change e to 3]

rules

usenix

security

usenix1

security1

us3nix

s3curity

guesses

John the Ripper

usenix

security

wordlist

[ ]

[add 1 at end]

[change e to 3]

rules

usenix

security

usenix1

security1

us3nix

s3curity

guesses

John the Ripper

usenix

security

wordlist

[ ]

[add 1 at end]

[change e to 3]

rules

usenix

security

usenix1

security1

us3nix

s3curity

guesses

Hashcat

- Guesses variants of input wordlist

Hashcat

- Guesses variants of input wordlist
- Wordlist mode requires:
  - Wordlist (passwords and dictionary entries)
  - Mangling rules

Hashcat

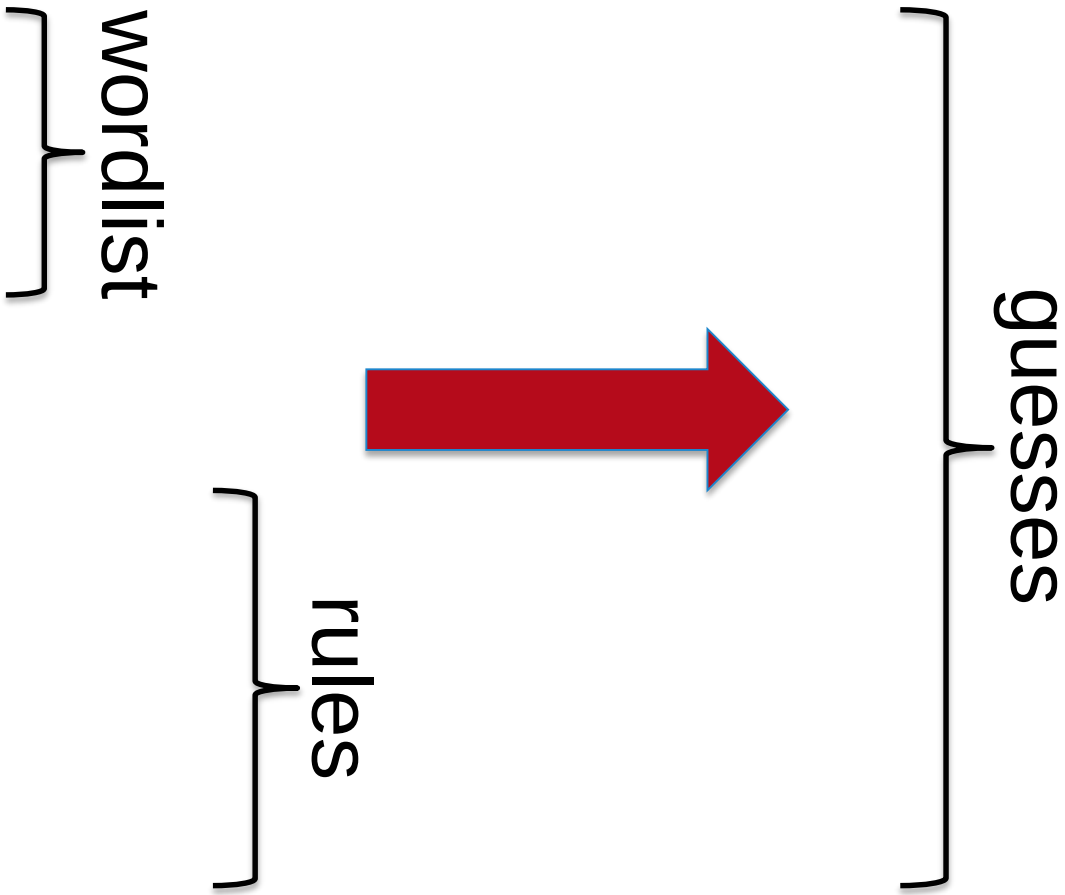
- Guesses variants of input wordlist
- Wordlist mode requires:
  - Wordlist (passwords and dictionary entries)
  - Mangling rules
- Speed: Fast

Hashcat

- Guesses variants of input wordlist
- Wordlist mode requires:
  - Wordlist (passwords and dictionary entries)
  - Mangling rules
- Speed: Fast
  - 10^{13} guesses

Hashcat


hashcat
advanced
password
recovery


wordlist
rules
guesses

Hashcat

usenix

security

wordlist

[ ]

[add 1 at end]

[change e to 3]

rules

guesses

Hashcat

usenix

security

wordlist

usenix

usenix1

us3nix

[ ]

[add 1 at end]

[change e to 3]

rules

security

security1

s3curity

guesses

Hashcat

usenix

security

wordlist

[ ]

[add 1 at end]

[change e to 3]

rules

usenix

usenix1

us3nix

security

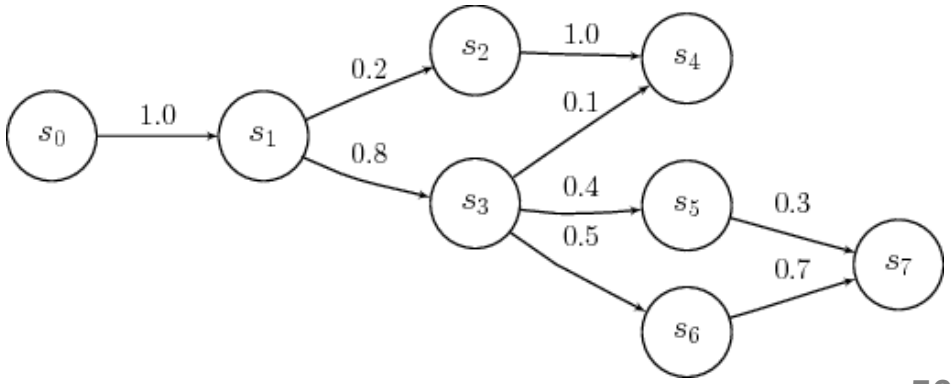
security1

s3curity

guesses

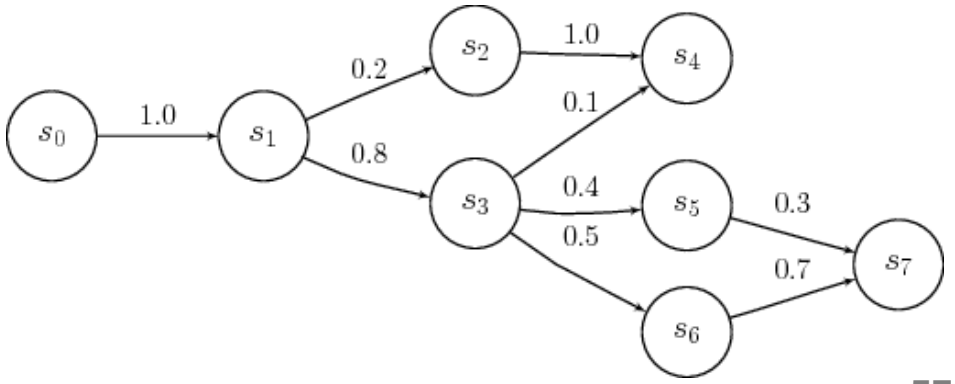
Markov Models

- Predicts future characters from previous



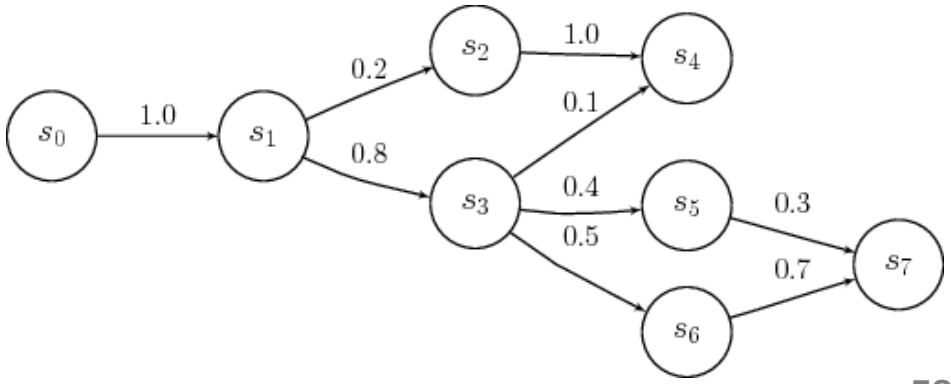
Markov Models

- Predicts future characters from previous
- Approach requires weighted data:
  - Passwords
  - Dictionaries



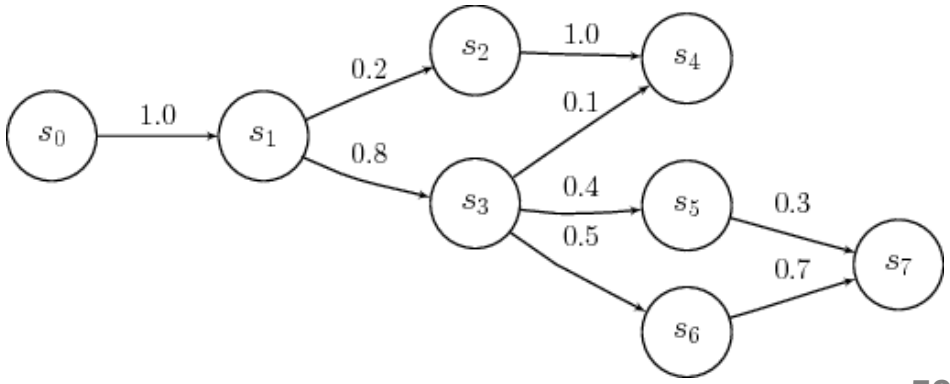
Markov Models

- Predicts future characters from previous
- Approach requires weighted data:
  - Passwords
  - Dictionaries
- Ma et al. IEEE S&P 2014



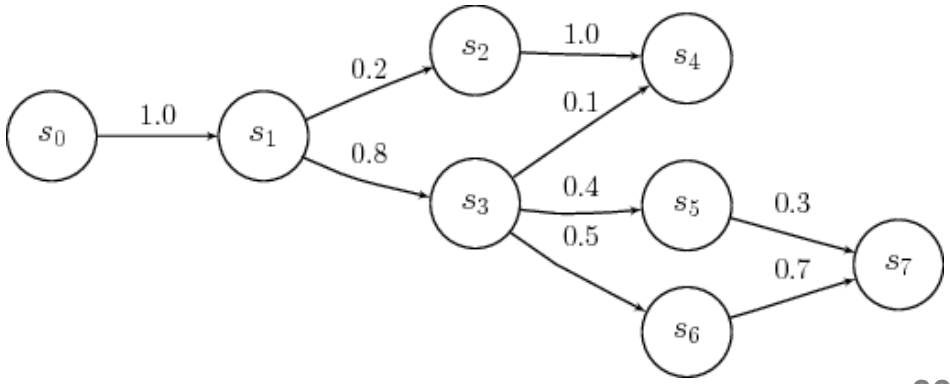
Markov Models

- Predicts future characters from previous
- Approach requires weighted data:
  - Passwords
  - Dictionaries
- Ma et al. IEEE S&P 2014
- Speed: Slow



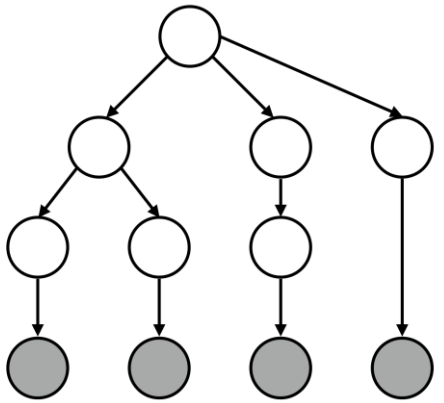
Markov Models

- Predicts future characters from previous
- Approach requires weighted data:
  - Passwords
  - Dictionaries
- Ma et al. IEEE S&P 2014
- Speed: Slow
  - 10^{10} guesses



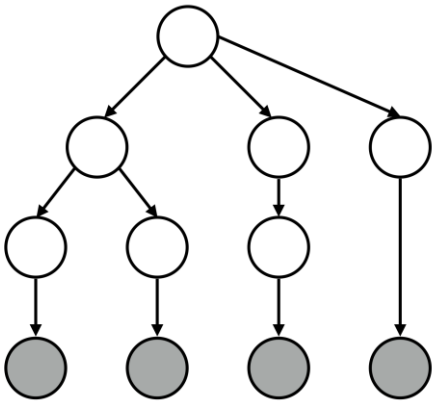
Probabilistic Context-Free Grammar

- Generate password grammar
  - Structures
  - Terminals



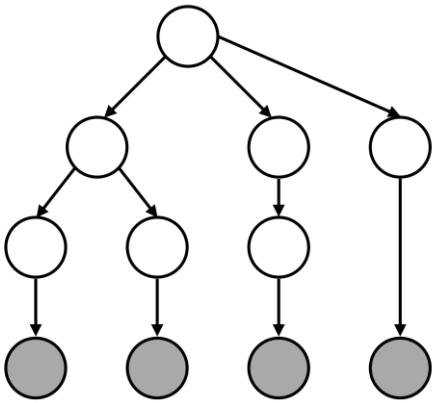
Probabilistic Context-Free Grammar

- Generate password grammar
  - Structures
  - Terminals
- Kelley et al. IEEE S&P 2012
  - Based on Weir et al. IEEE S&P 2009



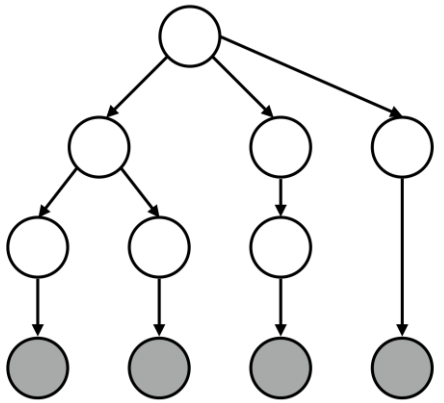
Probabilistic Context-Free Grammar

- Generate password grammar
  - Structures
  - Terminals
- Kelley et al. IEEE S&P 2012
  - Based on Weir et al. IEEE S&P 2009
- Speed: ~~Slow~~ Medium



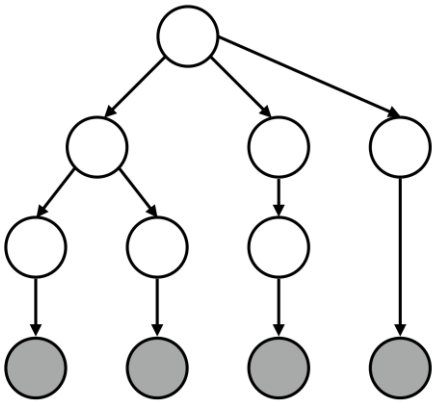
Probabilistic Context-Free Grammar

- Generate password grammar
  - Structures
  - Terminals
- Kelley et al. IEEE S&P 2012
  - Based on Weir et al. IEEE S&P 2009
- Speed: ~~Slow~~ Medium
  - 10^{14} guesses



Probabilistic Context-Free Grammar

- Generate password grammar
  - Structures
  - Terminals
- Kelley et al. IEEE S&P 2012
  - Based on Weir et al. IEEE S&P 2009
- Speed: ~~Slow~~ Medium
  - 10^{14} guesses
- “PCFG”



Professionals (“Pros”)

Professionals (“Pros”)

- Contracted KoreLogic
  - Password audits for Fortune 500 companies
  - Run DEF CON “Crack Me If You Can”

KoreLogic SECURITY

Professionals (“Pros”)

- Contracted KoreLogic
  - Password audits for Fortune 500 companies
  - Run DEF CON “Crack Me If You Can”
- Proprietary wordlists and configurations

KoreLogic SECURITY

Professionals (“Pros”)

- Contracted KoreLogic
  - Password audits for Fortune 500 companies
  - Run DEF CON “Crack Me If You Can”
- Proprietary wordlists and configurations
  - 10^{14} guesses

KoreLogic SECURITY

Professionals (“Pros”)

- Contracted KoreLogic
  - Password audits for Fortune 500 companies
  - Run DEF CON “Crack Me If You Can”
- Proprietary wordlists and configurations
  - 10^{14} guesses
  - Manually tuned, updated

KoreLogic SECURITY

Approach

4 password sets

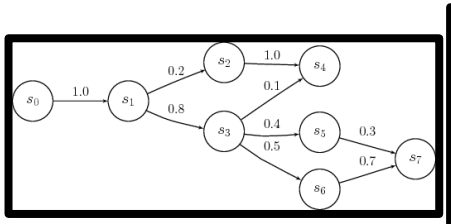
```
password
iloveyou
teamo123
…
```

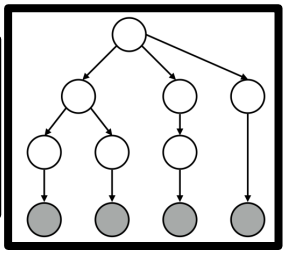
```
passwordpassword
1234567812345678
!1@2#3$4%5^6&7*8
…
```

```
Pa$$w0rd
iLov3you!
1QaZ2W@x
…
```

```
pa$$word1234
12345678asDF
!q1q!q1q!q1q
…
```

✖ 5 approaches



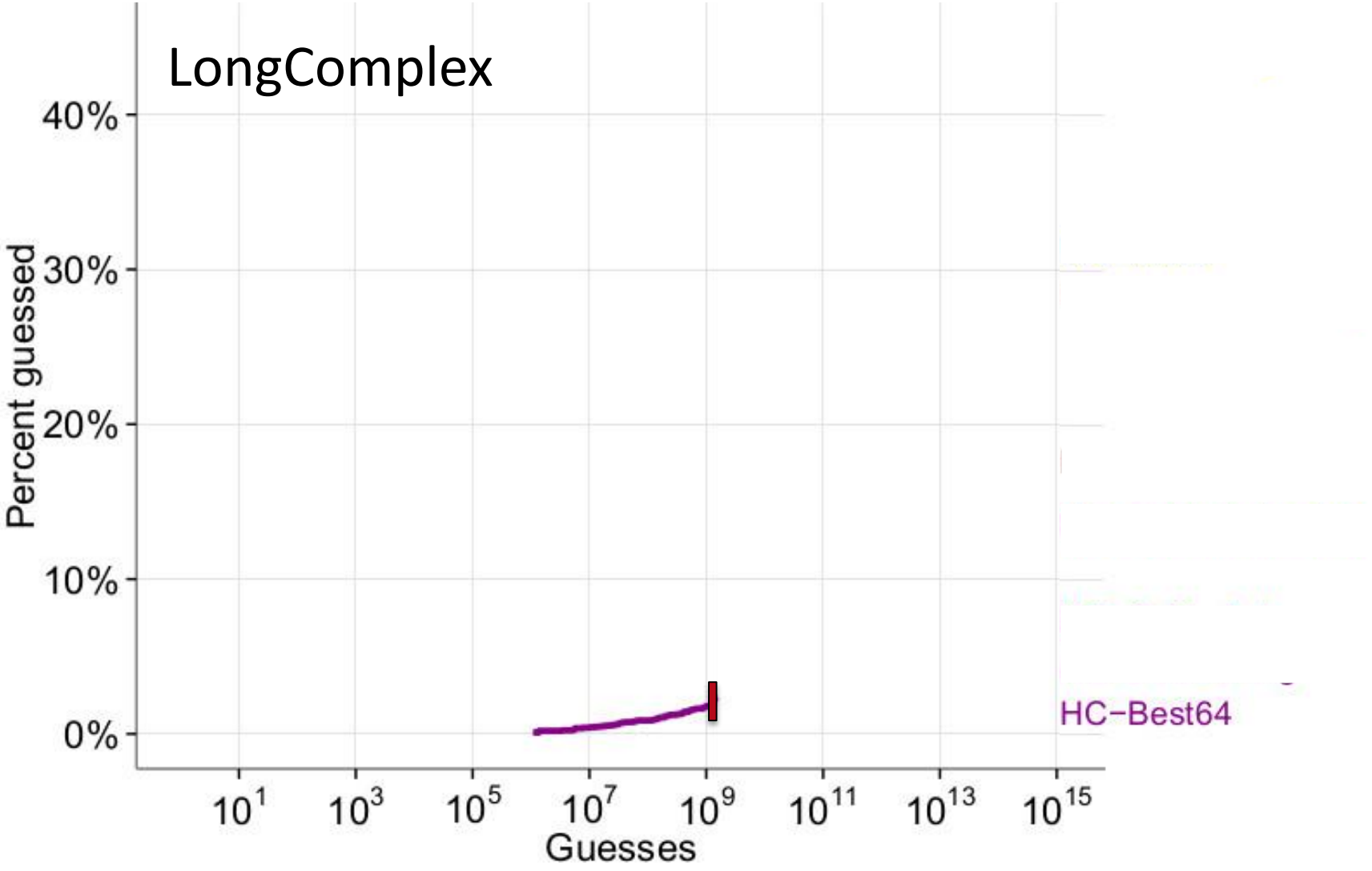


KoreLogic SECURITY

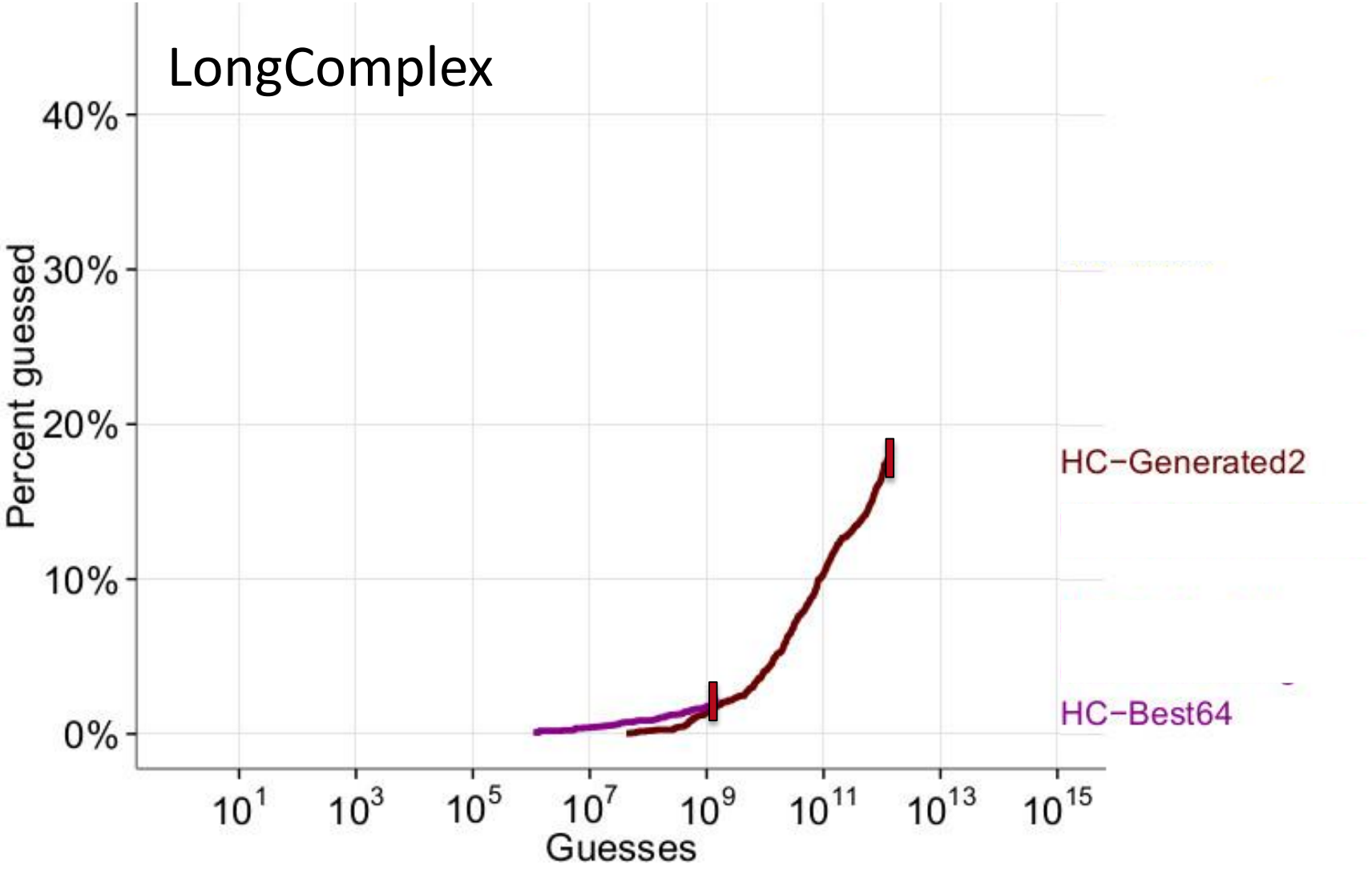
Outline of Results

- Importance of Configuration
- Comparison of Approaches
- Impact on Research Analyses

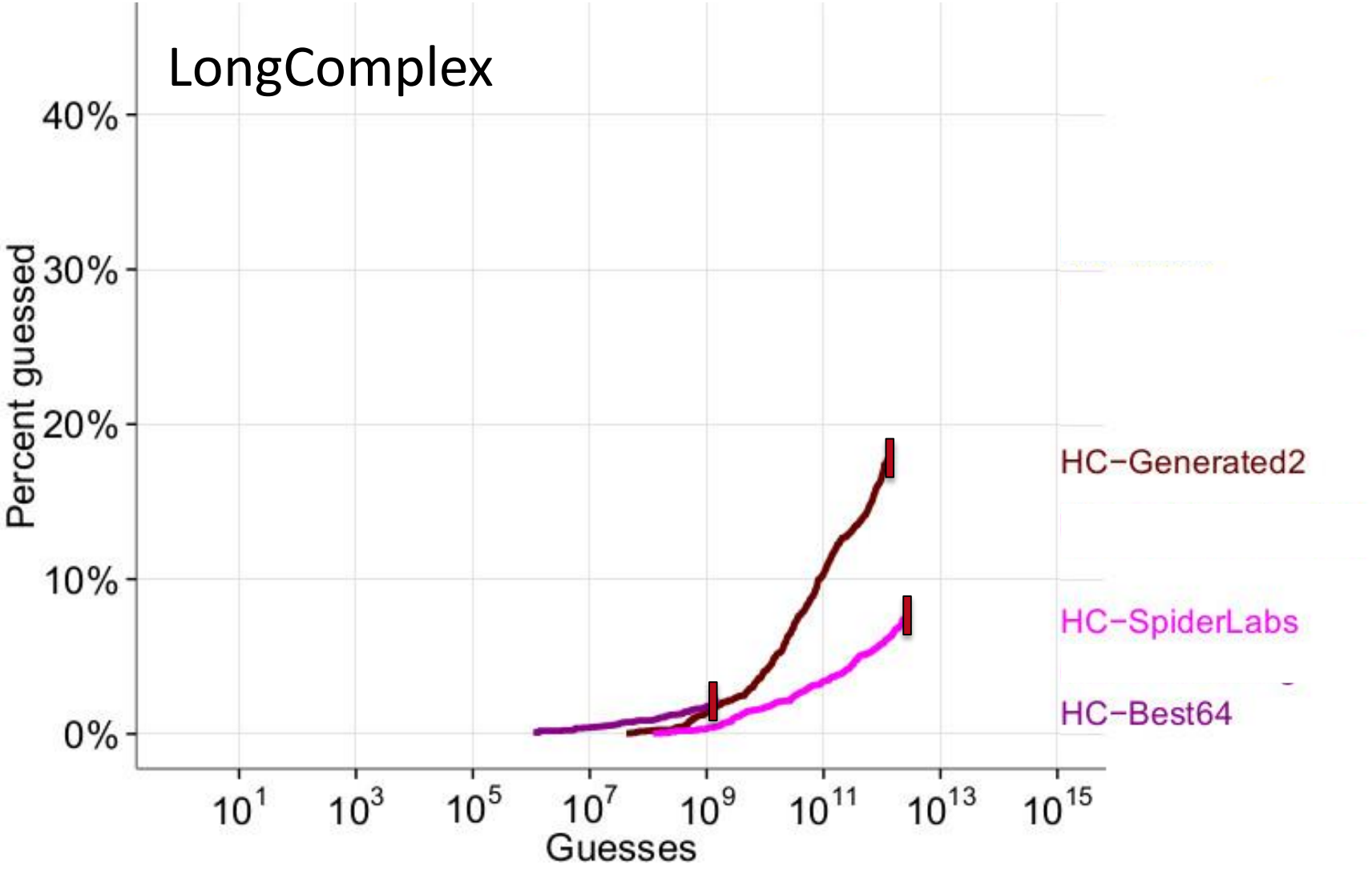
Configuration Is Crucial



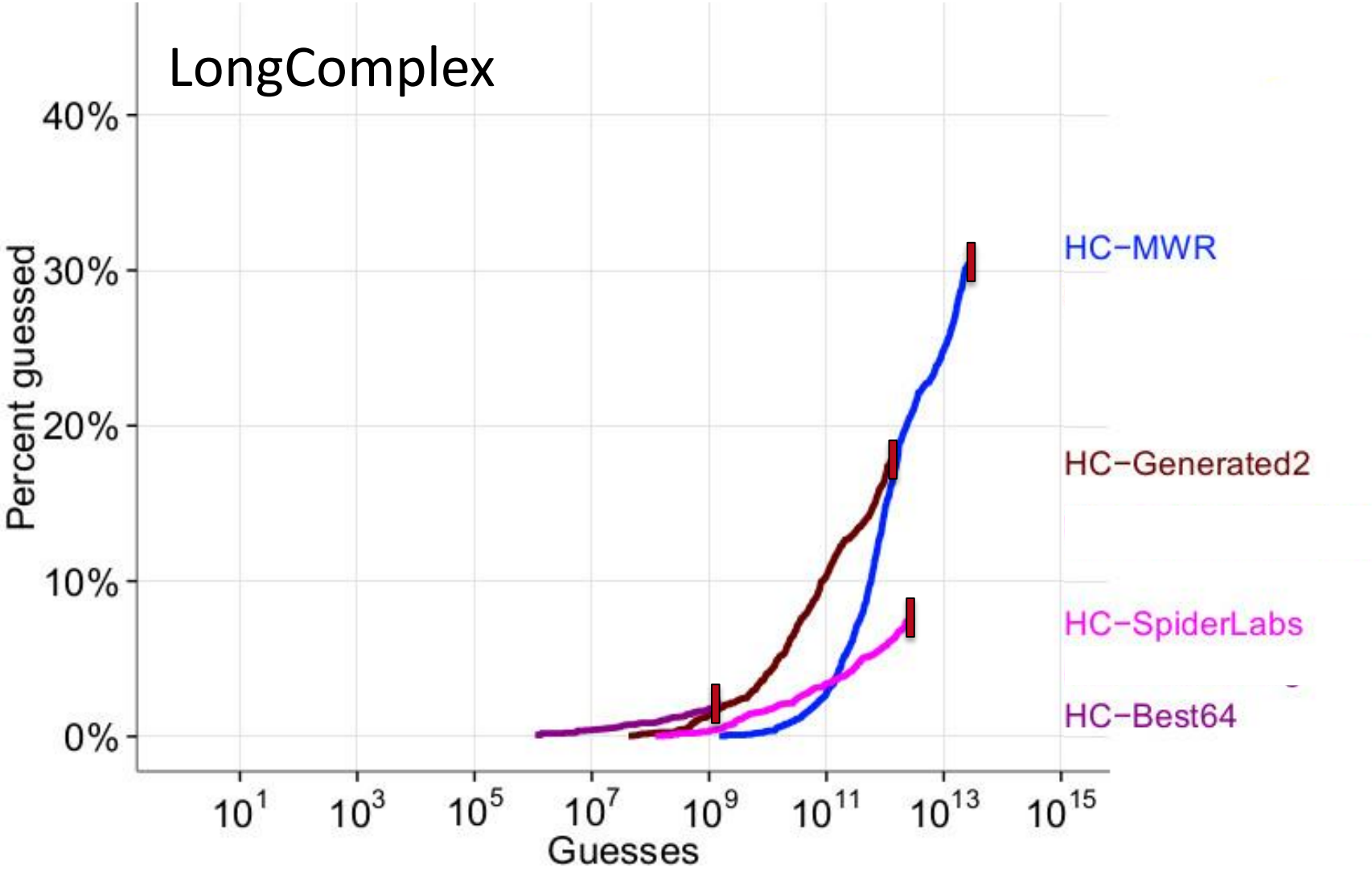
Configuration Is Crucial



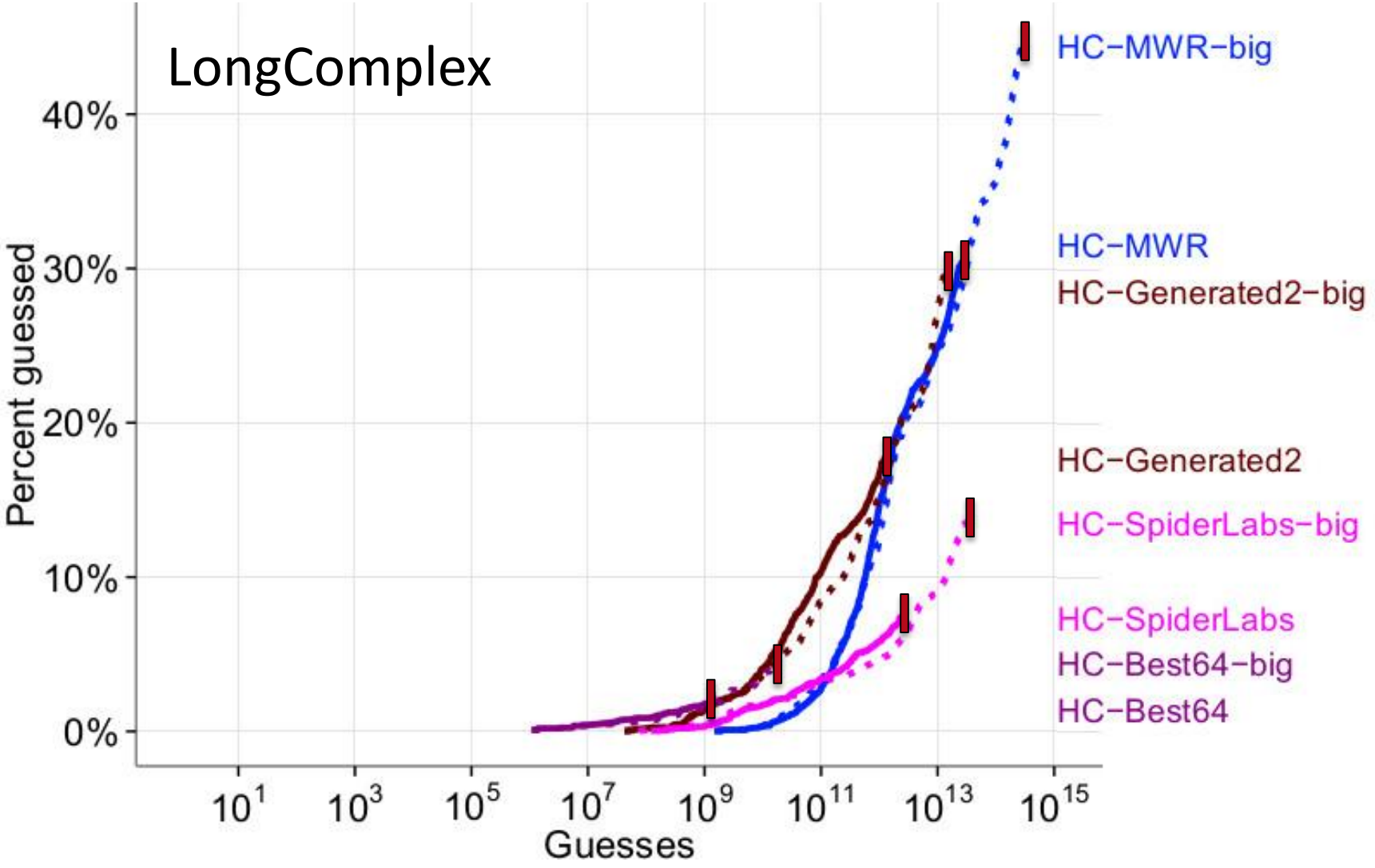
Configuration Is Crucial



Configuration Is Crucial



Configuration Is Crucial

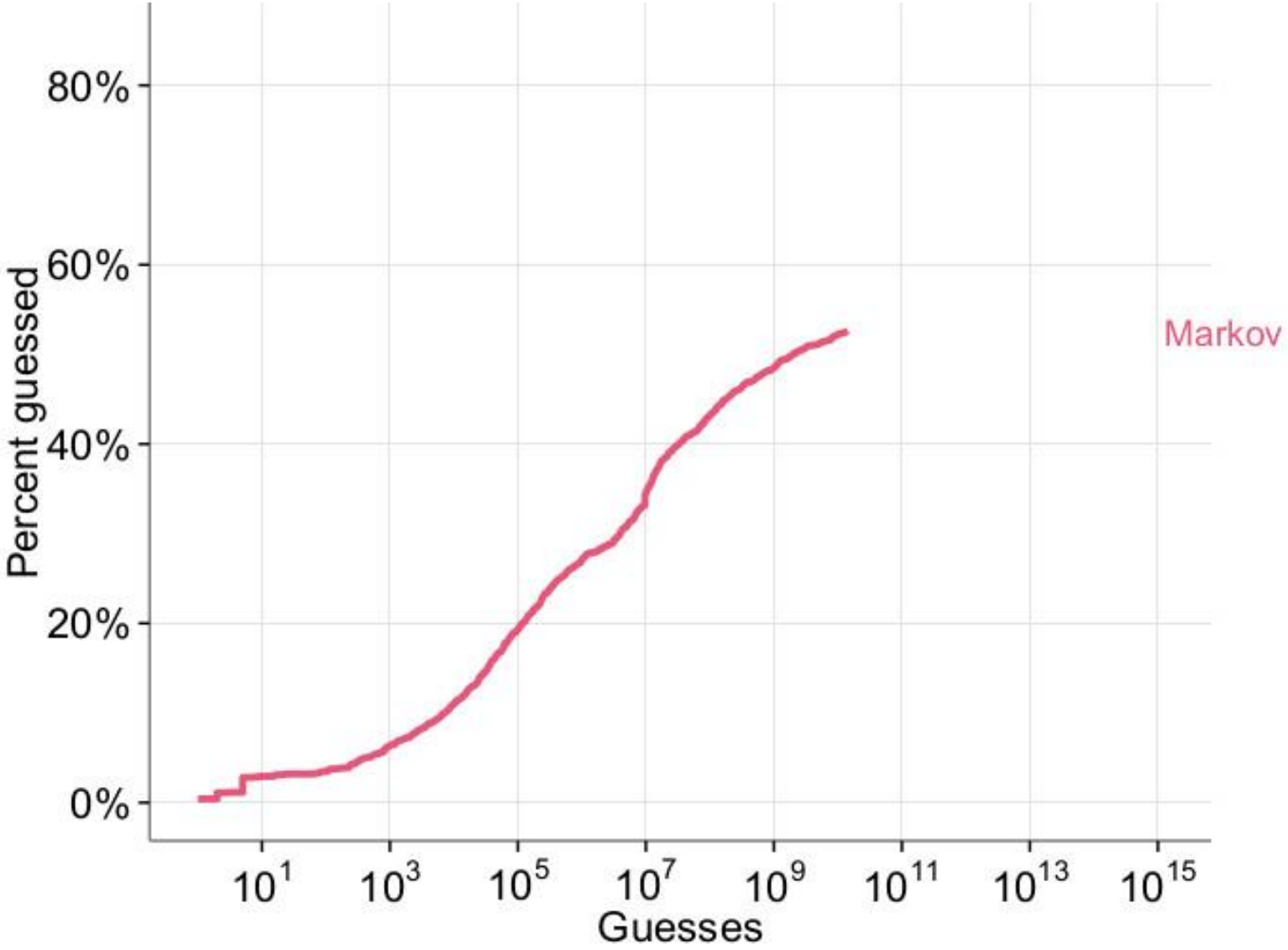


Outline of Results

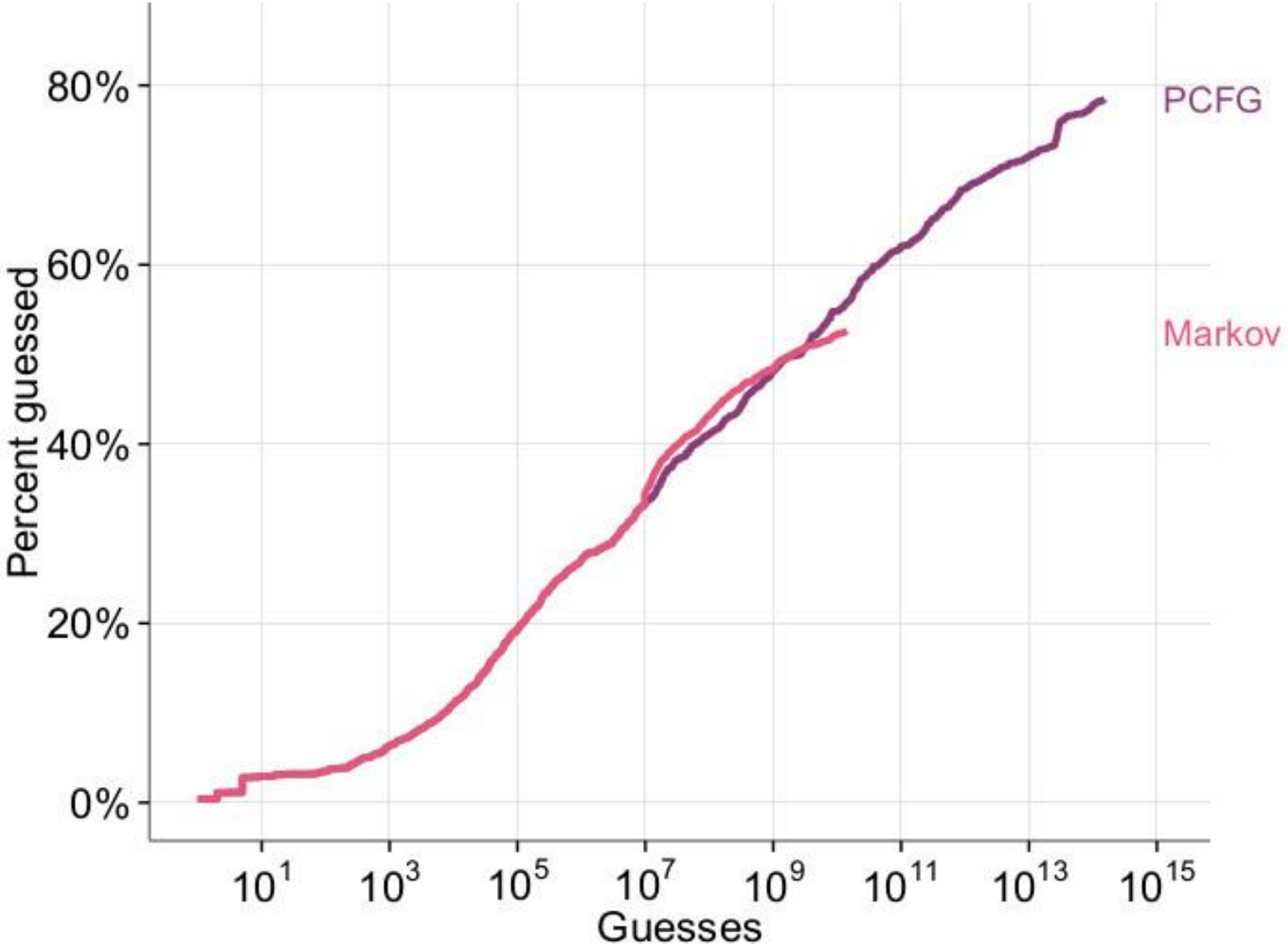
- Importance of Configuration
- Comparison of Approaches
- Impact on Research Analyses

Comparison for Basic Passwords

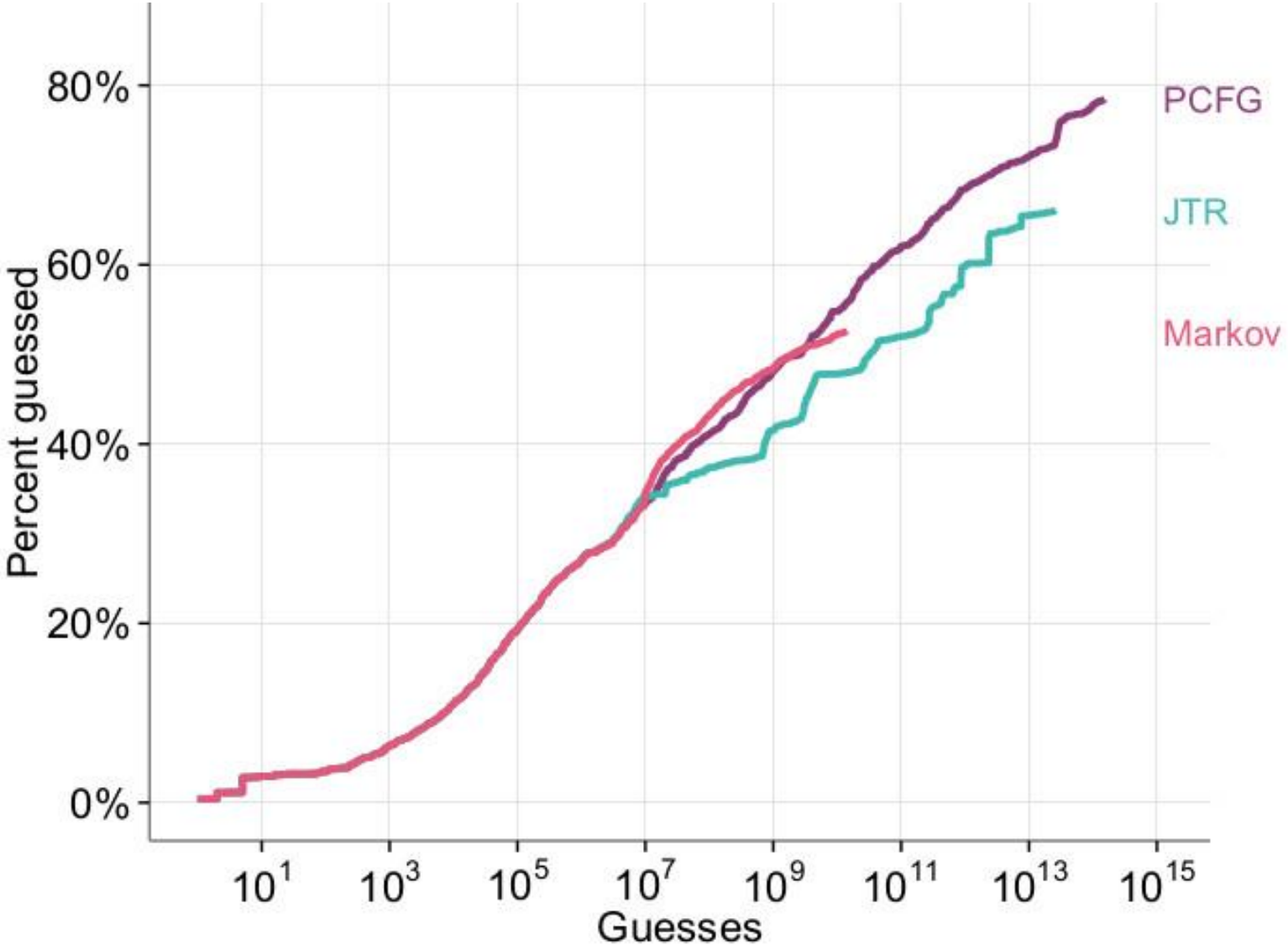
Comparison for Basic Passwords



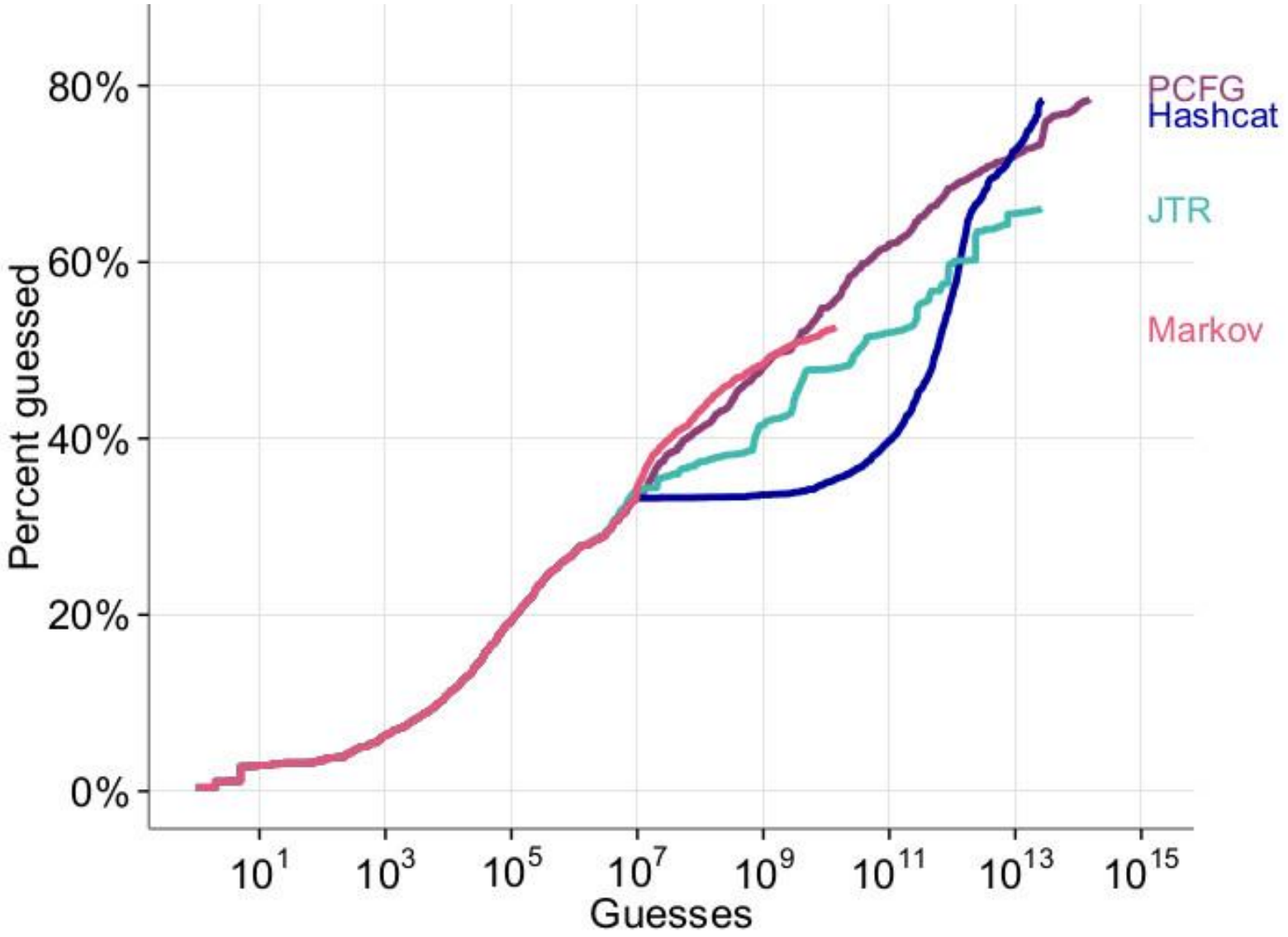
Comparison for Basic Passwords



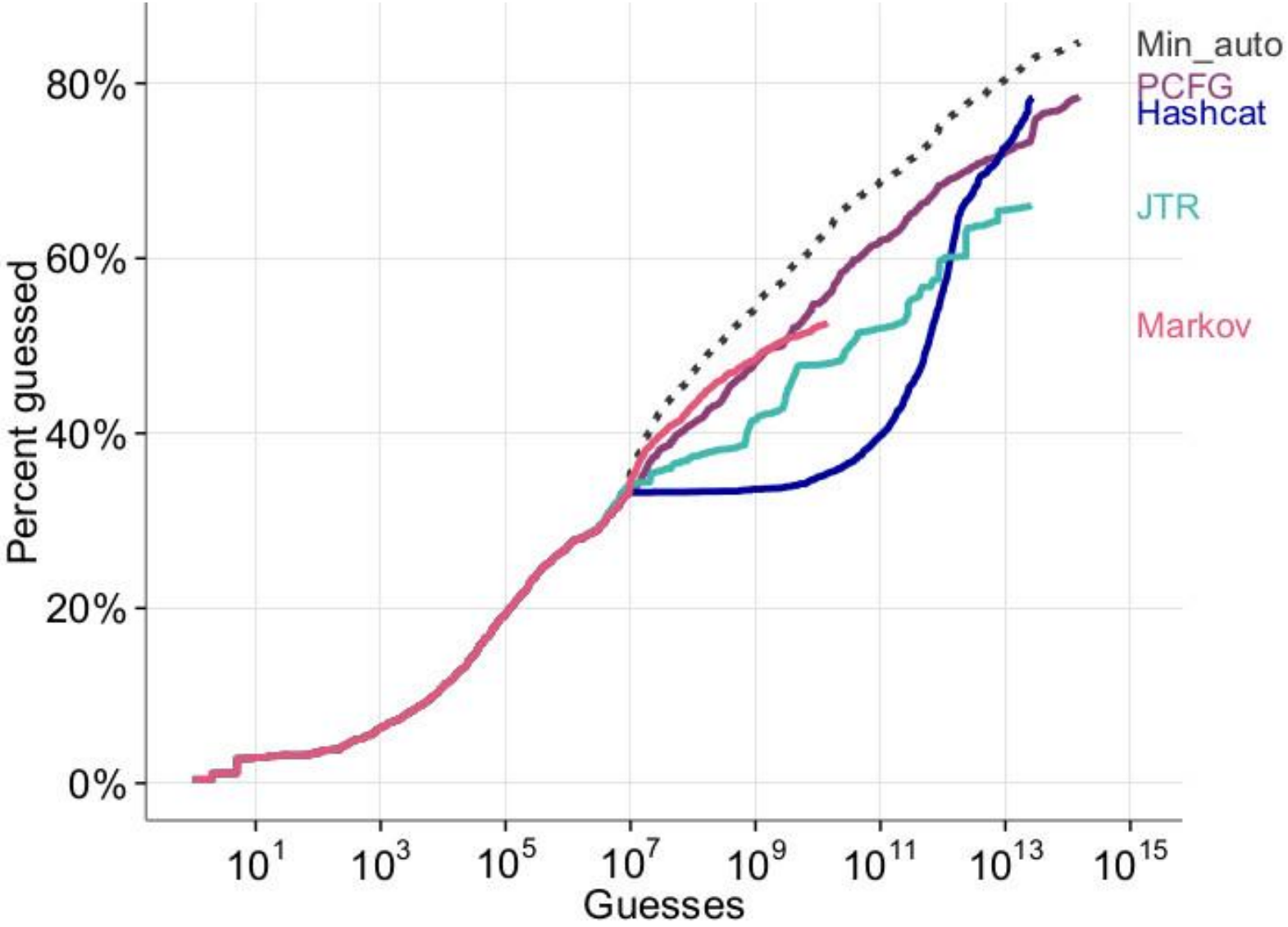
Comparison for Basic Passwords



Comparison for Basic Passwords

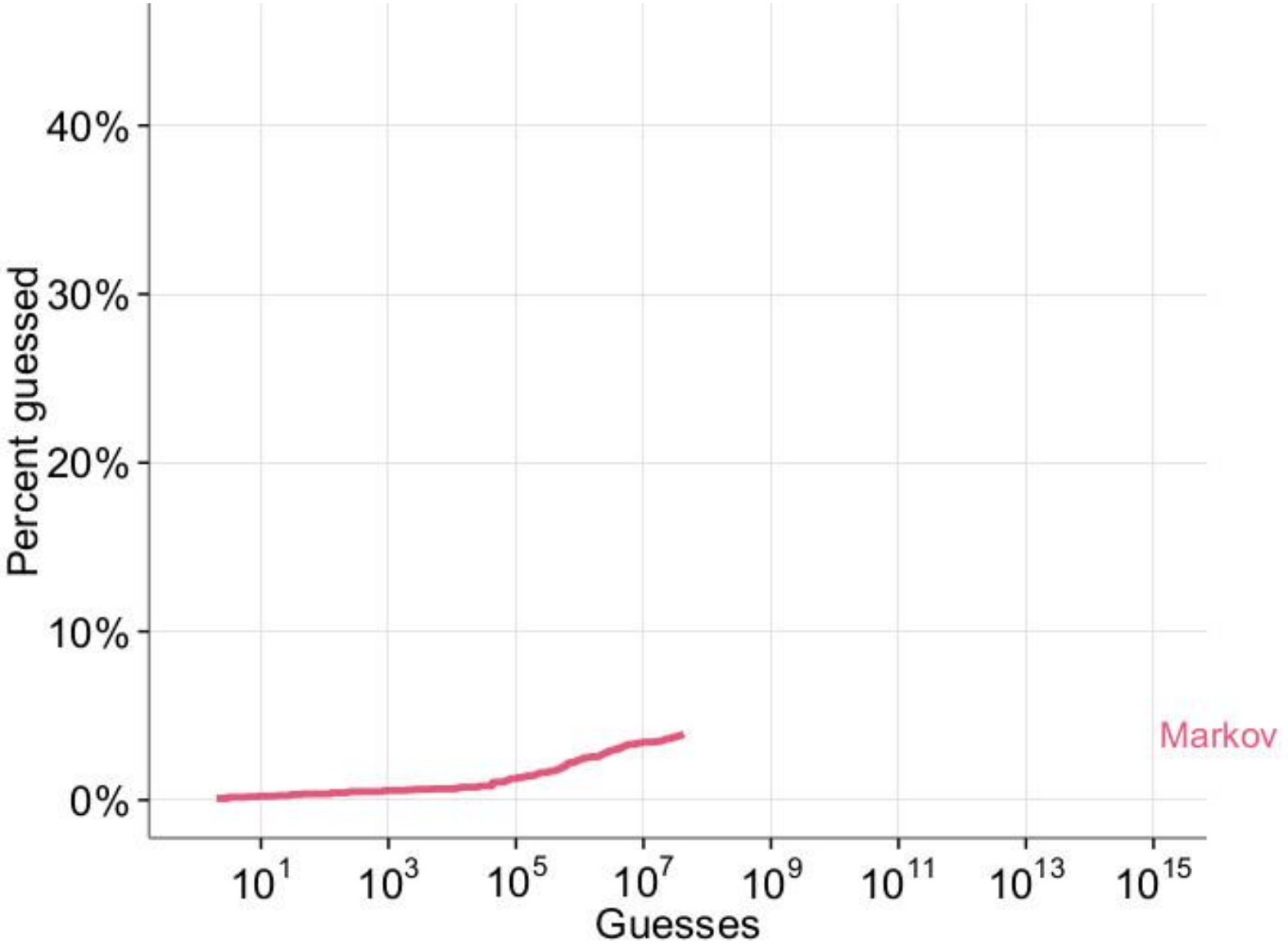


Comparison for Basic Passwords

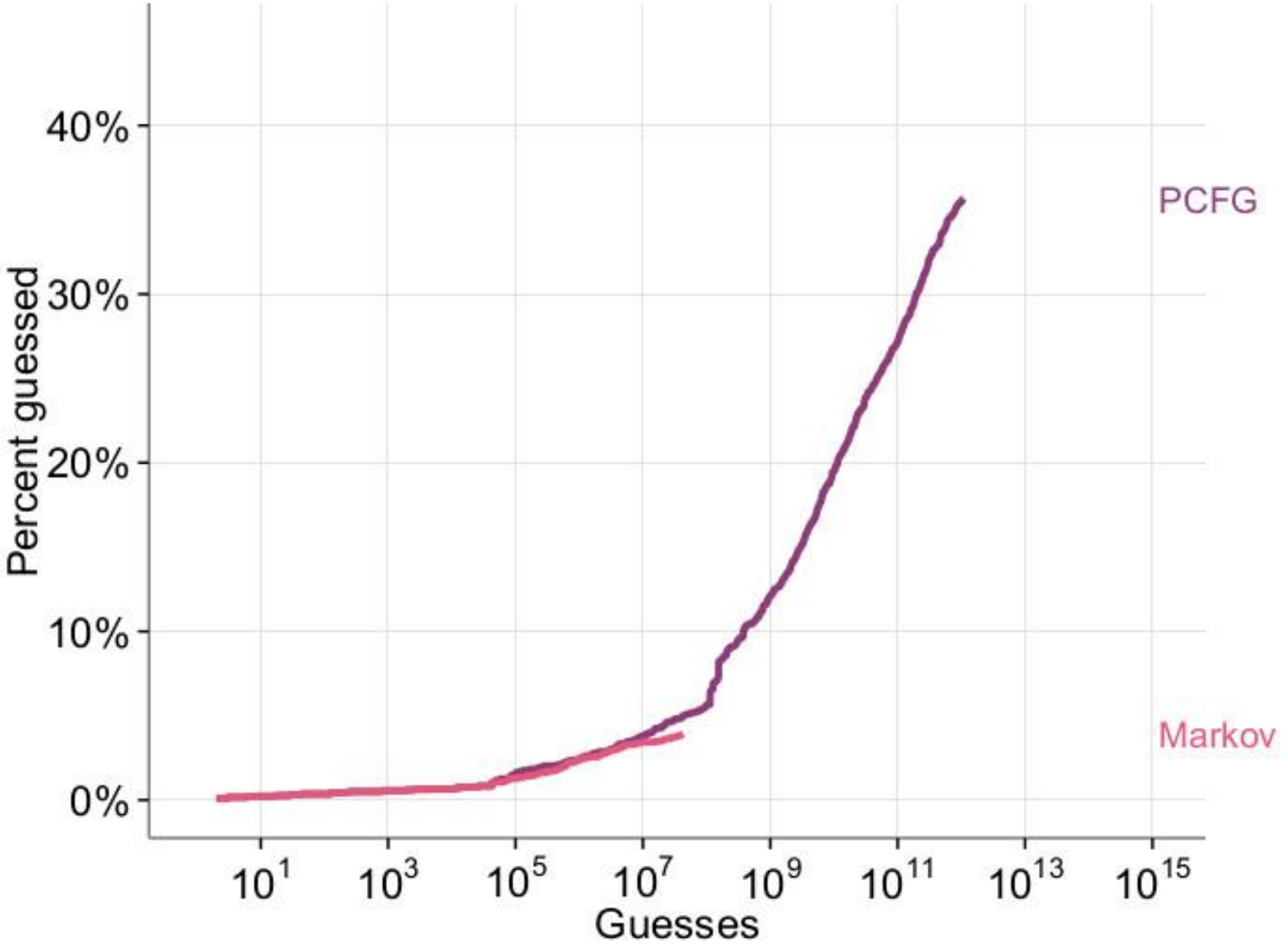


Comparison for Complex Passwords

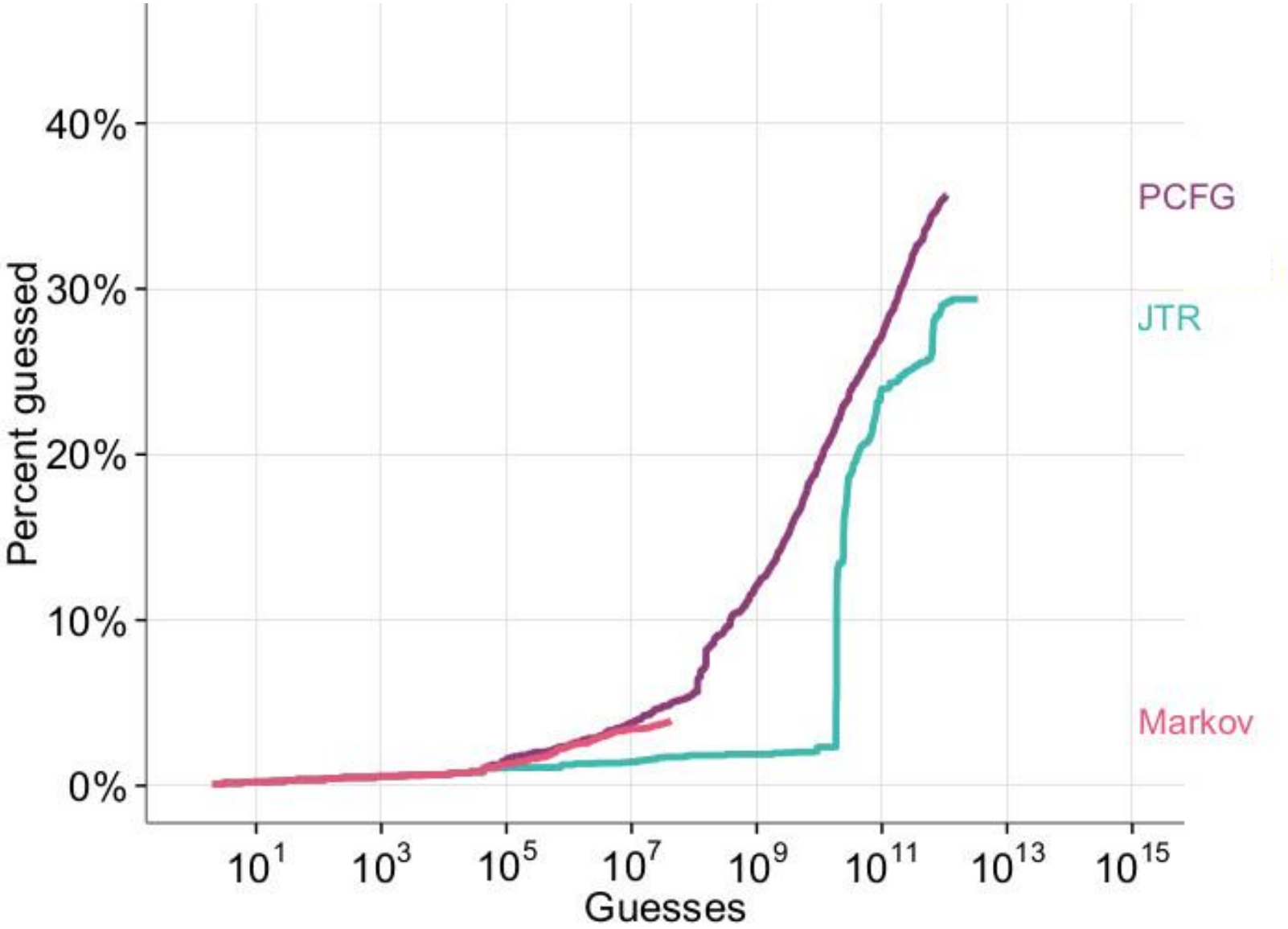
Comparison for Complex Passwords



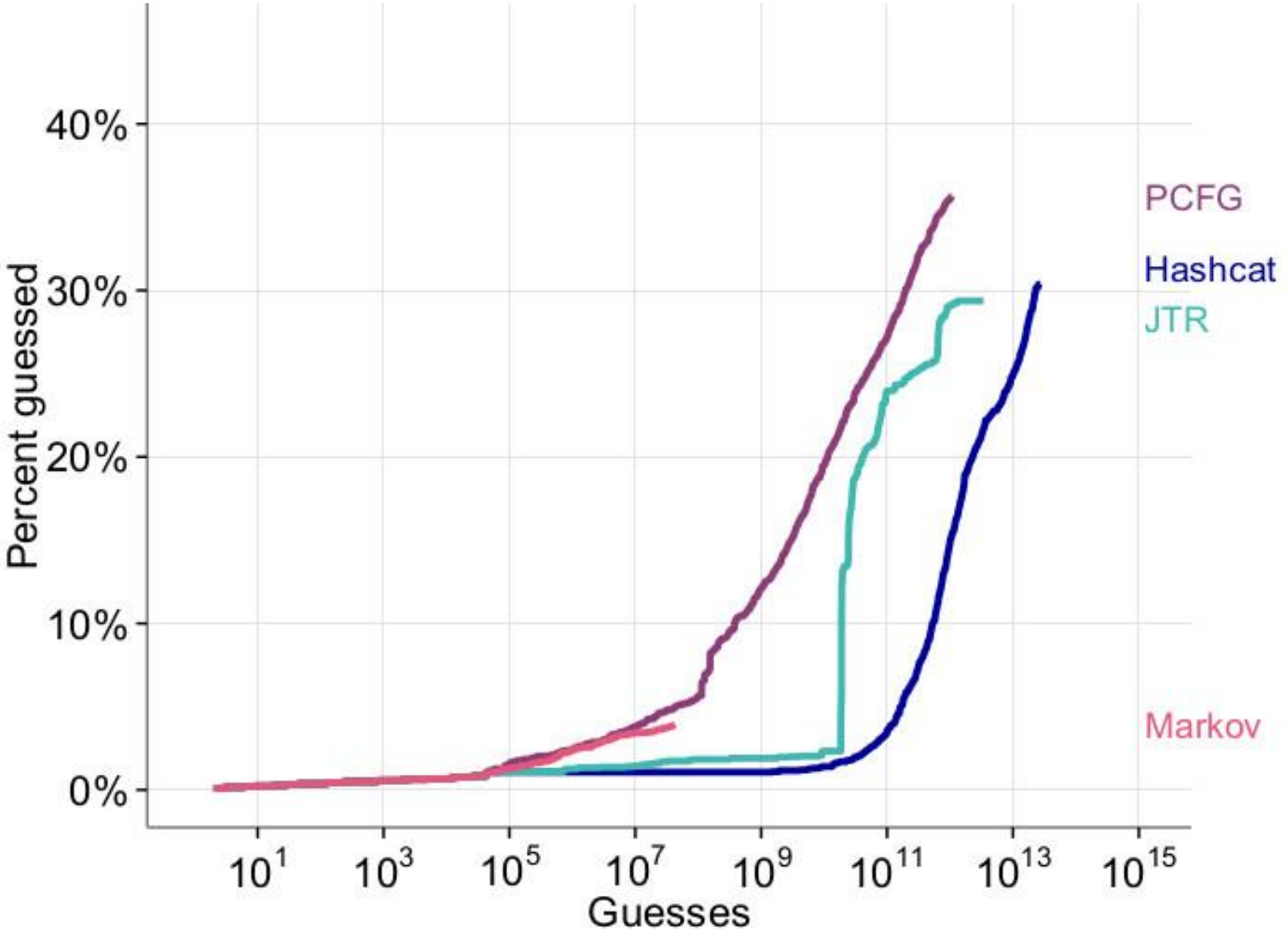
Comparison for Complex Passwords



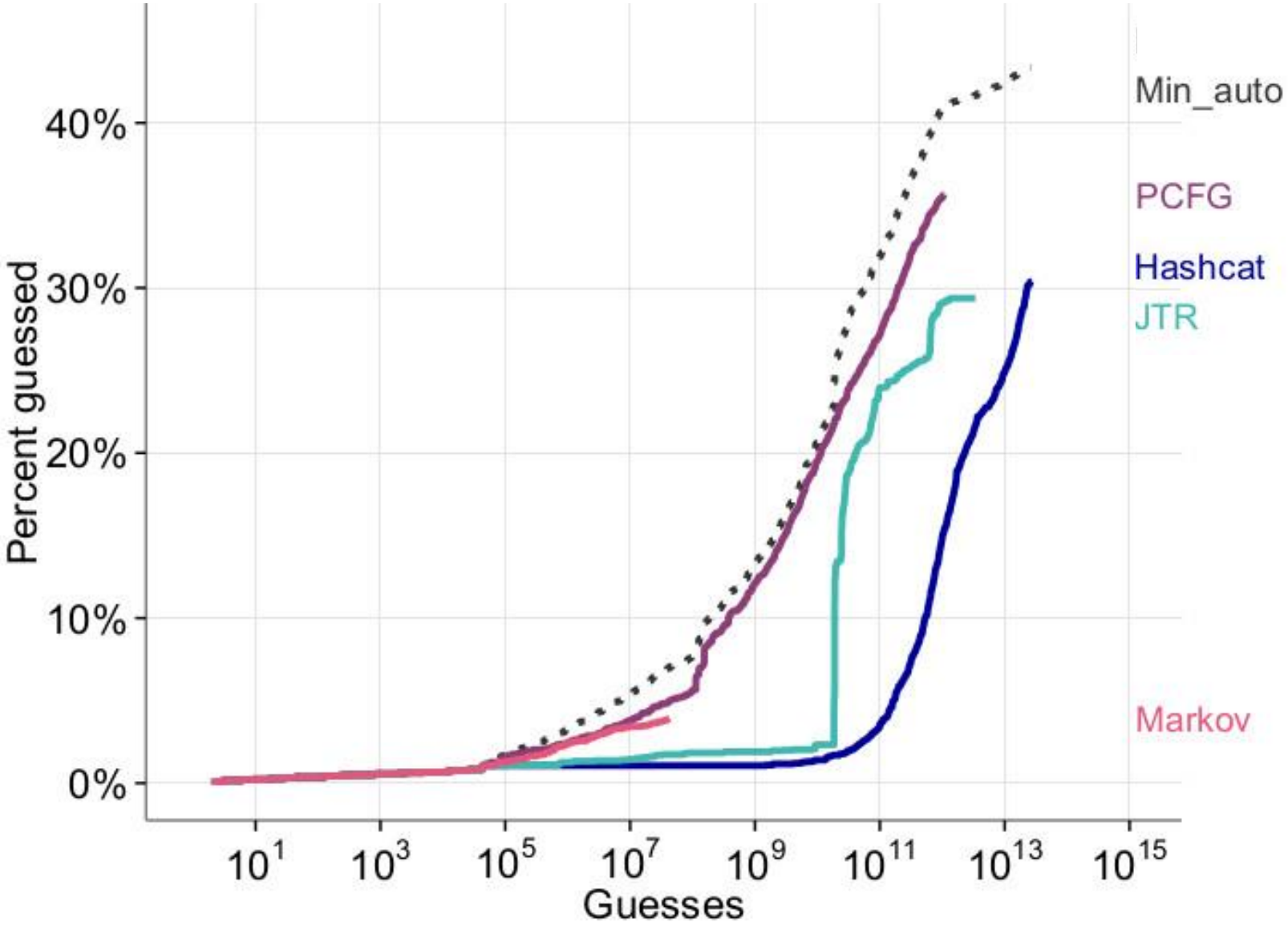
Comparison for Complex Passwords



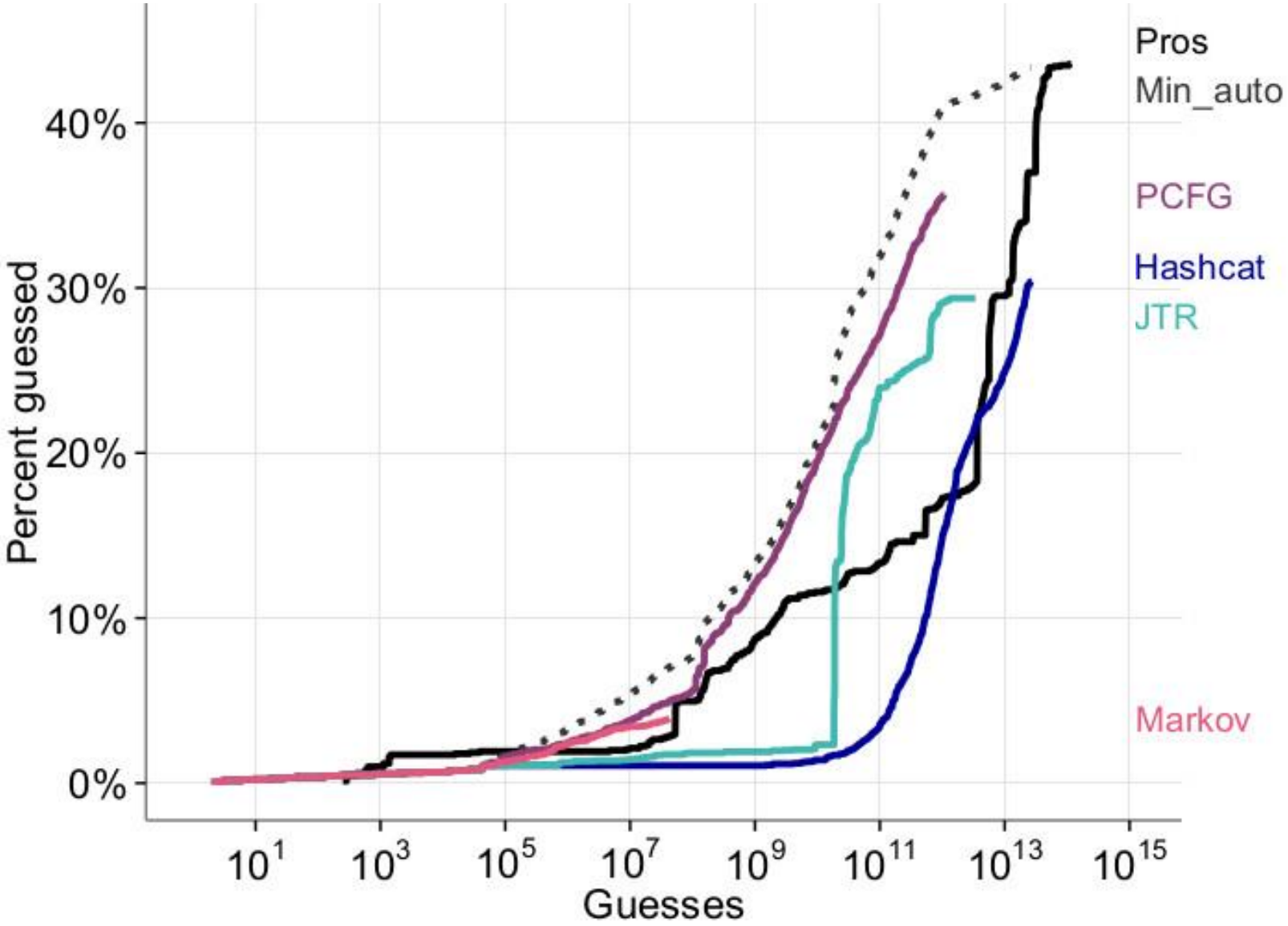
Comparison for Complex Passwords



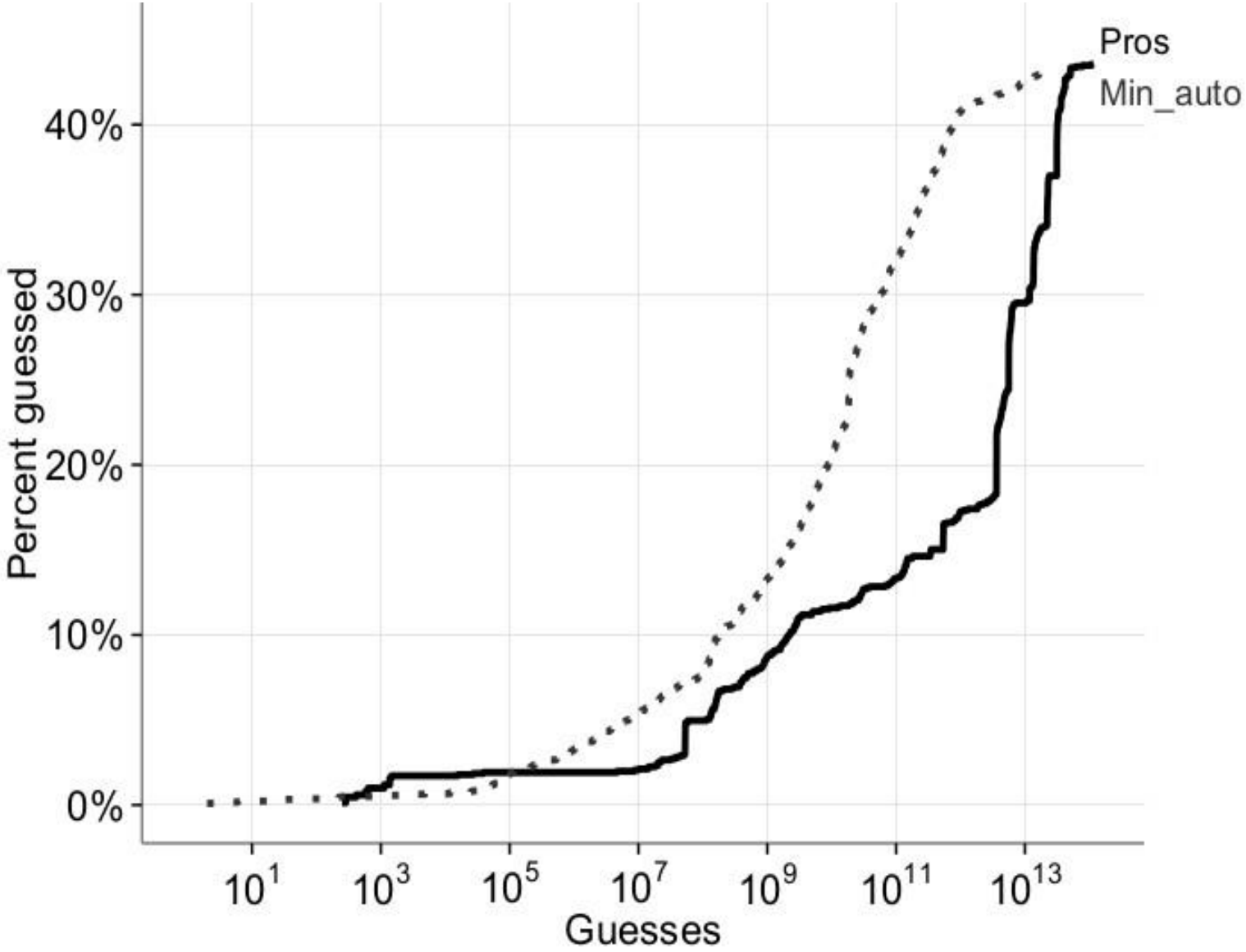
Comparison for Complex Passwords



Comparison for Complex Passwords



Min_auto Conservative Proxy for Pros



Outline of Results

- Importance of Configuration
- Comparison of Approaches
- Impact on Research Analyses

Impact on Research

- Coarse-grained analyses
- Fine-grained analyses
- Analysis of one password

Impact on Research

- Coarse-grained analyses **same results**
- Fine-grained analyses
- Analysis of one password

Impact on Research

- Coarse-grained analyses **same results**
- Fine-grained analyses **different**
- Analysis of one password

Impact on Research

- Coarse-grained analyses **same results**
- Fine-grained analyses **different**
- Analysis of one password **different**

Per-Password Highly Impacted

P@ssw0rd!

Per-Password Highly Impacted

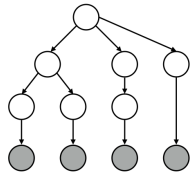
- JTR guess # 801 

P@ssw0rd!

Per-Password Highly Impacted

- JTR guess # 801

- Not guessed in 10^{14} PCFG guesses

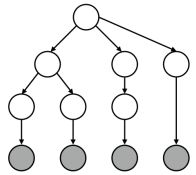


P@ssw0rd!

Per-Password Highly Impacted

- JTR guess # 801

- Not guessed in 10^{14} PCFG guesses



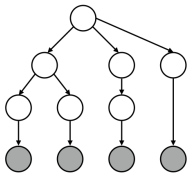
P@ssw0rd!

Per-Password Highly Impacted

```
12345678password
```

Per-Password Highly Impacted

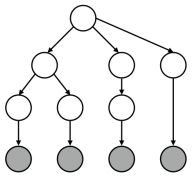
- PCFG guess # 130,555



12345678password

Per-Password Highly Impacted

- PCFG guess # 130,555



- Not guessed in 10^{10} JTR guesses


```
12345678password
```

Conclusions

Conclusions

- Running a single approach is insufficient
  - Especially out of the box

Conclusions

- Running a single approach is insufficient
  - Especially out of the box
- Min_auto conservative proxy for pros

Conclusions

- Running a single approach is insufficient
  - Especially out of the box
- Min_auto conservative proxy for pros
- Coarse-grained analyses **same results**
- Fine-grained analyses **different**
- Analysis of one password **different**

Password Guessability Service (PGS)

- Guessability of plaintext passwords

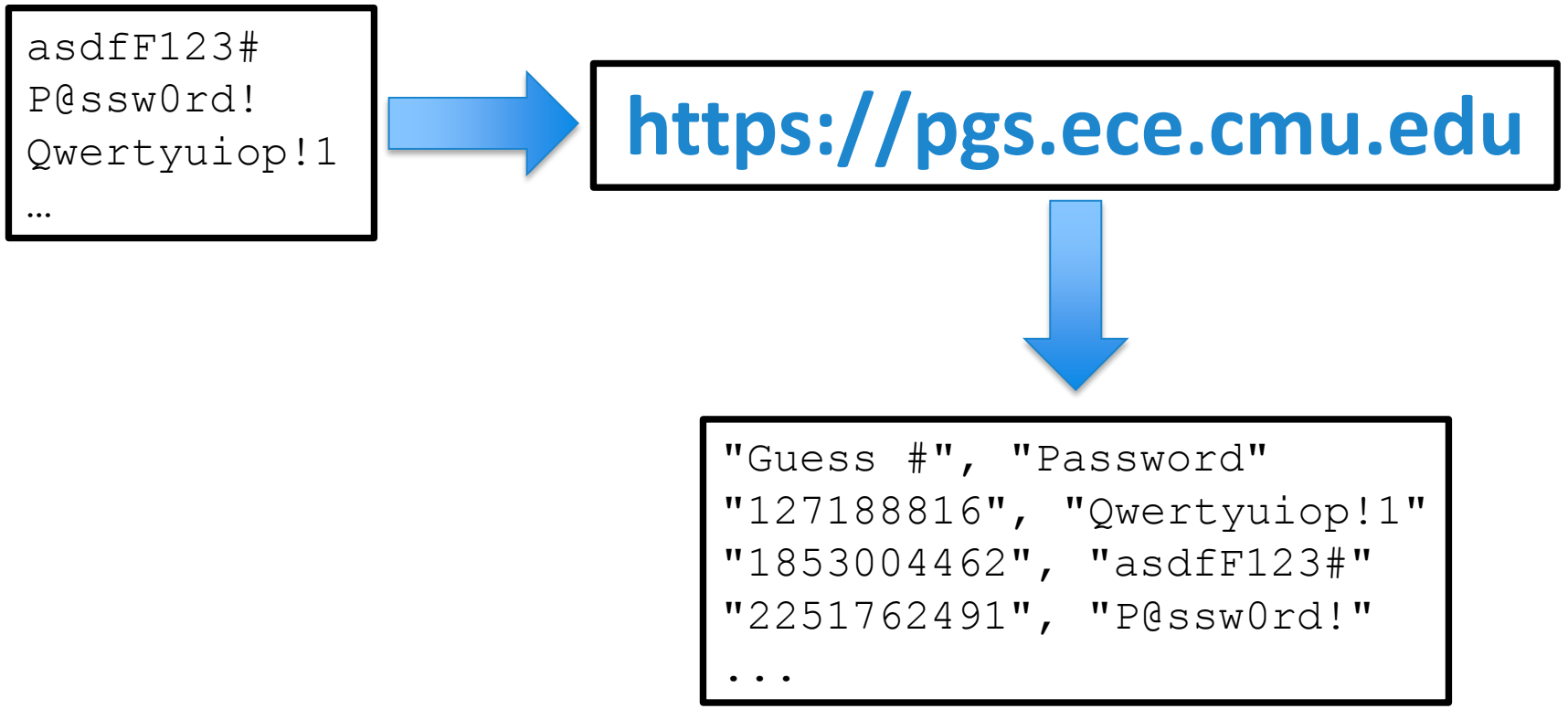
https://pgs.ece.cmu.edu

Password Guessability Service (PGS)

- Guessability of plaintext passwords

Password Guessability Service (PGS)

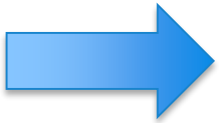
- Guessability of plaintext passwords



Password Guessability Service (PGS)

- Guessability of plaintext passwords

```
asdfF123#
P@ssw0rd!
Qwertyuiop!1
…
```



https://pgs.ece.cmu.edu


```
"Guess #", "Password"
"127188816", "Qwertyuiop!1"
"1853004462", "asdfF123#"
"2251762491", "P@ssw0rd!"
...
```

Measuring Real-World Accuracies and Biases in Modeling Password Guessability

https://pgs.ece.cmu.edu

Blase Ur, Sean M. Segreti, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Saranga Komanduri, Darya Kurilova, Michelle L. Mazurek, William Melicher, Richard Shay

Carnegie Mellon

UNIVERSITY OF MARYLAND

Acknowledgments

- Per Thorsheim and Jeremi Gosney (PasswordsCon)
- Hashcat / JTR developers
- Matt Marx (@tehnlulz)
- Jerry Ma, Weining Yang, Ninghui Li (Purdue)
- KoreLogic (@CrackMeIfYouCan)
- Dustin Heywood (@Evil_Mog)
- Jonathan Bees
- Michael Stroucken and Chuck Cranor (CMU)

114