Digit Semantics based Optimization for Practical Password Cracking Tools

Haodong Zhang, Chuanwang Wang, Wenqiang Ruan, Junjie Zhang, Ming Xu, Weili Han

Presenter: Haodong Zhang

Laboratory for Data Analytics and Security, Fudan University

Shanghai Key Laboratory of Data Science, Fudan University

Introduction

Textual passwords

One of the most widely used authentication schemes at present

- Low cost
- Friendly usage

Users lean to make password meaningful by employing semantic patterns in order to facilitate memorization and input.

Semantics represented with digits (digit semantics) Date, Phone, Postcode …

- Largely missed in most studies on password semantics.
- Limited in one/two types of digit semantics or the length of digit string

⇨ **The lack of a comprehensive analysis of digit semantics in passwords.**

- No applications on the practical password cracking tools.

⇨ **The lack of the combination of digit semantics and practical password cracking tools**

Introduction

Our Work

The lack of a comprehensive analysis of digit semantics in passwords.

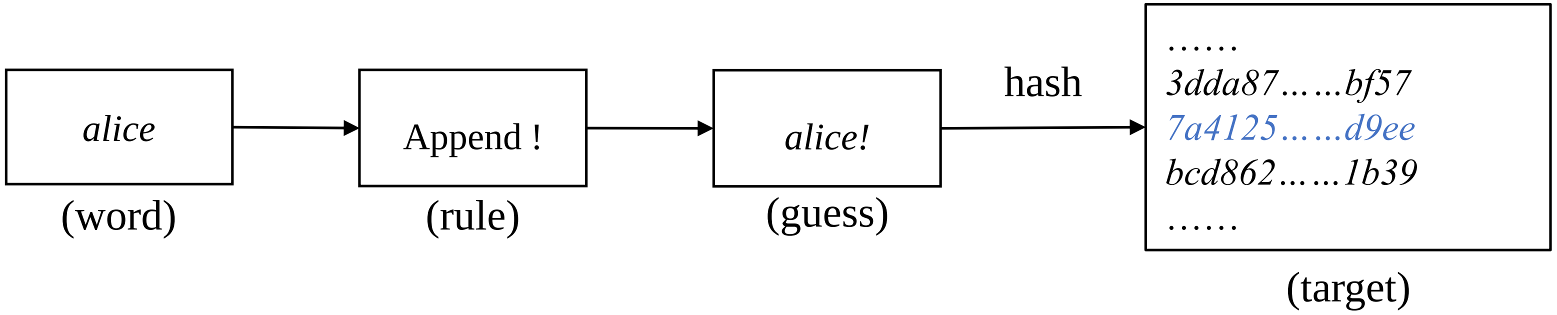
The lack of the combination of digit semantics and practical password cracking tools

- The digit semantics extraction tool and a large-scale comprehensive analysis of digit semantics in the passwords from the real world.

- Password cracking optimization based on digit semantics: new operations on the level of digit semantics and the digit semantics mangling rules constructed from them.

Background

Rule-based Attacks



Wordlist : leaked passwords (plaintext), words from dictionaries, etc.

Rule set : mangling rules, which indicate the operations to be done on the word

Target file: leaked passwords which are protected by hash algorithms

"wordlist mode" in JtR (rule-major order)

"rule-based attacks" in Hashcat (word-major order)

* Note that JtR and Hashcat order guesses differently

Background

Language of Mangling Rules

$! $3 sa@

operation

- Written in a specific language
- Consists of one or more operations
- Parsed left to right.

Operation	Description	Example Rule	Input Word	Output Word
l	Lowercase all letters	l	p@ssW0rd	p@ssw0rd
$X	Append character X to end	$1	p@ssW0rd	p@ssW0rd1
sXY	Replace all instances of X with Y	ss$	p@ssW0rd	p@$$W0rd
<N	Reject plains if their length is greater than N	<G		
!X	Reject plains which contain char X	!z		
…	…….	…	……	……

52 operations in JtR; 55 operations in Hashcat (32 operation in common)

Content

Digit Semantics

Common Digit Patterns

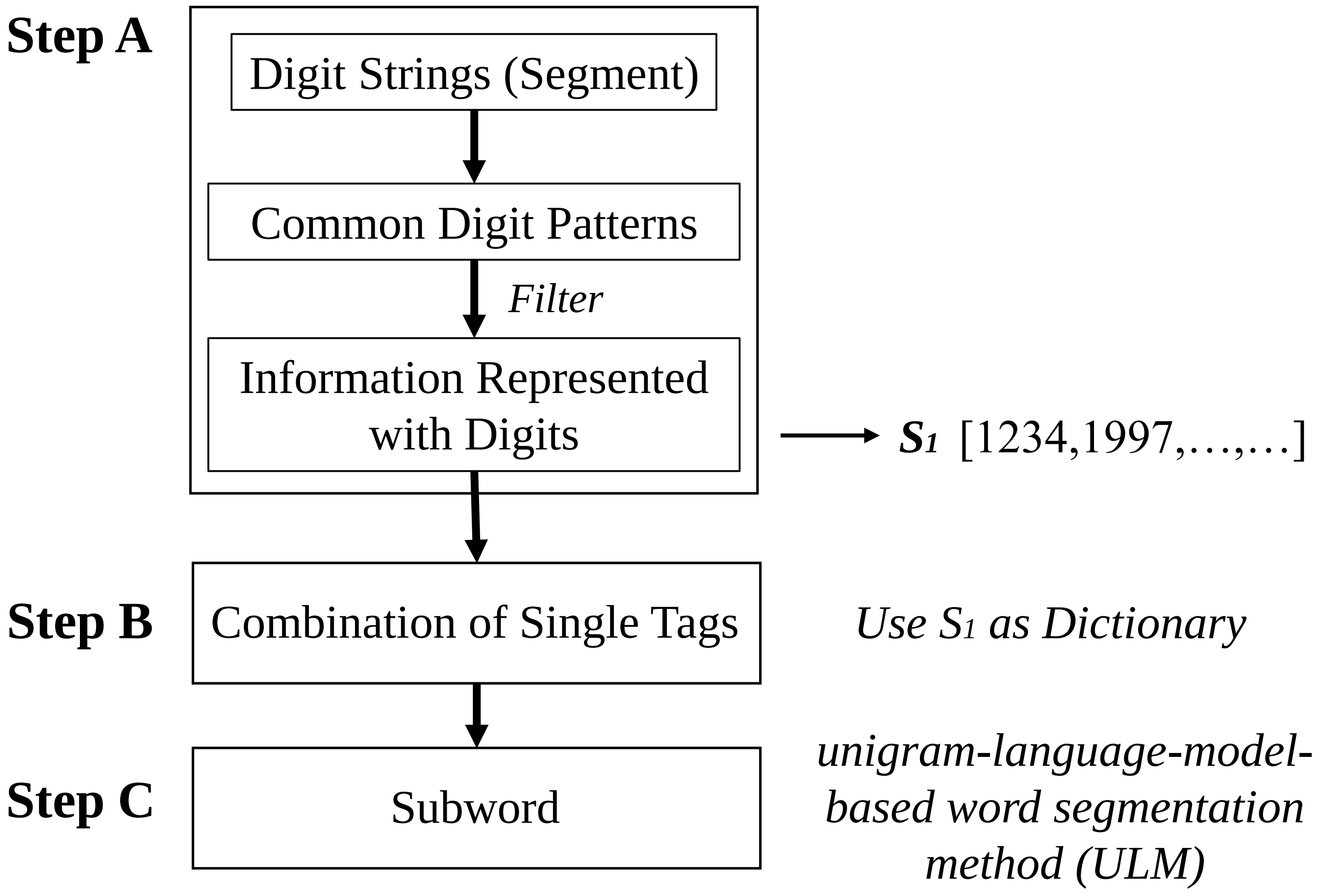
Repeat	1111
Continuation	1234
Leap	1357
Repeat+	121212
Palindrome	1235789

Information Represented with Digits

Phone	110, 139xxxxxxxx
MathConstant	31415
Date	1997
Postcode	200433
Idiom	520

Combination of Single Tags

Combination	123520



Digit Semantics

Empirical Analysis

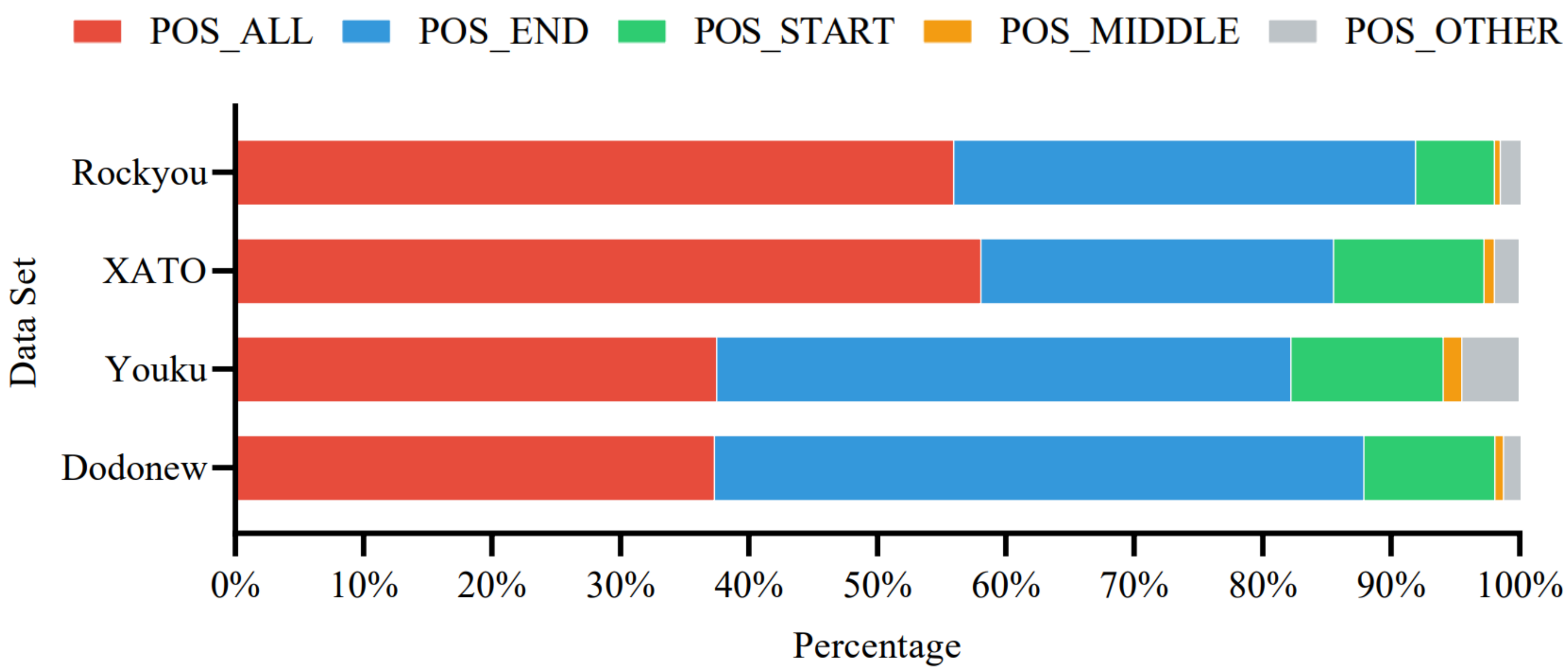
- Rich digit semantics in both English passwords (XATO & Rockyou) and Chinese passwords (Dodonew & Youku).
- The important role of Date.
- Differences in the distributions of Common Digit Patterns, Postcode, Phone, Idiom, Combination.

Tags	Dodonew		Youku		XATO		Rockyou	
	in segs	in passwords	in segs	in passwords	in segs	in passwords	in segs	in passwords
Repeat	2.32%	1.86%	0.92%	0.80%	3.21%	1.16%	2.50%	0.74%
Continuation	8.56%	6.82%	2.45%	2.11%	8.36%	3.03%	12.20%	3.60%
Leap	0.32%	0.25%	0.36%	0.30%	0.46%	0.16%	0.61%	0.18%
Repeat+	1.87%	1.50%	1.04%	0.92%	3.54%	1.30%	2.65%	0.79%
Palindrome	1.06%	0.85%	0.82%	0.73%	2.17%	0.79%	2.33%	0.69%
Numpad	4.03%	3.23%	3.30%	2.91%	3.55%	1.30%	3.42%	1.01%
Total Above	18.16%	14.51%	8.89%	7.77%	21.29%	7.73%	23.71%	7.01%
Phone	4.27%	3.43%	10.62%	9.41%	0.81%	0.30%	5.35%	1.59%
MathConstant	0.12%	0.09%	0.11%	0.09%	0.16%	0.06%	0.15%	0.05%
Date	21.19%	17.01%	19.52%	17.22%	42.92%	15.79%	32.06%	9.50%
Postcode	5.41%	4.35%	4.47%	3.96%	7.56%	2.79%	8.70%	2.58%
Idiom	5.05%	4.03%	3.04%	2.65%	1.10%	0.40%	1.08%	0.32%
Total Above	51.05%	40.83%	44.03%	38.60%	68.34%	25.04%	64.34%	19.02%
Combination	16.86%	13.55%	22.94%	20.36%	6.62%	2.44%	10.56%	3.14%
Total Above	67.91%	54.37%	66.97%	58.94%	74.96%	27.47%	74.90%	22.15%

Digit Semantics

Distribution of Location

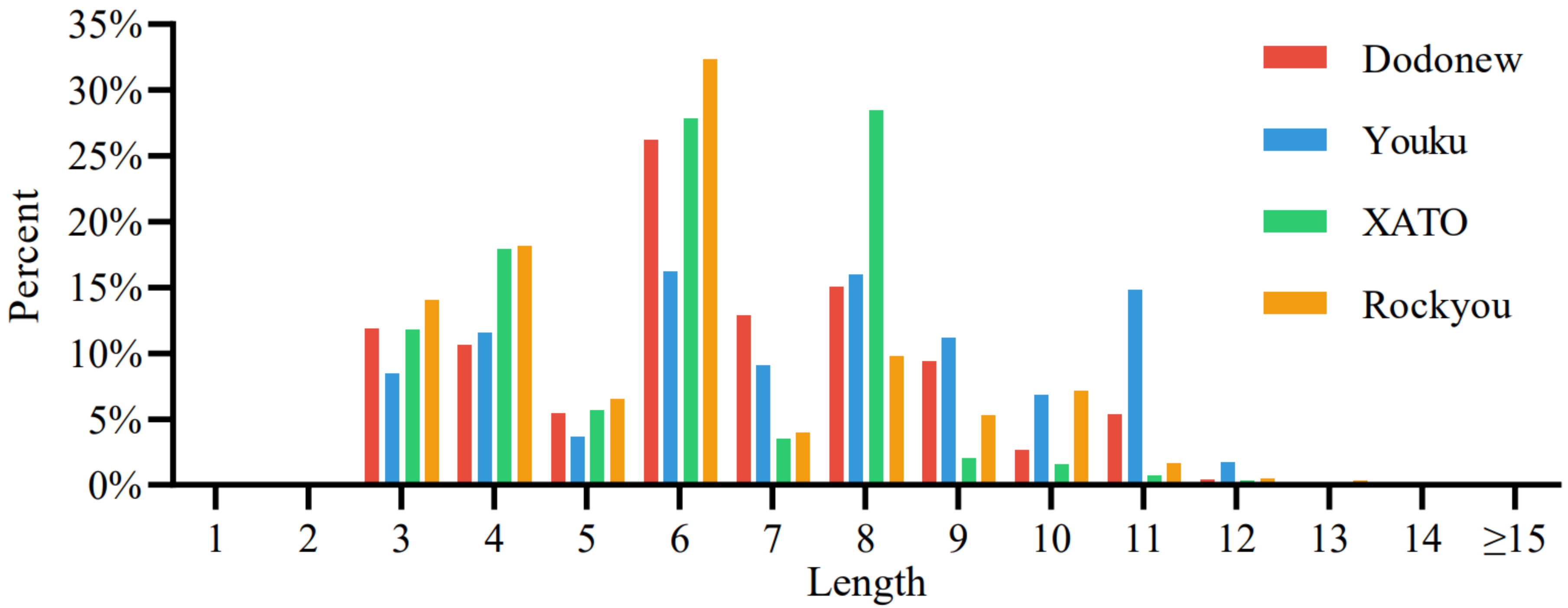
POS_ALL, POS_START, and POS_END can describe almost all tagged segments (over 94.08%)



Digit Semantics

Distribution of Length

- The length of most tagged segments (over 99.30%) is distributed below 12.
- Segments with even length are significantly more than those with odd length.



Optimization

Design & Enforcement

Digit Semantics Operations

Tag_Trans *B tag pos p1 p2*

- Tags that are highly structured and easy to deform
- To transform matched segments according to the specific format.

Repeat, Continuation, Leap	111 => 1111, 11111, …
Repeat+, Palindrome	123 => 12321, 123321
Date	1997 (YYYY) => 9701, 9702, … (YYMM)

Tag_Replace *F tag pos p1 p2*

- All tags
- To replace the matched segment of a certain tag with a dictionary 1997 => 111, 8888, …

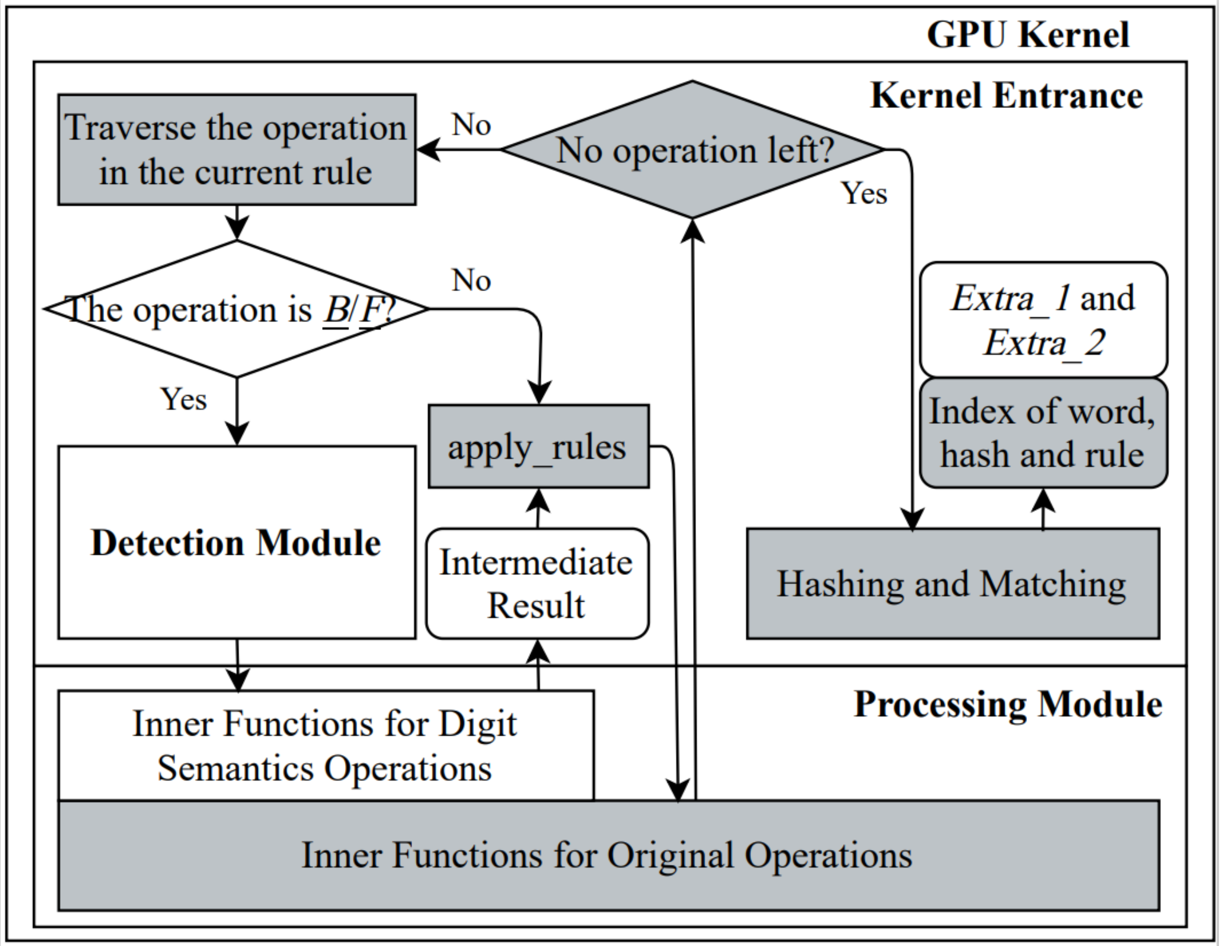
Digit Semantics Rules

B9214 To transform (**B**) a date string (**9**) matching YYYY (**1**) at the end of a word (**2**) into date strings matching YYMM (**4**)

B9214 $1

Optimization

Design & Enforcement



Kernel process of modified Hashcat

The gray part represents the original process without modification

- Detection Module

- Processing Module

- Running Logic

Evaluation

Rule Sets & Data Sets

Rule Sets:

Digits (1,974 rules)

- Tag_Trans 1,740 rules
- Tag_Replace 234 rules

SpiderLabs (5,146 rules)

Best64 (77 rules)

T0XlC (4,085 rules)

Generated2 (65,117 rules)

Random[1] (15,085 rules)

HR_n (n represents the rule count)

Evaluation Sets:

UUU9 (Chinese)	2,209,915 (Training)	551,689 (Testing)
Neopets (English)	2,115,419 (Training)	528,953 (Testing)

* Filter out the passwords that do not contain a segment with more than 2 digits in evaluation sets.

Wordlist:

Dodonew (Chinese)	10,119,695
XATO (English)	5,189,384

* Deduplicated and reordered by frequency.

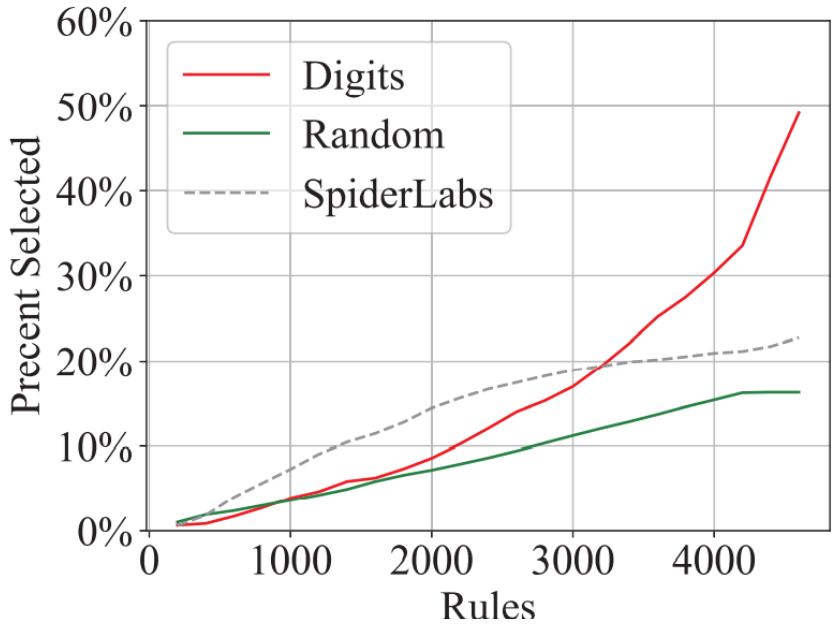
[1] Enze Liu, Amanda Nakanishi, Maximilian Golla, David Cash, and Blase Ur. 2019. Reasoning Analytically about Password-Cracking Software. In 2019 IEEE Symposium on Security and Privacy, SP 2019, San Francisco, CA, USA, May 19-23, 2019. 380–397.

Evaluation

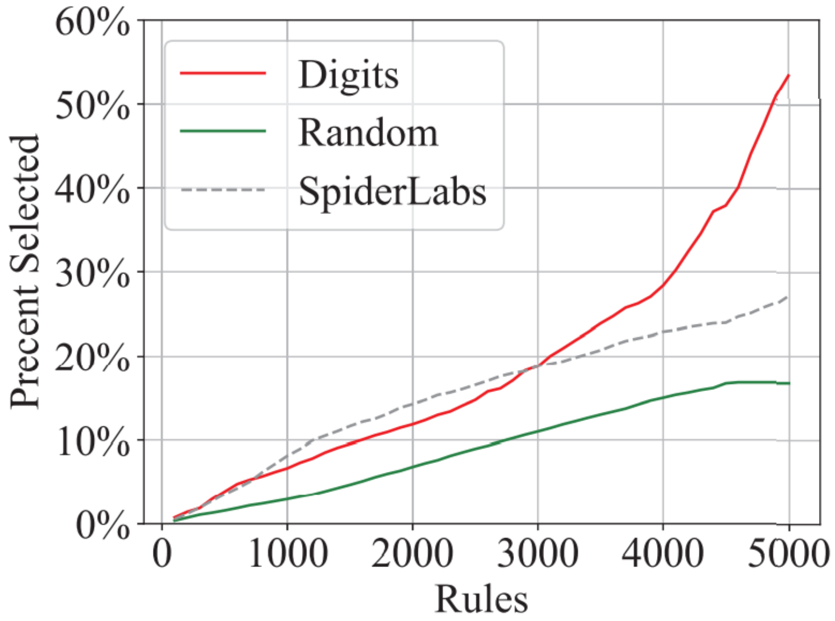
JtR: Rule Order

Mix_Digits	SpiderLabs + (Random - 1974 rules) + Digits
Mix_Compare	SpiderLabs + Random
Mix_Base	SpiderLabs

Reordered iteratively in descending order of *success density (Hit Count / Guess Count)*



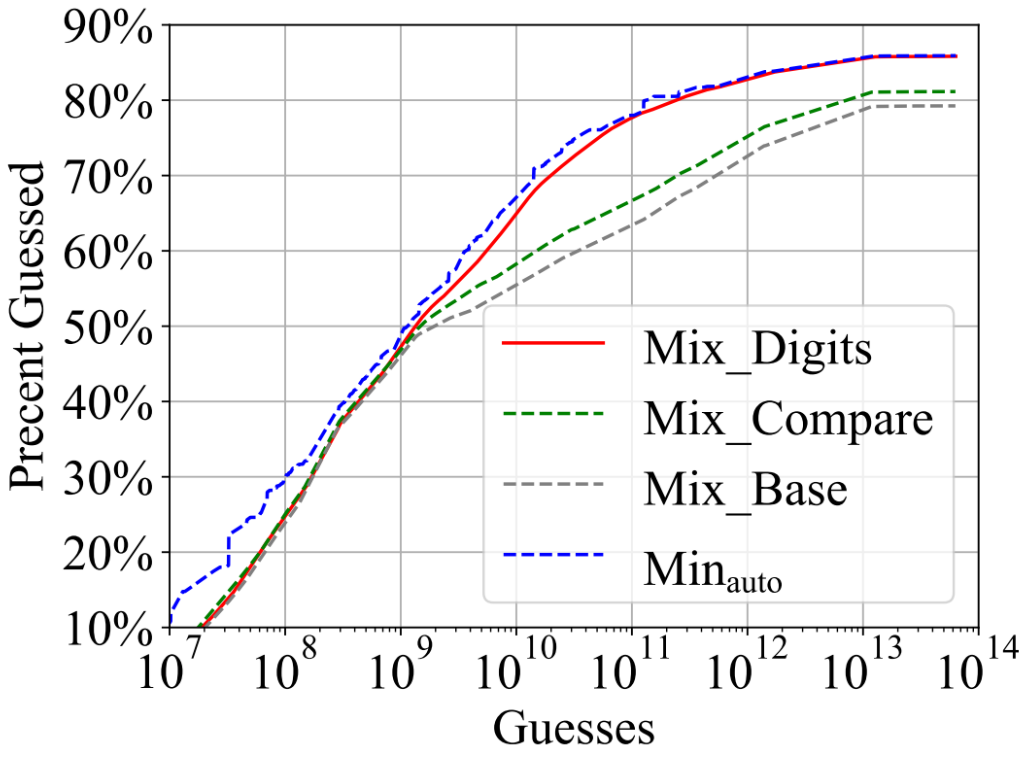
Dodonew-UUU9
(Chinese Passwords)



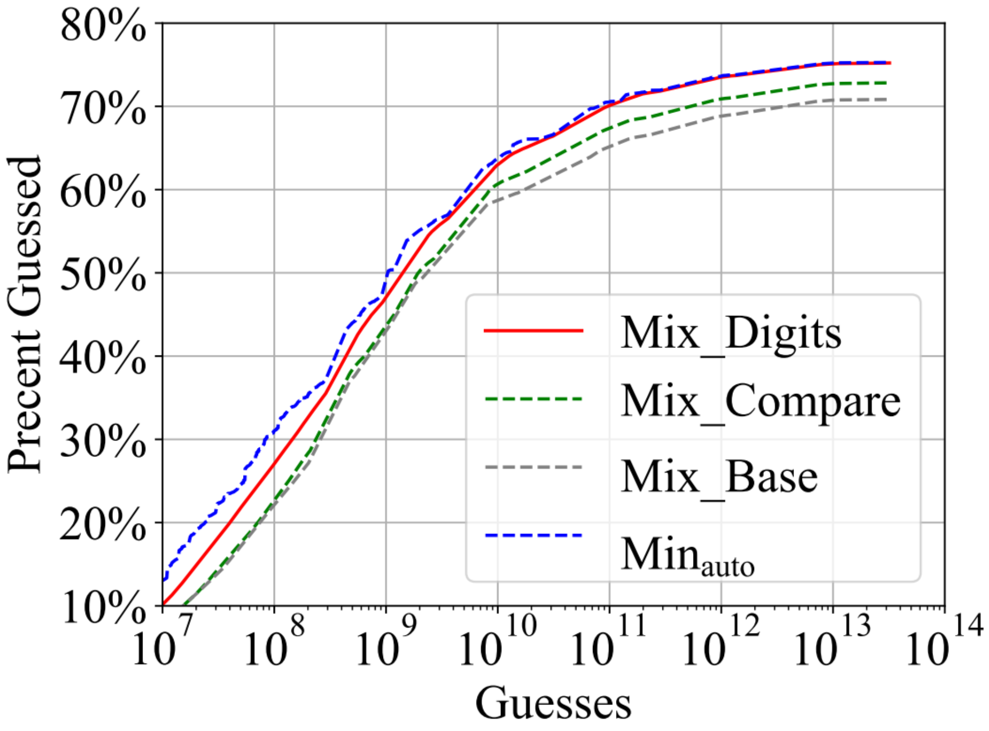
XATO-Neopets
(English Passwords)

Evaluation

JtR: Cracking Results



Dodonew-UUU9
(Chinese Passwords)

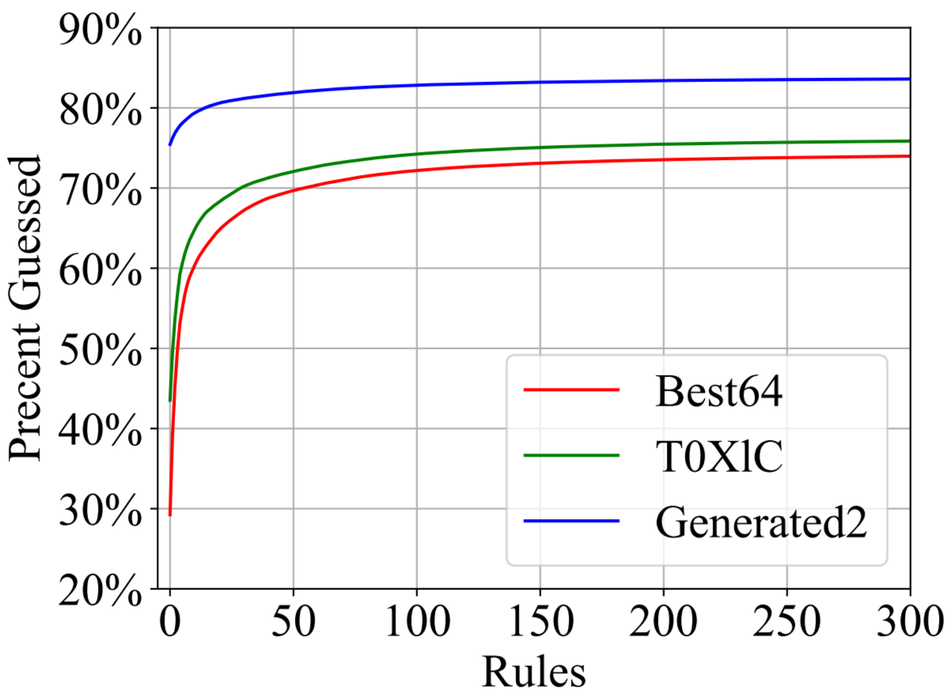


XATO-Neopets
(English Passwords)

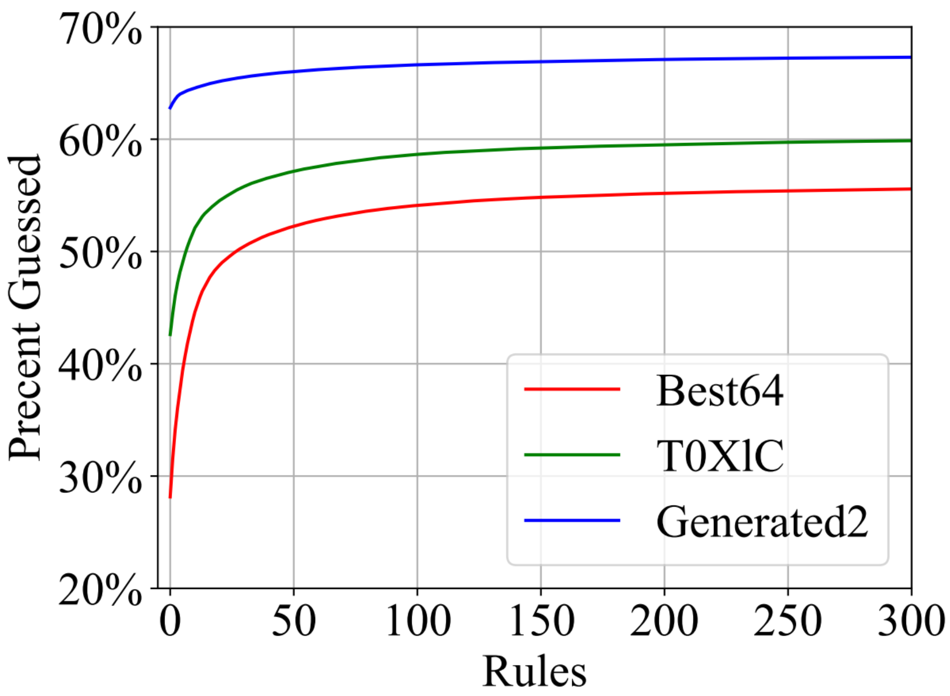
Evaluation

Hashcat

- A significant increase when cracking both Chinese and English passwords under each existent rule set
- A promising result when adding the top 100 digit semantics rules



Dodonew-UUU9
(Chinese Passwords)



XATO-Neopets
(English Passwords)

Evaluation

Hashcat

Dodonew-UUU9

Digits_100 **vs** HR_10000 (similar amount of extra guesses)

Digits_100 **vs** HR_100000 (guesses of one more order of magnitude)

Wordlist	# Word	Target Set	Rule Set	Extra Guesses	Improvement in Each Built-in Rule Set		
					Best64	T0XlC	Generated2
Dodonew	10,119,695	UUU9	Digits_100	1.17×10^{11}	146.78%	70.57%	9.79%
			Digits	4.78×10^{11}	154.09%	75.00%	11.03%
			HR_10000	1.01×10^{11}	93.50%	35.04%	0.34%
			HR_100000	1.01×10^{12}	136.09%	60.16%	2.33%
			HR_500000	5.05×10^{12}	160.74%	75.97%	5.71%
XATO	5,189,384	Neopets	Digits_100	1.81×10^{10}	92.24%	37.66%	6.09%
			Digits	1.15×10^{11}	98.77%	41.30%	7.48%
			HR_10000	5.19×10^{10}	61.46%	21.76%	0.18%
			HR_100000	5.19×10^{11}	96.66%	38.28%	1.28%
			HR_500000	2.59×10^{12}	117.17%	48.92%	3.54%

Conclusion

- The digit semantics extraction tool and a large-scale comprehensive analysis of digit semantics in the passwords from the real world.

- Password cracking optimization based on digit semantics: new operations on the level of digit semantics and the digit semantics mangling rules constructed from them.

Q & A