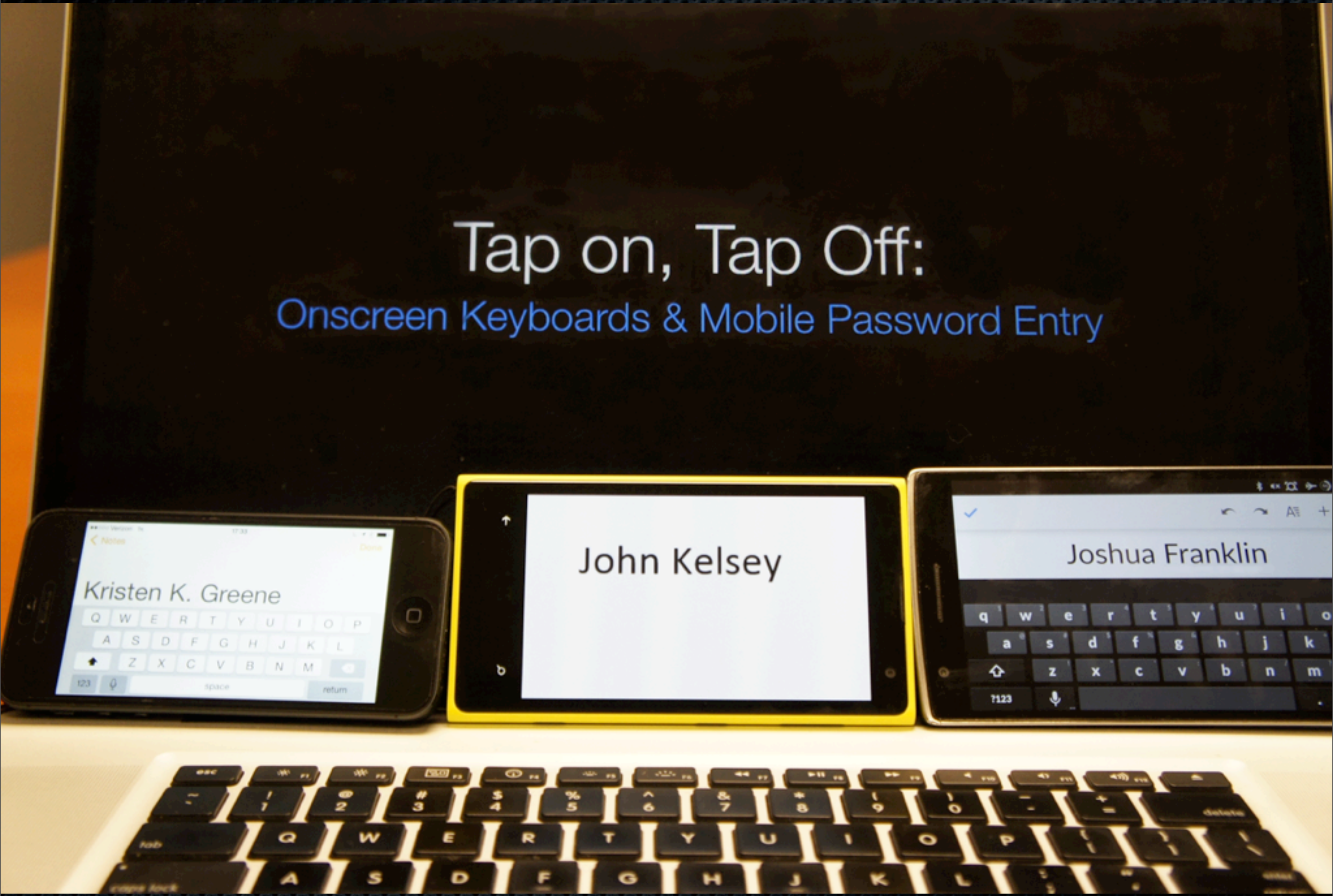
Tap on, Tap off:

Onscreen Keyboards & Mobile Password Entry

Kristen Greene
Josh Franklin
John Kelsey

National Institute of
Standards and Technology
U.S. Department of Commerce



Tap on, Tap Off:

Onscreen Keyboards & Mobile Password Entry

Kristen K. Greene

John Kelsey

Joshua Franklin

Disclaimer

Certain commercial entities, equipment, or materials may be identified in this presentation in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Outline

- Who we are
- Purpose
- Usability background
- Password security background
- Prior work
- Current methodology and results
- Conclusions

Kristen Greene

Cognitive Scientist
NIST Information Access Division
Rice University
Usable Security
Computational Cognitive Modeling
Voting Usability

Joshua Franklin

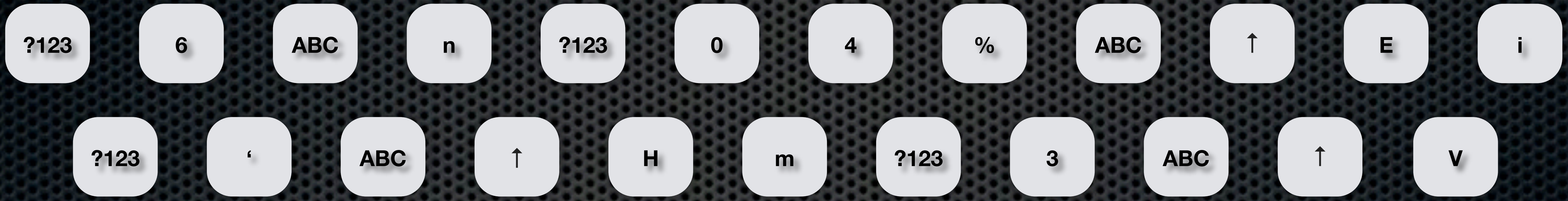
Information Security Engineer
NIST Computer Security Division
George Mason University
Cellular Security
Mobile Security
Voting Security

John Kelsey

Cryptographer
NIST Computer Security Division
University of Missouri Columbia
Symmetric Cryptography
PRNGs
Voting Security

The Problem

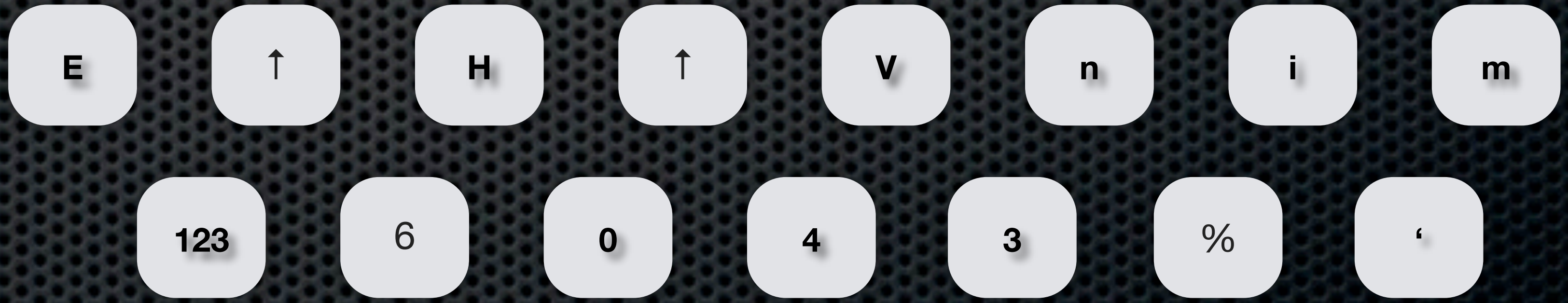
6n04%Ei'Hm3V is 23 taps



?123 6 ABC n ?123 0 4 % ABC ↑ E i

?123 ‘ ABC ↑ H m ?123 3 ABC ↑ V

EHVnim6043%' is 15 taps



E ↑ H ↑ V n i m

123 6 0 4 3 % ‘

Using Keyboard from Android Lollipop

Purpose

- Explore current state of usability and security metrics for passwords
- Assign strength metrics to passwords for which we already had usability metrics
  - How much entropy is lost as a result of permuting passwords to be easier to enter on mobile devices?

Usability Background

Tap On, Tap Off

Usability

- Context of use
- Effectiveness
- Efficiency
- Satisfaction

Usability: ISO 9241

- "The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use."

Usability: Context of Use

- “Users, tasks, equipment (hardware, software and materials), and the physical and social environments in which a product is used.” [ISO 9241]
  - Mobile vs. desktop context

Usability: Effectiveness

- “Accuracy and completeness with which users achieve specified goals.” [ISO 9241]
- Generally measured via **error rates**
  - Password entry errors

Usability: Efficiency

- “Resources expended in relation to the accuracy and completeness with which users achieve specified goals.” [ISO 9241]
- Generally measured via **time on task**
  - Password entry time
  - Number of keystrokes (taps)

Usability: Satisfaction

- “Freedom from discomfort, and positive attitudes towards the use of the product.” [ISO 9241]
- Generally measured via standardized or customized **questionnaires**

Usability & Security Parallels

Confidentiality	Effectiveness
Integrity	Efficiency
Availability	Satisfaction

Password Security Background

Tap On, Tap Off

Attacks on Passwords

- Password guessing
  - Brute force
  - Intelligent guessing

} *We are only concerned with these classes of attacks*

- Eavesdropping
- Social Engineering
- Physical attacks

Password Strength

- Password strength is often expressed in terms of entropy
    - *Note: Entropy is at most only loosely related to the use of the term in thermodynamics.*
- Entropy was originally defined by Claude Shannon in the 1950s

Password Metric Groups

- Two password metric groups
- Classified by how a password is created
  - **user generated** passwords
  - **system generated** passwords (a.k.a. randomly generated)
- Password metrics measure only one of these groups

Randomly Generated Password Metrics

- Shannon entropy formula: $H = \log_2 (B\text{^}L)$
  - H = total entropy
  - B = number of characters to choose from
  - L = password length
- [Kuo, 2006] uses modified Shannon entropy

Shannon Entropy Examples

Password	Entropy Estimate
5c2'Qe	39.33
3.bH1o	39.33
a7t?C2#	45.88
m3)61fHw	52.44
p4d46*3TxY	65.55
q80<U/C2mv	65.55
d51)u4;X3wrf	78.66
6n04%Ei'Hm3V	78.66
m#o)fp^2aRf207	91.76
4i_55fQ$2Mnh30	91.76

User Generated Password Metrics

- “Guessing entropy”
  - Estimate of the average amount of work required to guess the password of a selected user
  - Uses Shannon entropy as a foundation
  - “Measures” password strength based on a ruleset

User Generated Password Metrics

- “Min-entropy”
  - Difficulty of guessing the easiest single password to guess in the population
  - NIST specifies dictionary tests and password histories as heuristics to ensure at least 10 bits of entropy

800-63 Entropy Heuristic

- From NIST SP 800-63-2:
  - 1st character = 4 bits per character
  - 2nd thru 8th = 2 bits per character
  - 9th thru 20th = 1.5 bits per character
  - 21+ = 1 bit per character
  - Upper + lower + non-alphabetic = 6 bit bonus
  - Dictionary check = 6 bit bonus

800-63 Min-Entropy Ruleset

- Search a dictionary of at least 50,000 words for the password
  - If found, reject password
- Passwords that are detectable permutations of the username are not allowed

Our Research & Results

Tap On, Tap Off

Prior Work

Tap On, Tap Off

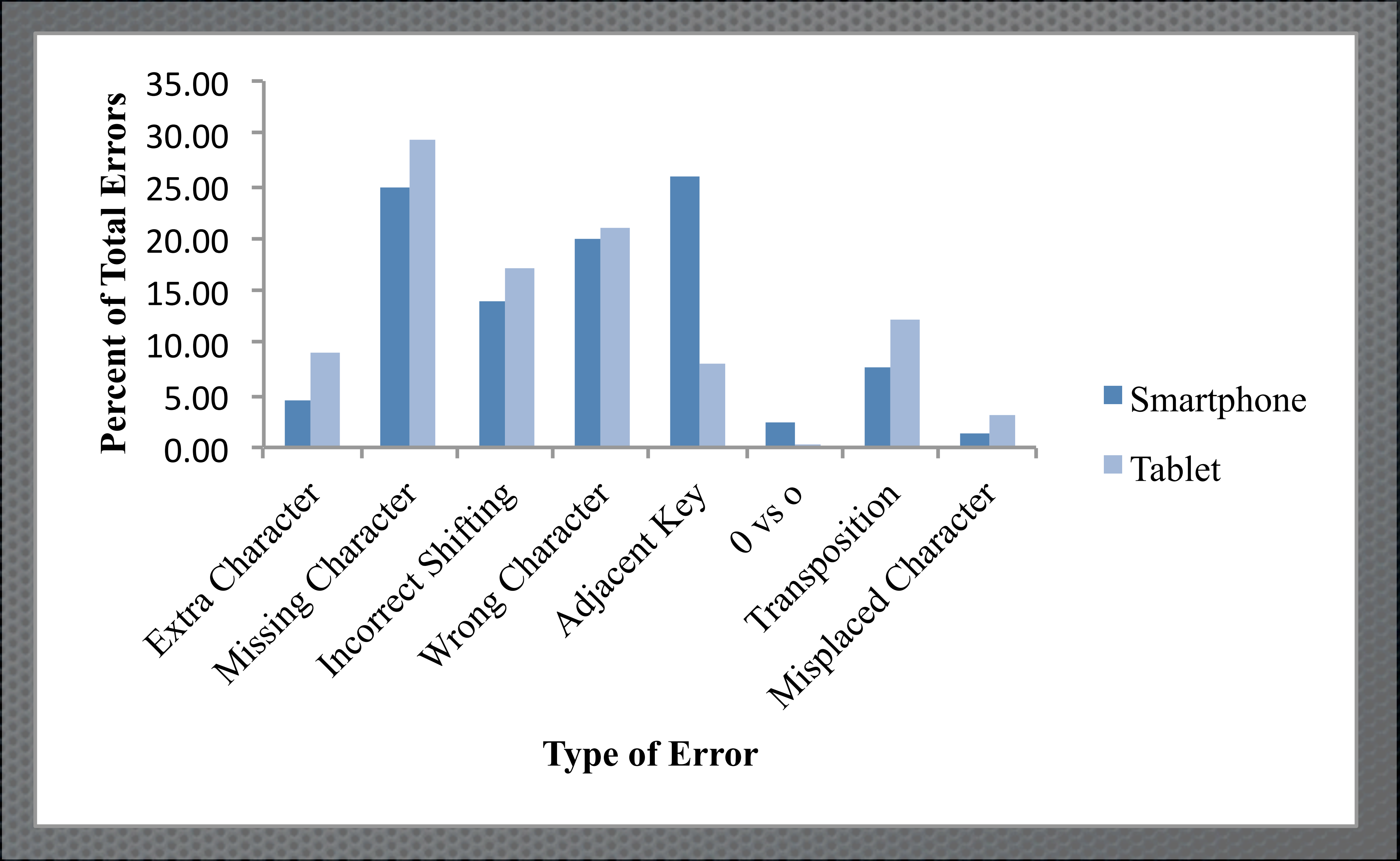
Prior Work

- Recent behavioral study on mobile password entry
- Participants had to learn, input, and recall 10 random passwords
- Onscreen keyboard switching significantly increased input time and introduced errors [Greene, Gallagher, Stanton, & Lee, 2014]

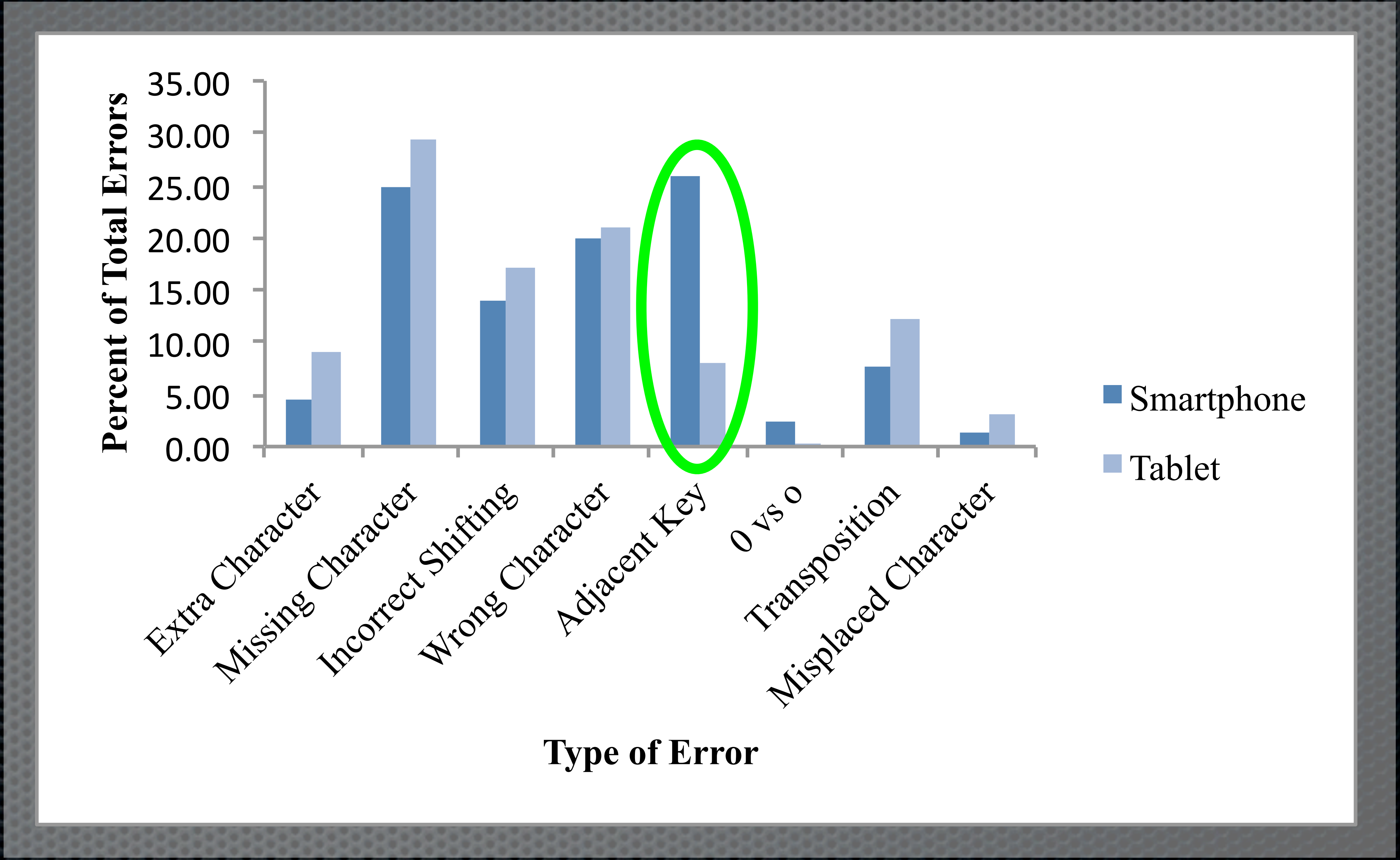
Measurement Granularity

- Password level
  - The entire password is either accepted or fails
- Character level
  - Multiple types of character errors (e.g., transposition, deletion, substitution)
- Important to look at the nature and number of errors users make when inputting passwords

Tiny Keyboards = More Errors

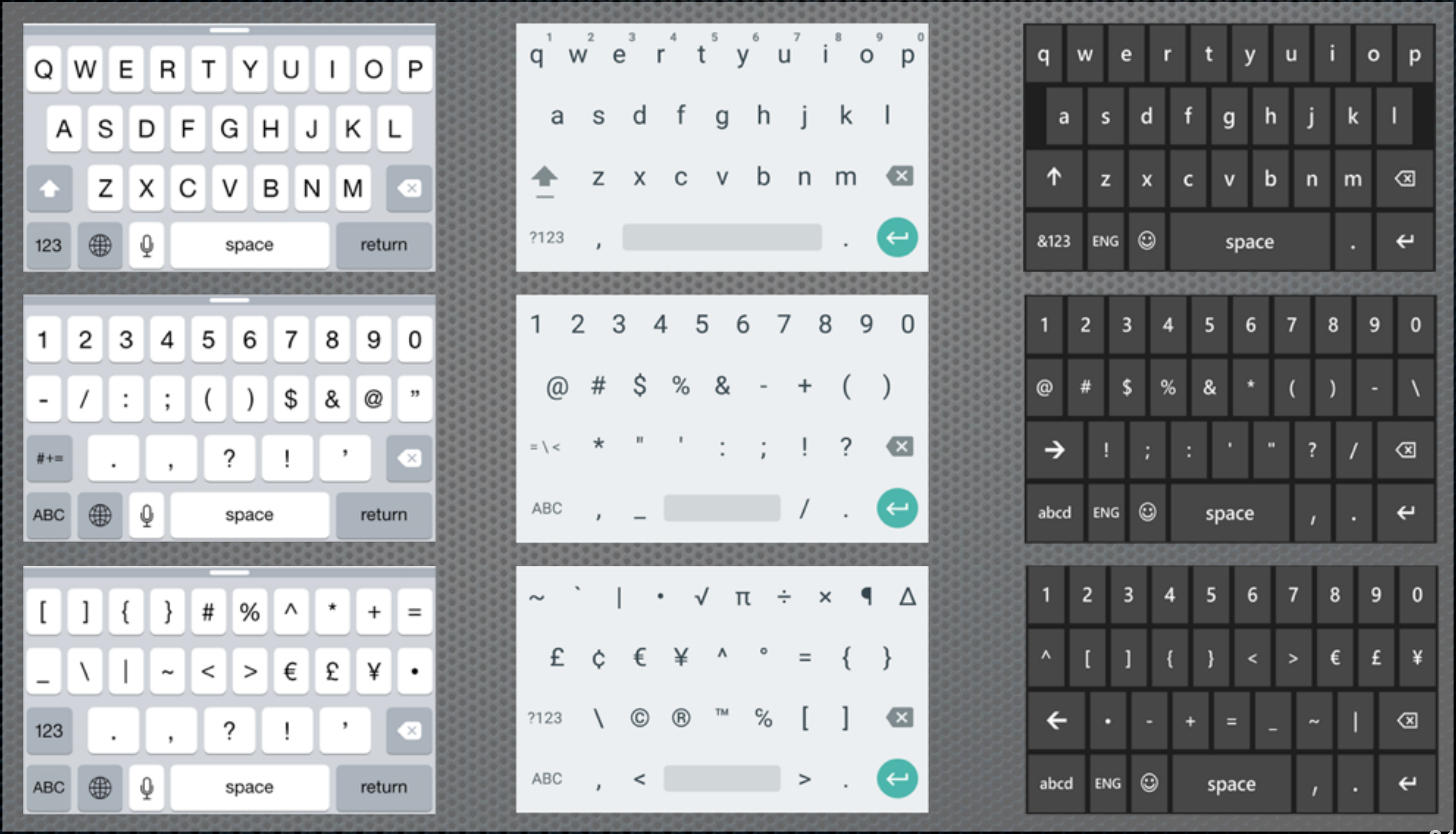


Tiny Keyboards = More Errors

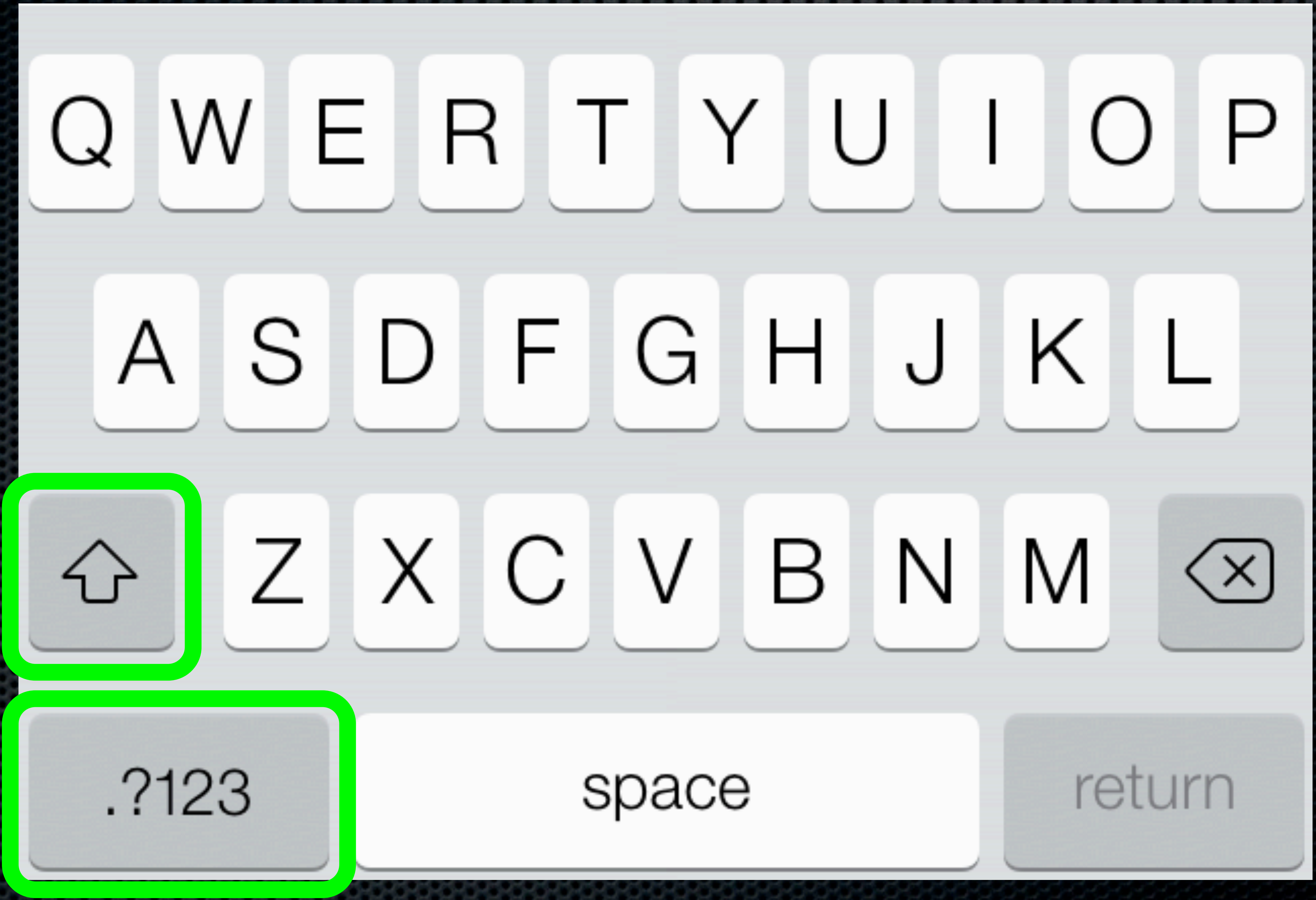


30

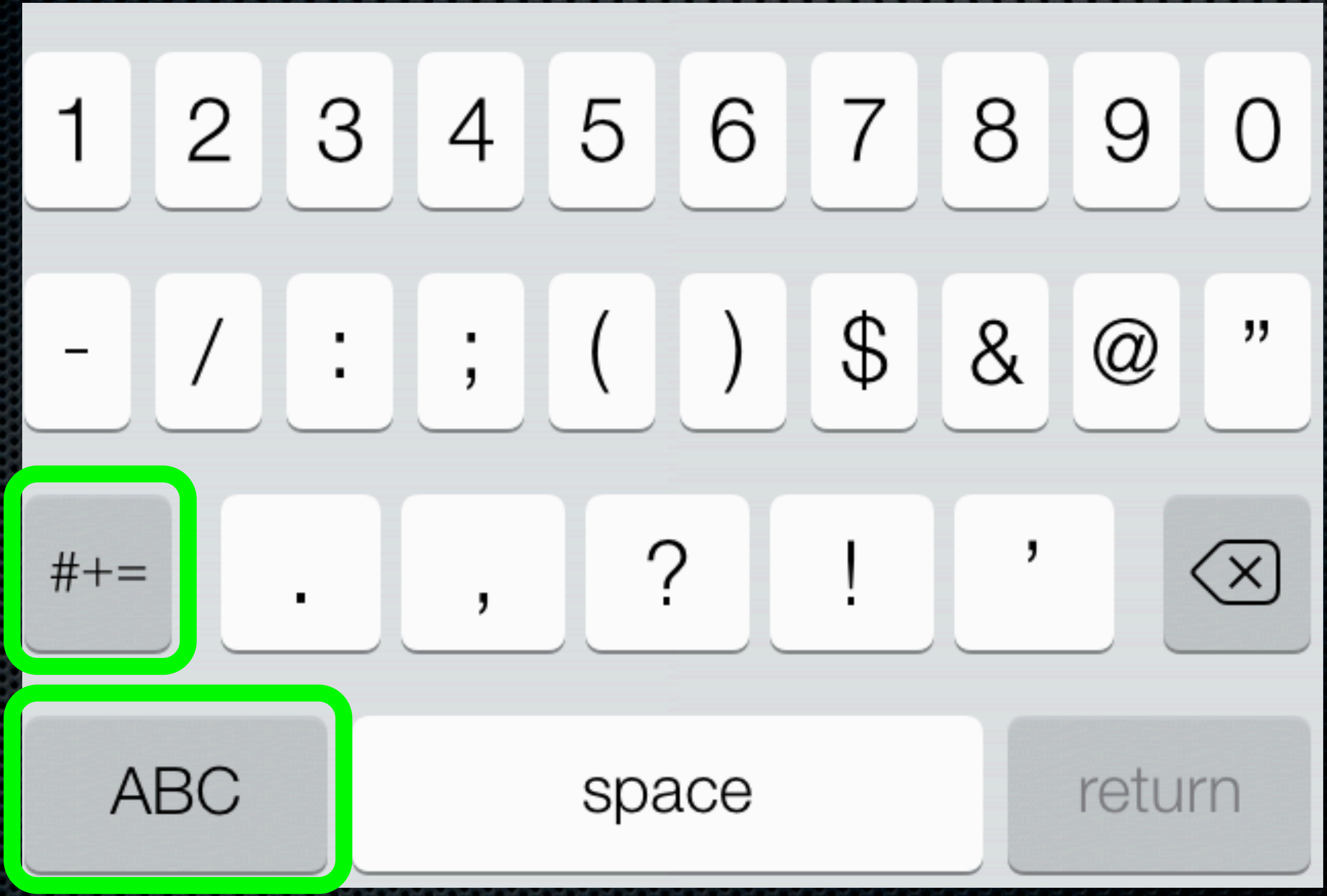
Onscreen Keyboards



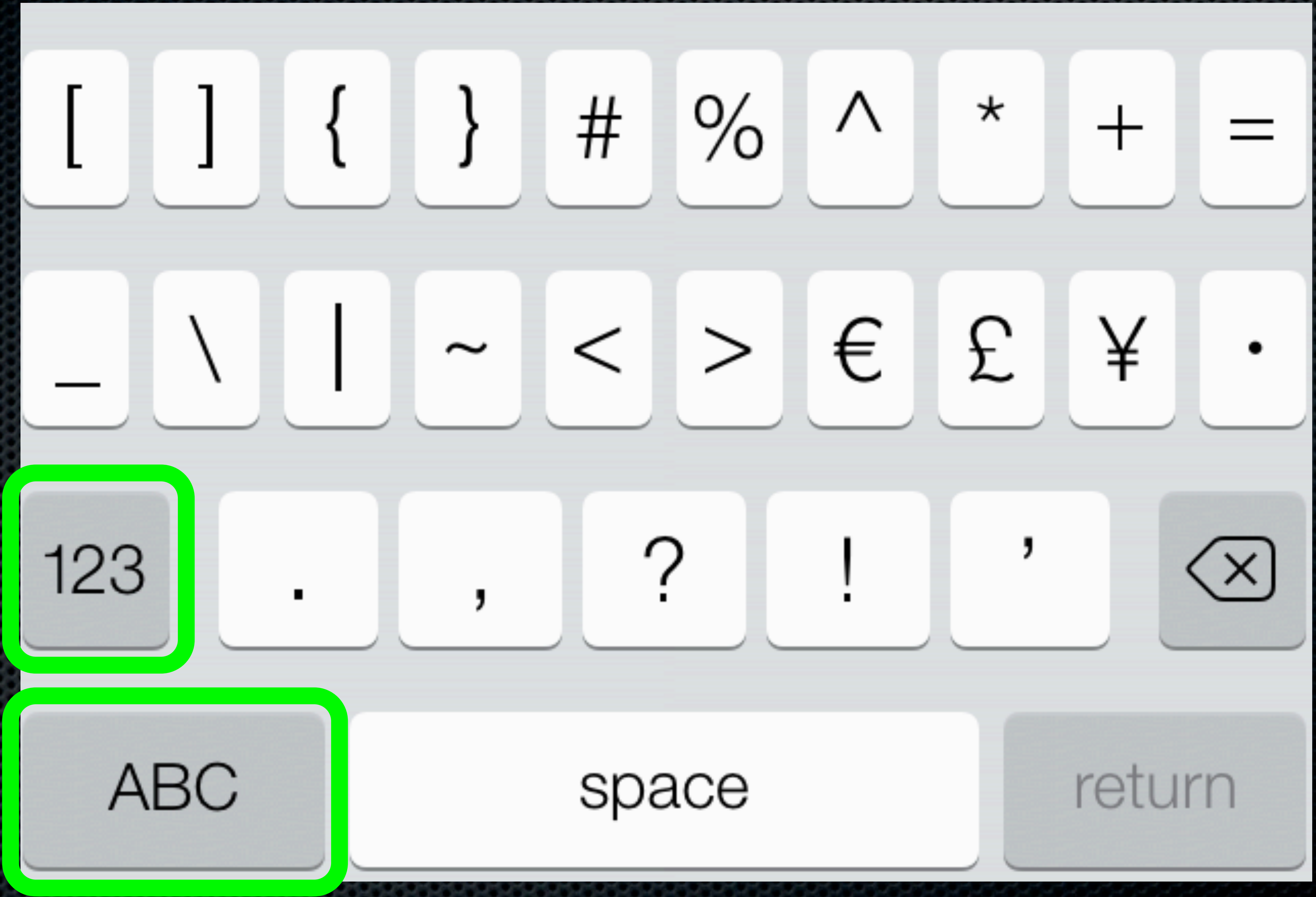
Screen Depth 1



Screen Depth 2



Screen Depth 3



Current Work

Tap On, Tap Off

Methodology

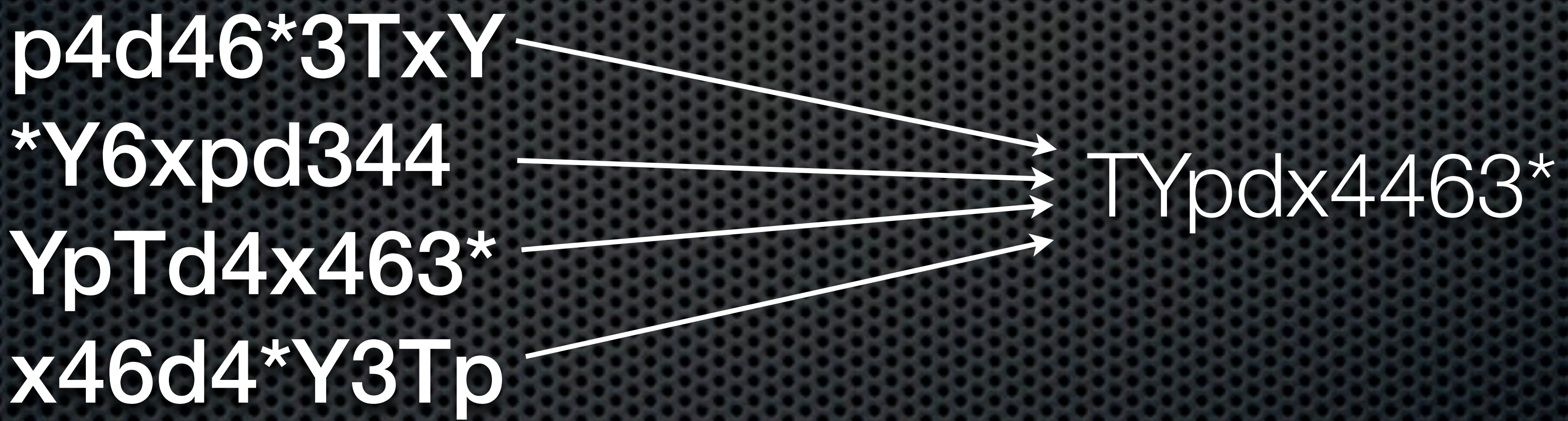
- Defined a password permutation
  - Divided characters in password into “classes”
  - Uppercase (U), lowercase (L), numbers (N), and symbols (S)
  - Group similar characters together
- Example:
  - 5c2'Qe is permuted to Qce52'

Permutation and Tap Counts

Original Password	Permuted Password	Length	Taps: Original, Permuted	Keyboard Changes: Original, Permuted	Taps Saved
5c2'Qe	Qce52'	6	11, 8	4, 1	3
m3)61fHw	Hmfw361)	8	11, 10	2, 1	1
q80<U/C2mv	UCqmv802</	10	19, 15	7, 3	4
6n04%Ei'Hm3V	EHVnim6043%'	12	24, 17	9, 2	7
m#o)fp^2aRf207	Rmofpaf2207#)^	14	24, 19	10, 4	6

Password Collisions

- Multiple unique passwords can permute to the same password:



p4d46*3TxY

*Y6xpd344

YpTd4x463*

x46d4*Y3Tp

TYpdx4463*

Our Results

Tap On, Tap Off

Experiment 1: Fan-Out

How many passwords collide with the same user-friendly password?

How Many Collisions?

Length	10th Percentile	90th Percentile	Average
6	120	180	159
8	840	1680	1329
10	5040	25200	12659
12	27720	277200	132492
14	360360	3153150	1438513
16	2402400	40360320	17187712
18	24504480	514594080	208414540
20	221707200	6518191680	2327087101

Experiment 2: Entropy Loss

How much entropy is lost by permuting passwords?

How Much Entropy Is Lost?

Length	10th Percentile	90th Percentile	Average	Additional Letters
6	6.9	7.5	7.3	2
8	9.7	10.7	10.4	3
10	12.3	14.6	13.6	3
12	14.8	18.1	17.0	4
14	18.0	21.6	20.4	5
16	21.5	25.0	24.0	6
18	24.5	28.9	27.6	6
20	27.9	32.6	31.2	7

Experiment 3: All-Lowercase

How much additional password length would we need to just change over to all lowercase letters?

What About All Lowercase?

Complex Password	All-Lowercase	Extra Letters
6	9	3
8	12	4
10	14	4
12	17	5
14	20	6
16	23	7
18	25	7
20	28	8

q80<U/C2mv

vs

dmstpjnwqiwqok

Unholster your phones and type this:

m#o)fp^2aRf207

Now type this:

Rmofpaf2207#)^

Recap

- Entering complex passwords on mobile devices is difficult
- Our password permutation makes it easier
  - We precisely measure the security loss
  - Fixed by adding a couple extra characters

Conclusions

- **Device constraints matter**
- Old password policies play badly with new devices
- Both usability and security must be considered

Code

- https://github.com/usnistgov/PasswordMetrics
- https://github.com/usnistgov/DataVis

Questions?

- For additional research, visit NIST’s Information Technology Laboratory:
    - Kristen Greene
      Information Access Division
      nist.gov/itl/iad
    - John Kelsey
      Joshua Franklin
      Computer Security Division
      csrc.nist.gov

Acknowledgements

- Cathryn Ploehn
- Andrew Rukhin
- Jim Filliben

References

[Greene, Gallagher, Stanton, & Lee, 2014] I Can’t Type That! P@$$w0rd Entry on Mobile Devices. In Human Aspects of Information Security, Privacy, and Trust, Lecture Notes in Computer Science Volume 8533, 2014, pp 160-171.

[ISO 9241] Ergonomic requirements for office work with visual display terminals (VDTs) -- Part 11: Guidance on usability.

[Kuo, 2006] Human Selection of Mnemonic Phrase-based Passwords, CUPS 2006.

[NIST SP 800-63-2] Burr et al, Electronic Authentication Guideline, National Institute of Standards and Technology, 2013.

[Shannon, 1948] C. E. Shannon, “A mathematical Theory of Communication, 1948.

Tap on, Tap off:

Onscreen Keyboards & Mobile Password Entry

Kristen Greene
Josh Franklin
John Kelsey

National Institute of Standards and Technology
U.S. Department of Commerce

Extras

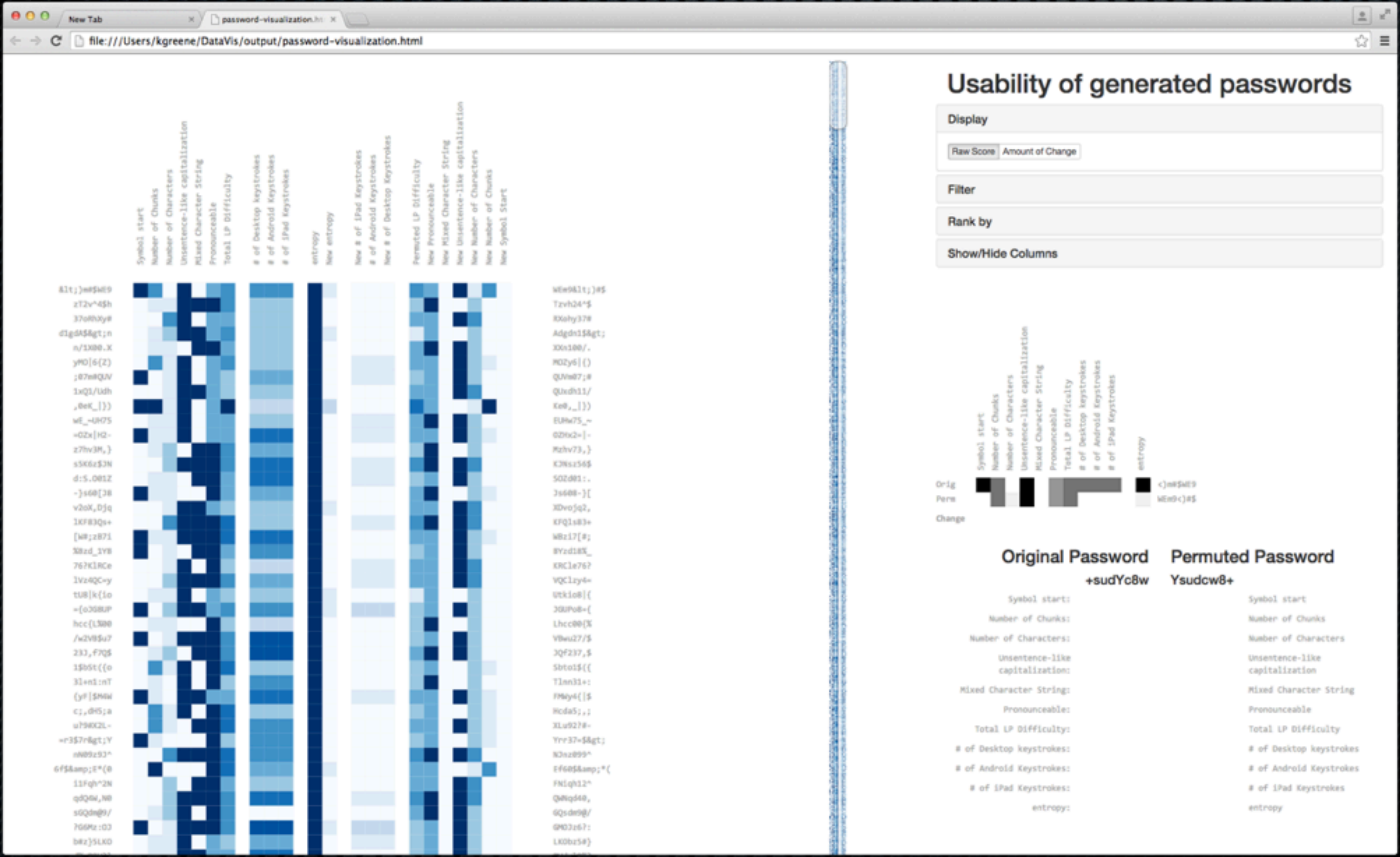
Tap On, Tap Off

Data Viz Tool

Tap On, Tap Off

Prior NIST Tool

- Cathryn Ploehn’s SURF (Summer Undergraduate Research Fellowship) project
- Shows usability and security metrics side-by-side for original and permuted passwords
- Multiple levels of granularity
- Filtering options
- https://github.com/usnistgov/DataVis



Usability of generated passwords

Display

Raw Score | Amount of Change

Filter

Rank by

Show/Hide Columns

Original Password	Permuted Password
+sudYc8w	Ysudcw8+

Symbol start: | Symbol start

Number of Chunks: | Number of Chunks

Number of Characters: | Number of Characters

Unsentence-like capitalization: | Unsentence-like capitalization

Mixed Character String: | Mixed Character String

Pronounceable: | Pronounceable

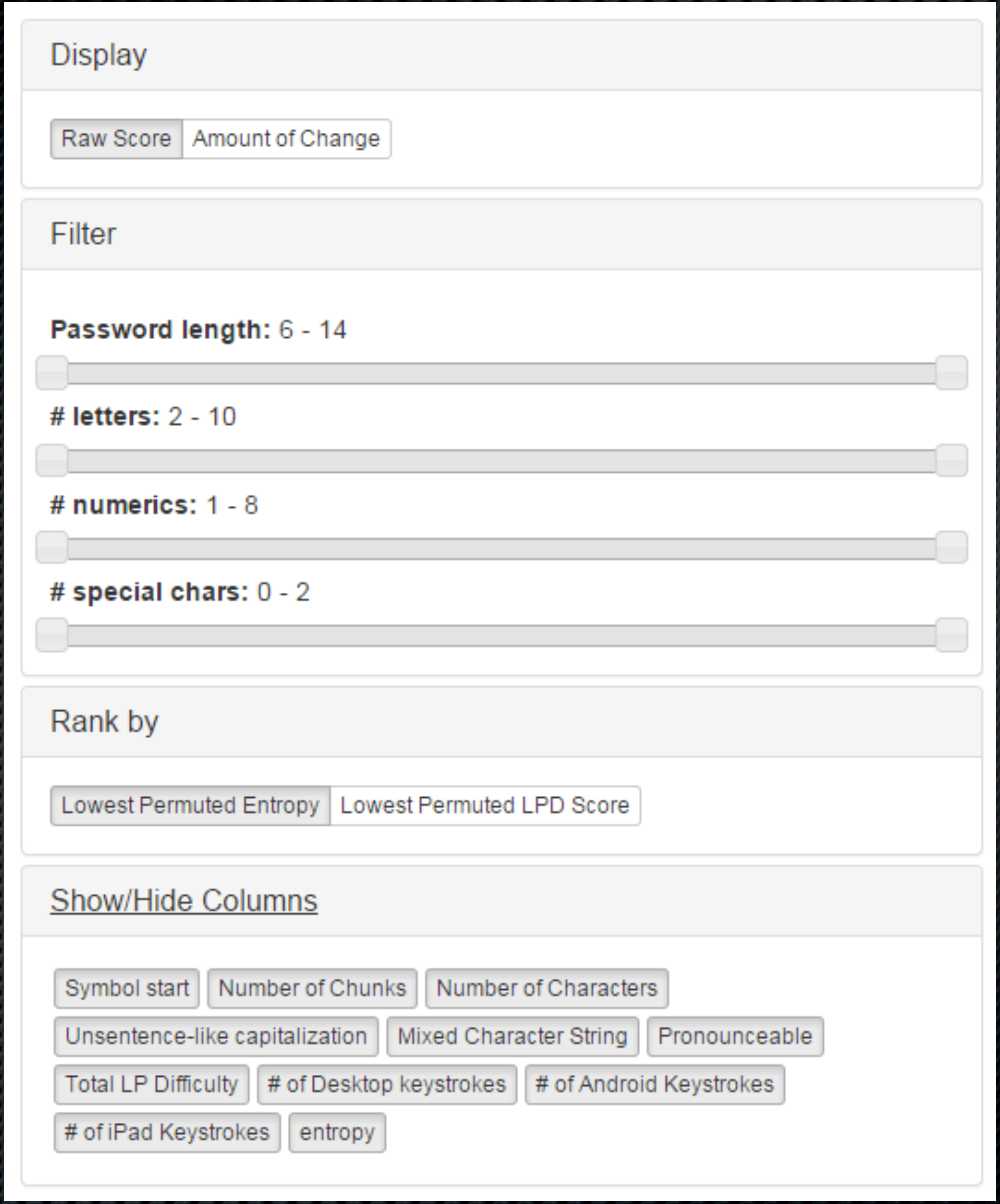
Total LP Difficulty: | Total LP Difficulty

# of Desktop keystrokes: | # of Desktop keystrokes

# of Android Keystrokes: | # of Android Keystrokes

# of iPad Keystrokes: | # of iPad Keystrokes

entropy: | entropy



Display

Filter

Password length: 6 - 14

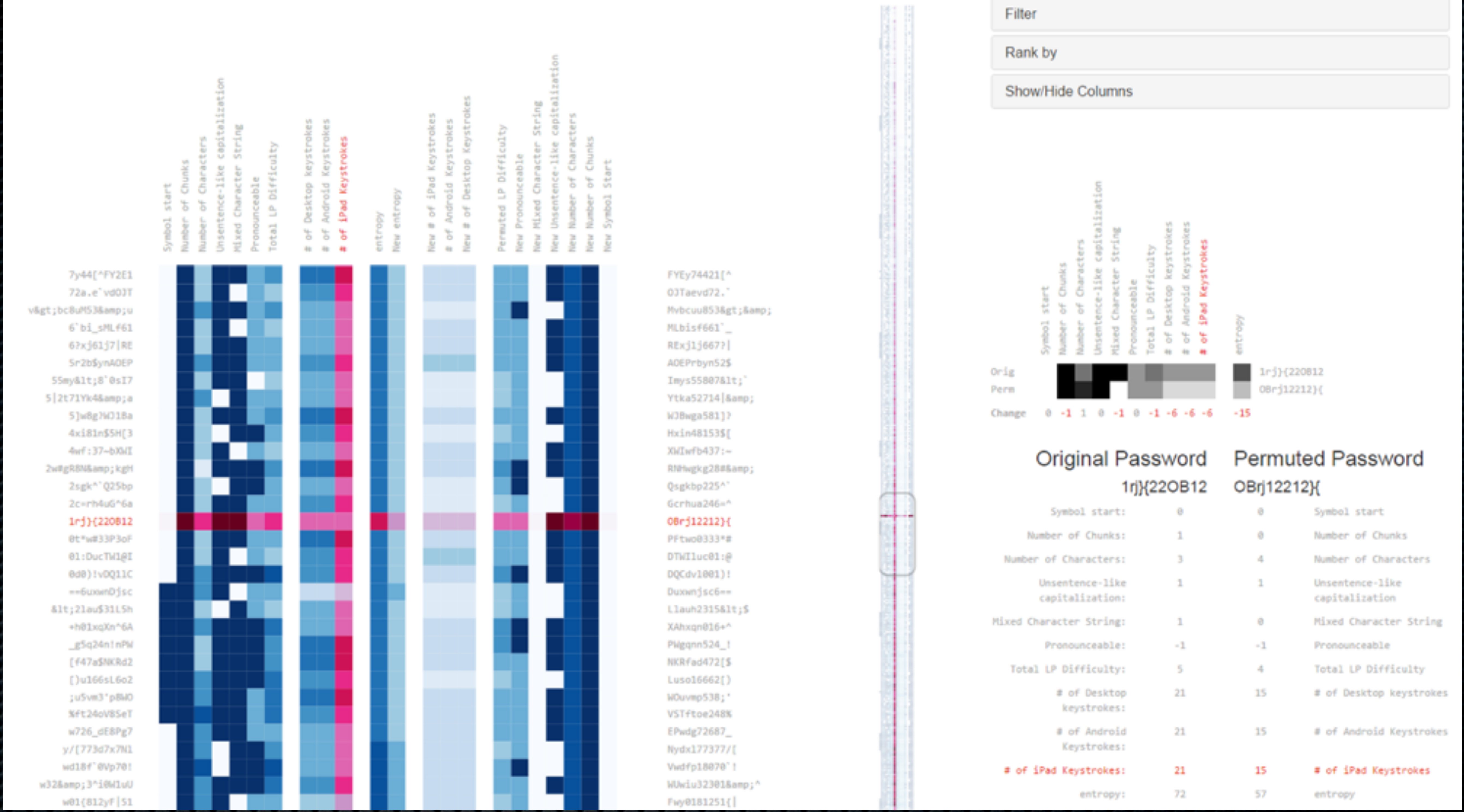
# letters: 2 - 10

# numerics: 1 - 8

# special chars: 0 - 2

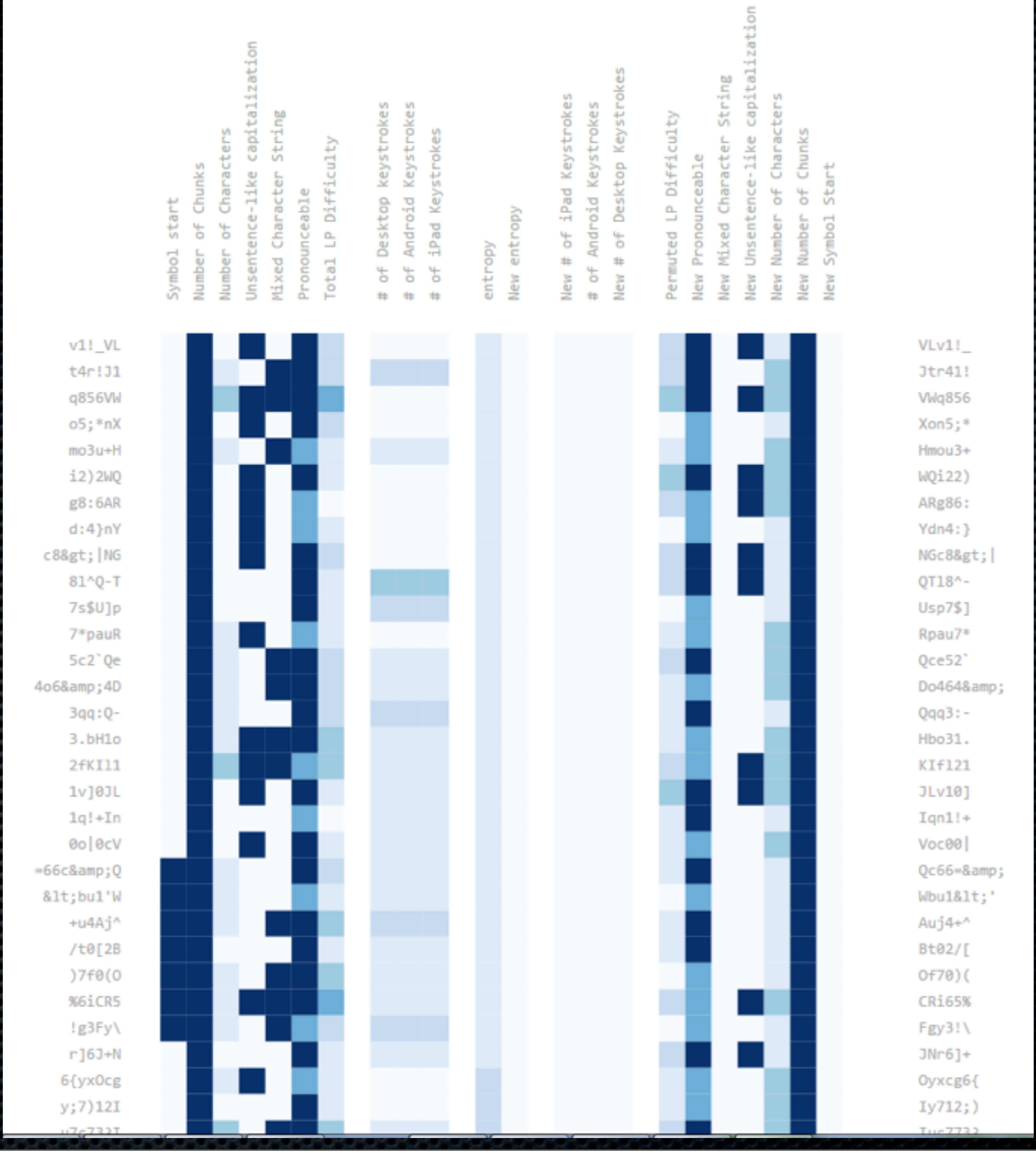
Rank by

Show/Hide Columns



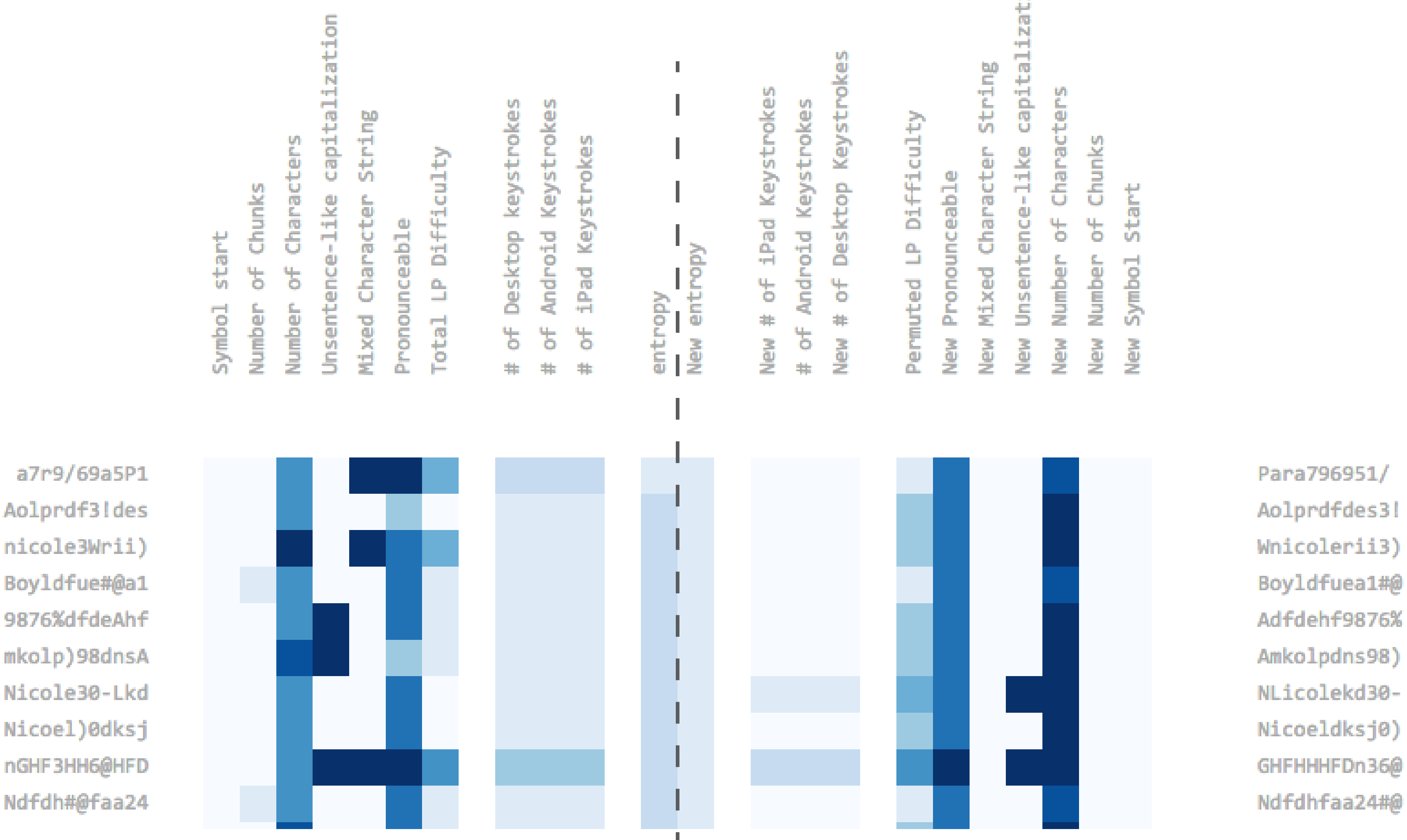
	Symbol start	Number of Chunks	Number of Characters	Unsentence-like capitalization	Mixed Character String	Pronounceable	Total LP Difficulty	# of Desktop keystrokes	# of Android Keystrokes	# of iPad Keystrokes	entropy
Change	0	-1	1	0	-1	0	-1	-6	-6	-6	-15

Original Password			Permuted Password
	1rj}{22OB12	OBrj12212}{	
Symbol start:	0	0	Symbol start
Number of Chunks:	1	0	Number of Chunks
Number of Characters:	3	4	Number of Characters
Unsentence-like capitalization:	1	1	Unsentence-like capitalization
Mixed Character String:	1	0	Mixed Character String
Pronounceable:	-1	-1	Pronounceable
Total LP Difficulty:	5	4	Total LP Difficulty
# of Desktop keystrokes:	21	15	# of Desktop keystrokes
# of Android Keystrokes:	21	15	# of Android Keystrokes
# of iPad Keystrokes:	21	15	# of iPad Keystrokes
entropy:	72	57	entropy


Symbol start
Number of Chunks
Number of Characters
Unsentence-like capitalization
Mixed Character String
Pronounceable
Total LP Difficulty
# of Desktop keystrokes
# of Android Keystrokes
# of iPad Keystrokes
entropy
New entropy
New # of iPad Keystrokes
# of Android Keystrokes
New # of Desktop Keystrokes
Permuted LP Difficulty
New Pronounceable
New Mixed Character String
New Unsentence-like capitalization
New Number of Characters
New Number of Chunks
New Symbol Start
v1!_VL
t4r!J1
q856VW
o5;*nX
mo3u+H
i2)2WQ
g8:6AR
d:4}nY
c8&gt;|NG
81^Q-T
7s$U]p
7*pauR
5c2`Qe
4o6&amp;4D
3qq:Q-
3.bH1o
2fKI11
1v]0JL
1q!+In
0o|0cV
=66c&amp;Q
&lt;bu1'W
+u4Aj^
/t0[2B
)7f0(O
%6iCR5
!g3Fy\
r]6J+N
6{yxOcg
y;7)12I
VLv1!_
Jtr41!
VWq856
Xon5;*
Hmou3+
WQi22)
ARg86:
Ydn4:}
NGc8&gt;|
QT18^-
Usp7$]
Rpau7*
Qce52`
Do464&amp;
Qqq3:-
Hbo31.
KIf121
JLv10]
Iqn1!+
Voc00|
Qc66=&amp;
Wbu1&lt;'
Auj4+^
Bt02/[
Of70)(
CRi65%
Fgy3!\
JNr6]+
Oyxcg6{
Iy712;)

LPD per-rule and total scores

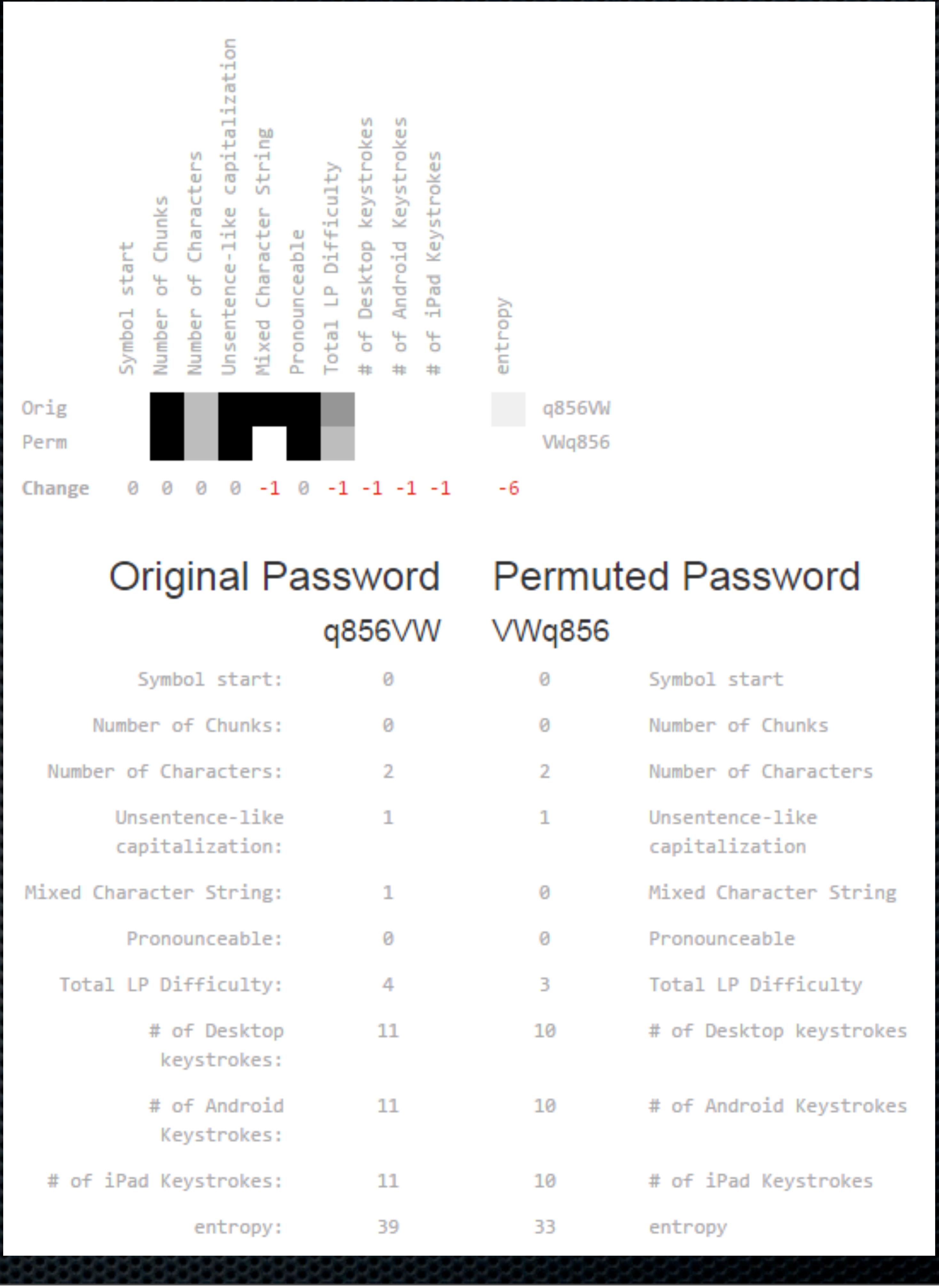
keystrokes



Line of symmetry

Metrics for original password

Metrics for permuted password



	Symbol start	Number of Chunks	Number of Characters	Unsentence-like capitalization	Mixed Character String	Pronounceable	Total LP Difficulty	# of Desktop keystrokes	# of Android Keystrokes	# of iPad Keystrokes	entropy	
Orig												q856VW
Perm												VWq856
Change	0	0	0	0	-1	0	-1	-1	-1	-1	-6	

Original Password	q856VW	VWq856	Permuted Password
Symbol start:	0	0	Symbol start
Number of Chunks:	0	0	Number of Chunks
Number of Characters:	2	2	Number of Characters
Unsentence-like capitalization:	1	1	Unsentence-like capitalization
Mixed Character String:	1	0	Mixed Character String
Pronounceable:	0	0	Pronounceable
Total LP Difficulty:	4	3	Total LP Difficulty
# of Desktop keystrokes:	11	10	# of Desktop keystrokes
# of Android Keystrokes:	11	10	# of Android Keystrokes
# of iPad Keystrokes:	11	10	# of iPad Keystrokes
entropy:	39	33	entropy

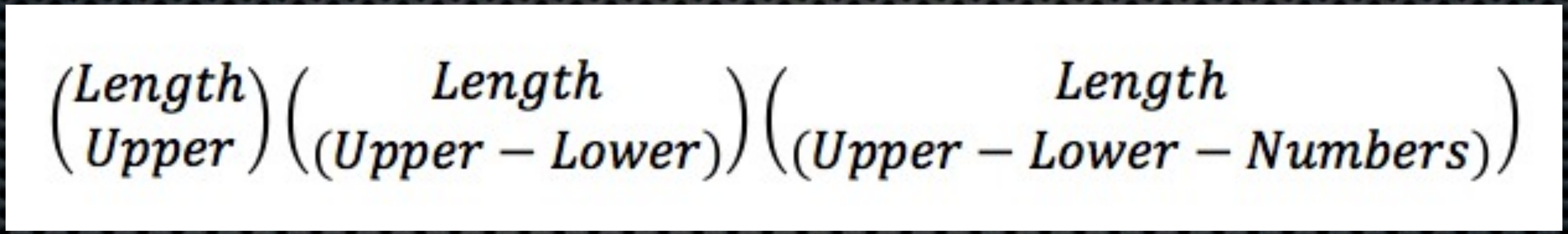
Tap on, Tap off:

Onscreen Keyboards & Mobile Password Entry

Kristen Greene
Josh Franklin
John Kelsey

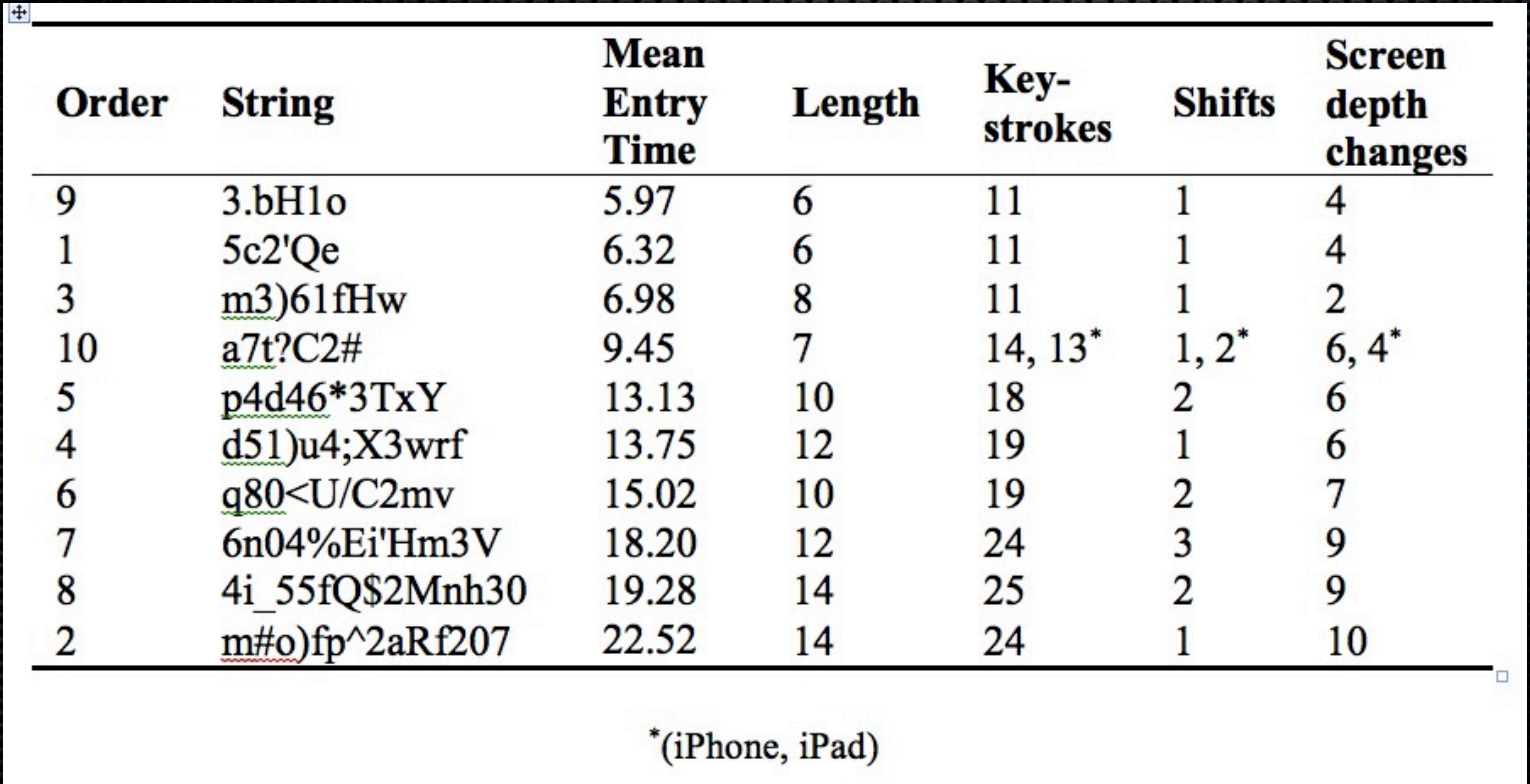
National Institute of
Standards and Technology
U.S. Department of Commerce

Our Entropy Loss



$$\binom{Length}{Upper}\binom{Length}{(Upper-Lower)}\binom{Length}{(Upper-Lower-Numbers)}$$

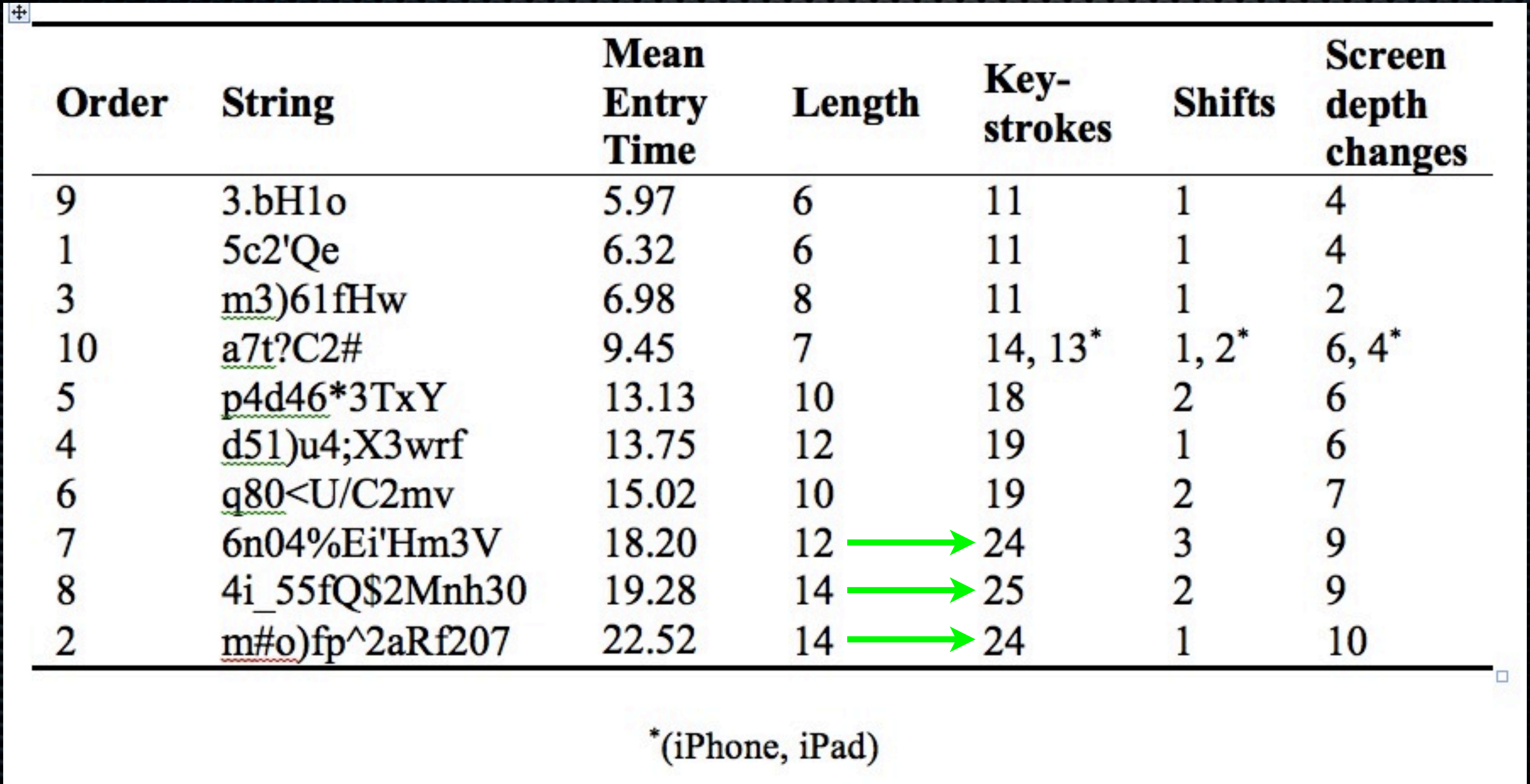
Prior Work: Entry Times



Order	String	Mean Entry Time	Length	Key-strokes	Shifts	Screen depth changes
9	3.bH1o	5.97	6	11	1	4
1	5c2'Qe	6.32	6	11	1	4
3	m3)61fHw	6.98	8	11	1	2
10	a7t?C2#	9.45	7	14, 13*	1, 2*	6, 4*
5	p4d46*3TxY	13.13	10	18	2	6
4	d51)u4;X3wrf	13.75	12	19	1	6
6	q80<U/C2mv	15.02	10	19	2	7
7	6n04%Ei'Hm3V	18.20	12	24	3	9
8	4i_55fQ$2Mnh30	19.28	14	25	2	9
2	m#o)fp^2aRf207	22.52	14	24	1	10

*(iPhone, iPad)

Prior Work: Entry Times

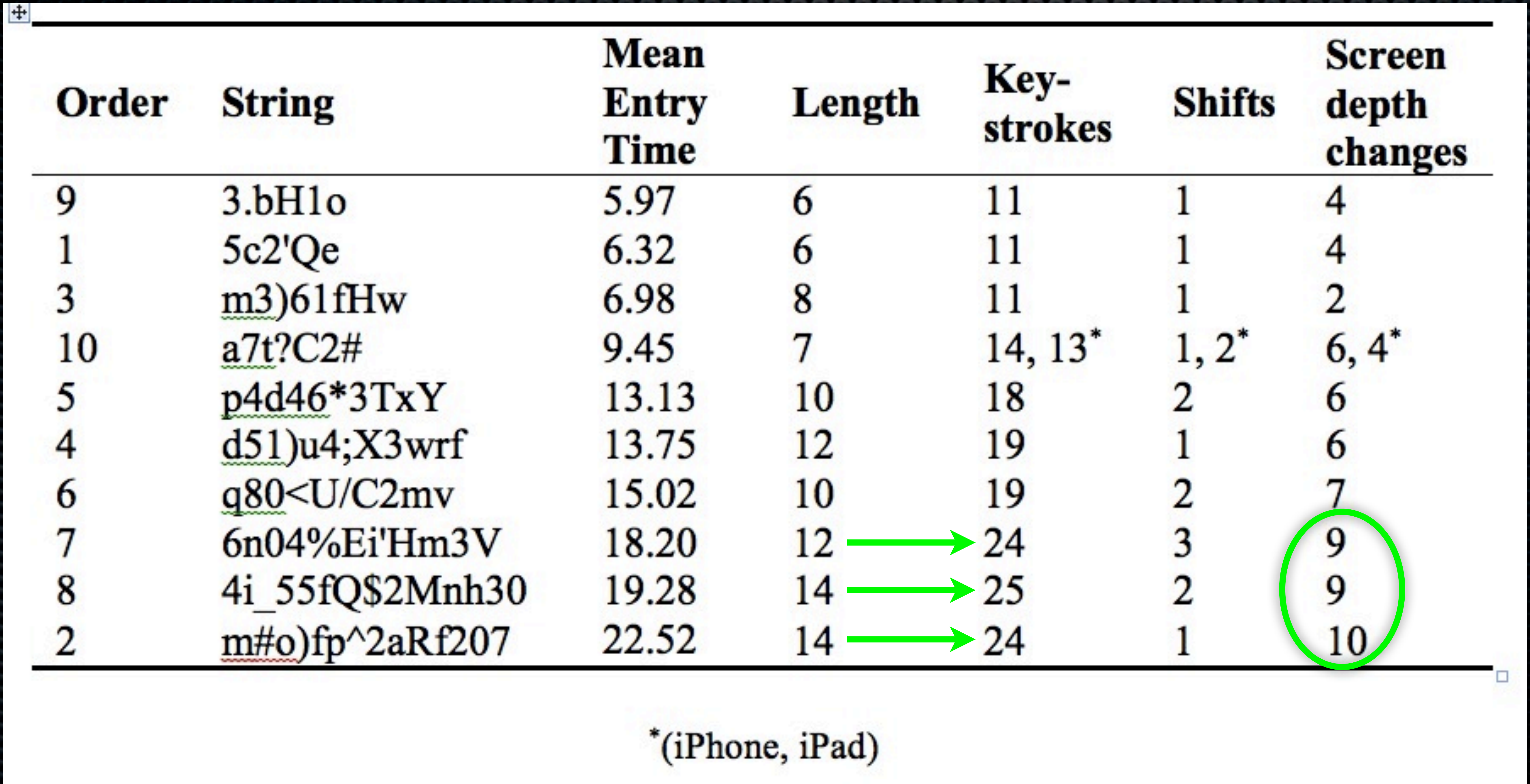


Order	String	Mean Entry Time	Length	Key-strokes	Shifts	Screen depth changes
9	3.bH1o	5.97	6	11	1	4
1	5c2'Qe	6.32	6	11	1	4
3	m3)61fHw	6.98	8	11	1	2
10	a7t?C2#	9.45	7	14, 13*	1, 2*	6, 4*
5	p4d46*3TxY	13.13	10	18	2	6
4	d51)u4;X3wrf	13.75	12	19	1	6
6	q80<U/C2mv	15.02	10	19	2	7
7	6n04%Ei'Hm3V	18.20	12	24	3	9
8	4i_55fQ$2Mnh30	19.28	14	25	2	9
2	m#o)fp^2aRf207	22.52	14	24	1	10

*(iPhone, iPad)

67

Prior Work: Entry Times

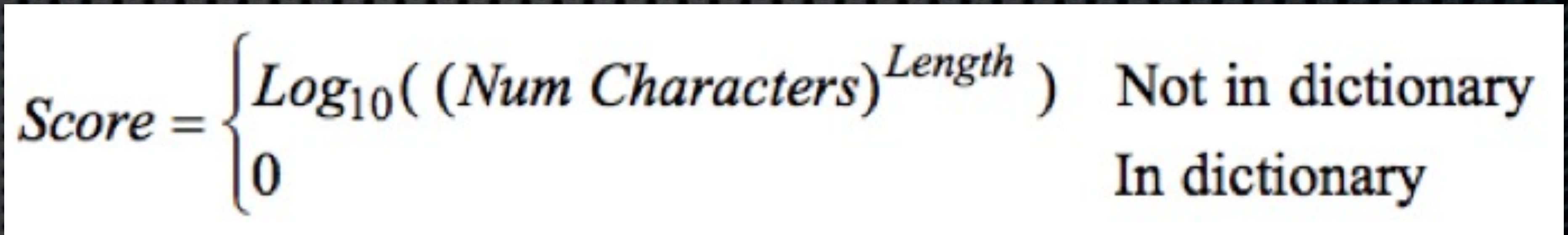


Order	String	Mean Entry Time	Length	Key-strokes	Shifts	Screen depth changes
9	3.bH1o	5.97	6	11	1	4
1	5c2'Qe	6.32	6	11	1	4
3	m3)61fHw	6.98	8	11	1	2
10	a7t?C2#	9.45	7	14, 13*	1, 2*	6, 4*
5	p4d46*3TxY	13.13	10	18	2	6
4	d51)u4;X3wrf	13.75	12	19	1	6
6	q80<U/C2mv	15.02	10	19	2	7
7	6n04%Ei'Hm3V	18.20	12	24	3	9
8	4i_55fQ$2Mnh30	19.28	14	25	2	9
2	m#o)fp^2aRf207	22.52	14	24	1	10

*(iPhone, iPad)

Modified Shannon Entropy

- Kuo, 2006



$$Score = \begin{cases} Log_{10}(\,(Num\ Characters)^{Length}\,) & \text{Not in dictionary} \\ 0 & \text{In dictionary} \end{cases}$$