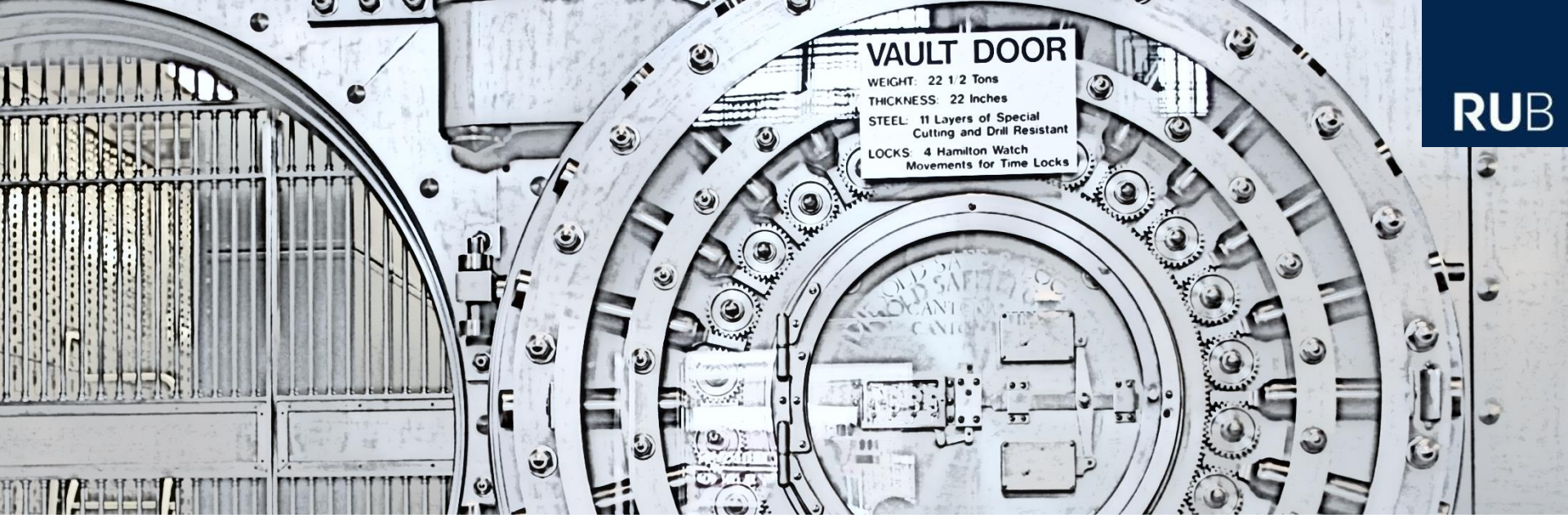


RUB

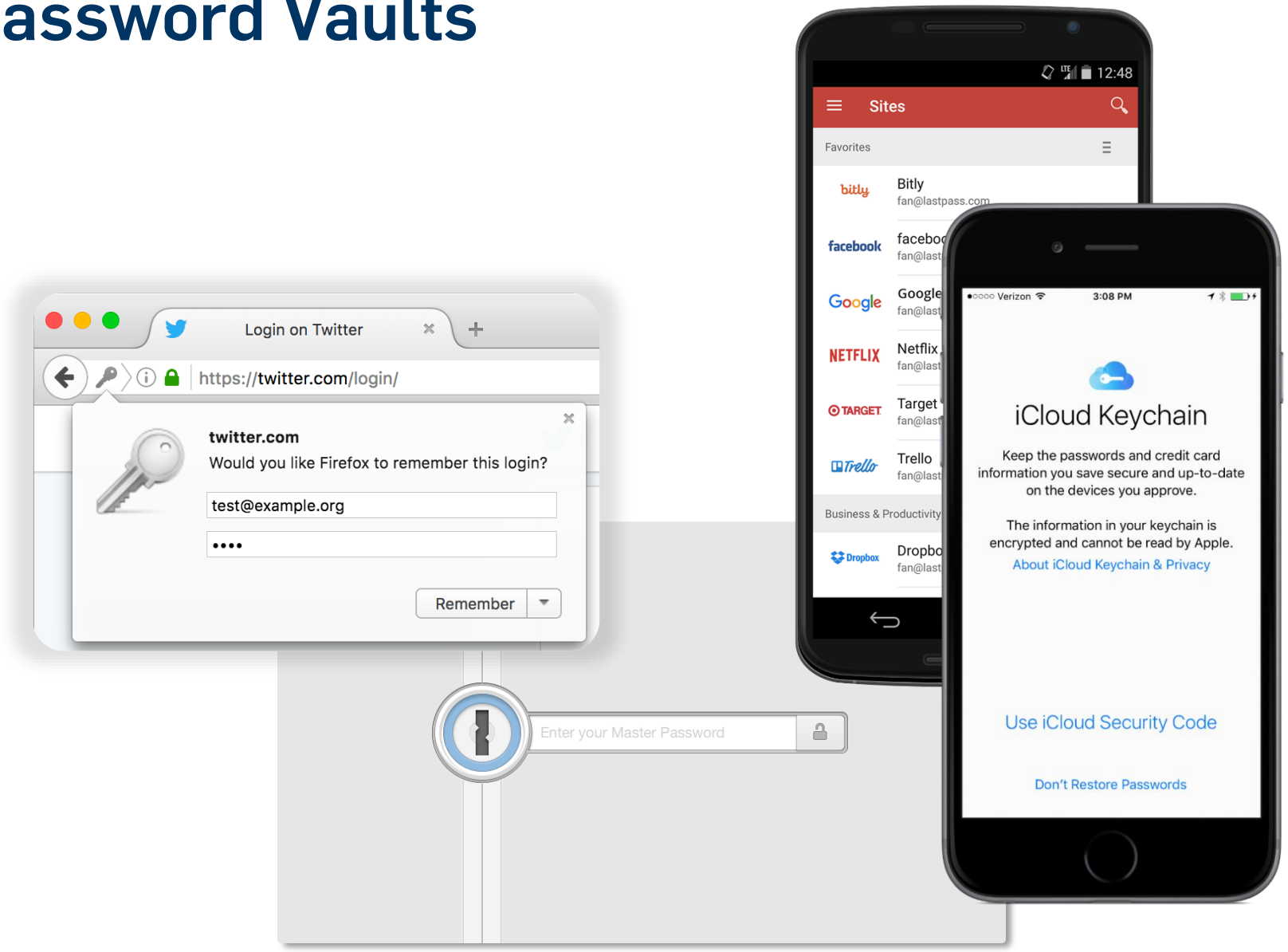
RUHR-UNIVERSITÄT BOCHUM

On the Security of Cracking-Resistant Password Vaults

Maximilian Golla, Benedict Beuscher, and Markus Dürmuth

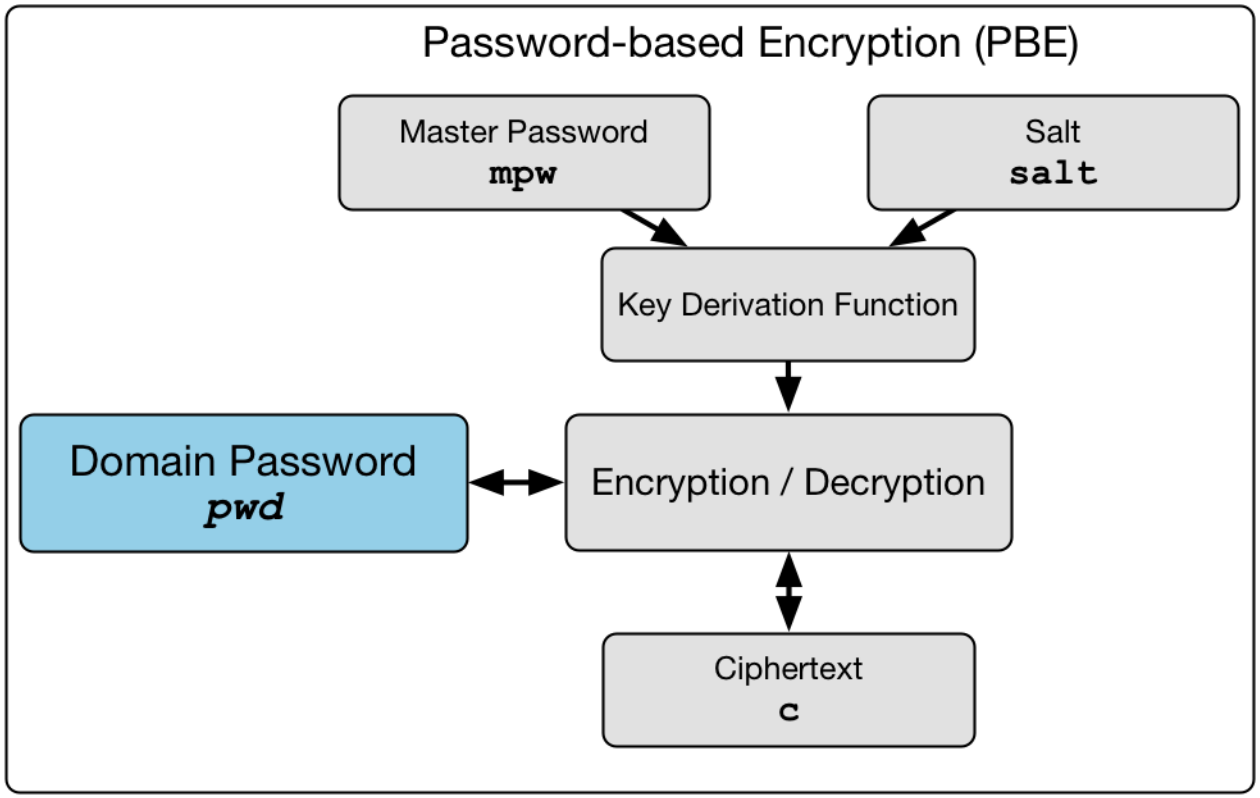
Horst Görtz Institute for IT-Security
Ruhr-University Bochum

Password Vaults



[Image 1-2] "LastPass Password Mgr" by LastPass, "iCloud Keychain iOS 9" by 9to5mac.com

Password-based Encryption (PBE)

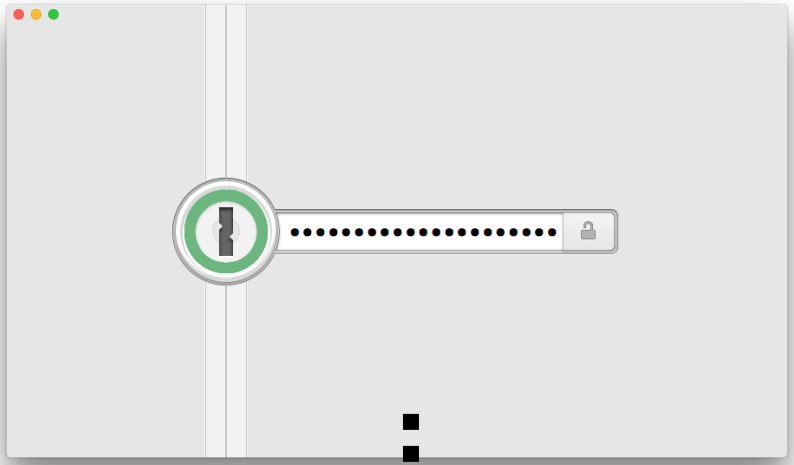


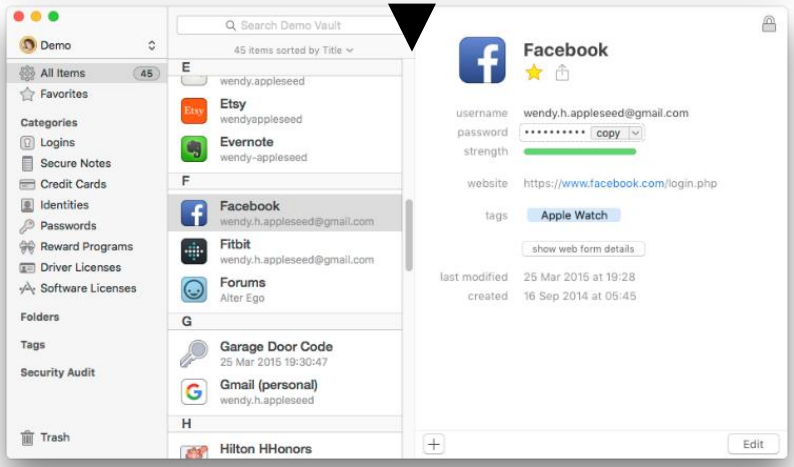
Normal Password Vault

RUB

Correct

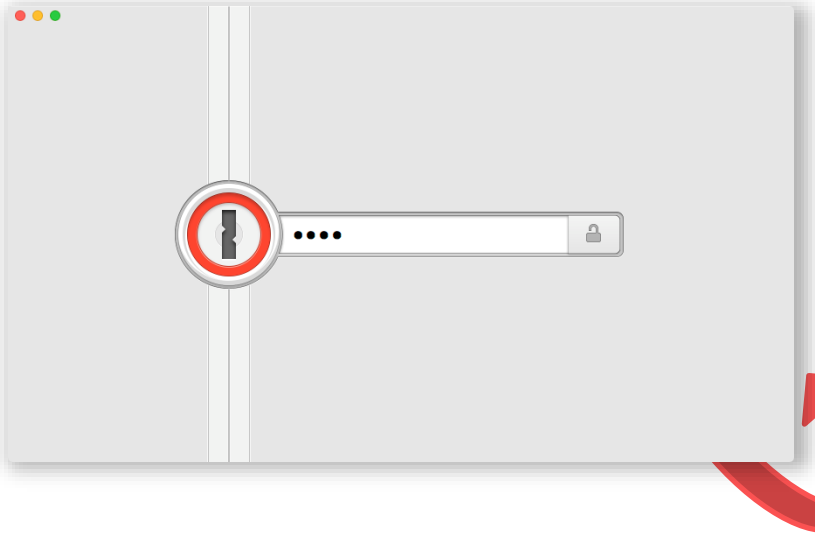
Master Password





Incorrect

Master Password



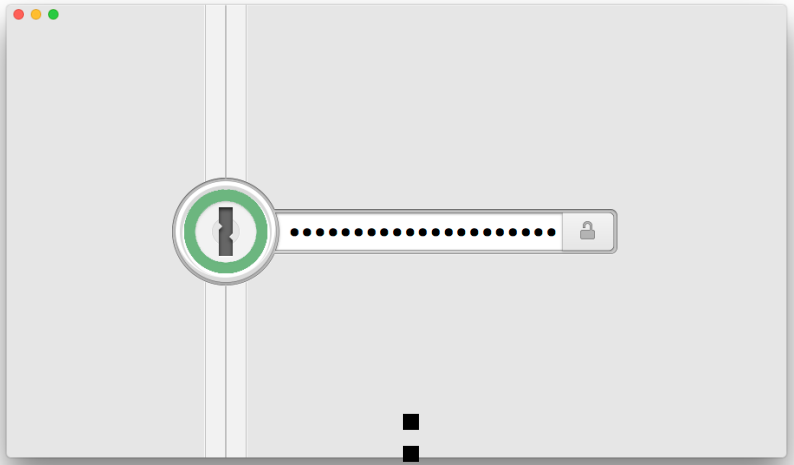
Try again, ...

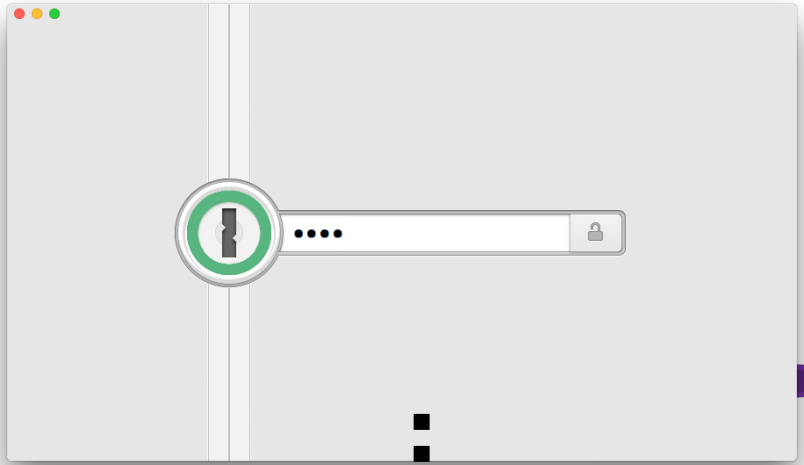
Cracking-Resistant Password Vault

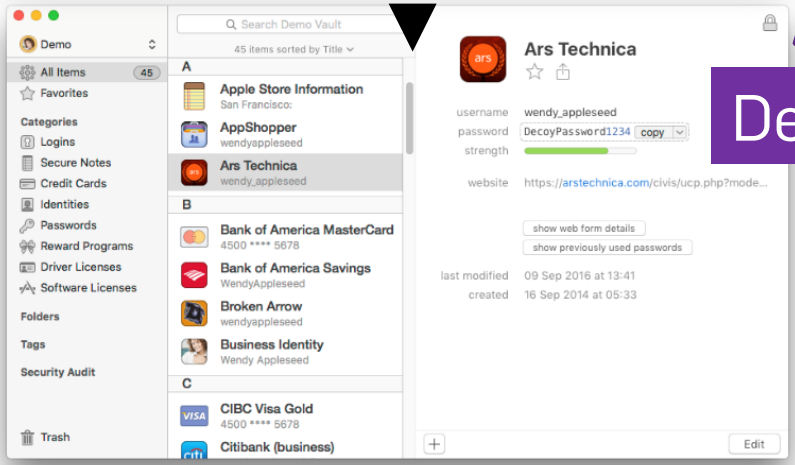
RUB

Correct Master Password

Incorrect Master Password







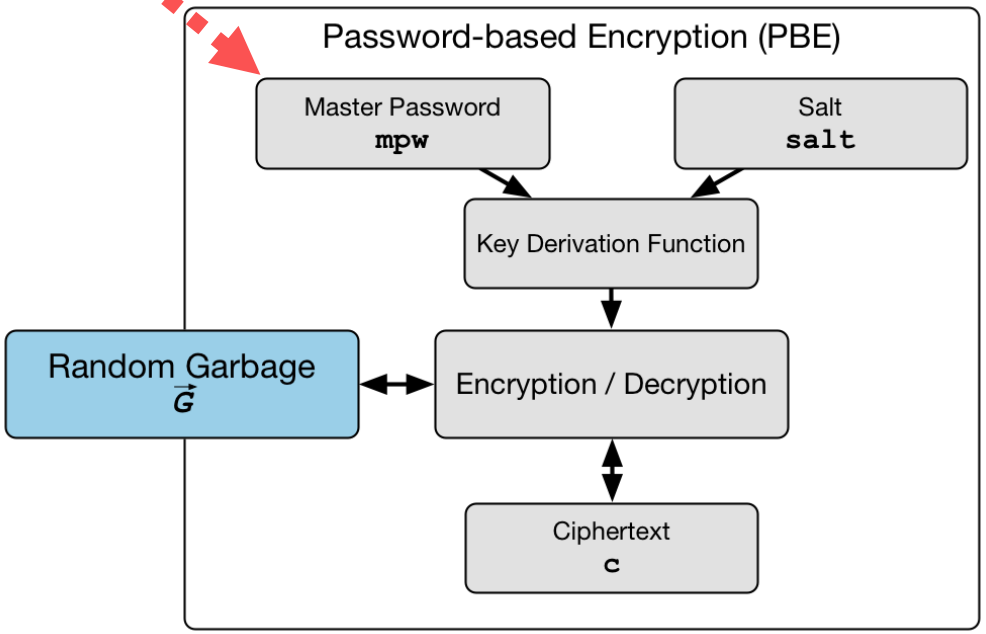
Decoy![1]

[Ref. 1] Hristo Bojinov, Elie Bursztein, Xavier Boyen, and Dan Boneh. Kamouflage: Loss-Resistant Password Management. (ESORICS '10)

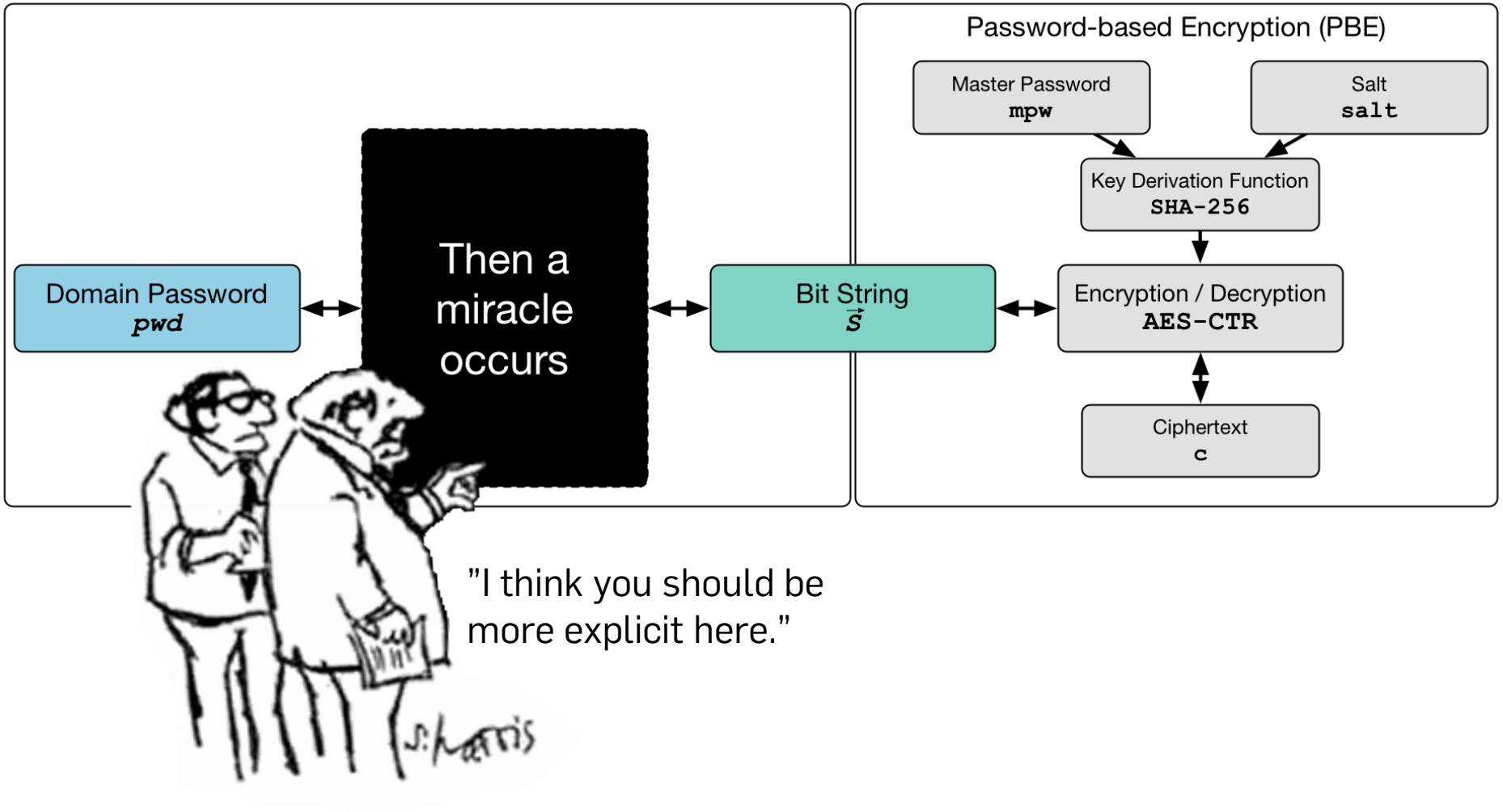
Password-based Encryption (PBE)

If MPW is incorrect

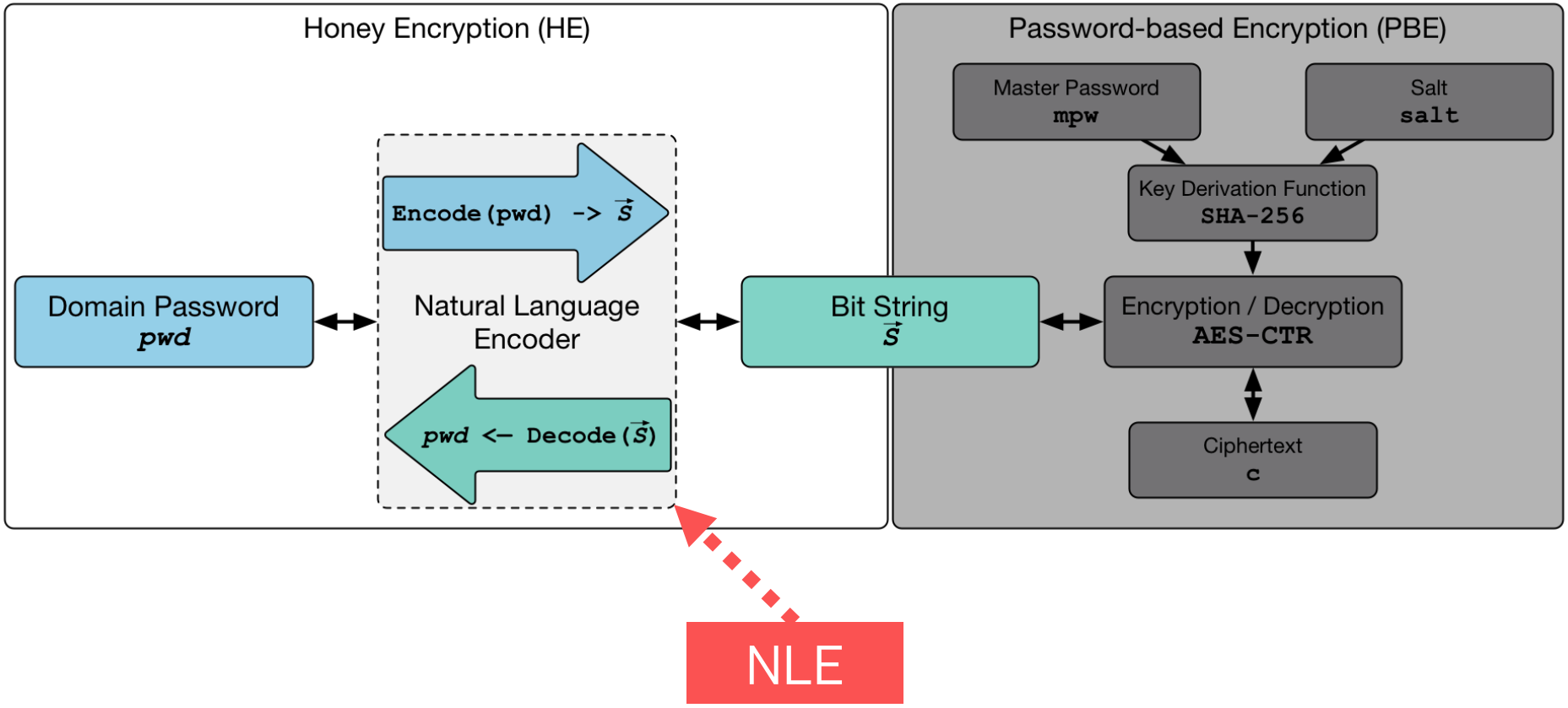
DEL34<(ä/!°$9▒01
+■#ôNUL(°x+#.,%=
@<^SOHÇ4!ô°$)!ô?
=$°%($ — 4^ACKf
Σ3d4



PBE + ?

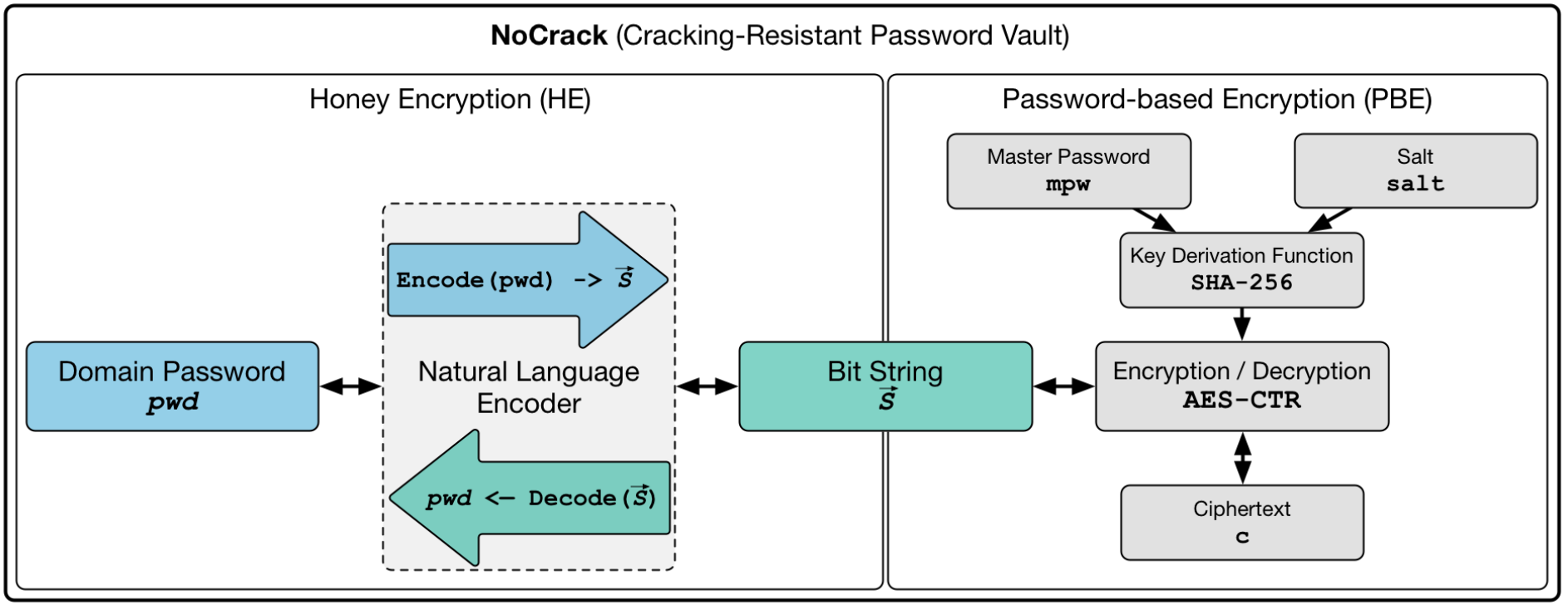

Password-based Encryption (PBE)
Master Password
mpw
Salt
salt
Key Derivation Function
SHA-256
Domain Password
pwd
Then a miracle occurs
Bit String
$\vec{s}$
Encryption / Decryption
AES-CTR
Ciphertext
c
"I think you should be more explicit here."

PBE + Honey Encryption[2]



[Ref. 2] Ari Juels and Thomas Ristenpart.
Honey Encryption: Security Beyond the Brute-Force Bound. (EUROCRYPT '14)

PBE + Honey Encryption[2] -> NoCrack[3]



Cracking-Resistant vault based on **Honey Encryption**.

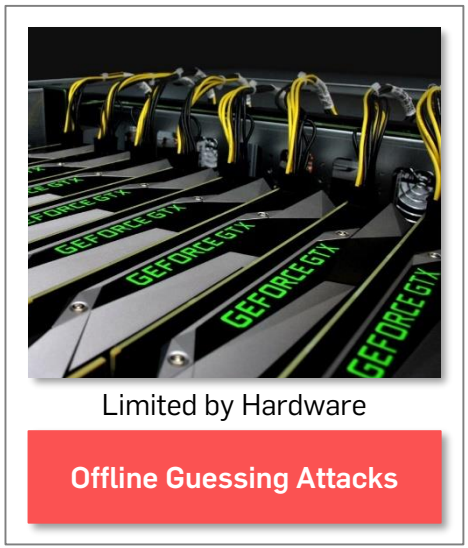
PCFG-based NLE.

[Ref. 3] Rahul Chatterjee, Joseph Bonneau, Ari Juels, and Thomas Ristenpart. Cracking-Resistant Password Vaults using Natural Language Encoders. (SP '15)

[Image 1] "NoCrack Icon" made by Rahul Chatterjee (SP Slides)

Benefits of Cracking-Resistant Vaults

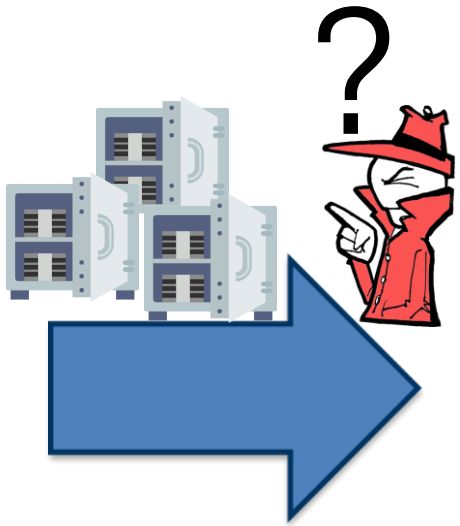
Attacker needs to **verify every guessed master password by** trying to **login with some** alleged **credentials**.



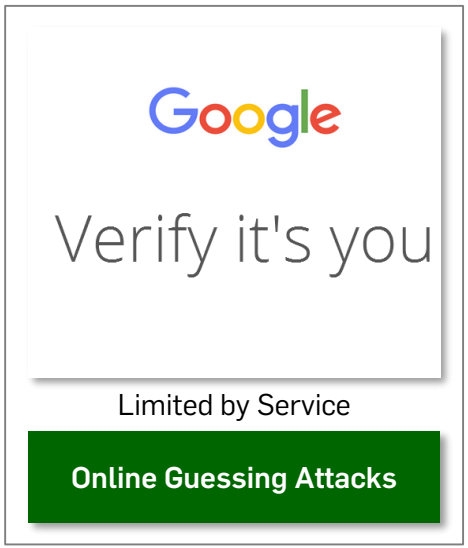
Limited by Hardware

Offline Guessing Attacks

e.g., 10^{12} guesses/day



Cracking-Resistance



Limited by Service

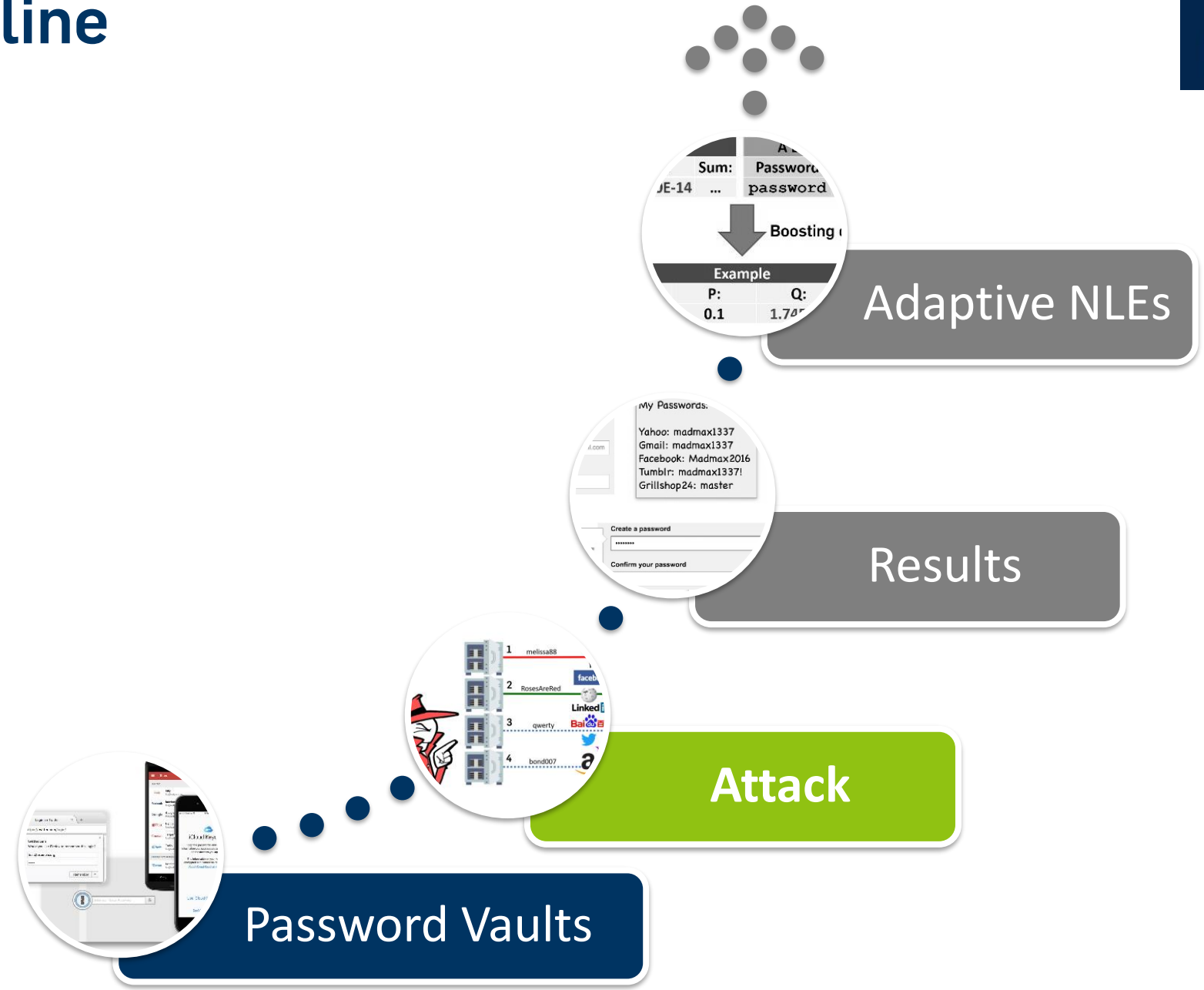
Online Guessing Attacks

e.g., 10 guesses/day

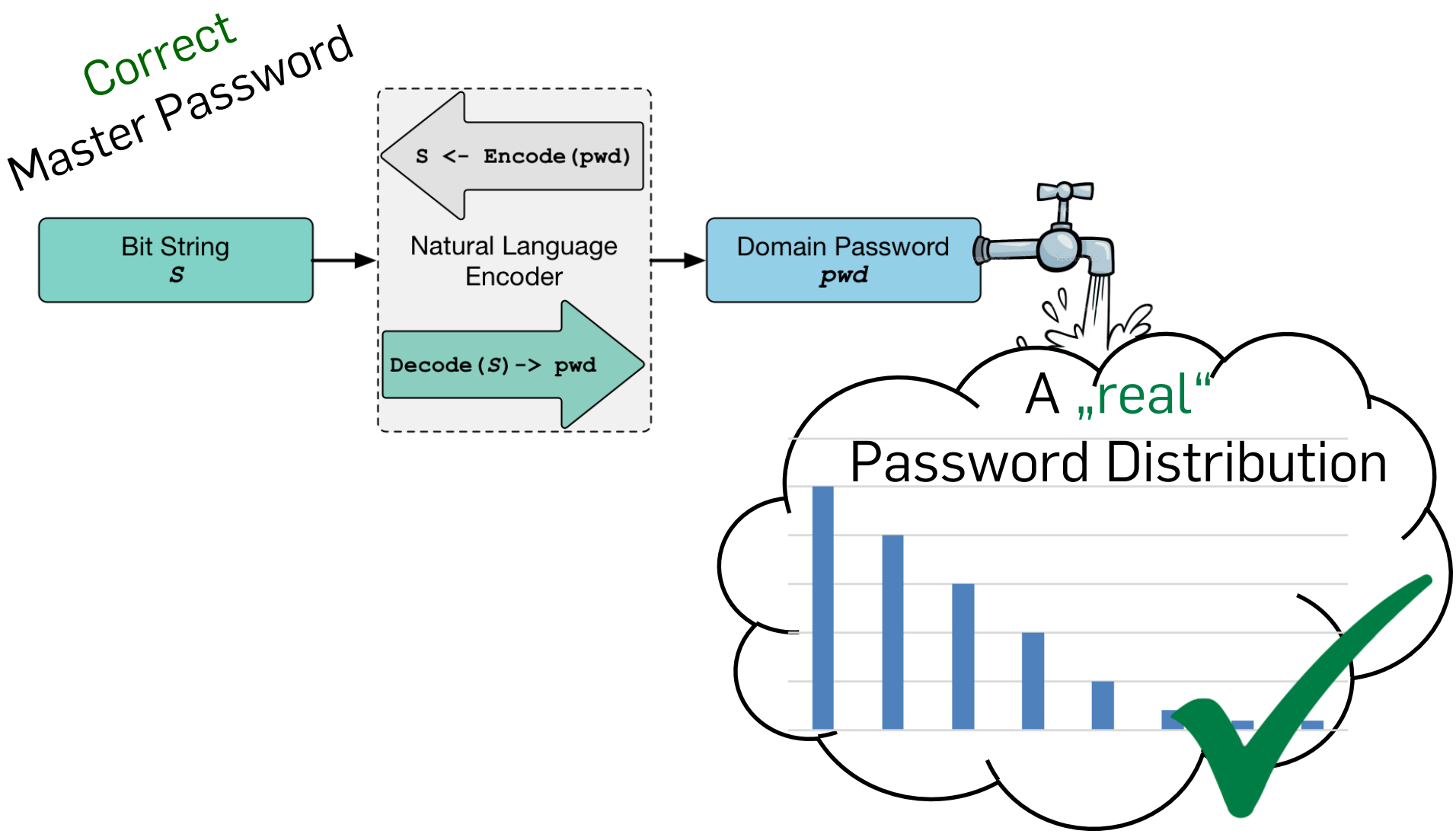
Via Honey Encryption we can generate decoys **on the fly**!

[Image 1] "8x GTX 1080" made by Sagitta HPC (sagitta.pw)

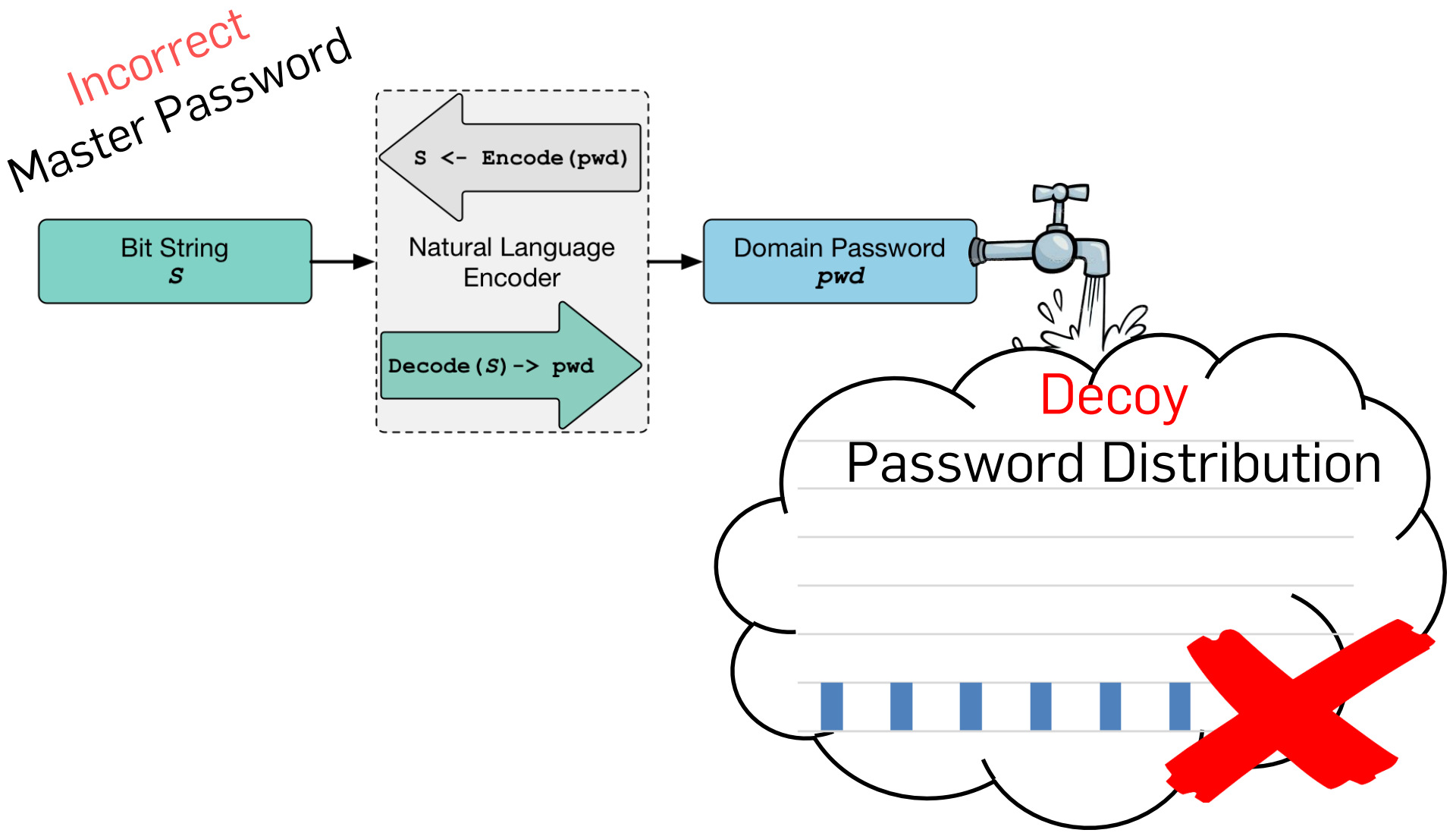
Outline


Sum:
password
Boosting
Example
P:
Q:
0.1
Adaptive NLEs
My Passwords.
Yahoo: madmax1337
Gmail: madmax1337
Facebook: Madmax2016
Tumblr: madmax1337!
Grillshop24: master
Create a password
Confirm your password
Results
1 melissa88
2 RosesAreRed
3 qwerty
4 bond007
Attack
Password Vaults

How to Crack a Cracking-Resistant Vault?



How to Crack a Cracking-Resistant Vault?

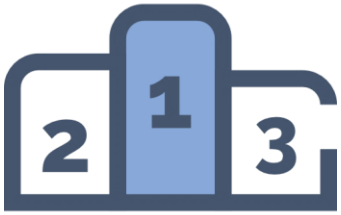


Attack Idea

- A realistic adversary **doesn't know** the "**real**" password **distribution**[4]
- but, can **approximate NoCrack's distribution**!
- If we **observe outliers** (not following NoCrack's distribution), we can **use** them **for ranking**.

[Ref. 4] Joseph Bonneau.
"Guessing Human-Chosen Secrets," PhD dissertation, University of Cambridge, 2012

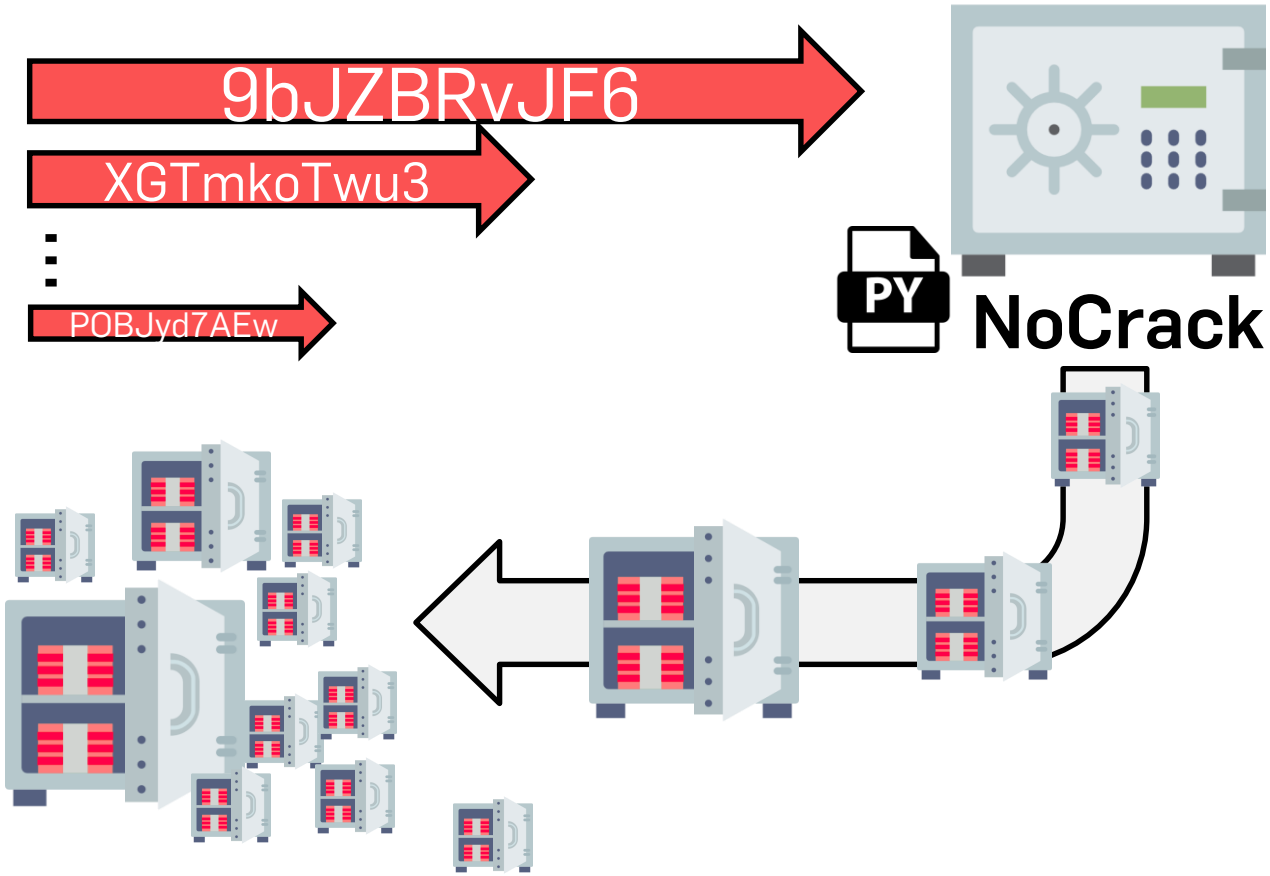
Attack Overview

1. Approximate Decoy Distribution 
2. Trial-Decryption 
3. Ranking of Vault Candidates 

4. Online Verification 

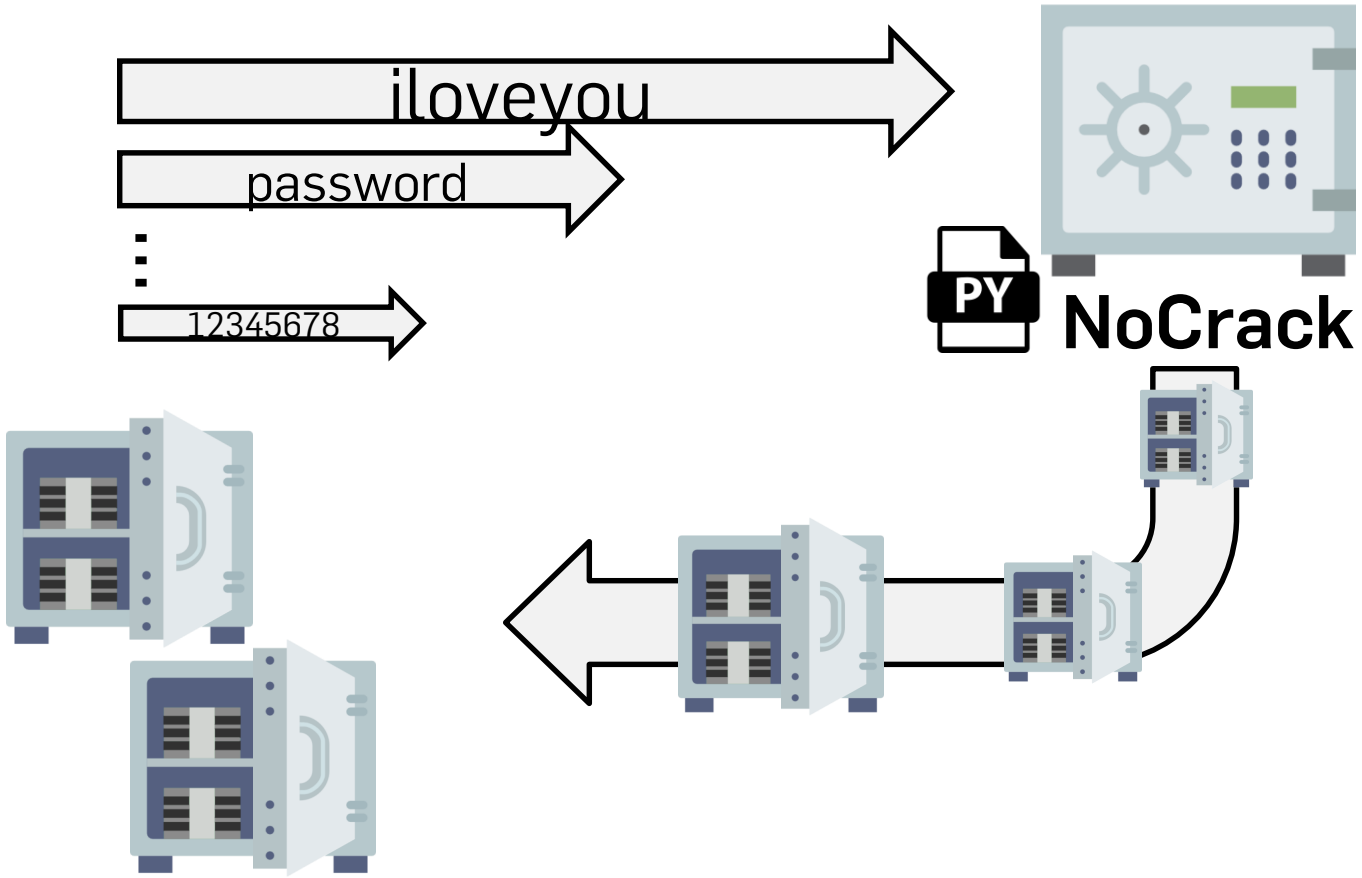
1. Approximate Distribution of Decoy Vaults

Repeatedly sample passwords from the distribution by evaluating the KDF and trial-decrypting the vault.



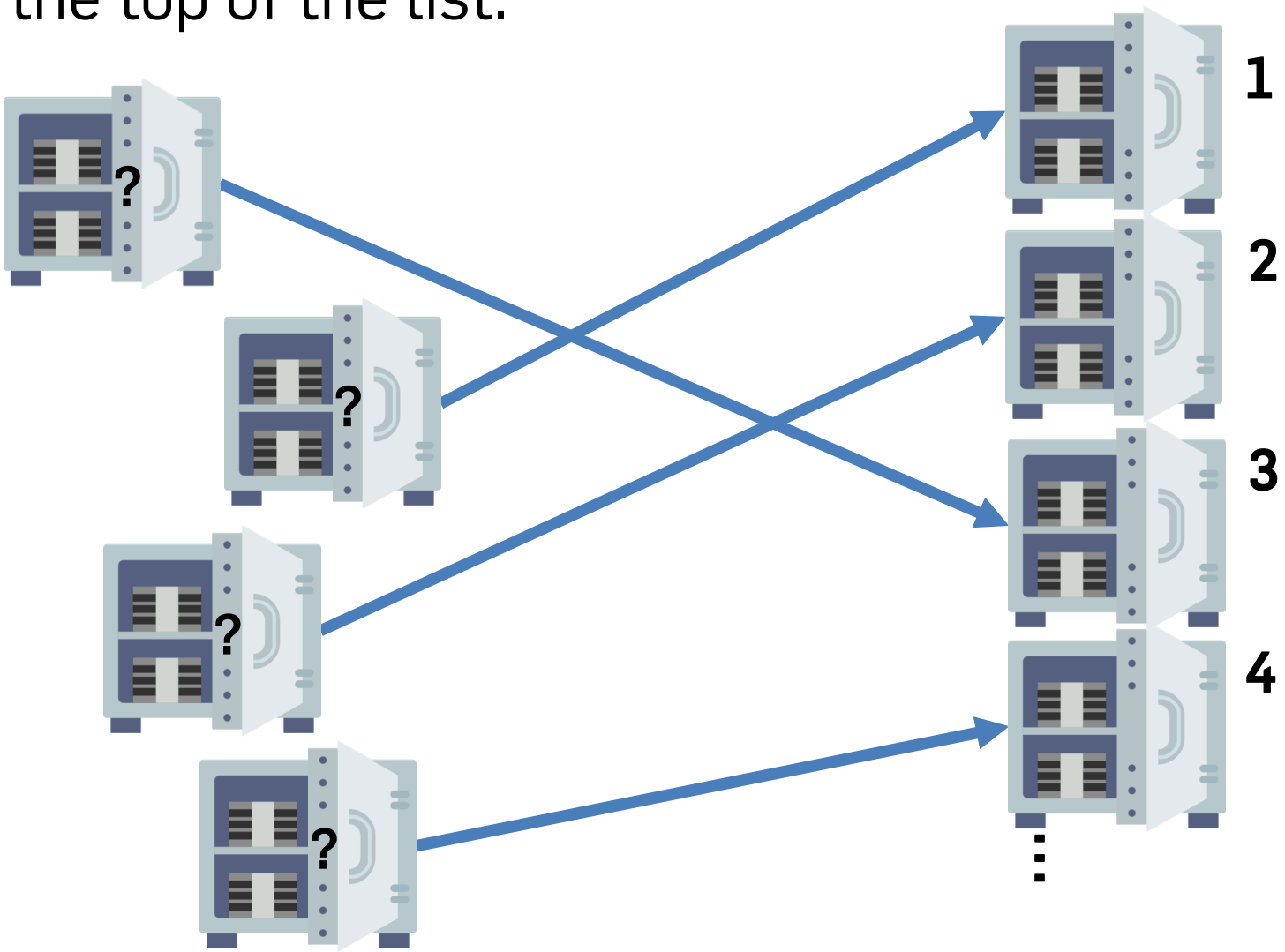
2. Trial-Decryption

Decrypt vault **with candidate master passwords**.
(Assume the correct master password is in this list.)



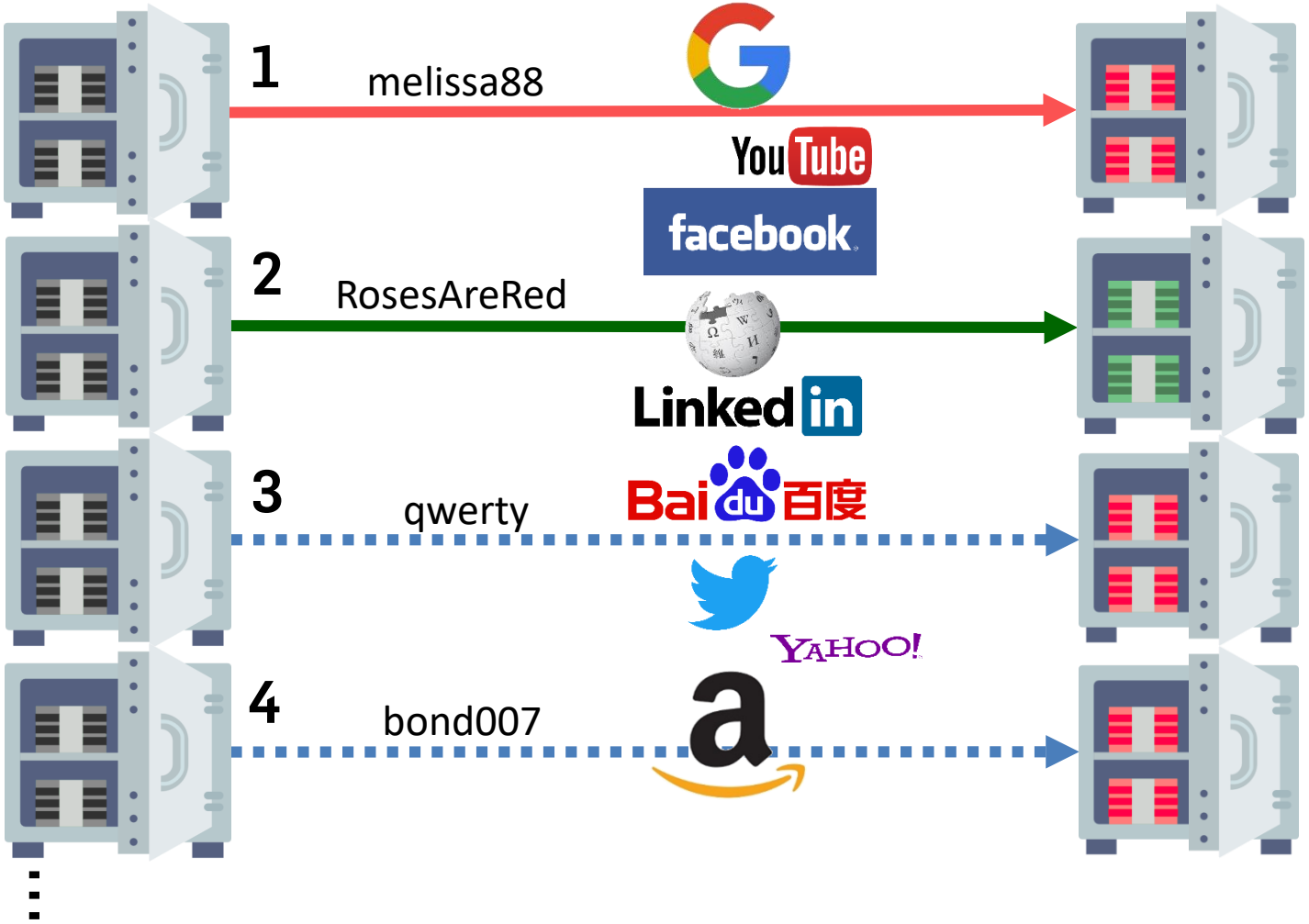
3. Ranking of Vault Candidates

Rank candidates so that the real vault is (hopefully) near the top of the list.

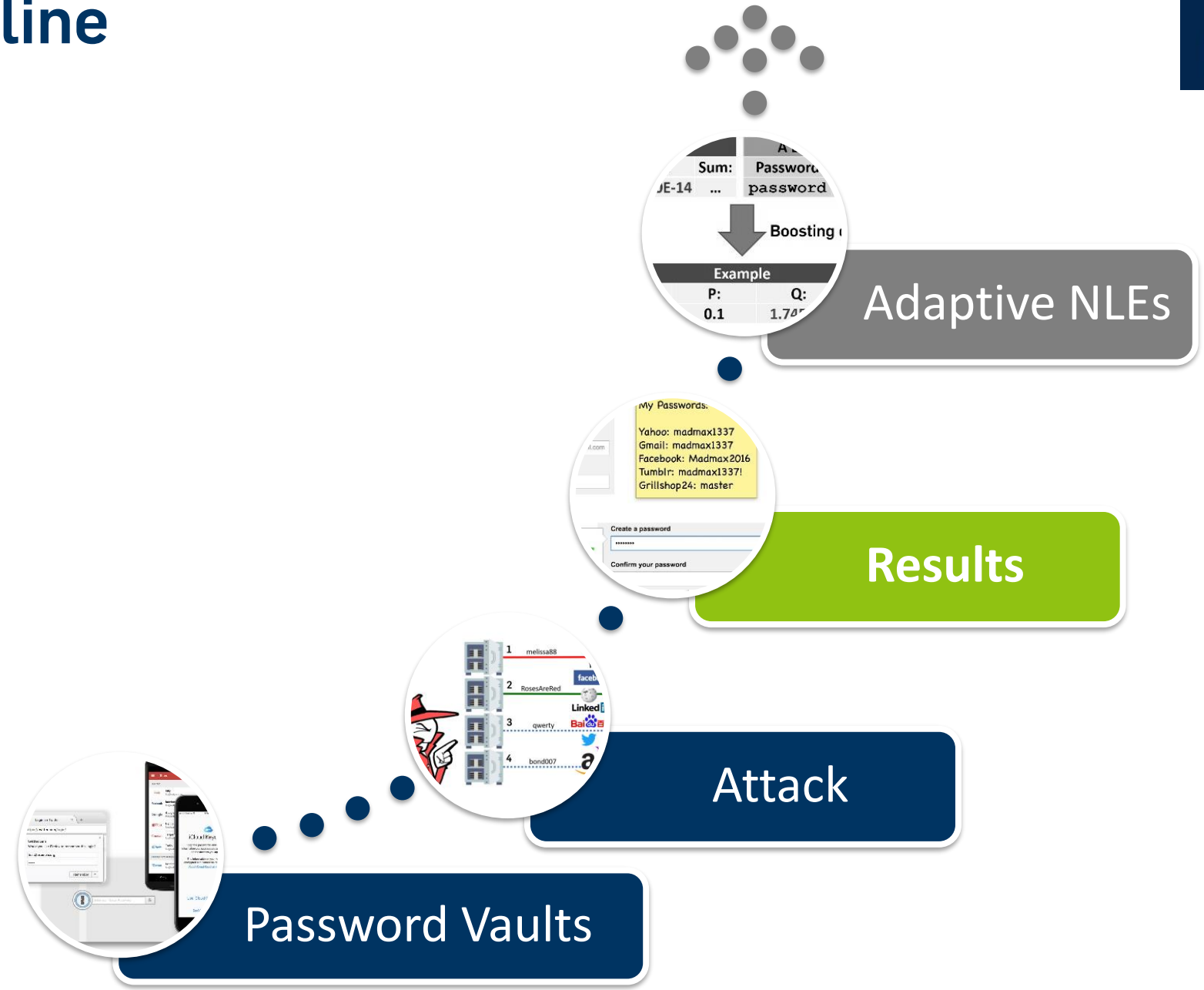


4. Online Verification

Go **online** and **verify** the correctness, starting with the highest ranked vault.



Outline


Sum:
password
Boosting
Example
P:
Q:
0.1
Adaptive NLEs
My Passwords:
Yahoo: madmax1337
Gmail: madmax1337
Facebook: Madmax2016
Tumblr: madmax1337!
Grillshop24: master
Create a password
Confirm your password
Results
1 melissa88
2 RosesAreRed
3 qwerty
4 bond007
Attack
Password Vaults

Experimental Setup

- Dataset from previous work[3]. (Org. gathered by malware)

Vault Size:	2-3	4-8	9-50
Samples	100	89	87

- Ranking with 1.000 vaults (relative ranking)
  - 999 decoy vaults, 1 real vault

[Ref. 3] Rahul Chatterjee, Joseph Bonneau, Ari Juels, and Thomas Ristenpart. Cracking-Resistant Password Vaults using Natural Language Encoders. (SP '15)

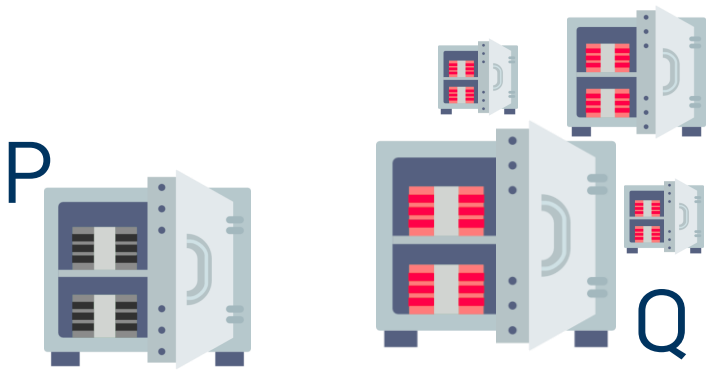
Experimental Setup

- Kullback–Leibler (KL) divergence
  - to measure the difference between the distributions.

$$D_{KL}(P \parallel Q) = \sum_{z \in \mathrm{supp}(P)} P[z] \cdot log \frac{P[z]}{Q[z]}$$

- Tested influence of approx. precision (1.000 - 30.000.000 vaults)

- Tested different vault sizes (2-50 passwords)

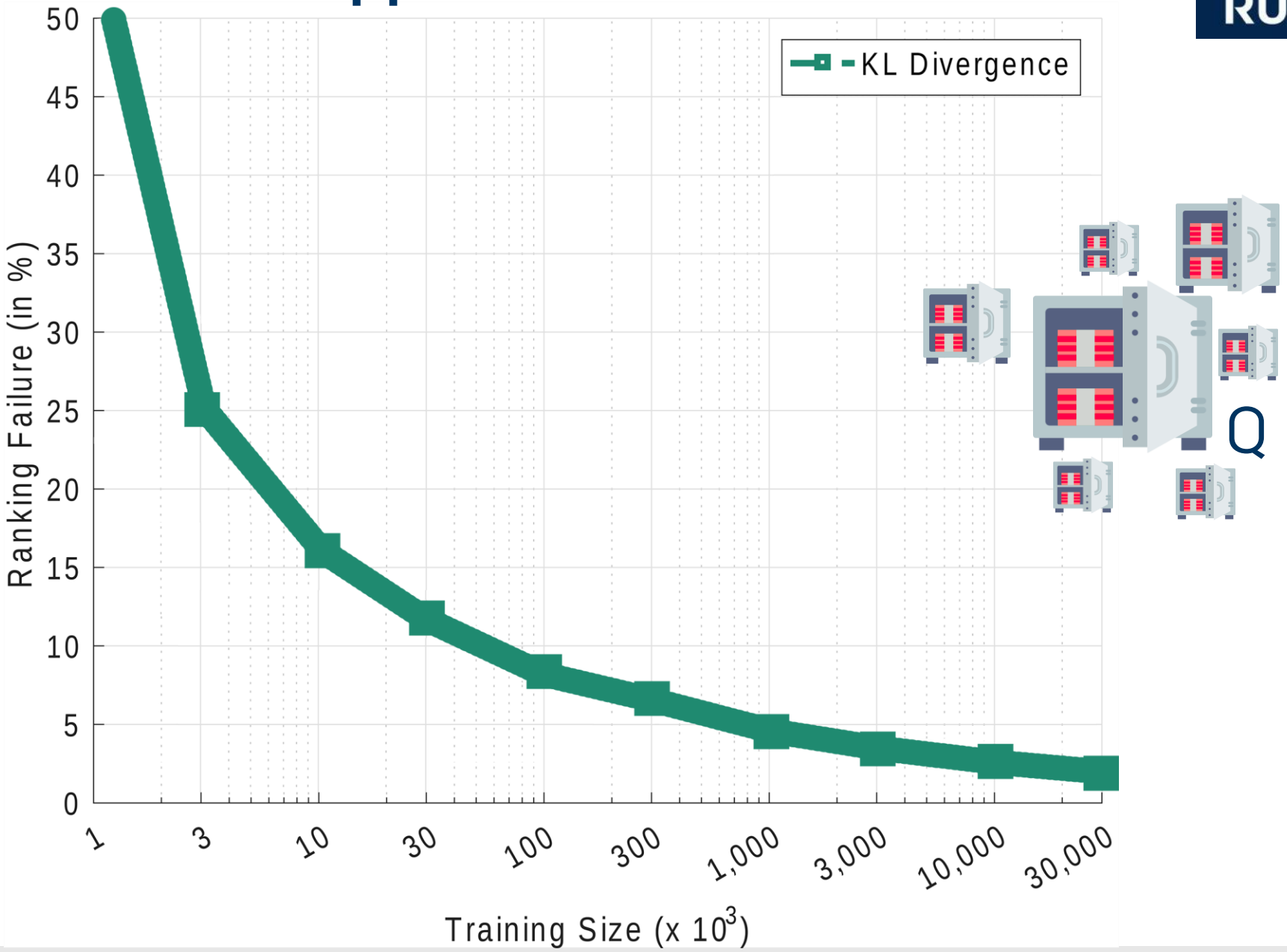


Results

	Perfect NLE	Prev. Work[3]	Our Classifier			
Attack	Guessing	ML	KL			
Mean Rank	50.0%	37.8%	6.2%			
Median Rank	50.0%	/	2.0%			

[Ref. 3] Rahul Chatterjee, Joseph Bonneau, Ari Juels, and Thomas Ristenpart. Cracking-Resistant Password Vaults using Natural Language Encoders. (SP '15)

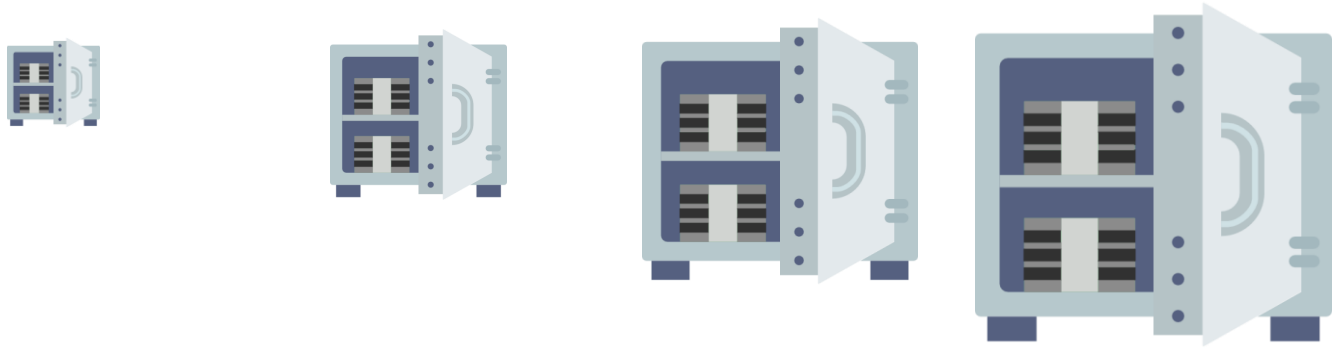
Influence of Approximation Precision



Difference in Vault Size

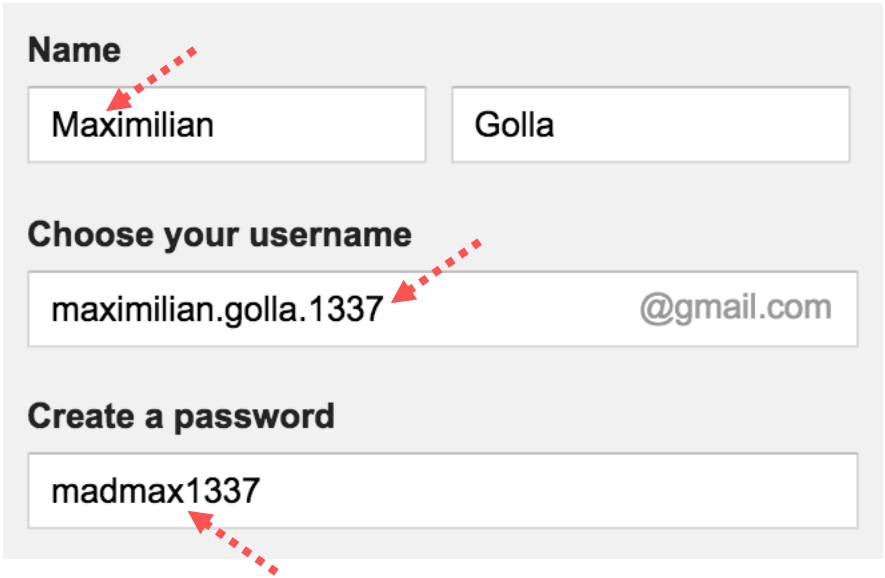
RUB

Vault Size:	2-3	4-8	9-50	All (2-50)
Mean Rank	9.6%	6.0%	3.1%	6.2%
Median Rank	2.1%	1.9%	1.7%	2.0%



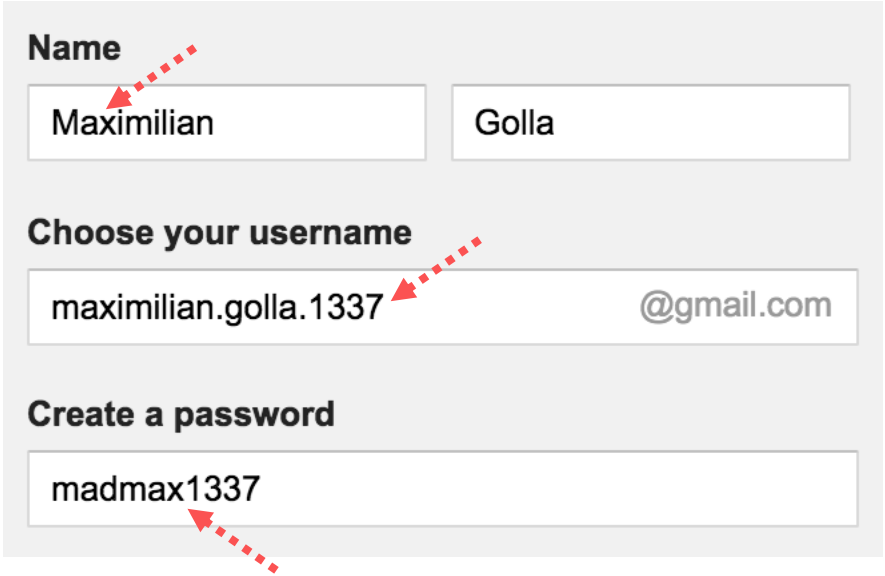
Correlation,

Correlation

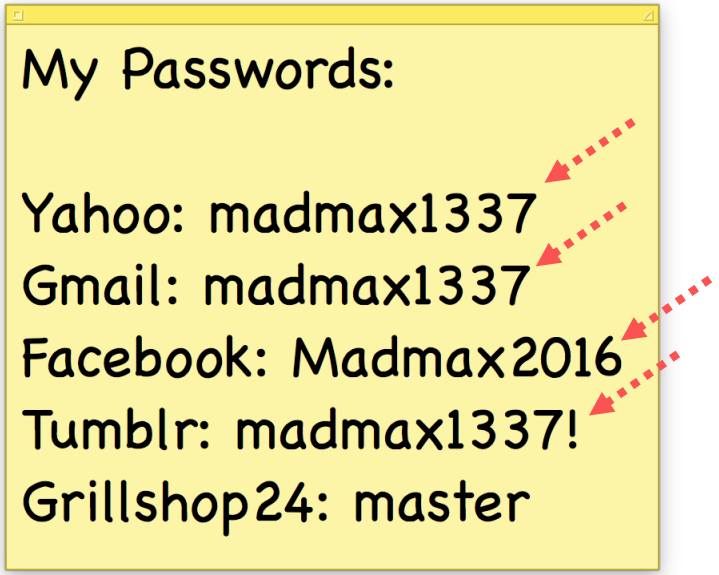


Correlation, Reuse,

Correlation

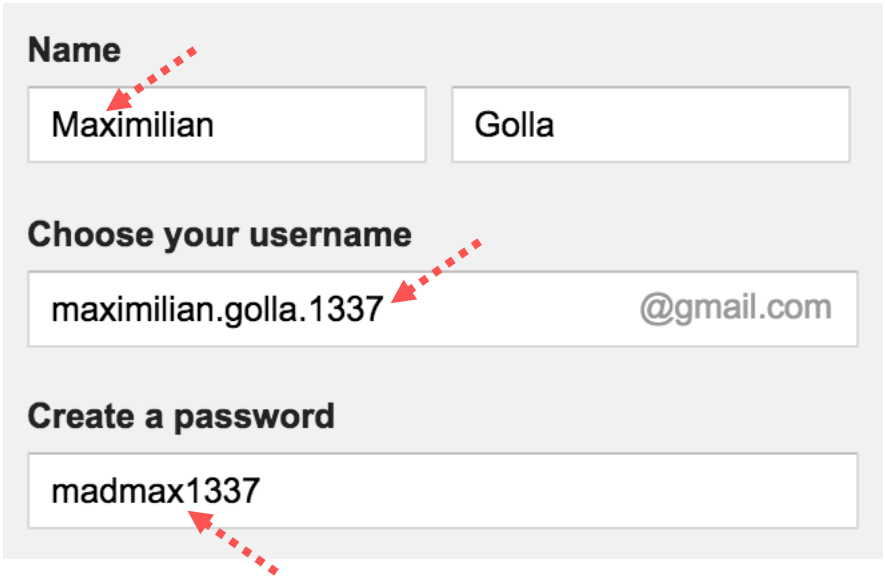


Reuse

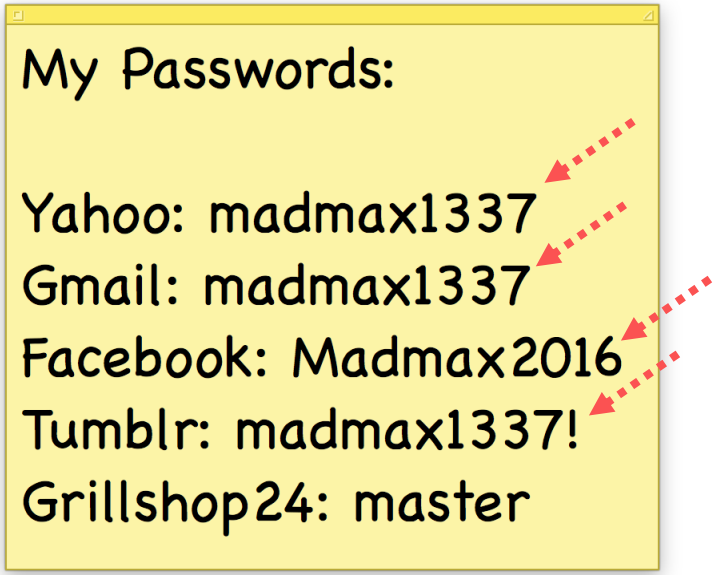


Correlation, Reuse, and Policies Issues

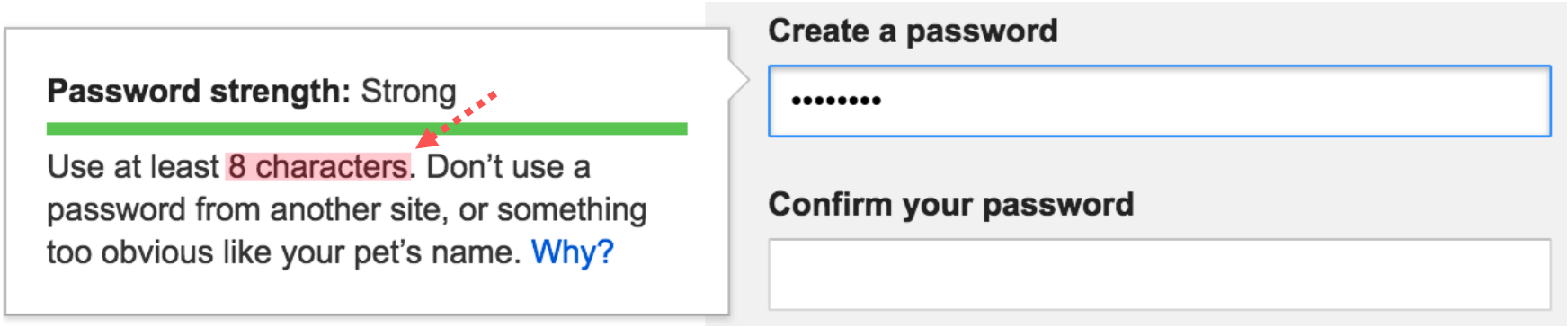
Correlation



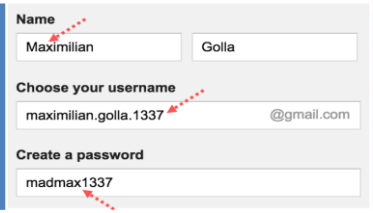
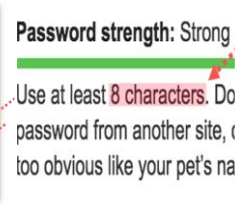
Reuse



Policies



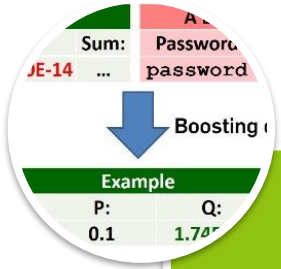
Results

	Perfect NLE	Prev. Work				
Attack	Guessing	ML	KL	Correlation	Reuse	Policy
Mean Rank	50.0%	37.8%	6.2%	6.4%	6.2%	2.5%
Median Rank	50.0%	/	2.0%	2.1%	2.0%	1.4%

→ KL: **Reduction** of required **online queries by** a factor of **8**.

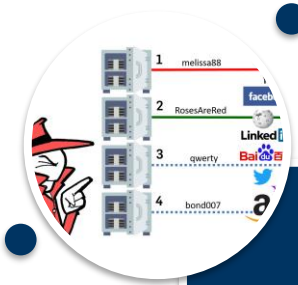
→ KL + background info: **Reduction by** a factor of **20**.

Outline



Adaptive NLEs

Results



Attack

Password Vaults

The Flaw

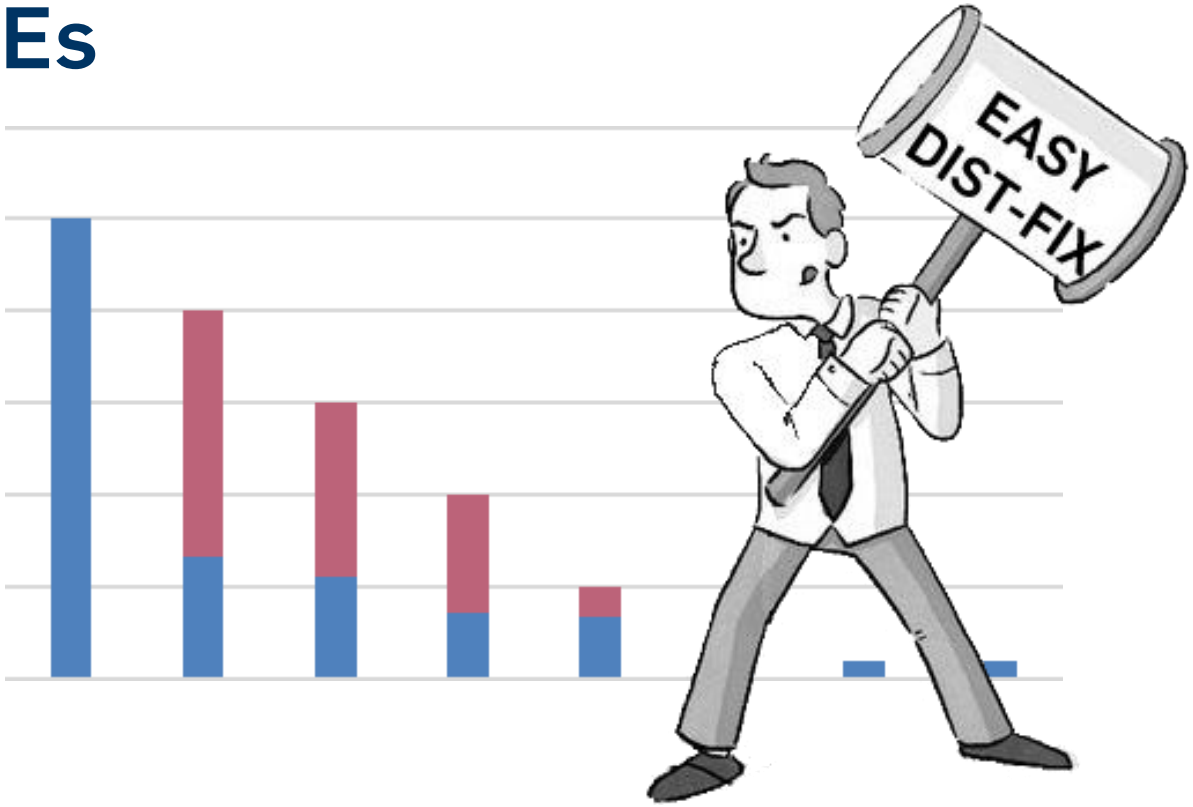
Improbable **password** are a **strong signal** for the real vault.

The Real Vault	
Password	Q:
kamaria	1.00E-14
khalilah	1.00E-14
…	…
pinkrose13	1.00E-14

A Decoy Vault (No. 23)	
Password	Q:
password	1.74E-02
JOHNCENA	4.02E-06
…	…
p4ssw0rd	8.05E-06

→ **Change NoCrack's NLE** to **simulate** the correct aka "**the real**" password **distribution**!

Static NLEs



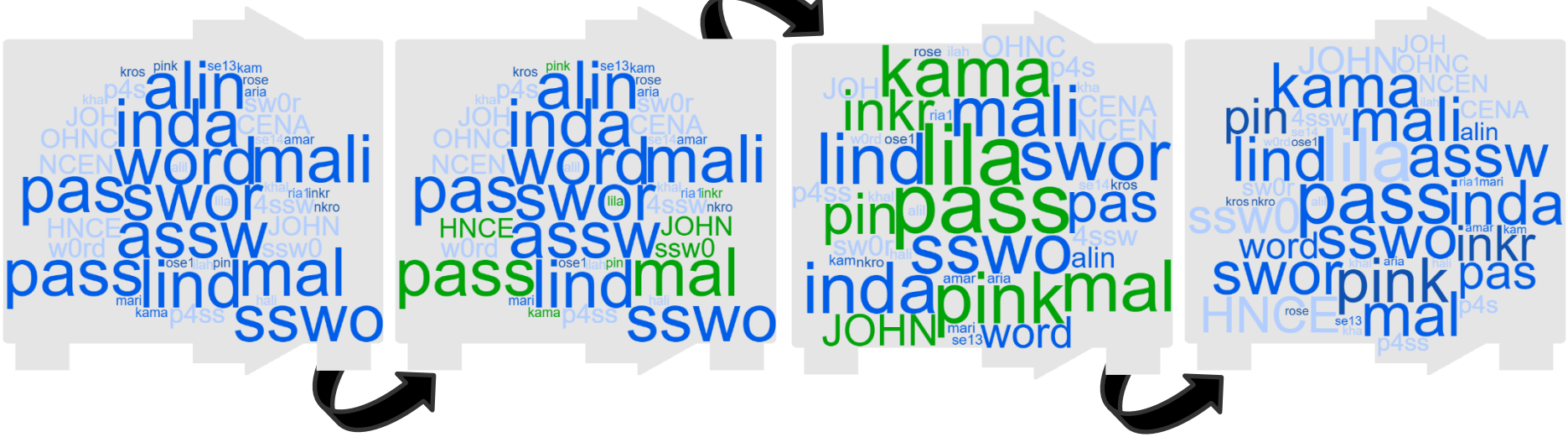
Static NLEs

There is no „the real“ password distribution!
Dist. differs by service and time → We can’t predict it

→ Do **not assign low probabilities** to **passwords** that **appear in** the **real vault**!

Adaptive NLEs

Boost their probabilities by a constant value



Select a fraction of ALL *n-grams* (real and decoy)

Re-normalize

Paper gives a **bound on** the amount of **information** that is **leaked**.

Limitations / Future Work

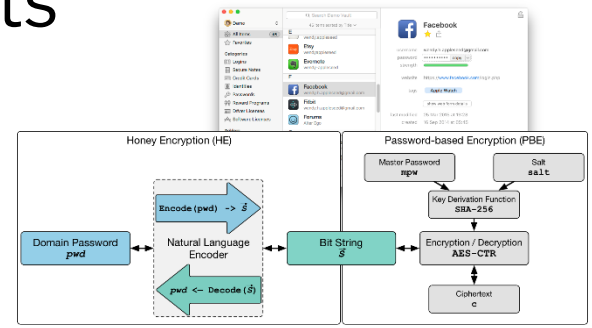
- **Lack** of sample **data**

- Are **master passwords guessable**?
- Is a master password related to the domain passwords inside the vault?

- Improve **adaptive NLEs**
- Improve attack

Takeaway

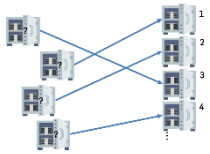
1. Honey Encryption → Cracking-Resistant Password Vaults



2. Building an NLE is challenging!
   (Distribution, Reuse, Correlation, Policies, …)

3. Adaptive NLE can solve the distribution problem.

Step 3: Ranking Example



The Real Vault			
Password	P:	Q:	Sum:
kamaria	0.1	1.00E-14	4.651
khalilah	0.1	1.00E-14	9.302
kamaria1	0.3	1.00E-14	13.952
kamaria1	0.3	1.00E-14	18.603
kamaria1	0.3	1.00E-14	23.254
pinkrose13	0.4	1.00E-14	27.904
pinkrose13	0.4	1.00E-14	32.555
pinkrose13	0.4	1.00E-14	37.206
pinkrose13	0.4	1.00E-14	41.856
pinkrose14	0.1	1.00E-14	46.507
KL-Div: 46.507			

A Decoy Vault (No. 23)			
Password	P:	Q:	Sum:
password	0.4	1.74E-02	0.181
password	0.4	1.74E-02	0.362
password	0.4	1.74E-02	0.543
password	0.4	1.74E-02	0.724
malinda	0.4	1.00E-14	5.374
malinda	0.4	1.00E-14	10.025
malinda	0.4	1.00E-14	14.676
malinda	0.4	1.00E-14	19.326
p4ssw0rd	0.1	8.05E-06	19.462
JOHNCENA	0.1	4.02E-06	19.608
KL-Div: 19.608			

Final Ranking		
Rank	Vault	KL-Div:
1	DECOY 12	49.829
2	REAL	46.507
3	DECOY 78	42.683
…	…	…
712	DECOY 23	19.608
…	…	…
999	DECOY 16	4.805
1000	DECOY 14	0.966