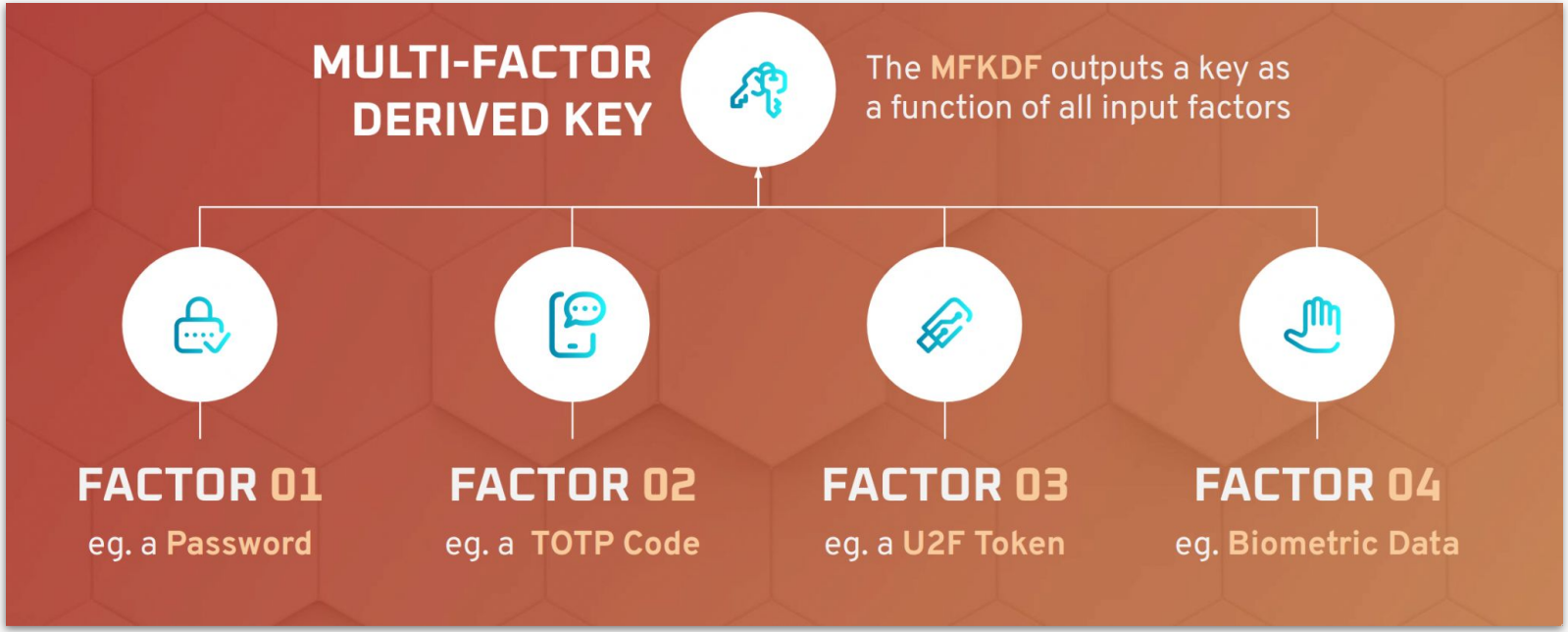
MULTIPLE FACTORS

KNOCKED DOWN FLAT

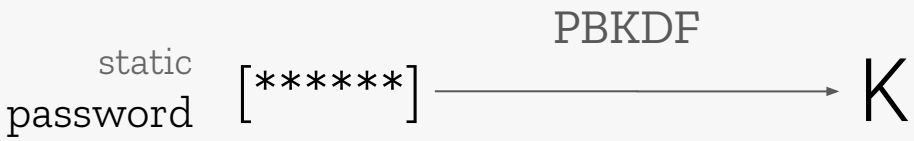
Matteo Scarlata – Matilda Backendal – Miro Haller

Photo by Johann Walter Bantz on Unsplash


usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION
Multi-Factor Key Derivation Function (MFKDF) for Fast, Flexible, Secure, & Practical Key Management
Vivek Nair and Dawn Song, University of California, Berkeley
https://www.usenix.org/conference/usenixsecurity23/presentation/nair-mfkdf


MULTI-FACTOR
DERIVED KEY
The MFKDF outputs a key as
a function of all input factors
FACTOR 01
eg. a Password
FACTOR 02
eg. a TOTP Code
FACTOR 03
eg. a U2F Token
FACTOR 04
eg. Biometric Data

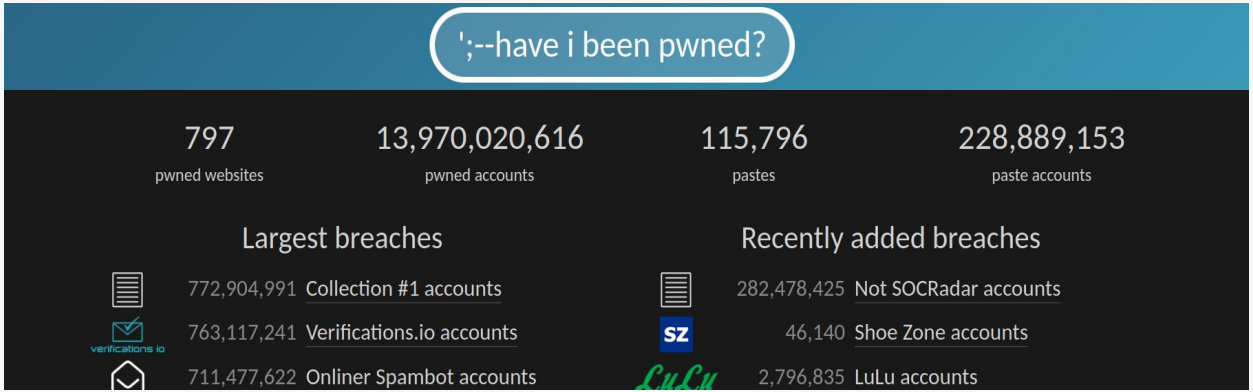
Password-Based Key Derivation



Static Passwords

SecLists/Passwords/Common-Credentials/10-million-password-list-top-100.txt

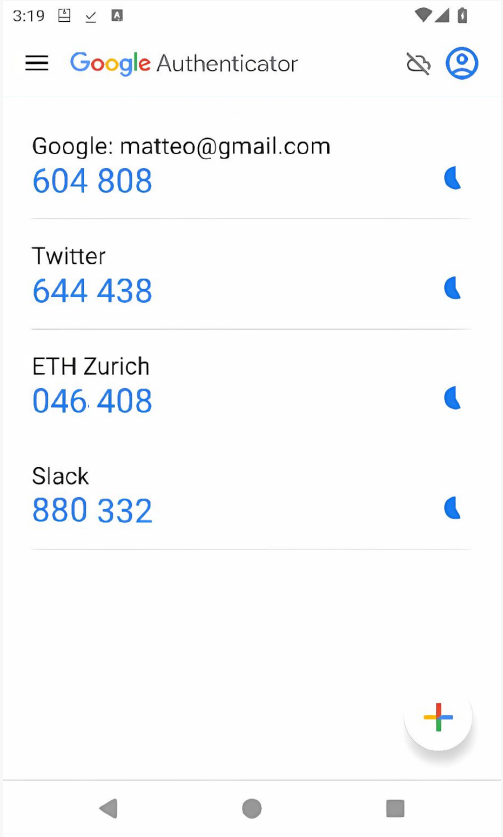
1. 123456
2. password
3. 12345678
4. qwerty
5. 123456789



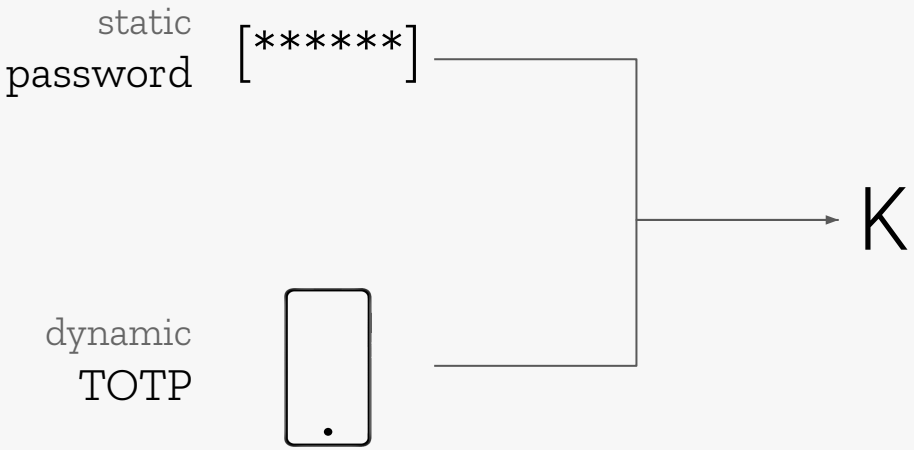
Static Passwords

From: https://www.keydemon.com

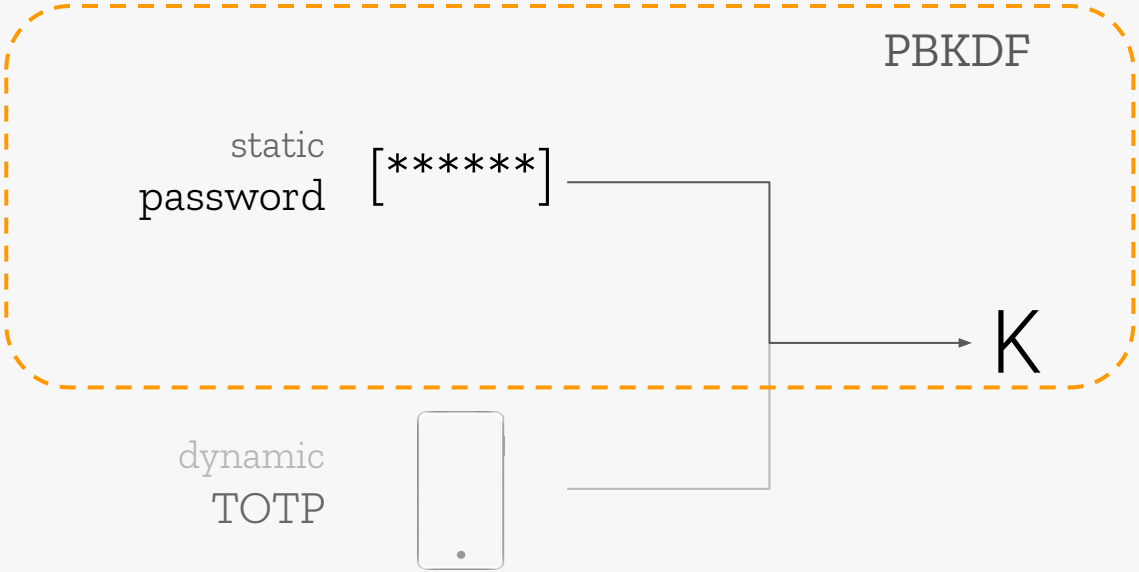
Time-Based One-Time Passwords



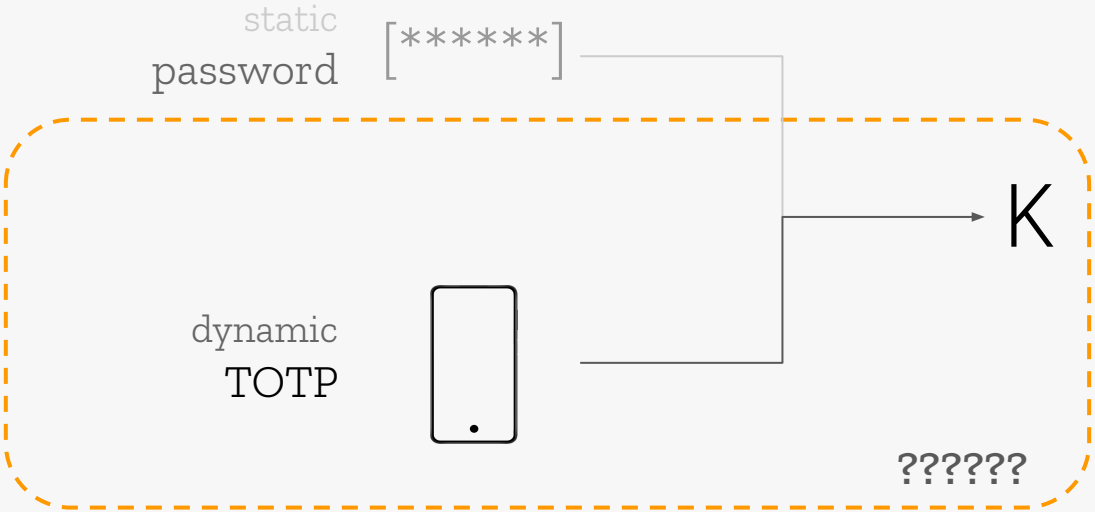
MFKDF



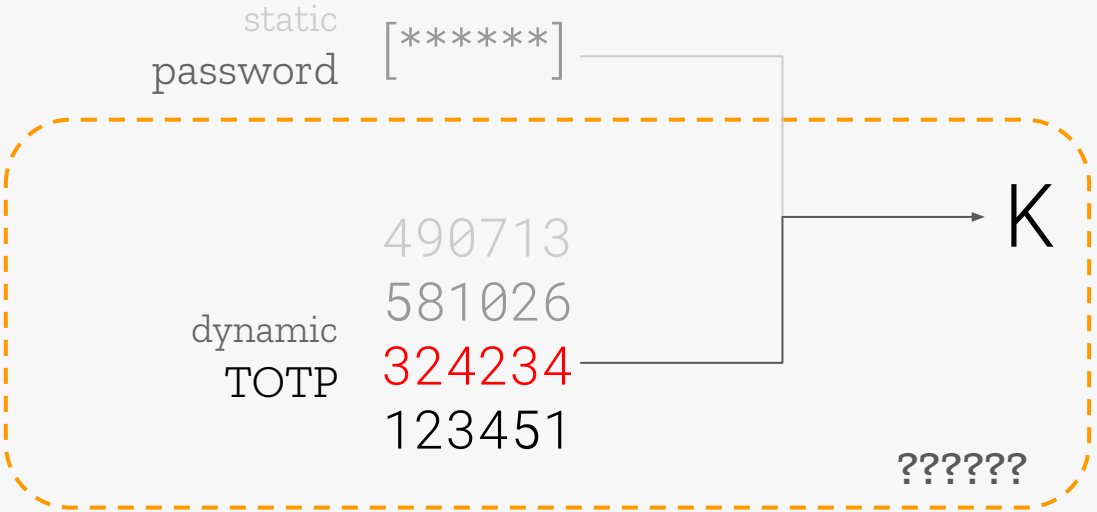
MFKDF



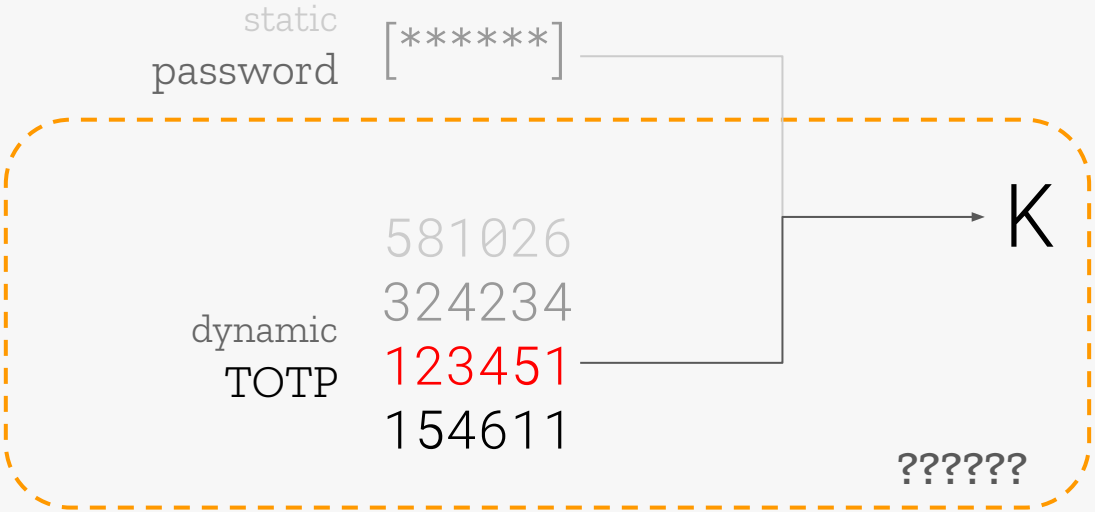
MFKDF



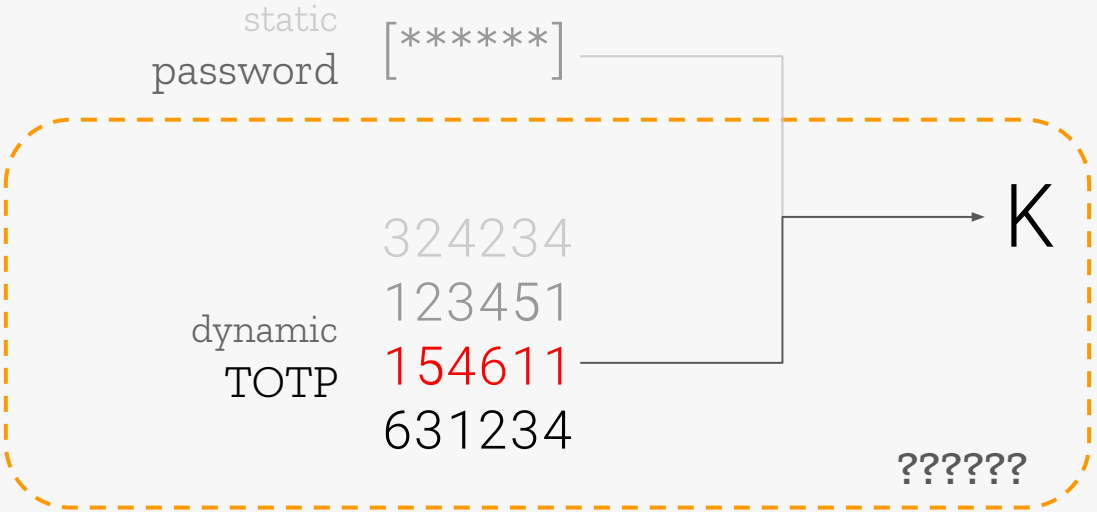
MFKDF - One Time Codes



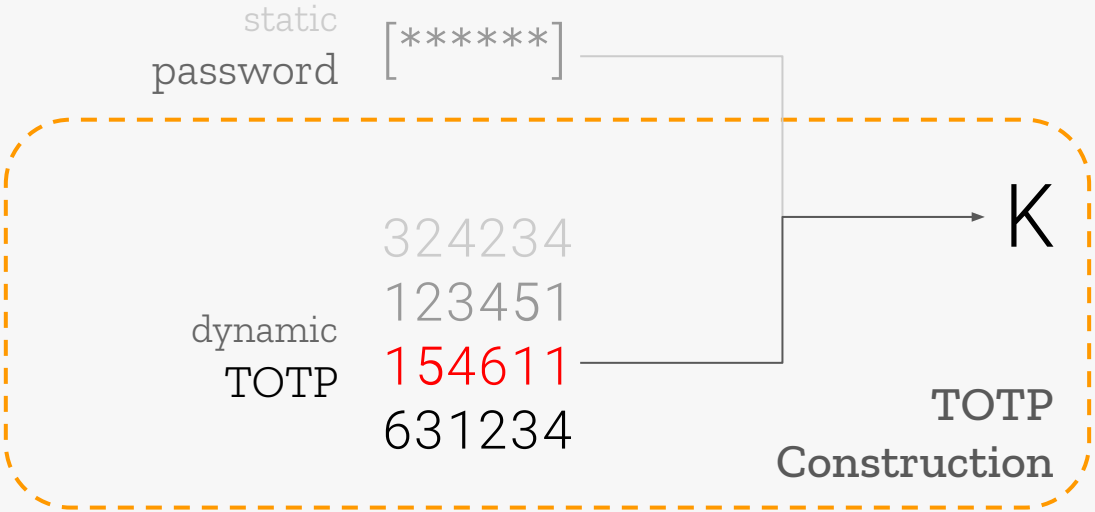
MFKDF - One Time Codes



MFKDF - One Time Codes

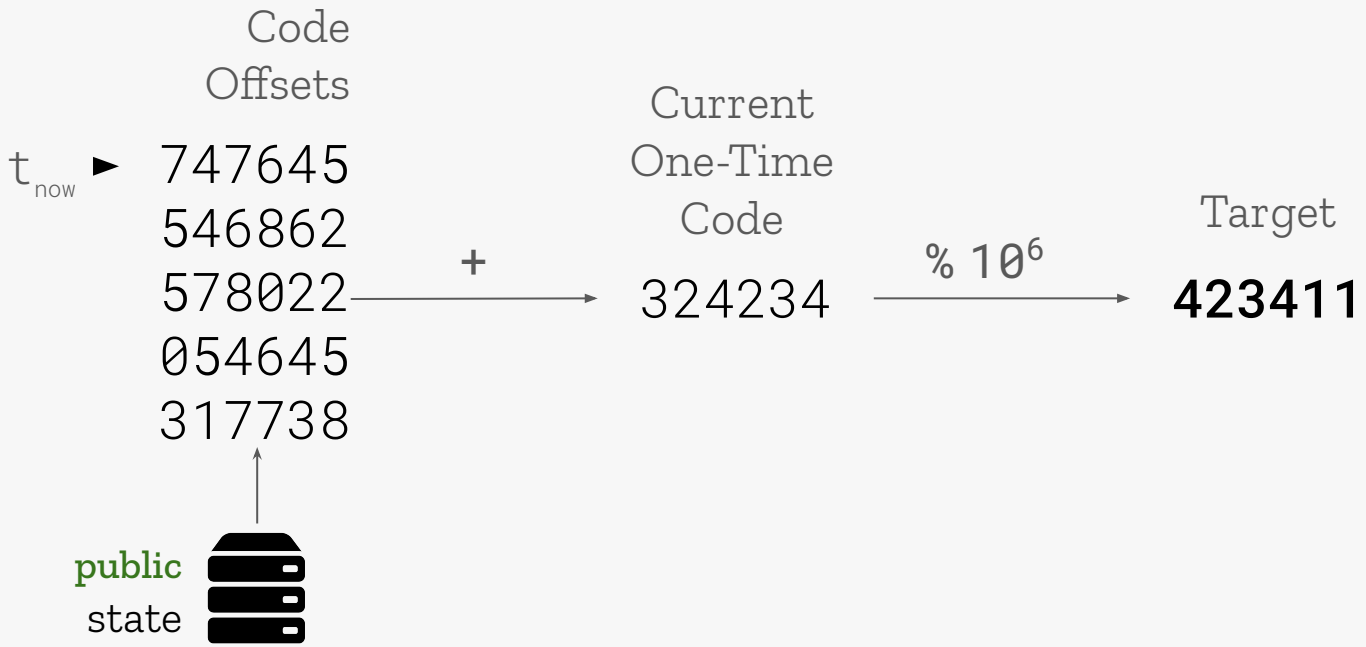


MFKDF - One Time Codes

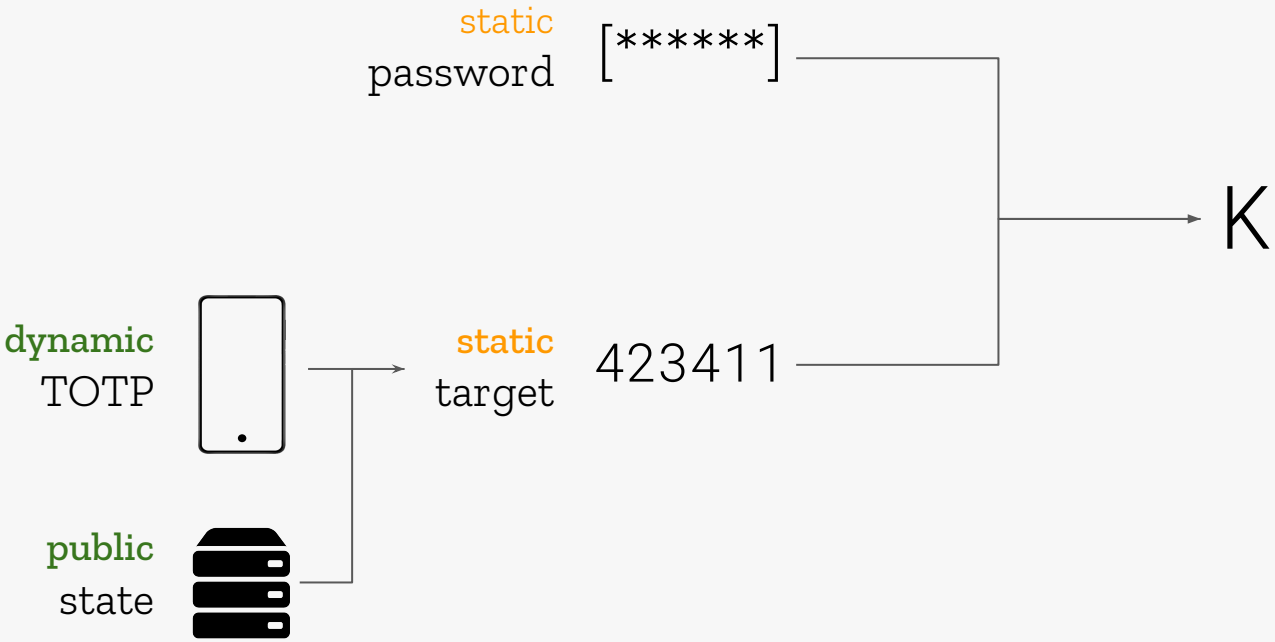


TOTP Construction

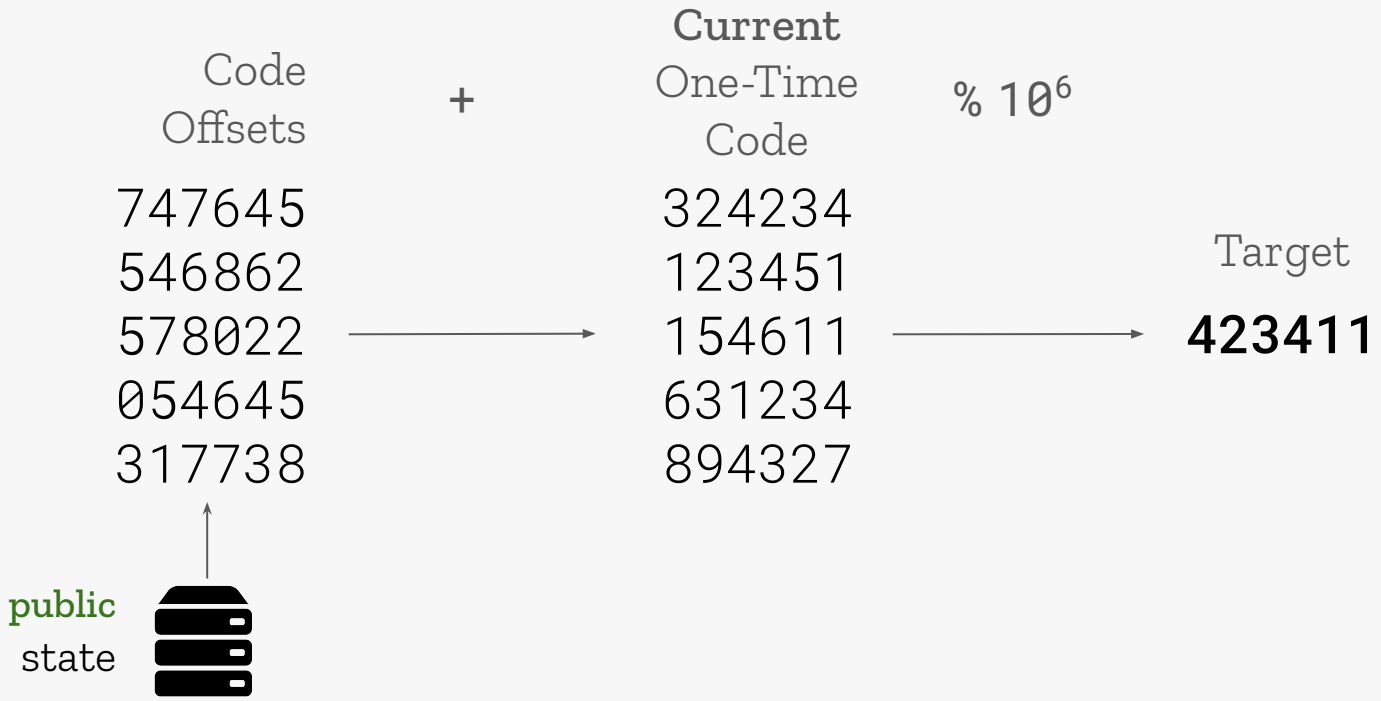
TOTP Construction



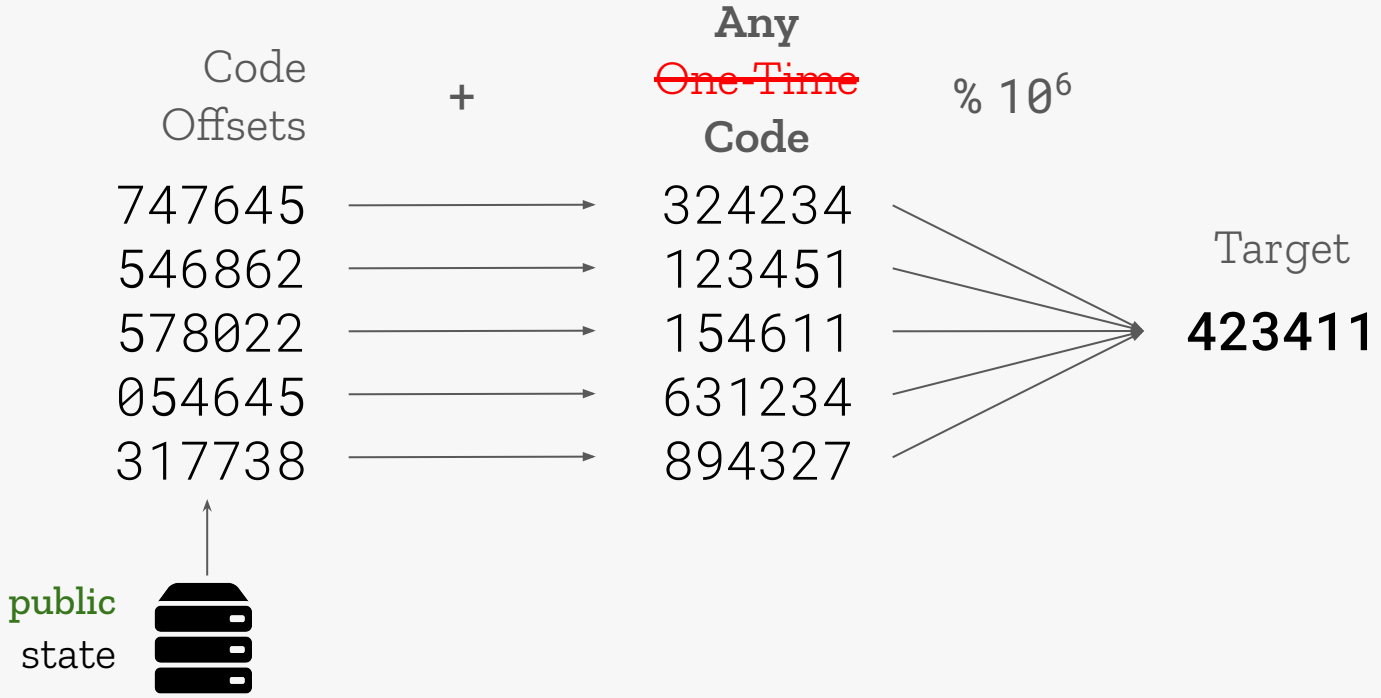
MFKDF - The Problem



Dynamic Factor Attack



Dynamic Factor Attack

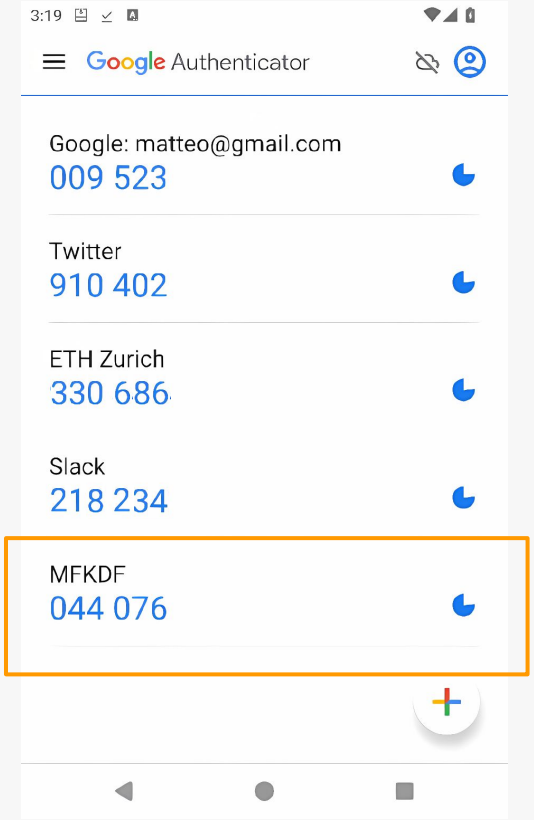


1. Public State

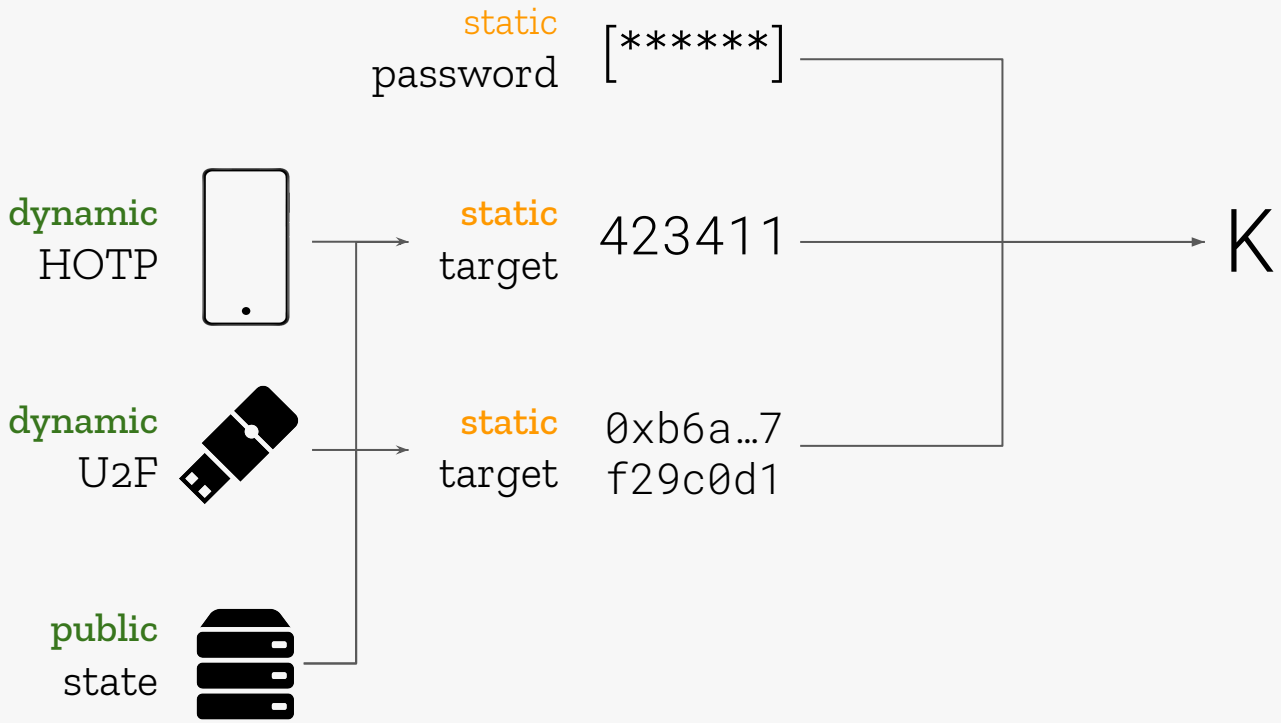
```
> curl 'https://demo.mfkdf.com/api/
                    policy?email=vivek@nair.me'
```

```
[...]
"id": "totp",
"params": {
        "start": 1655522549326,
        "hash": "sha1",
        "digits": 6,
        "step": 30,
        "window": 87600,
        "pad": "A04Ipqw2OIyDhwTzyHGSQSD3gKZYTXaL+rH8e0uBrU8=",
        "offsets":  "AAamyAAJymcADp3IAAoRGgAOIPkADfHTAAgSFAAMeAAC
                     OUAASlhAKrd0ADQz9AAJrFgAJhpIACD1tAAnEQgAGPLg
                     AC+yYAAi/iAACLtoABauAdLmQAG88kADGeEAAOa0gAGl
                     9QADhU9AAKbDgAI/KYADPkQAAnHQQACELwAC9/NAAIlt
                     gAO [...]
```

2. Any ~~One-Time~~ Code



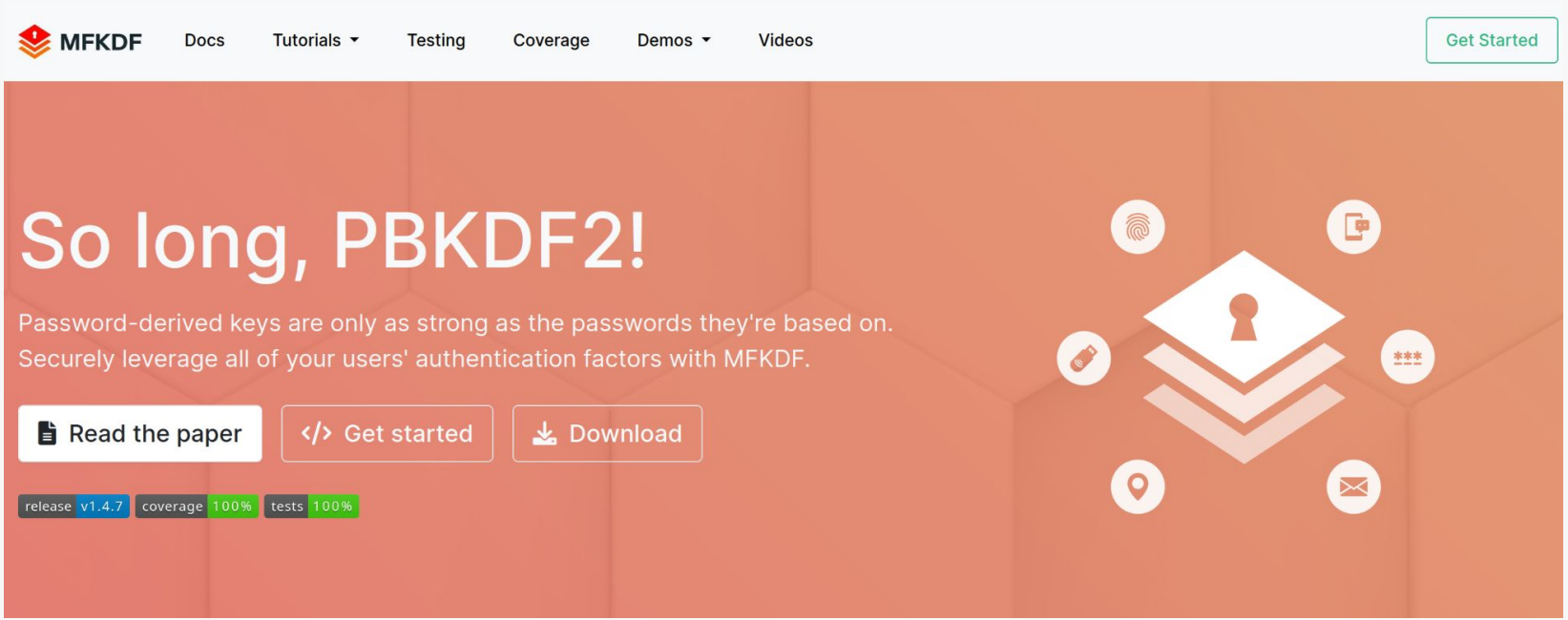
Dynamic Factor Attack



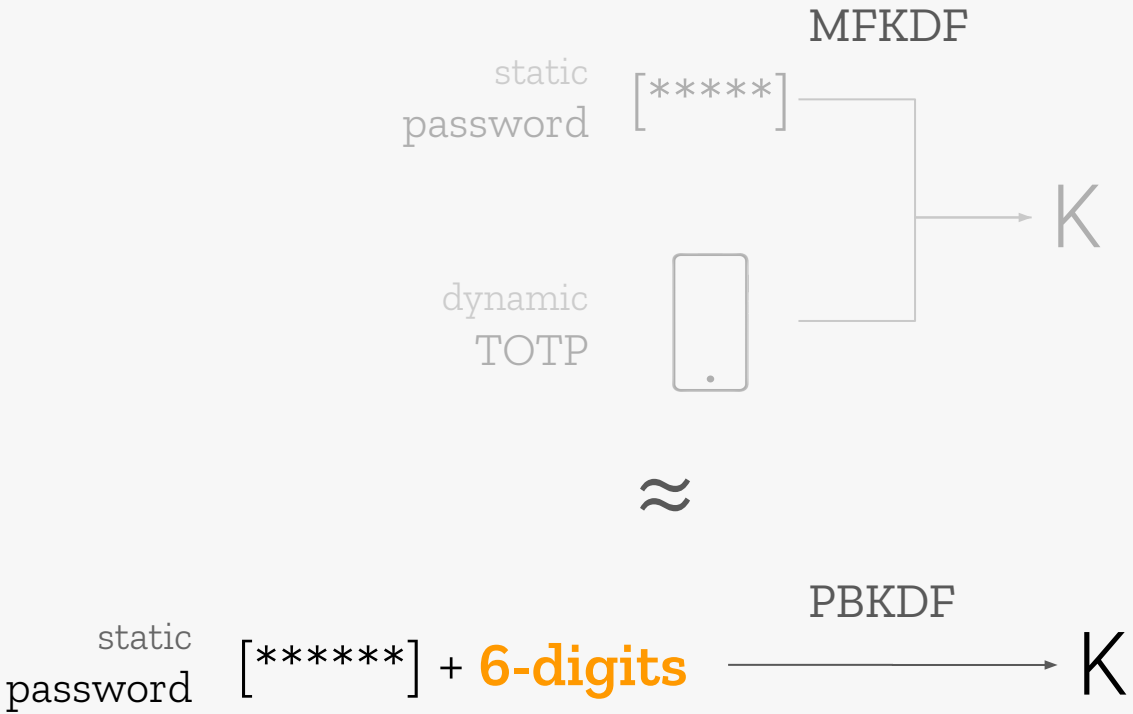
Static ~~One-Time~~ Codes

From: https://www.keydemon.com

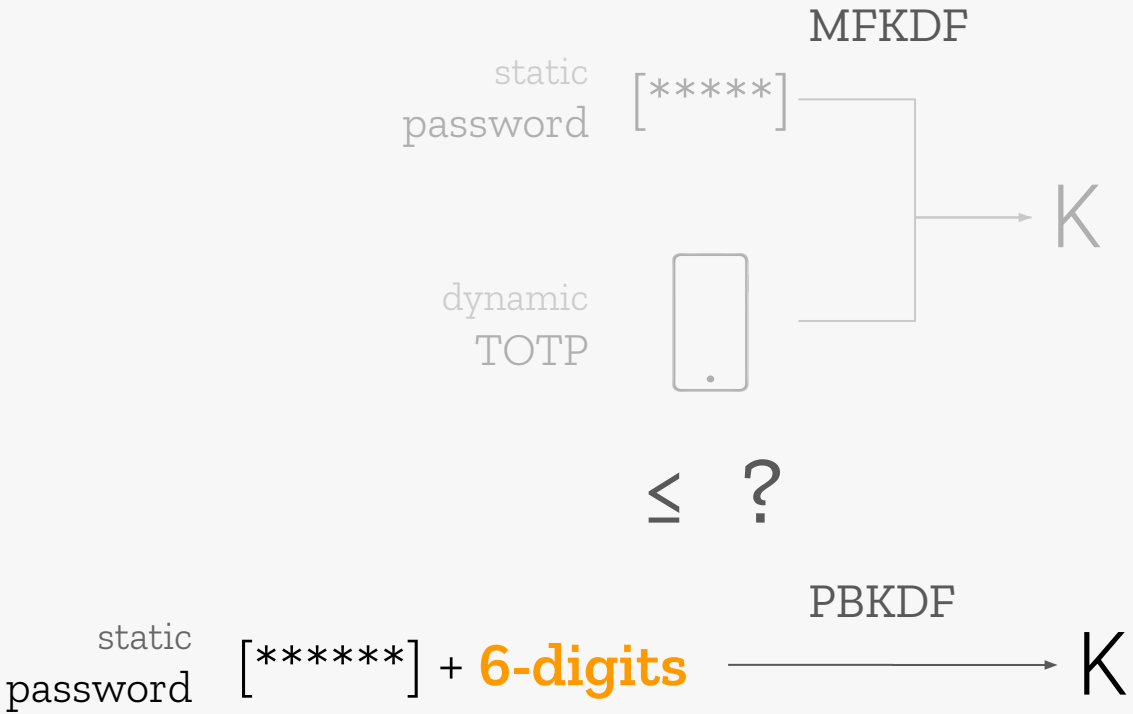
MFKDF vs PBKDF



MFKDF vs PBKDF



MFKDF vs PBKDF



TOTP Construction

"Information-Theoretical Security"

TOTP Bias Attack

One-Time Codes

324234
123451
154611
631234
894327

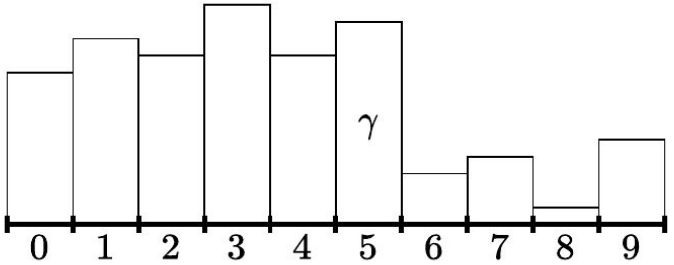


Figure 2: Bias of 1-digit TOTP witnesses for $n = 10$ bins.

"Information-Theoretical Security"

TOTP Bias Attack

Code
Offsets

747645
546862
578022
054645
317738

public
state

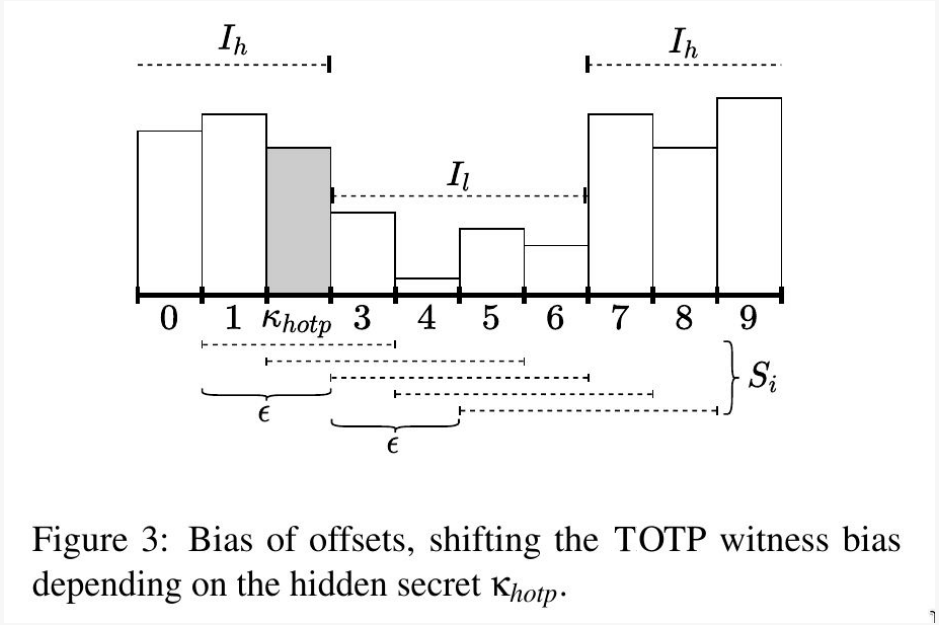


Figure 3: Bias of offsets, shifting the TOTP witness bias depending on the hidden secret κ_{hotp}.

TOTP Bias Attack

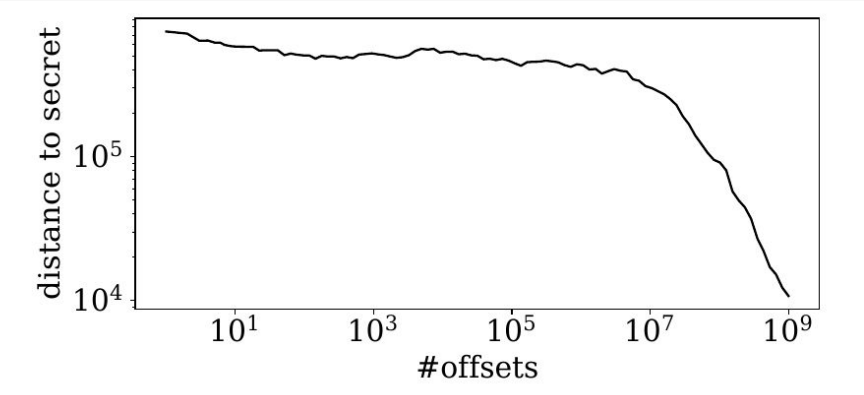
Code Offsets

747645
546862
578022
054645
317738

public state

+

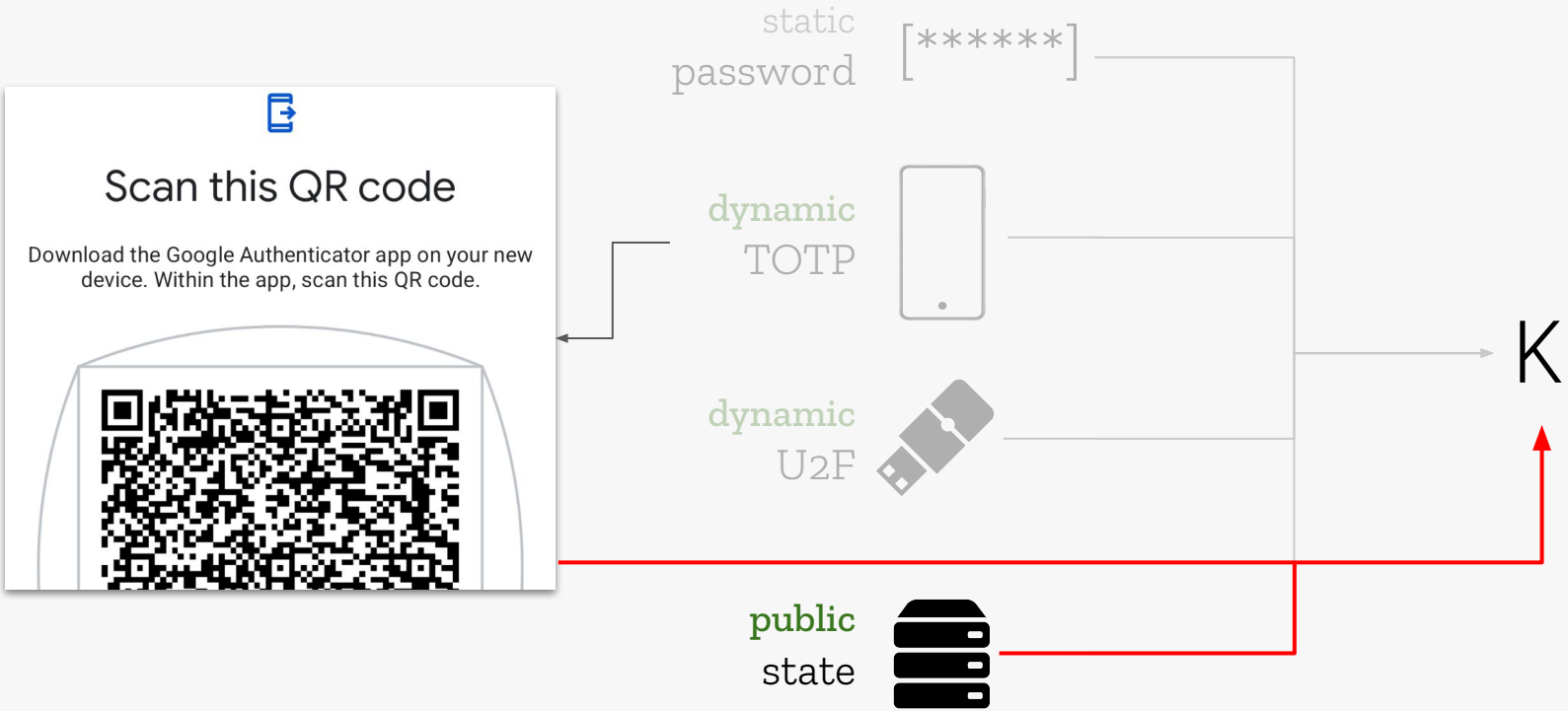
NO Code



Target

→ **423411**

TOTP Compromise Attack...



… and more!

ia.cr/2024/935

		Recover Final Key	Recover Src. Key Material	Break *'Safety'*	Break *'Entropy'*	Break Exp. Security	
Dynamic Factor (3.1)	fund	✗	✓	✗	✓	✓[c]	cannot fix
OOB Overwriting (3.2.1)	int	✗	✓	✗	✓	✓[c]	partial fix
Parameter Tampering (3.2.2)	int	✓	✗	✗	✓	✗	
Share Dilution (3.2.3)	int, impl	✓[a]	✗	✓	✓	✗	
HOTP Compromise (3.3.1)	spec, impl	✓	–	✗	✓	✓	fixable
HOTP Bias (3.3.2)	spec	✗	✓	✗	✓	✓[c]	
Share Recovery (3.3.3)	spec	✗	✓	✓	✓	✓[c]	
Share Format (3.3.4)	spec	✓[a]	✓	✗	✓	✓	
	Type			Impact			Mitigations