



MULTIPLE FACTORS

Photo by [Johann Walter](#)
[Bantz](#) on [Unsplash](#)

KNOCKED DOWN FLAT

Matteo Scarlata – Matilda Backendal – Miro Haller



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

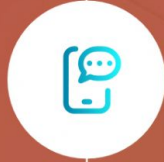


The **MFKDF** outputs a key as
a function of all input factors



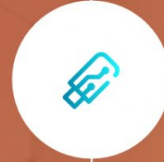
FACTOR 01

eg. a **Password**



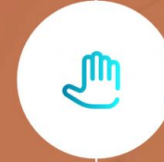
FACTOR 02

eg. a **TOTP Code**



FACTOR 03

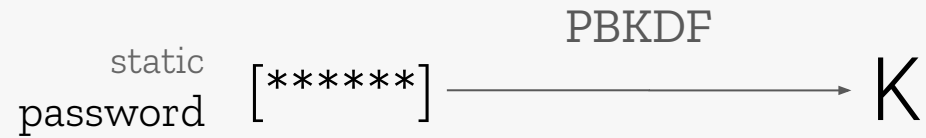
eg. a **U2F Token**



FACTOR 04

eg. **Biometric Data**

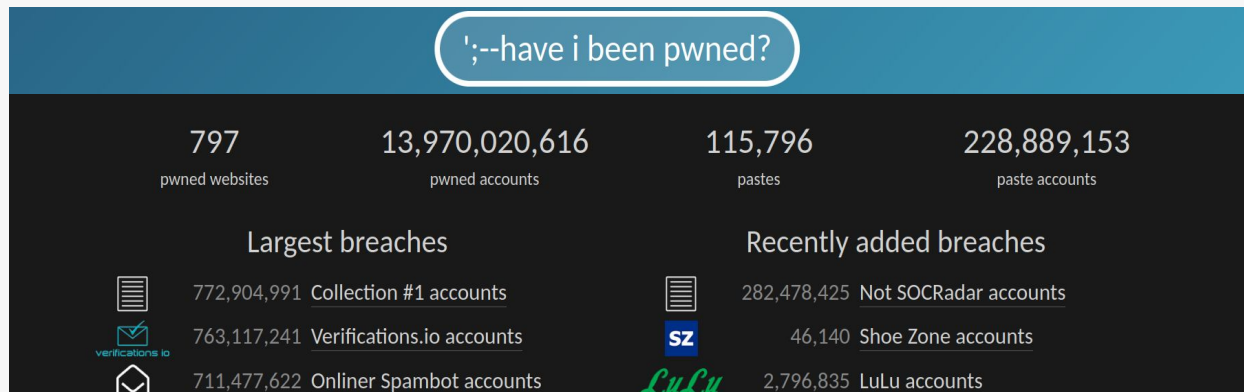
Password-Based Key Derivation



Static Passwords

[SecLists/Passwords/Common-Credentials/10-million-password-list-top-100.txt](#)

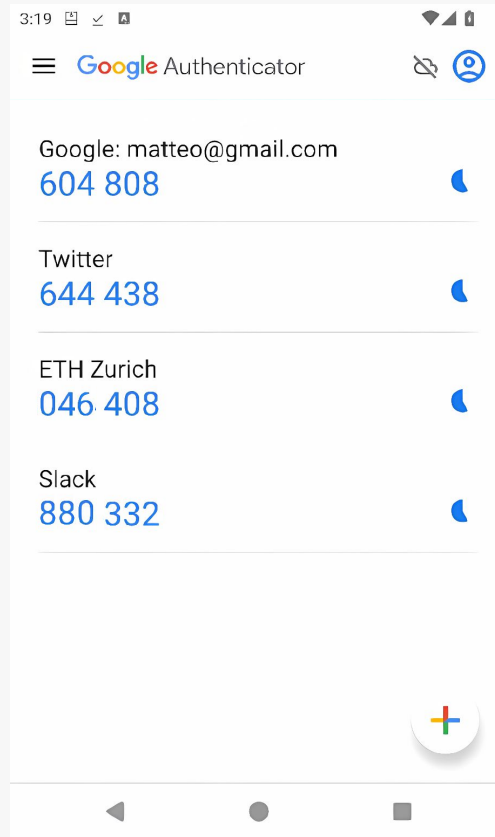
1. 123456
2. password
3. 12345678
4. qwerty
5. 123456789



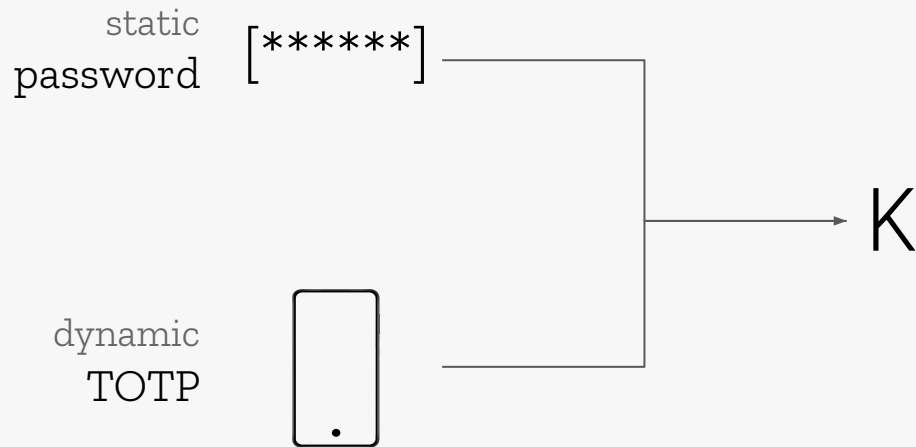
Static Passwords



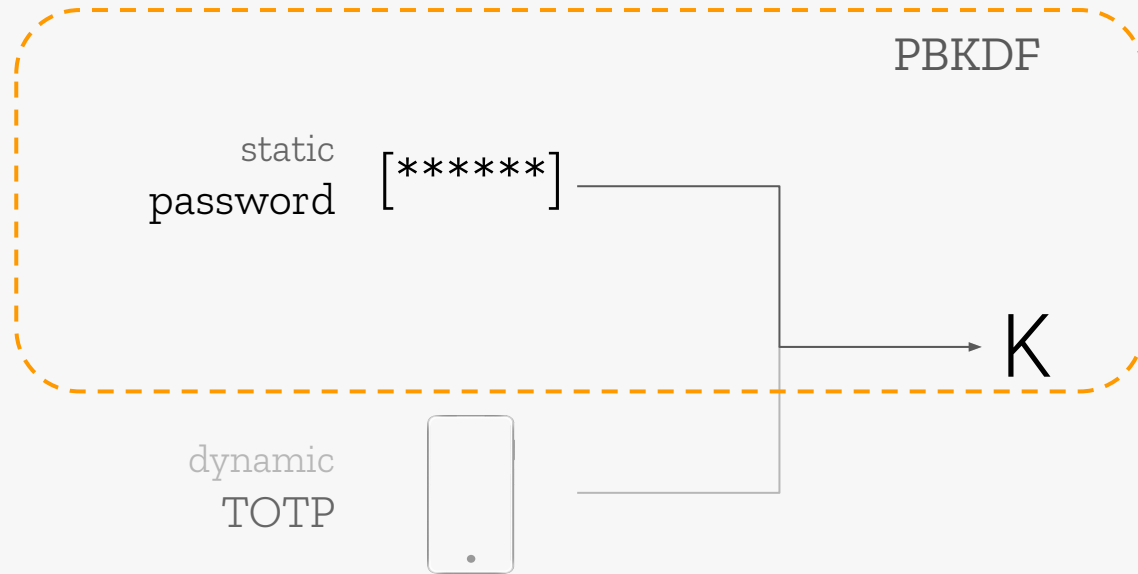
Time-Based One-Time Passwords



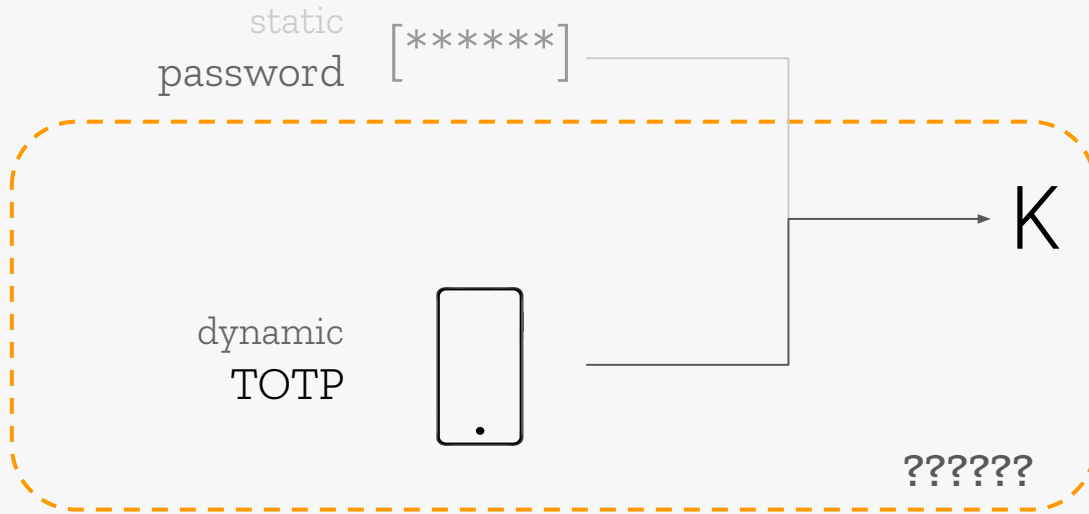
MFKDF



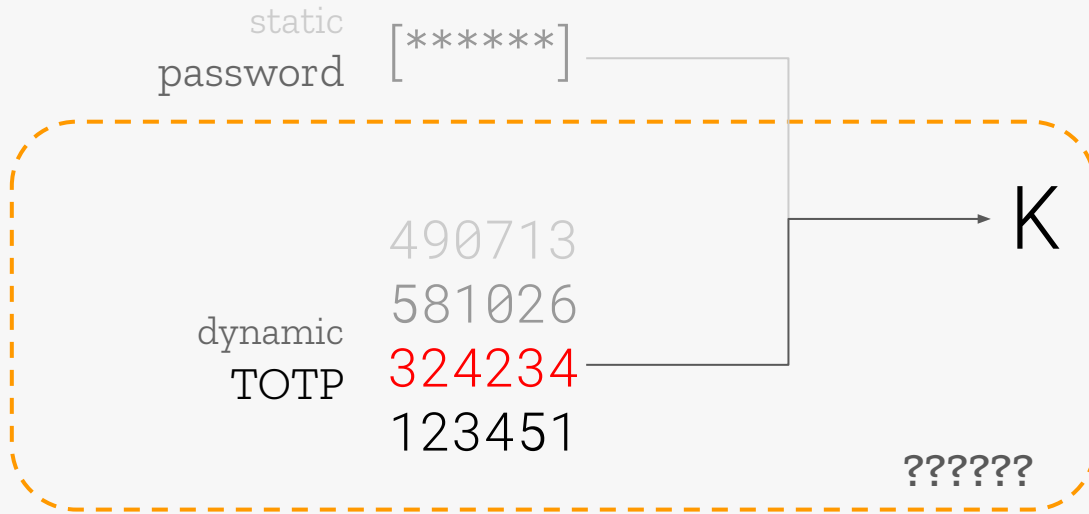
MFKDF



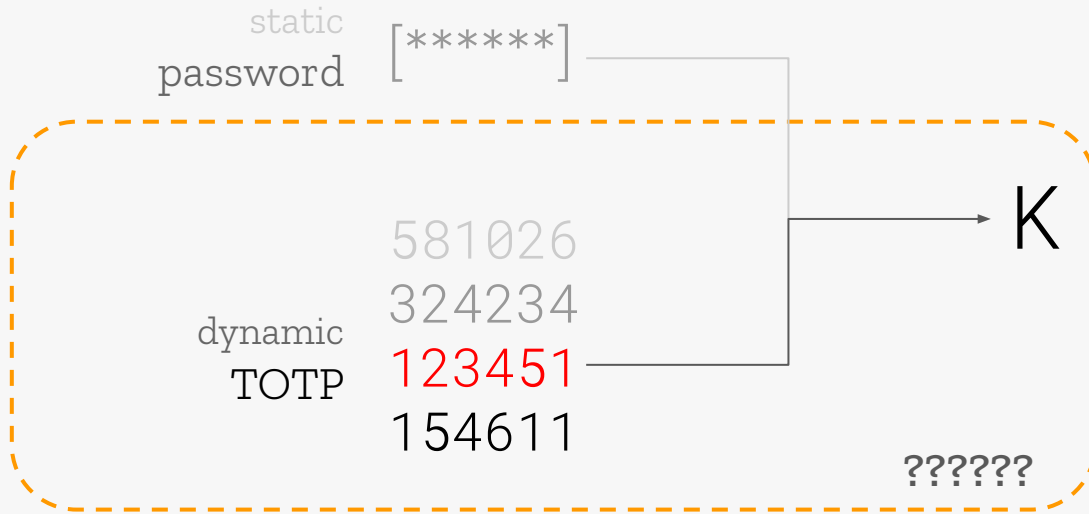
MFKDF



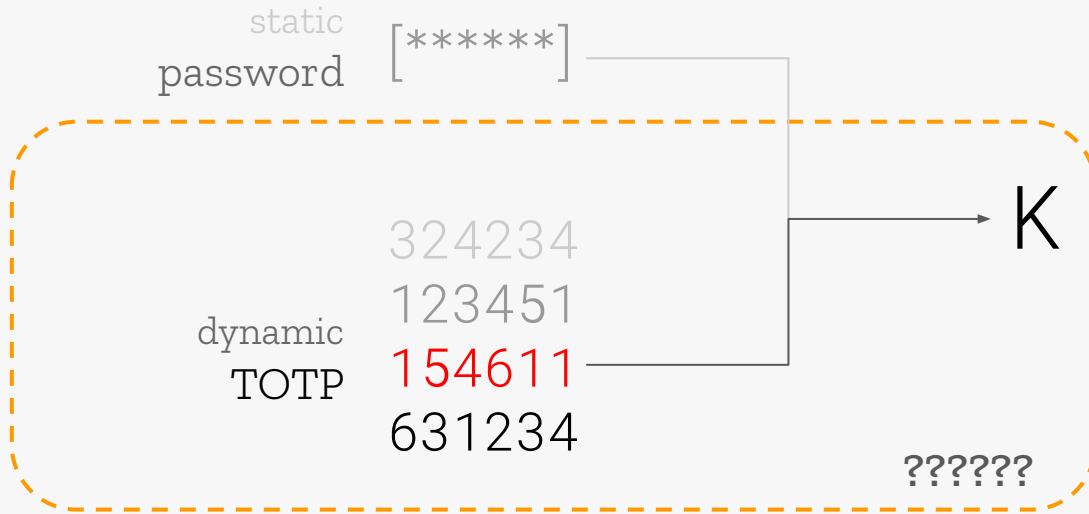
MFKDF - One Time Codes



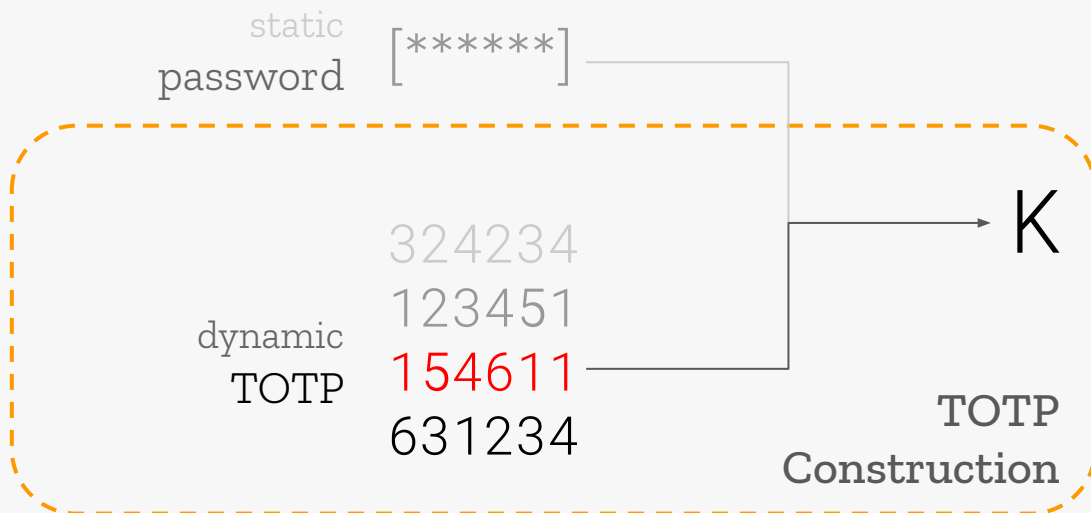
MFKDF - One Time Codes



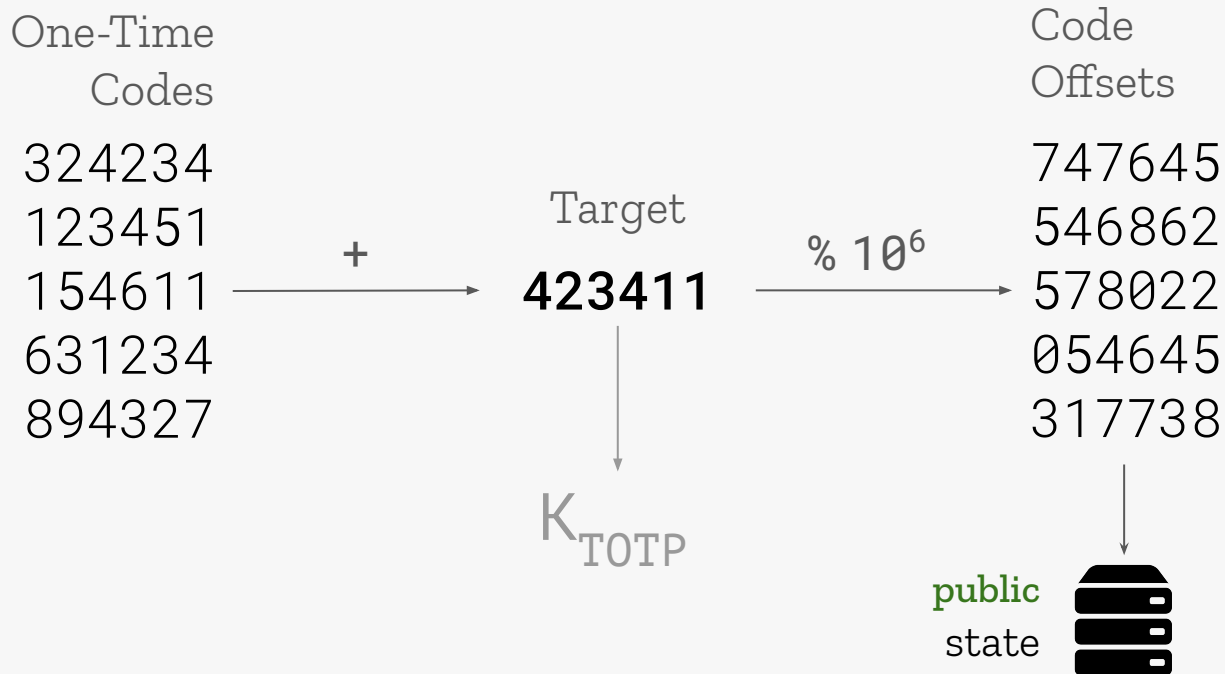
MFKDF - One Time Codes



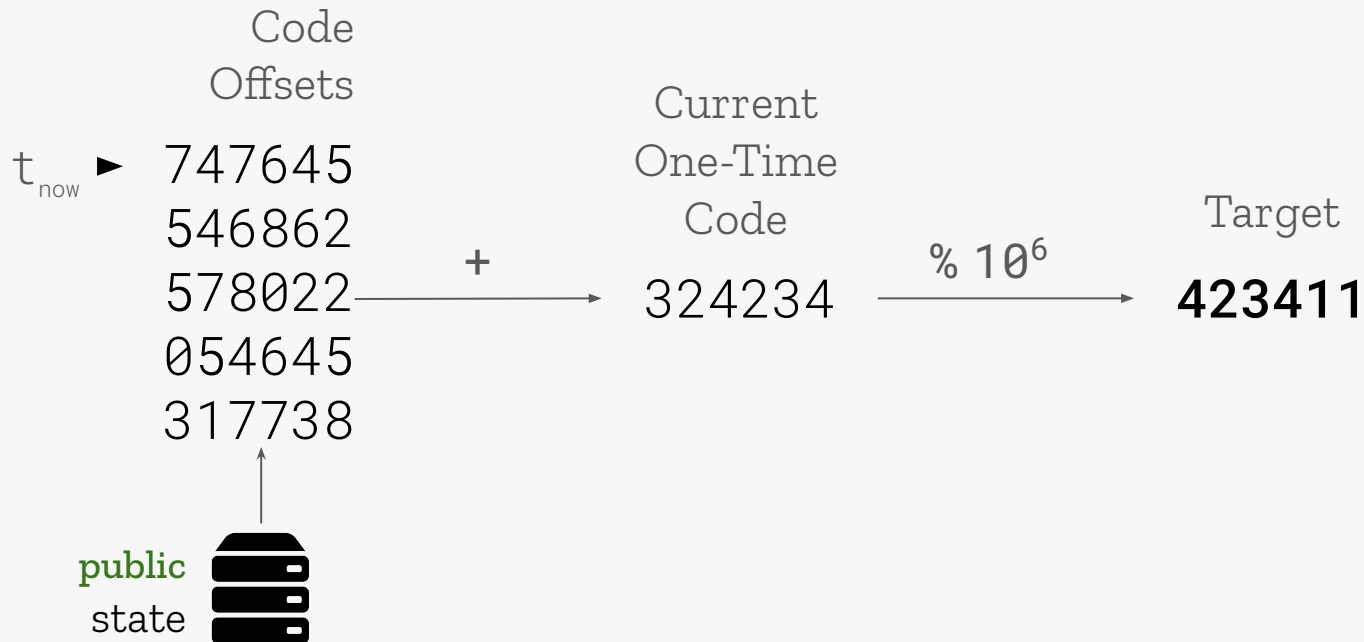
MFKDF - One Time Codes



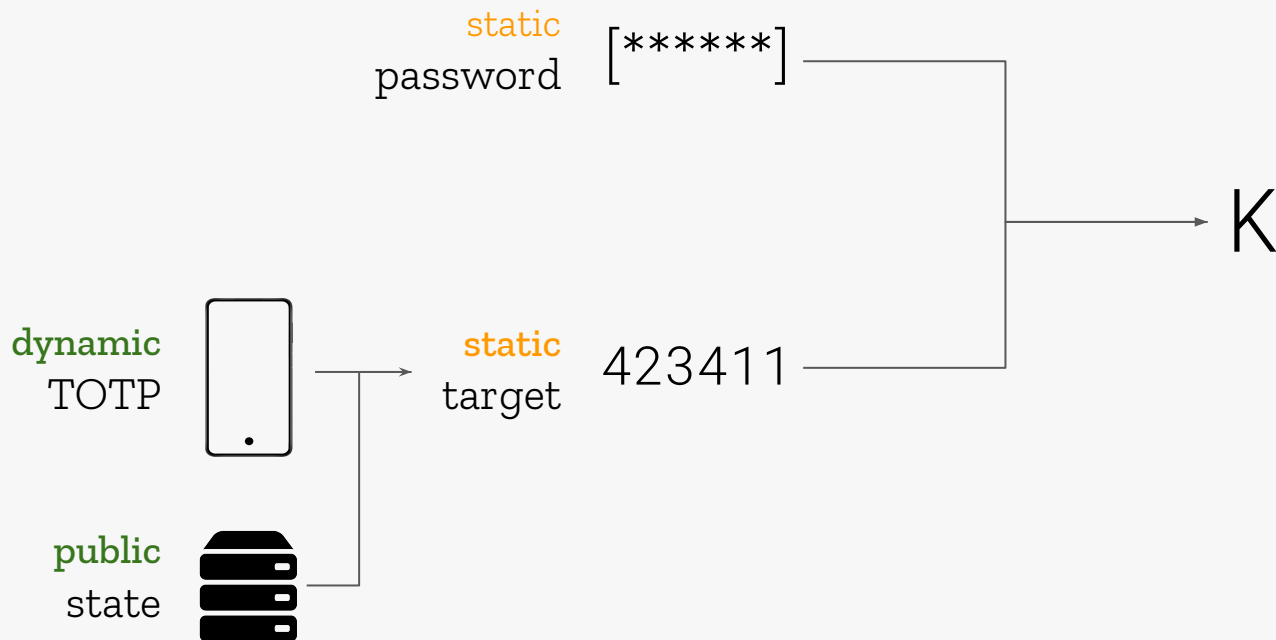
TOTP Construction



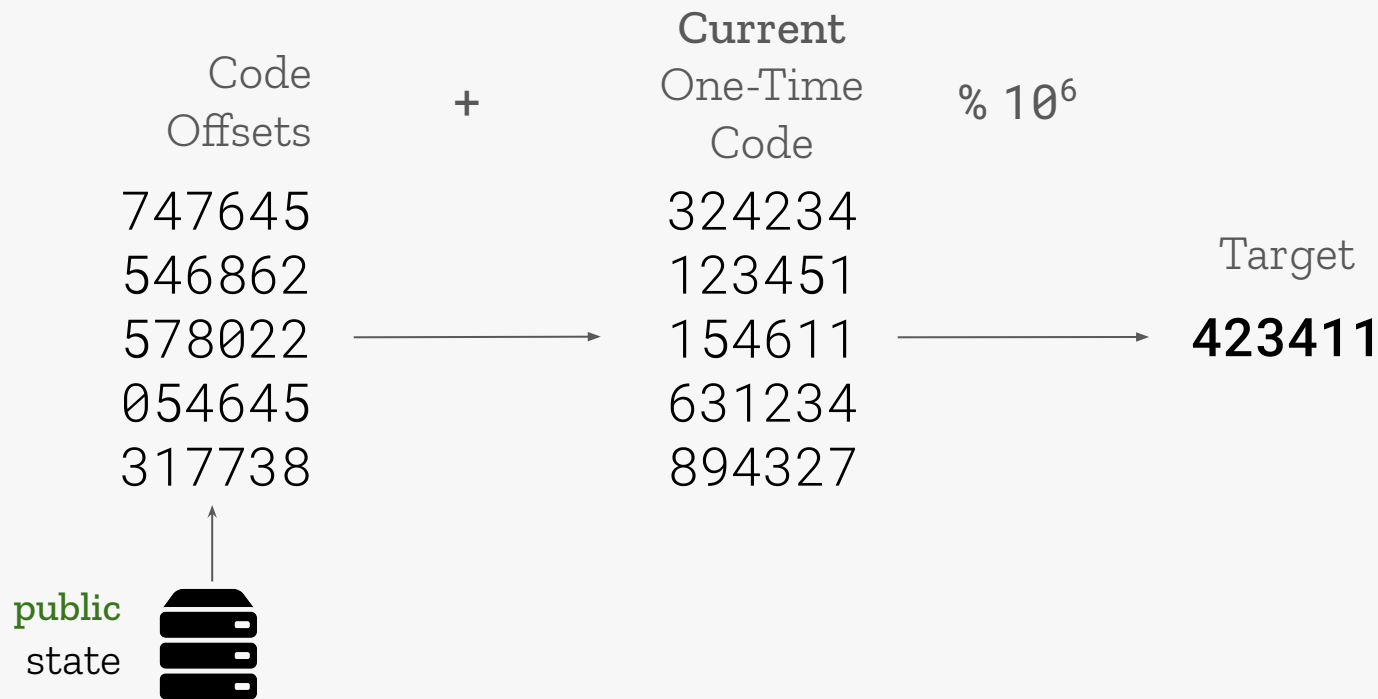
TOTP Construction



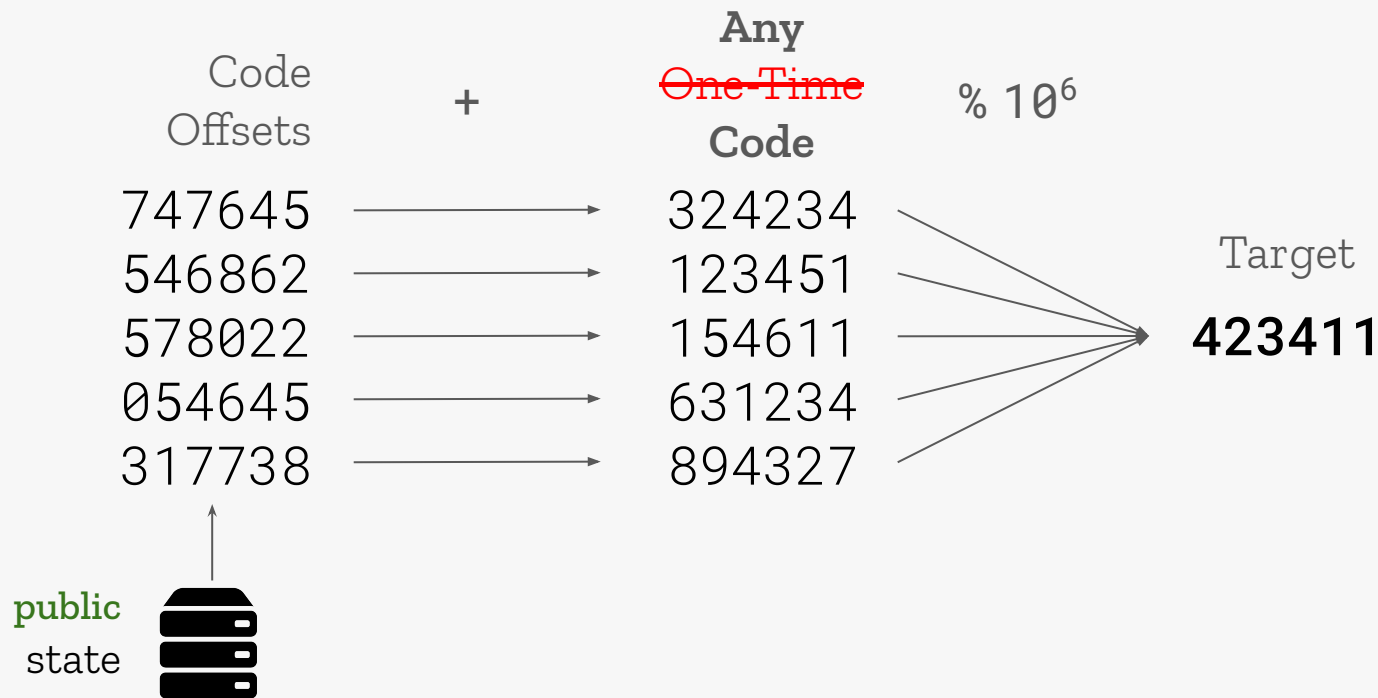
MFKDF - The Problem



Dynamic Factor Attack



Dynamic Factor Attack

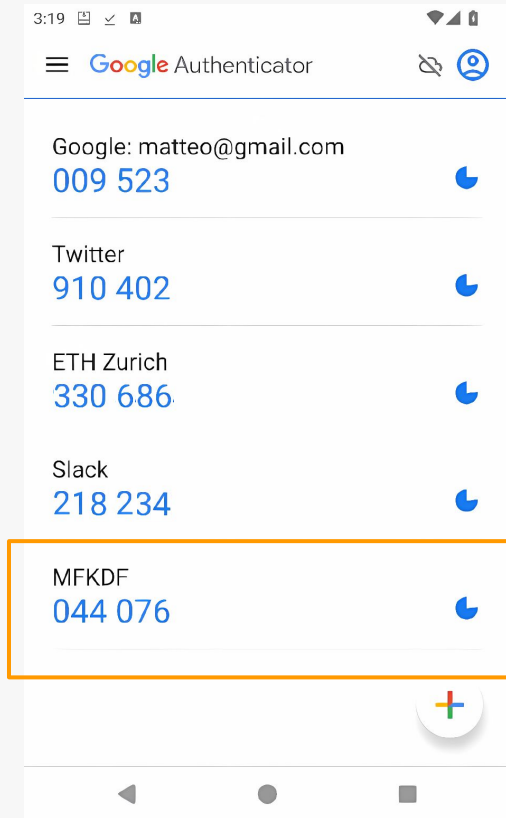


1. Public State

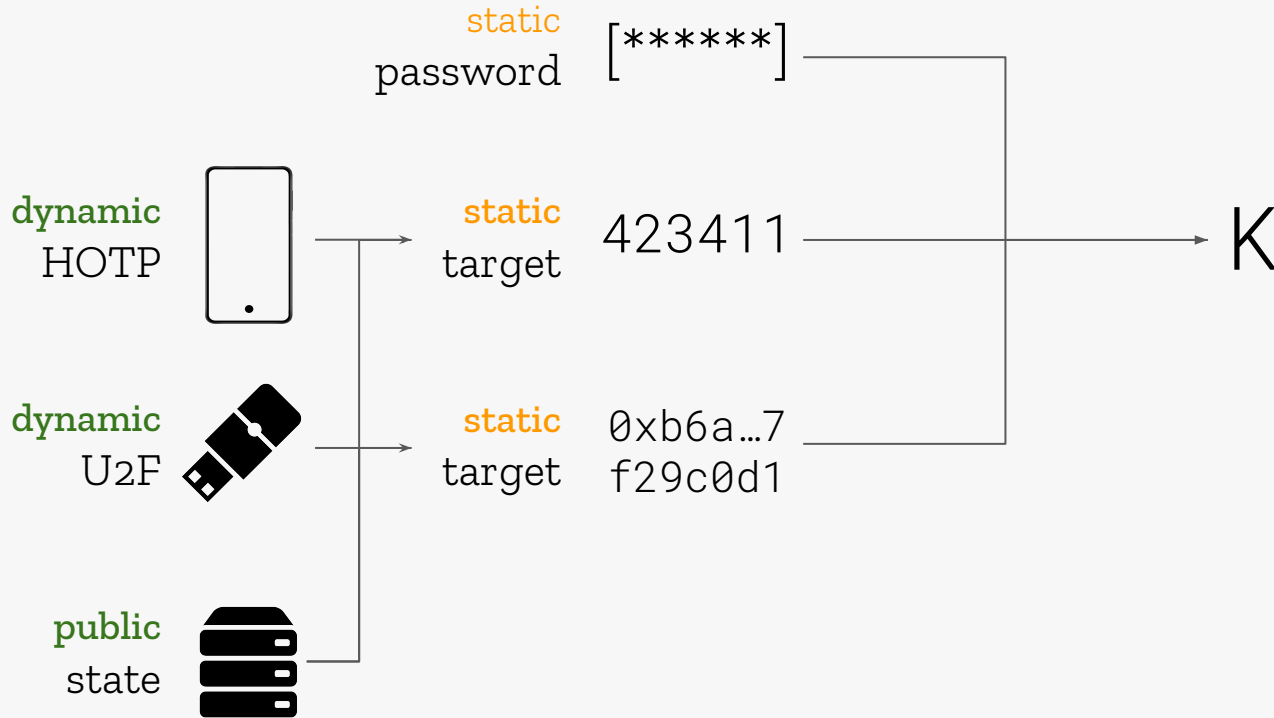
```
> curl 'https://demo.mfkdf.com/api/  
policy?email=vivek@nair.me'
```

```
1 [...]
2 "id": "totp",
3 "params": {
4     "start": 1655522549326,
5     "hash": "sha1",
6     "digits": 6,
7     "step": 30,
8     "window": 87600,
9     "pad": "A04Ipqw20IyDhwTzyHGSQSD3gKZYTxaL+rH8e0uBrU8=",
10    "offsets": "AAamyAAJymcADp3IAAoRGgA0IPkADfHTAAgSFAAMeAAC
11              OUAASlhAKrd0ADQz9AAJrFgAJhpIACD1tAAnEQgAGPLg
12              AC+yYAAi/iAACLtoABauAdLmQAG88kADGeEAA0a0gAGl
13              9QADhU9AAKbDgAI/KYADPkQAAnHQQACELwAC9/NAAIlt
14              gAO [...]
```

2. Any ~~One-Time~~ Code



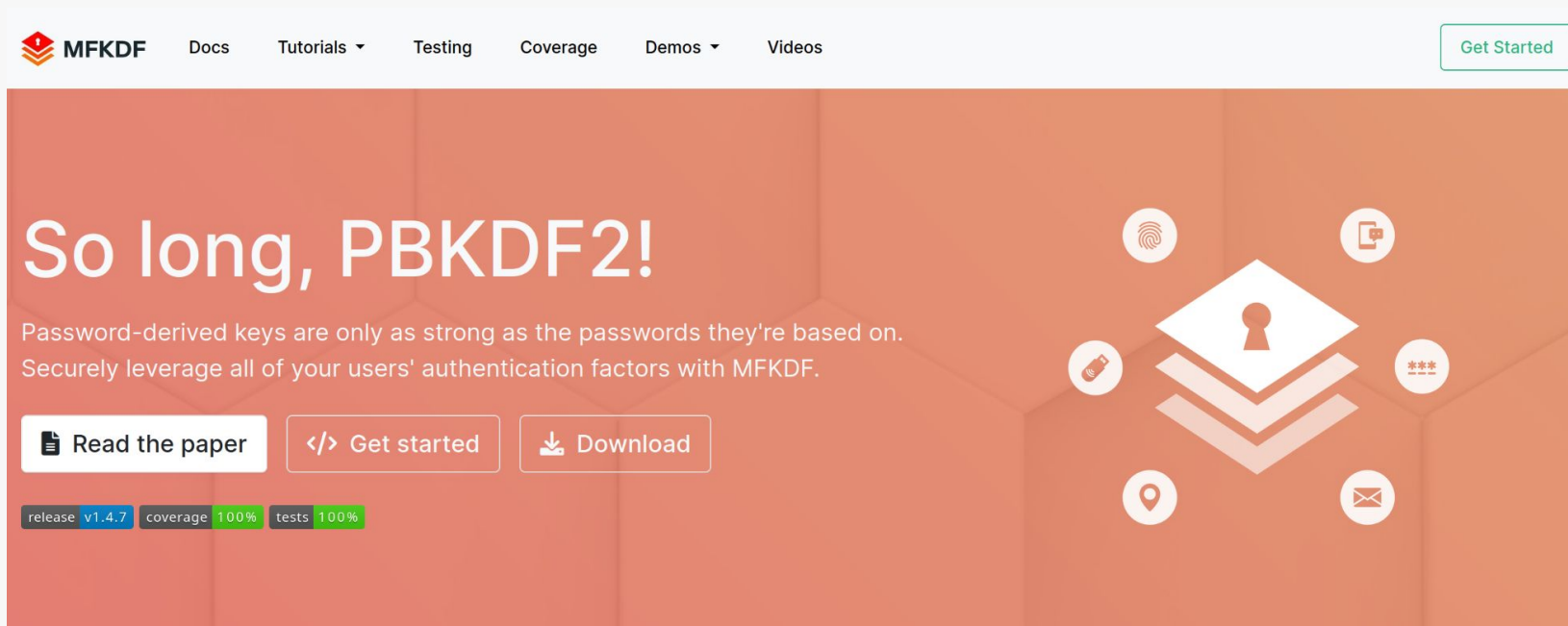
Dynamic Factor Attack



Static ~~One-Time~~ Codes



MFKDF vs PBKDF



The screenshot shows the homepage of the MFKDF project. At the top left is the MFKDF logo, followed by navigation links for Docs, Tutorials, Testing, Coverage, Demos, and Videos. A 'Get Started' button is located in the top right corner. The main content area has an orange background with a large white heading 'So long, PBKDF2!'. Below the heading is a paragraph: 'Password-derived keys are only as strong as the passwords they're based on. Securely leverage all of your users' authentication factors with MFKDF.' To the right of the text is a central graphic of a white diamond with a keyhole, surrounded by icons for various authentication factors: a fingerprint, a smartphone, a USB drive, a location pin, an envelope, and a password field with asterisks. Below the text are three buttons: 'Read the paper', 'Get started', and 'Download'. At the bottom left, there are three status boxes: 'release v1.4.7', 'coverage 100%', and 'tests 100%'.

MFKDF Docs Tutorials Testing Coverage Demos Videos [Get Started](#)

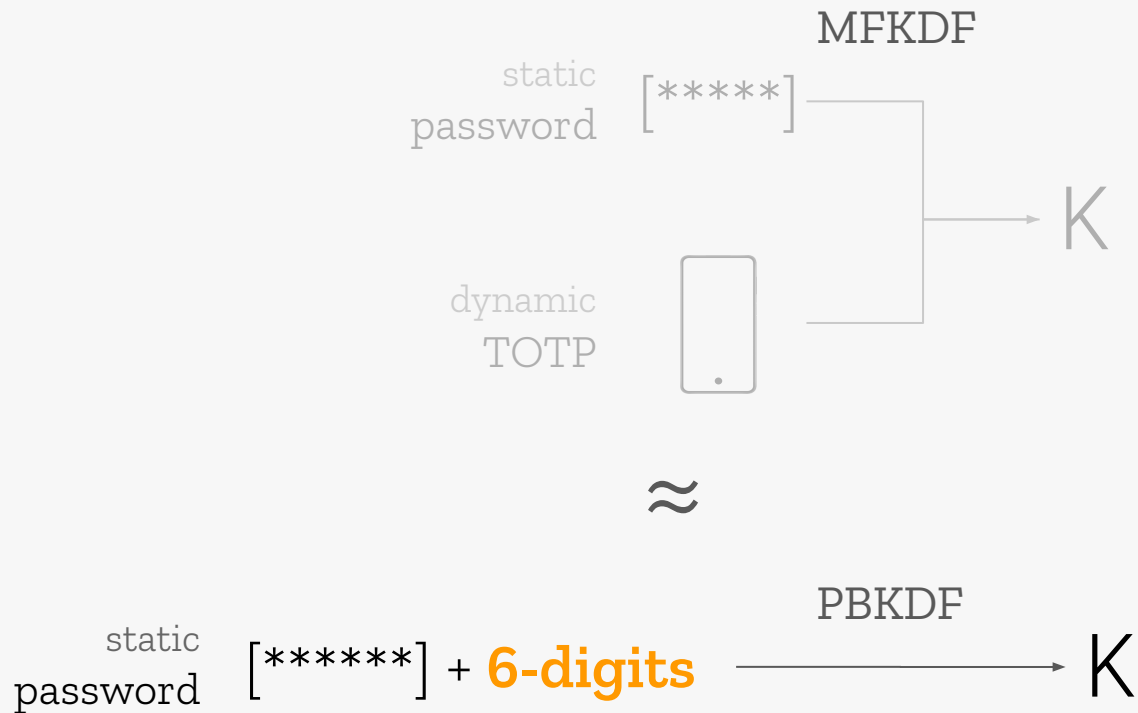
So long, PBKDF2!

Password-derived keys are only as strong as the passwords they're based on. Securely leverage all of your users' authentication factors with MFKDF.

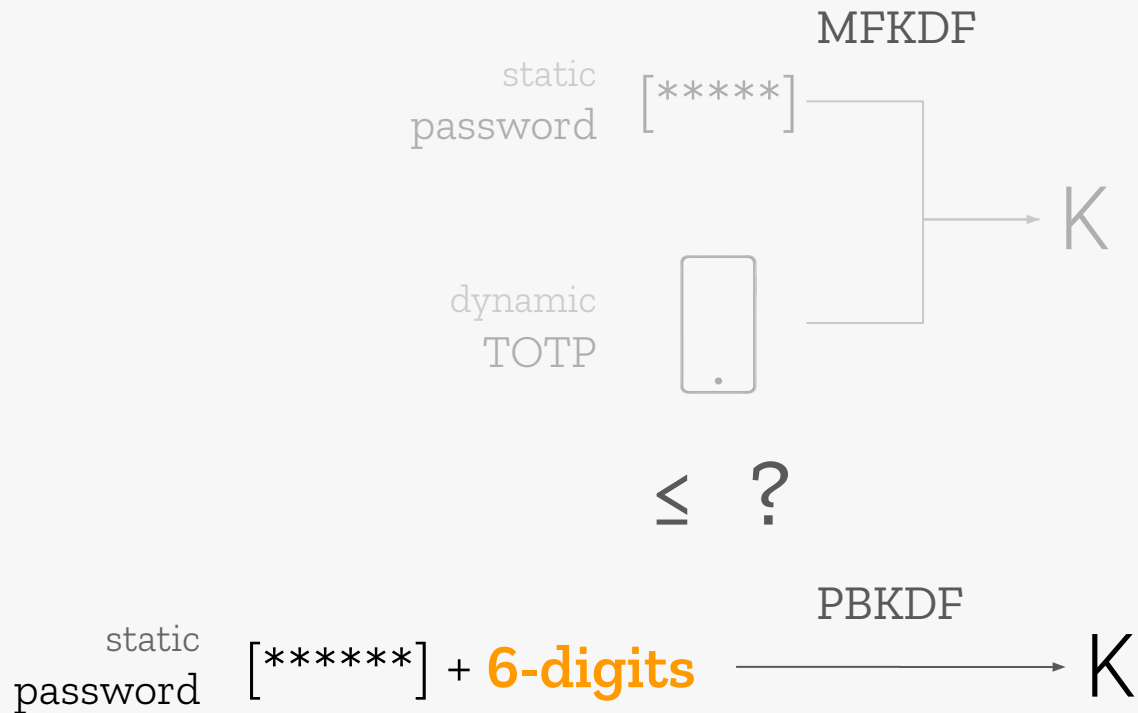
[Read the paper](#) [Get started](#) [Download](#)

release v1.4.7 coverage 100% tests 100%

MFKDF vs PBKDF



MFKDF vs PBKDF



TOTP Construction



“Information-Theoretical Security”

TOTP Bias Attack

One-Time
Codes

324234

123451

154611

631234

894327

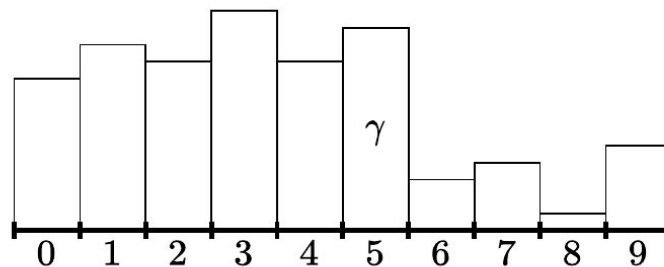


Figure 2: Bias of 1-digit TOTP witnesses for $n = 10$ bins.

“Information-Theoretical Security”

TOTP Bias Attack

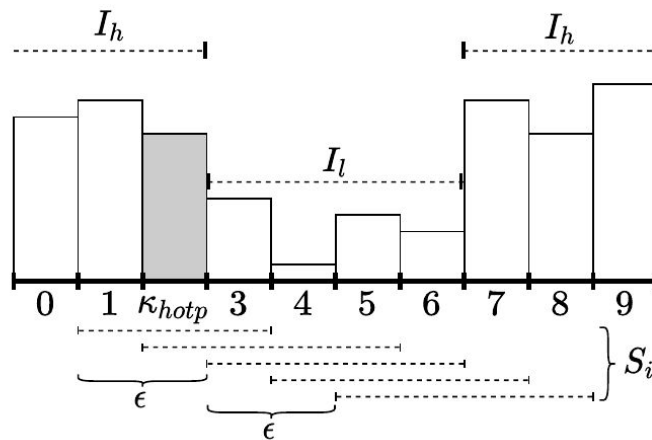
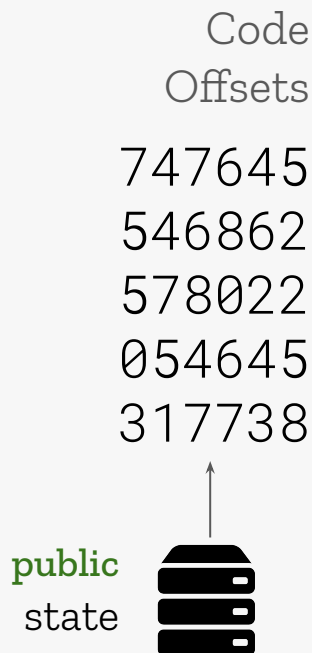
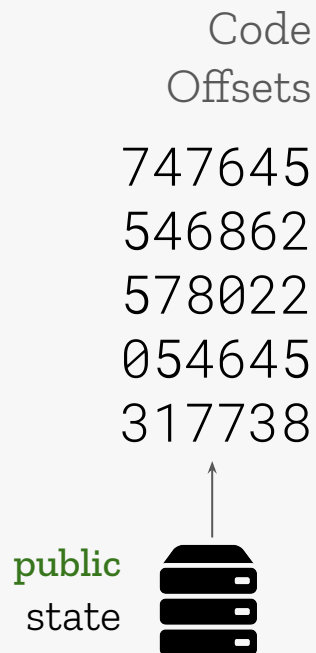
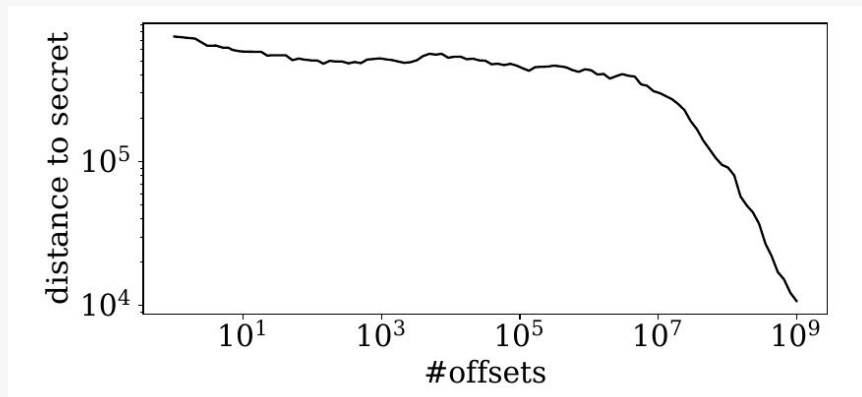


Figure 3: Bias of offsets, shifting the TOTP witness bias depending on the hidden secret κ_{hotp} .

TOTP Bias Attack

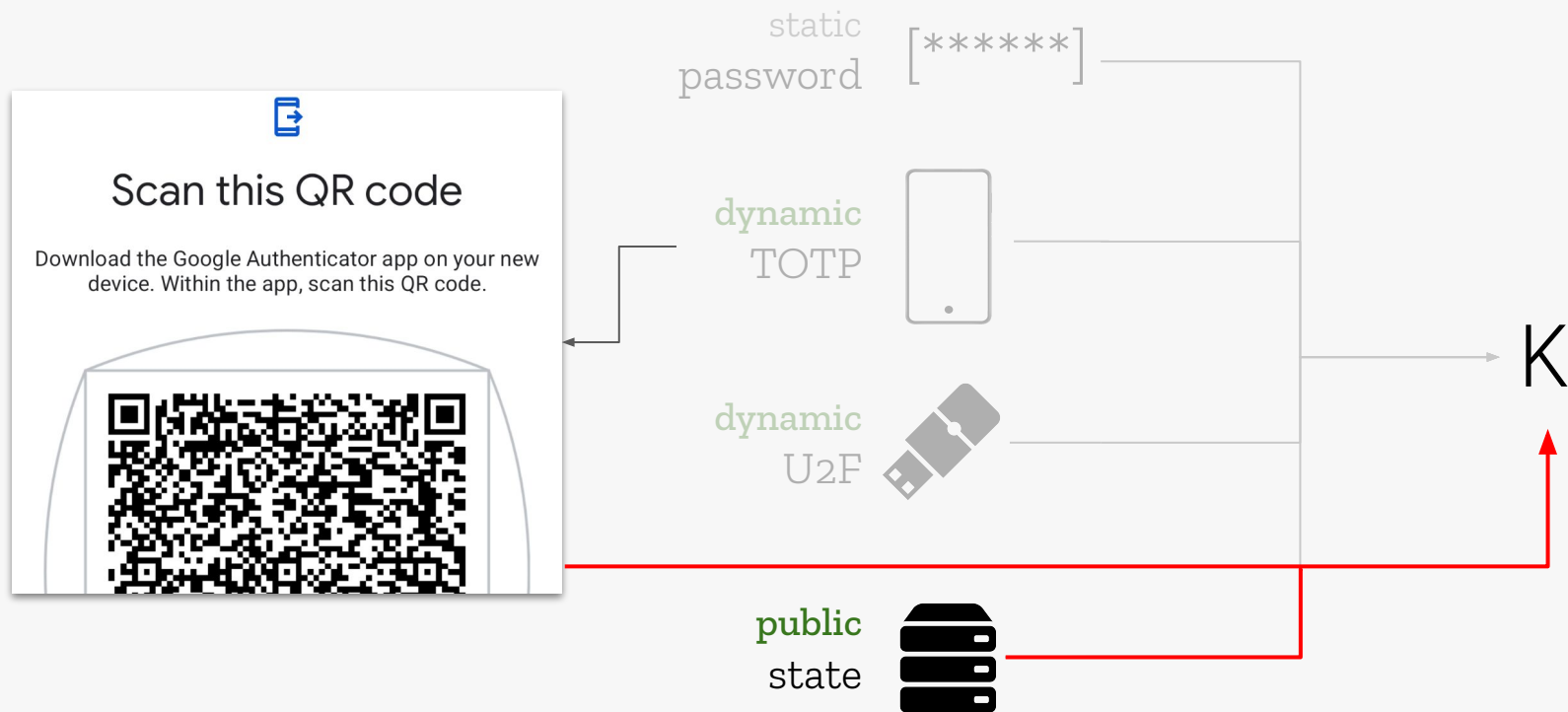


+ NO
Code



Target
→ **423411**

TOTP Compromise Attack...



... and more!



[ia.cr/
2024/935](https://ia.cr/2024/935)

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