Rowan University

Authentication and Credentials

Not All is Lost:

Partial Recovery & Memorability in Self-Sovereign Digital Identity

Sushanth Ambati
Dylan Jablonski
Charalampos Papachristou
Brian Pugliese
Jack Myers
Nikolay Ivanov

All Authors Affiliated with the ACSUS Lab of Rowan University https://ACSUSlab.org

USENIX SOUPS 2026 ✦ Hannover, Germany ✦ 24 August 2026

What is Self-Sovereign Digital Identity?

SSDI enables users to be in control of their identity rather than relying on identity brokers, as a cryptographic key.

A Cautionary Tale

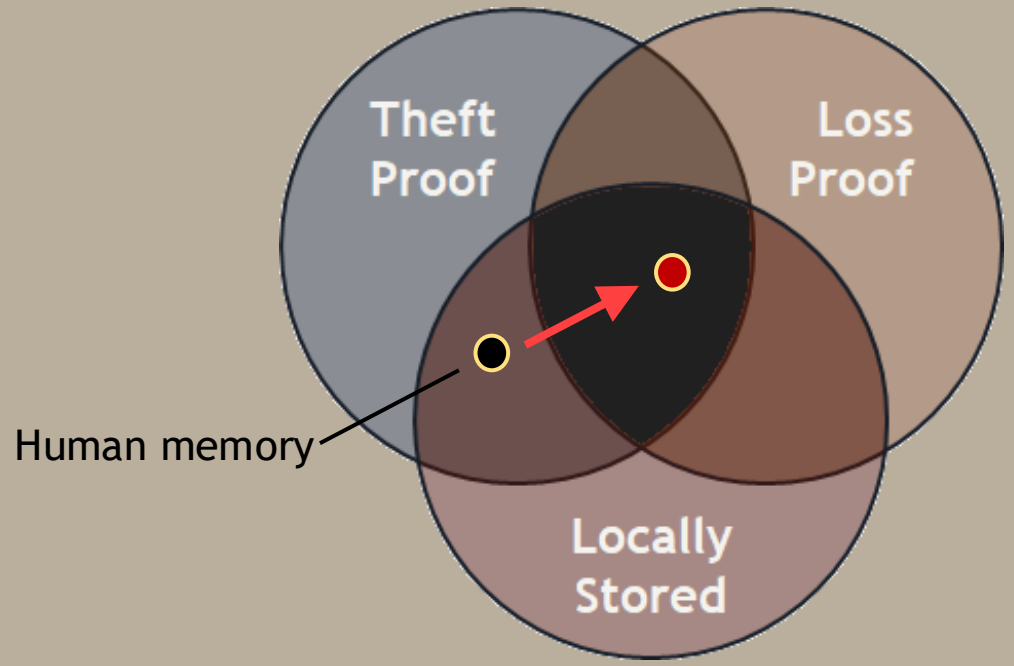


The Problem

- That was only one possible example
- Can occur wherever Self-Sovereign Digital Identities (SSDIs) are used
  - Giving control to the users (not ID brokers) has benefit
  - But private key recovery now becomes the user's exclusive responsibility
- How to solve this problem?

The Solution
"It's all about the backup"

- Backup of private key that is:
  - Theft proof
  - Loss proof
  - Locally stored

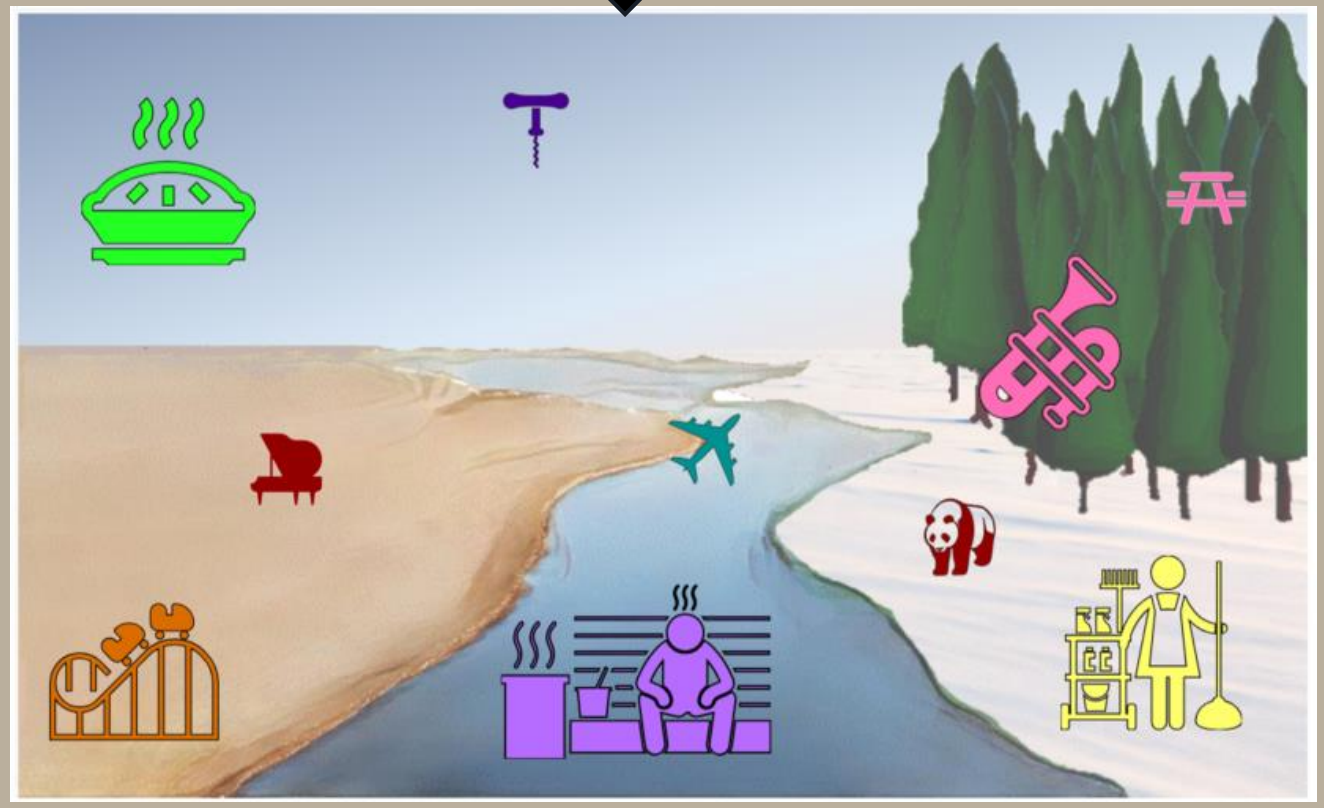


- **Human memory** might be the solution for a backup of self-sovereign digital identities, but memory is not loss proof.

Can we do better than memorizing 12 BIP-39 words?

- BIP-39 words are abstract and easy to confuse.
- We created a reasonable graphical authentication scheme with the same strength as de facto minimum standard 12-word BIP-39.

vicious, any, badge, faith, remove, ability, need, crane, shop, panther, dry, water



But wait...why not vaults or wallets?

Vaults

- One master credential unlocks everything — single high value target
- 2022 LastPass breach
- Autofill & desktop clients add phishing and clickjacking surface

Wallets (hardware, paper)

- Vulnerable to theft, loss, insider access and environmental damage
- No reset: if the medium is gone, the backup key is gone
- A misplaced steel plate is no safer than a breached server

An interesting observation

- What we were primarily designing for:
  - Memorability (graphic images vs. text)
  - Key strength (achieving 128-bit entropy)

- What we discovered:
  - While both BIP-39 and graphical keys demonstrated the ability to be partially recovered…
  - *the nature of our graphical key made it more amenable to partial recovery based on the granularity of image components*

Our main contributions

Baseline Evaluation of 128-bit Keys

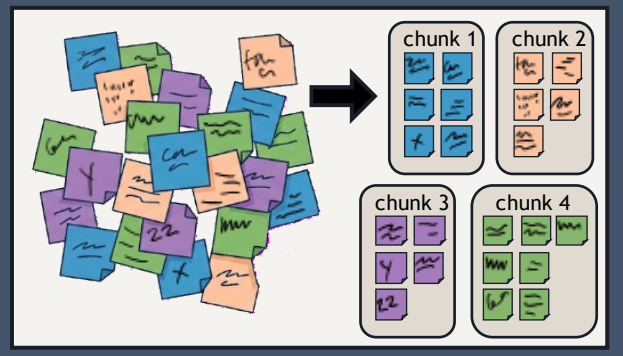
- Controlled, lab-based randomized AB/BA crossover trial — BIP-39 vs Graphical Key

Partial Key Recovery

- Partially forgotten private keys can still be recovered through combinatorial search

Cognitive-Driven Key Space Design

- We created a 128-bit graphical key space grounded in cognitive psych literature (contextual picture superiority, chunking, spatial memory, dual coding) that outperforms combinatorial recoverability of BIP-39.



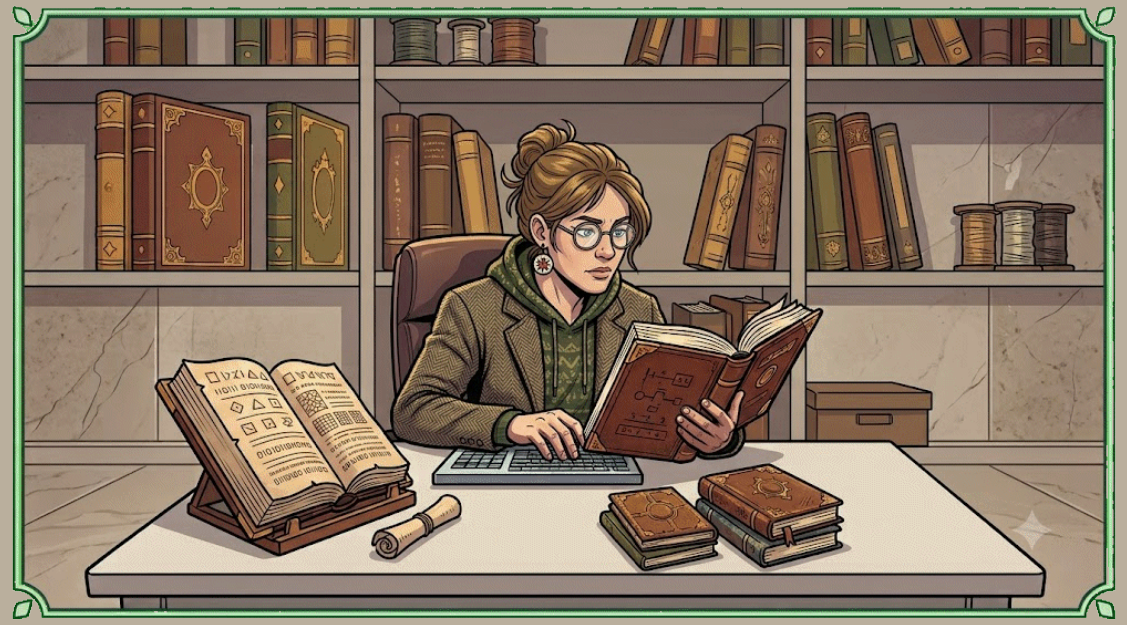
chunking



spatial memory



dual coding



What past research has uncovered

Standing on the shoulders of giants

PROJECTS

LociMotion (Doolani, et. al.)

- Loci-based: learn a secret via video house-tour
- 12 landmarks (~56 bits), lowercase only — moderate strength



MnemonicMaker (Vlahavas, et al.)

- Serious game for memorizing BIP-39 phrases
- Game mechanics drive repeated rehearsal of the words



RESEARCHERS

Clark, et. al.

- Memorizing strong system-assigned keys by traversing multiple scenes
- Measured ~55bits (5 BIP-39 words)



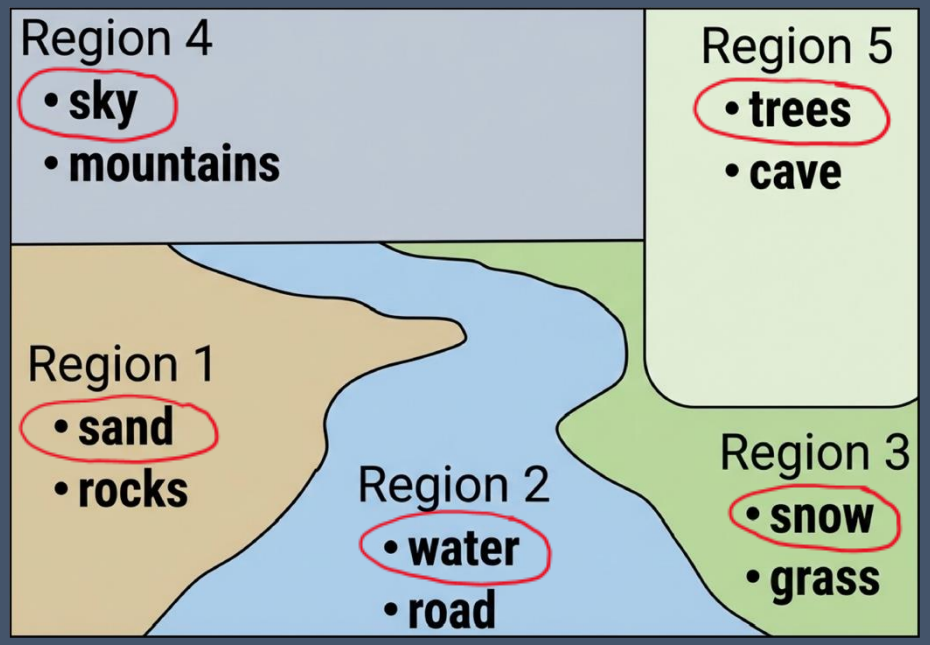
Stobert, et. al.

- Click-based graphical passwords on images
- Users cluster on predictable visual "hotspots"

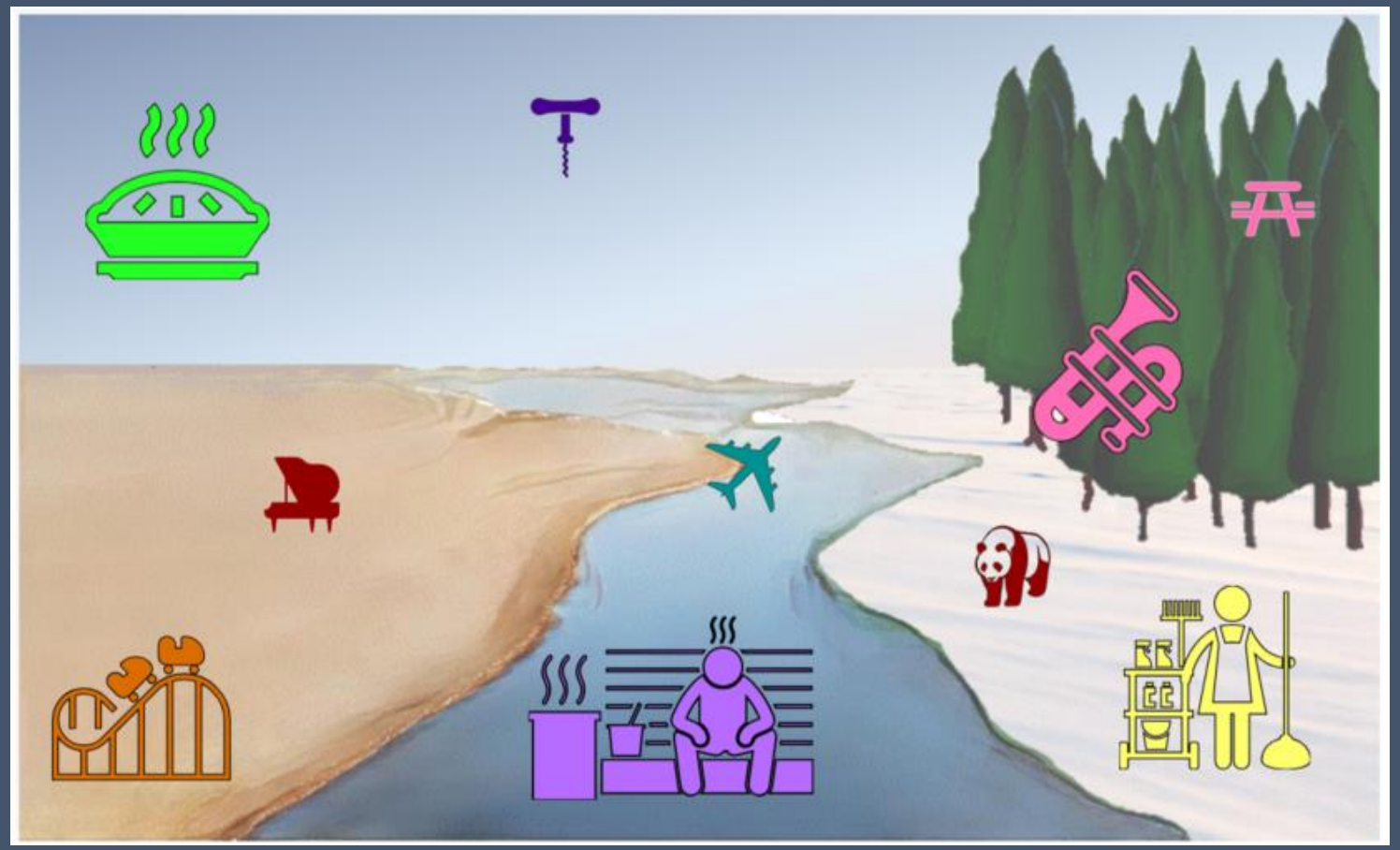


Images cropped from key research papers of the authors above.

This is our 128-bit key

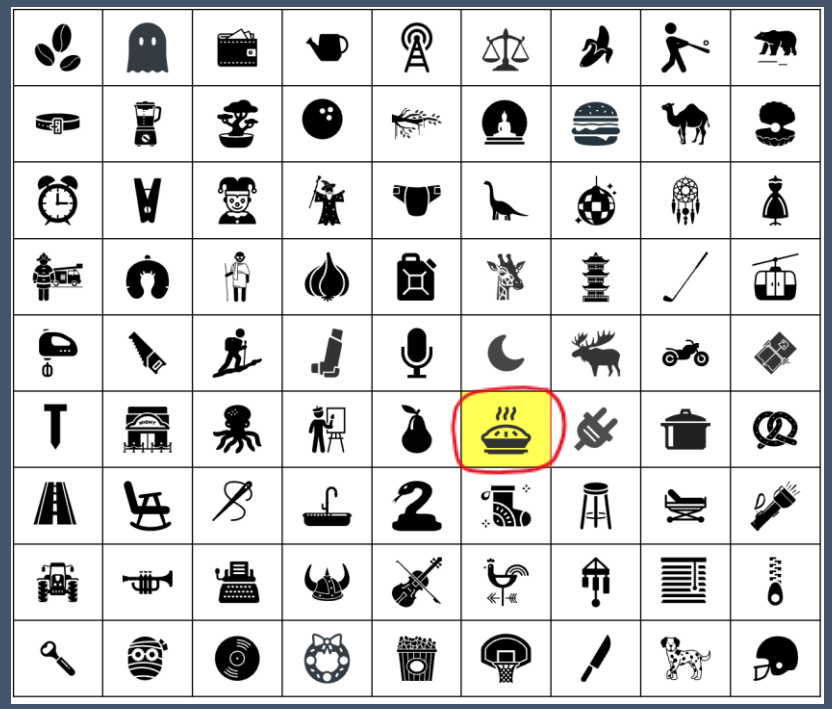


5 regions



The background scene is split into 5 regions with 2 icons per region

This is our 128-bit key



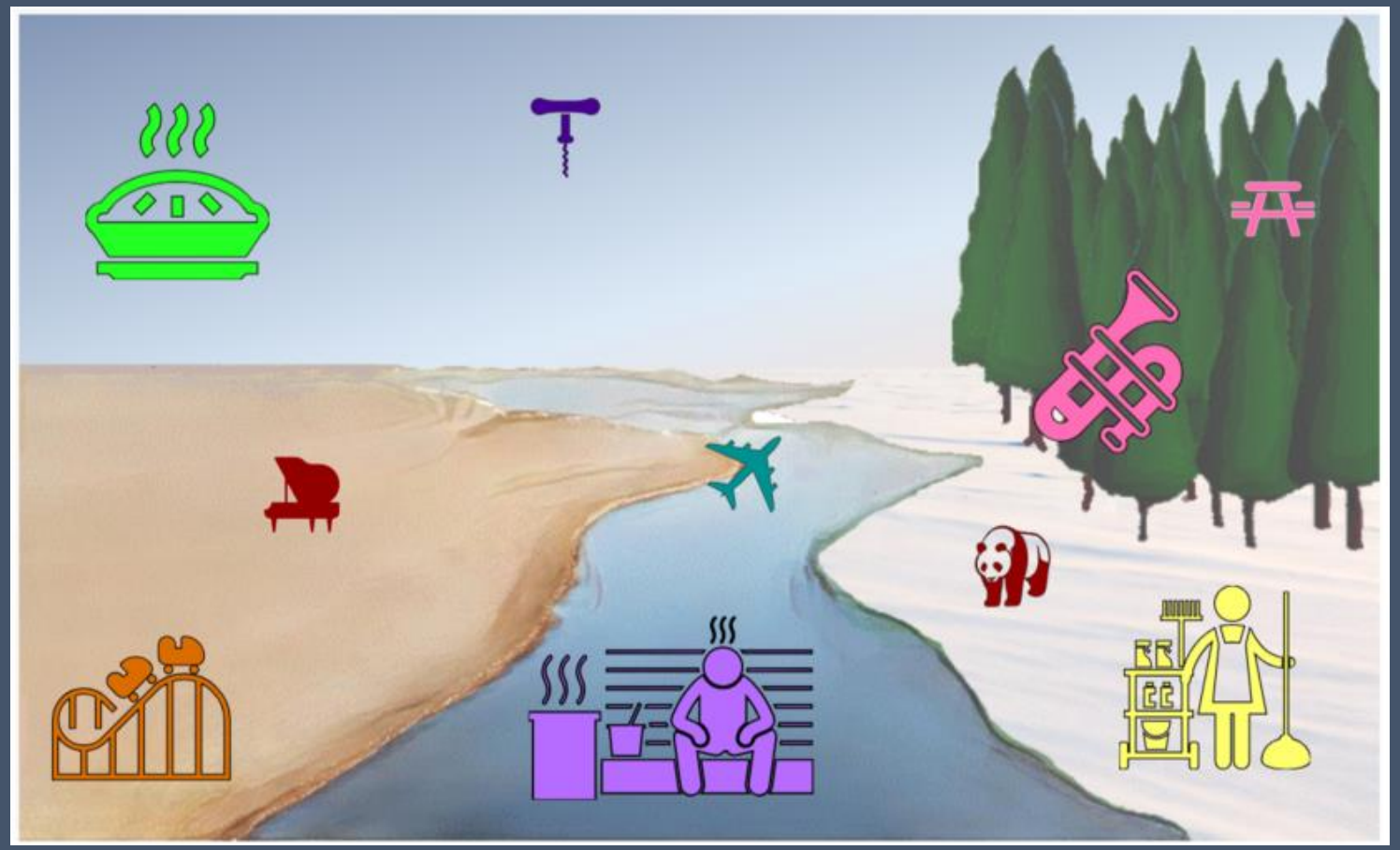
81 icons

pink
red
brown
orange
yellow
green
teal
blue
purple
violet

10 colors

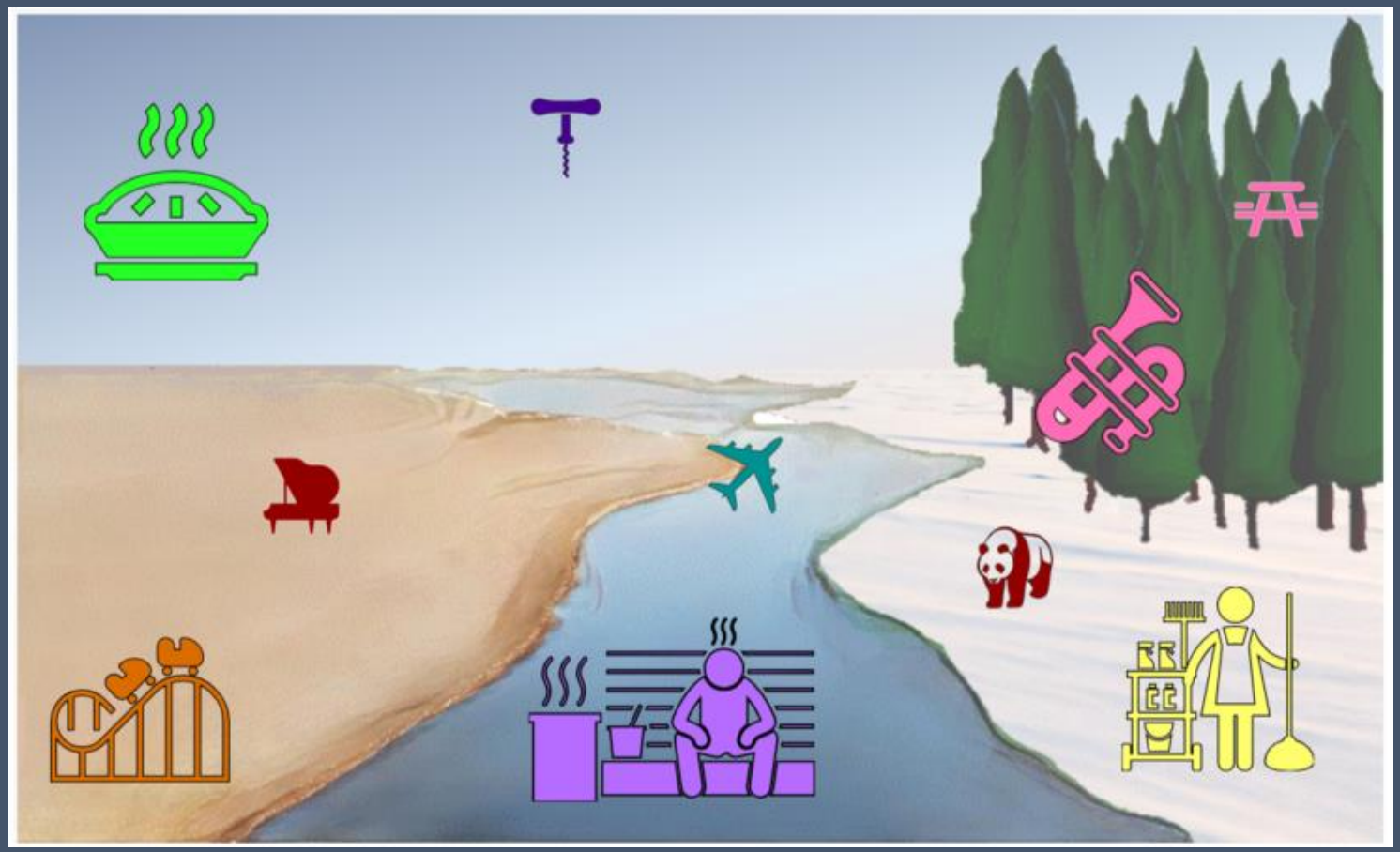


2 sizes



Each icon on the scene comes from 10 pools of 81 distinct unique icons
Each icon can be of 10 different colors and of 2 different sizes

compared to a BIP-39 key



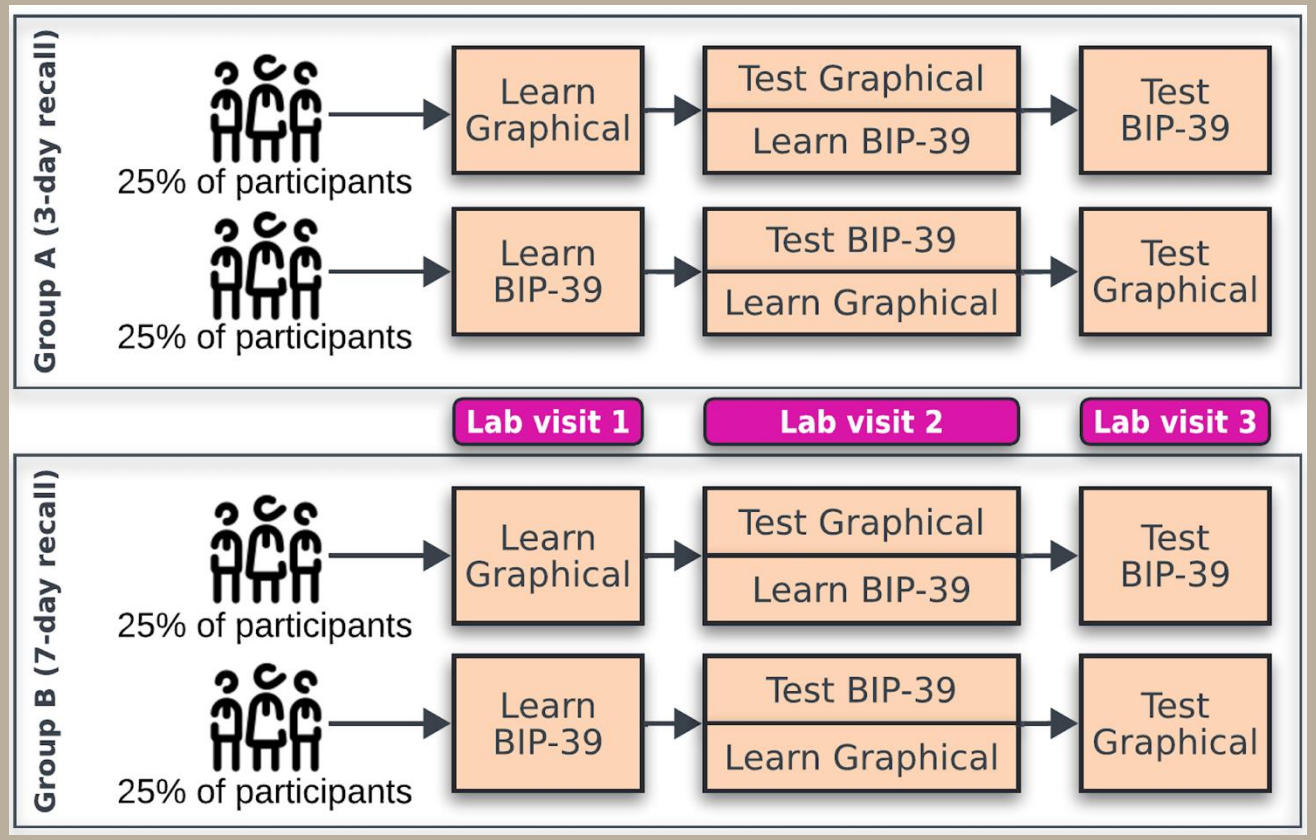
Word #1:	vicious
Word #2:	any
Word #3:	badge
Word #4:	faith
Word #5:	remove
Word #6:	ability
Word #7:	need
Word #8:	crane
Word #9:	shop
Word #10:	panther
Word #11:	dry
Word #12:	water



Experimental Setup and Our Results

- How we conducted our study
- What we discovered

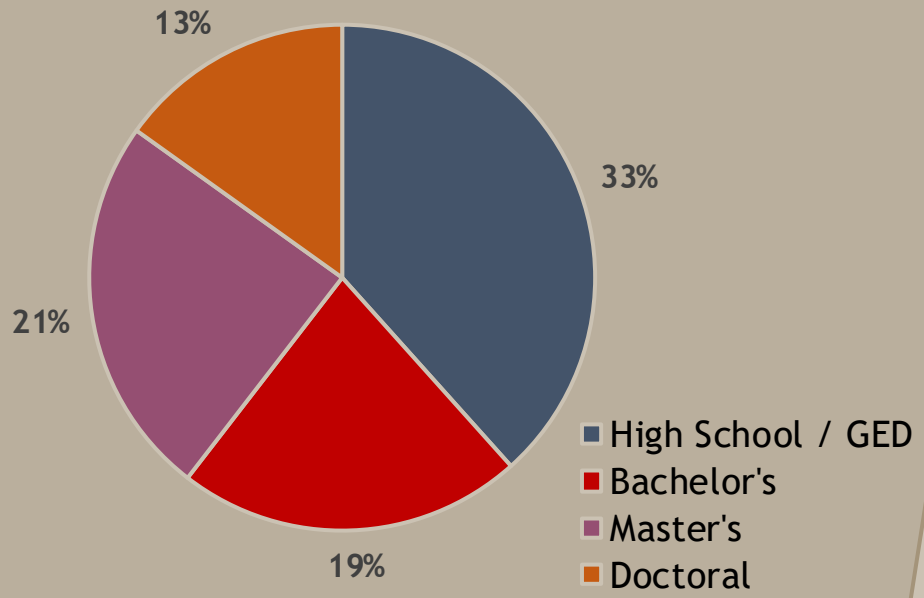
Here's how we tested



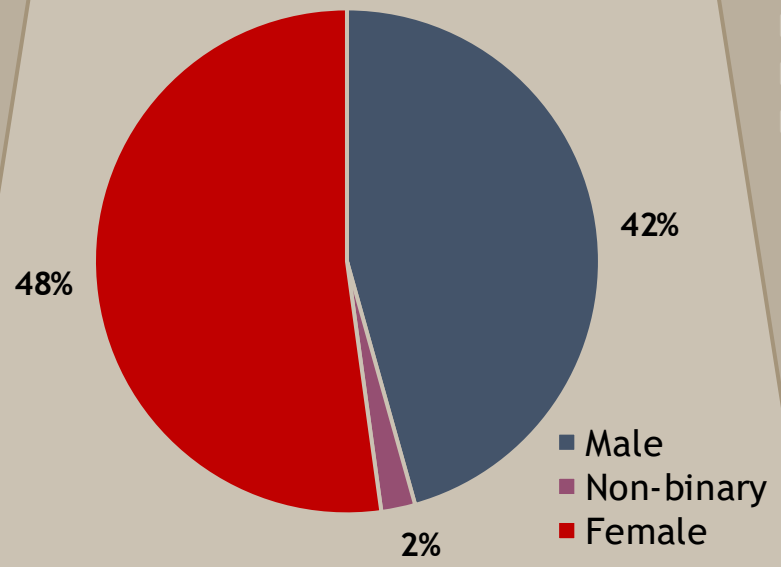
- N = 92, lab-controlled
- Crossover design, where every participant learns both keys
- Keys are system-assigned and random
- Recall tested at 3 and 7 days
- Order counterbalanced

Demographics

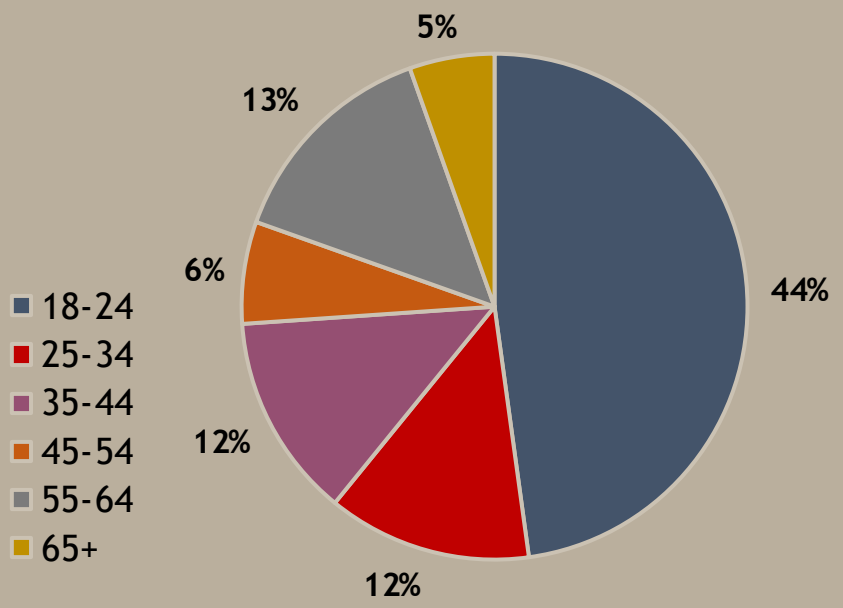
Education



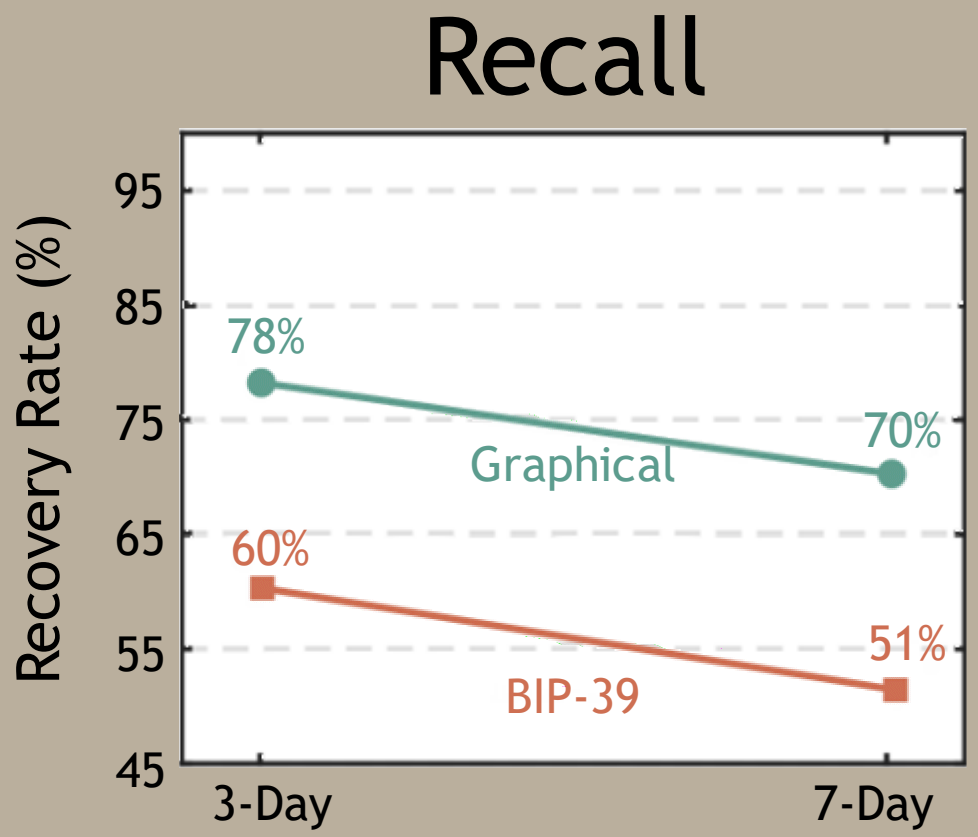
Gender



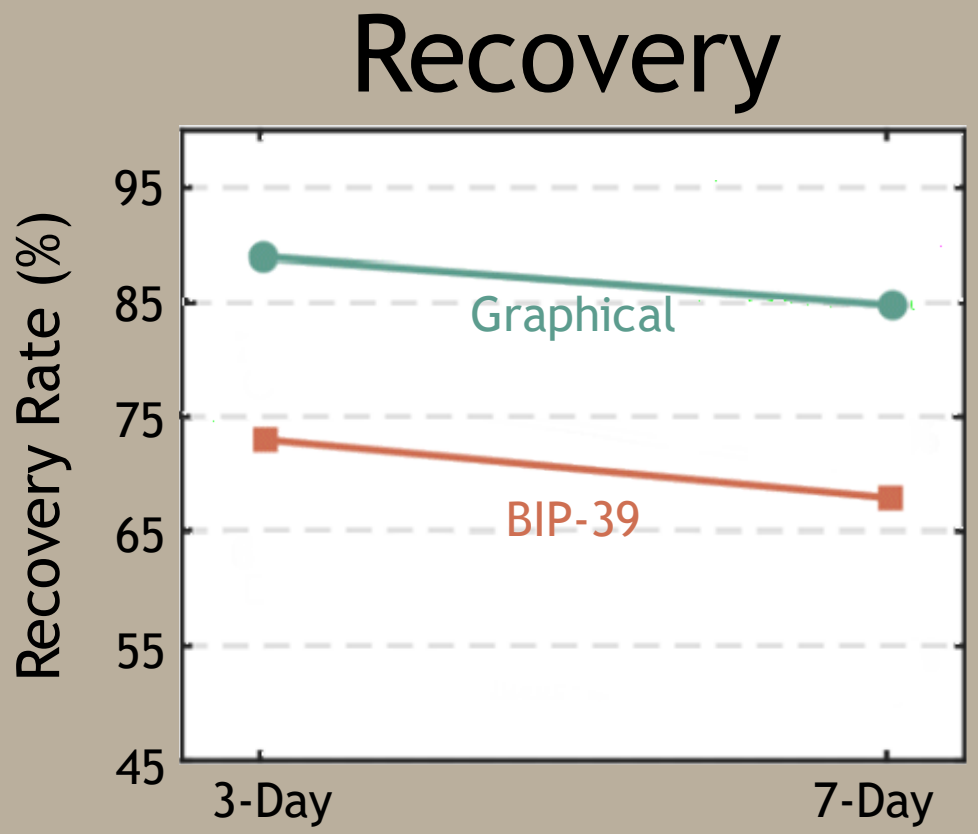
Age



Turns out, graphics win



Turns out, graphics win



	Recall Rate (%)		Recovery Rate (%)	
	3-Day	7-Day	3-Day	7-Day
Graphical	78%	70%	89%	85%
BIP-39	60%	51%	73%	68%

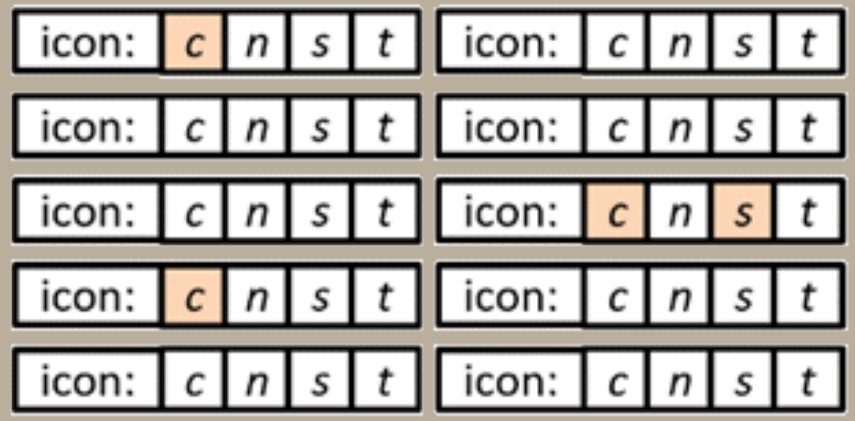
A failed attempt isn't a lost key, it's just a key with a few wrong pieces

12 indivisible items
Order matters



BIP-39

10 items split into components
Order not relevant



Graphical key

c = color
n = name of icon
s = size
t = terrain of icon

Splitting items into components makes recoverability more feasible.

Combinatorial search recovery results

We recovered participant 600's graphical key, despite four recall errors, in about 6.4 minutes.

In contrast, four recall errors in a BIP-39 key could require up to 8.708×10^{15} permutations, which could take approximately 95,000 years on consumer-grade hardware.

Successful **graphical** authentications via combinatorial key search

User	Attempt ID	Errors Made	Recovered
529	1308	3 colors	✔
	1311	1 color	✔
547	1486	1 color	✔
562	1513	1 color, 1 size	✔
571	1696	1 color	✔
574	1637	1 color, 1 size	✔
	1639	1 color	✔
586	1712	1 color	✔
	1716	1 color	✔
597	1855	2 colors, 1 size	✔
598	1980	1 color	✔
600	1952	4 colors, 1 size, 1 terrain	✘
	1953	4 colors	✔
601	1890	1 color, 1 size	✔
607	1928	3 colors	✔
617	1976	1 color	✔

50% of unsuccessfully authenticating users recovered.

BIP-39 authentication attempts recoverable under same recovery constraints as the graphical key.

User	Attempt ID	Errors Made
523	1285	1 wrong word
535	1342	1 wrong word
536	1363	1 wrong word, 1 flipped order
538	1424	1 wrong word, 1 flipped order
541	1327	1 wrong word
544	1430	1 wrong word, 1 flipped order
548	1487	1 wrong word
564	1602	1 wrong word
565	1596	1 wrong word
574	1700	1 wrong word
593	1841	1 wrong word
595	1913	1 wrong word
607	1989	1 wrong word
612	1948	1 wrong word, 1 flipped order

34.1% of unsuccessfully authenticating users recoverable.

The threat model



- **What's protected:**
  the seed is never on disk in plaintext,
  but only as an authenticated ciphertext.
- **Legitimate recovery:**
  runs locally, needs the stored check value and
  a recall attempt close to the real key.
- **Attacker with stolen device:**
  gets the check value, but without partial knowledge still
  faces the full 2^{128} search
- **Standard hardware-wallet defenses:**
  rate-limiting, bounded attempts

Caveats & future research directions

Limitations

- **Ecological Validity**
  Lab study, controlled conditions, structured rehearsal. Real backup is messier and less rehearsed.
- One week — tested feasibility, not long-haul durability

Future work

- Expanding on the potential of high-entropy keys where partial recovery becomes more viable
- Can graphical cues paired with BIP-39 mnemonics, alongside combinatorial recovery techniques improve memorability?

References

- Jayesh Doolani, Matthew Wright, Rajesh Setty, and SM Taiabul Haque. Locimotion: Towards learning a strong authentication secret in a single session. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2021.
- Michael Clark, Scott Ruoti, Michael Mendoza, and Kent Seamons. A Comparison of Three Approaches to Assist Users in Memorizing System-Assigned Passwords. In *Symposium on Usable Security and Privacy (USEC)2024*. Internet Society, 2024.
- George Vlahavas, Christos Karakasis, and Athena Vakali. MnemonicMaker: A Serious Game for Reconstructing Bitcoin Wallet Mnemonic Phrases. *International Journal of Serious Games*, 12(2):53–75, 2025.
- Elizabeth Stobert and Robert Biddle. Memory retrieval and graphical passwords. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, pages 1–14, 2013.
- Elizabeth Stobert, Alain Forget, Sonia Chiasson, P.C Van Oorschot, and Robert Biddle. Exploring usability effects of increasing security in click-based graphical passwords. In *Proceedings of the 26th Annual Computer Security Applications Conference*, pages 79–88, 2010.

RowanUniversity

Not All is Lost: Partial Recovery & Memorability in Self-Sovereign Digital Identity

Looking forward to follow-up questions at the Panel discussion, elsewhere in the conference, or even further in the future!

Thank you.

Sushanth Ambati, ambati23@rowan.edu

This material is based upon work supported by the National Science Foundation under Grant No. 2348344. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Graphics not originating in the paper were generated by Gemini 3.6 Flash