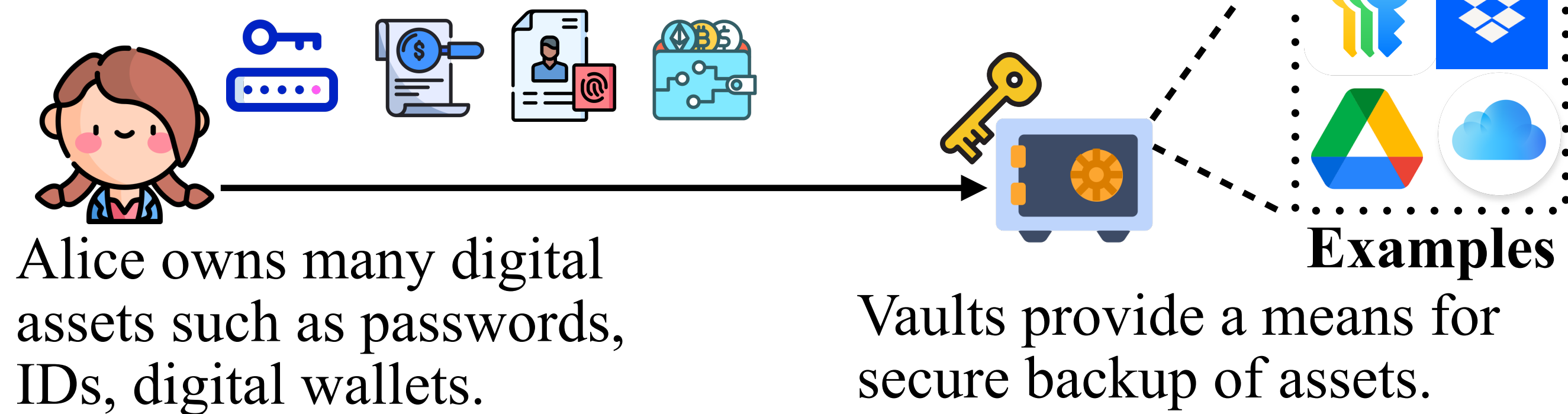


Towards Self-Recovery and Metadata Privacy in Social Vault Recovery with Apollo

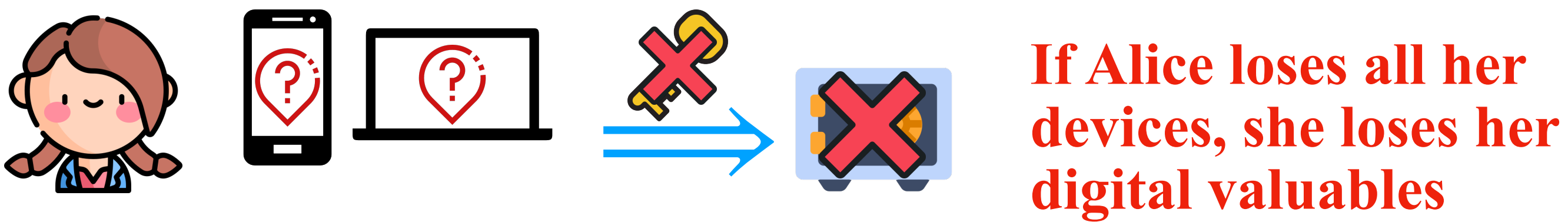
Shailesh Mishra¹, Simone Colombo¹, Pasindu Tennage¹, Martin Burkhart², Bryan Ford¹

¹EPFL, ²armasuisse

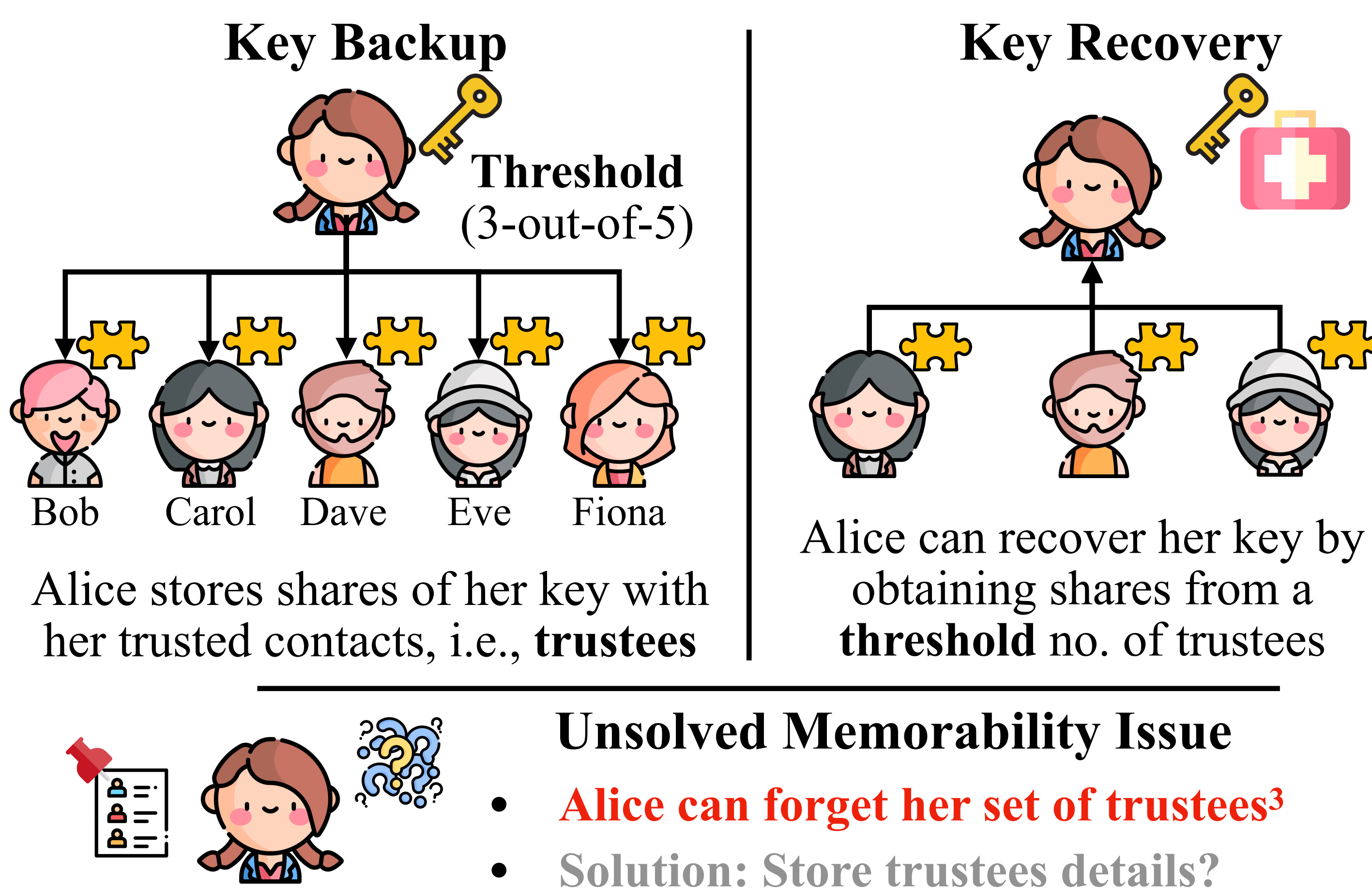
Digital Vaults: A Necessity



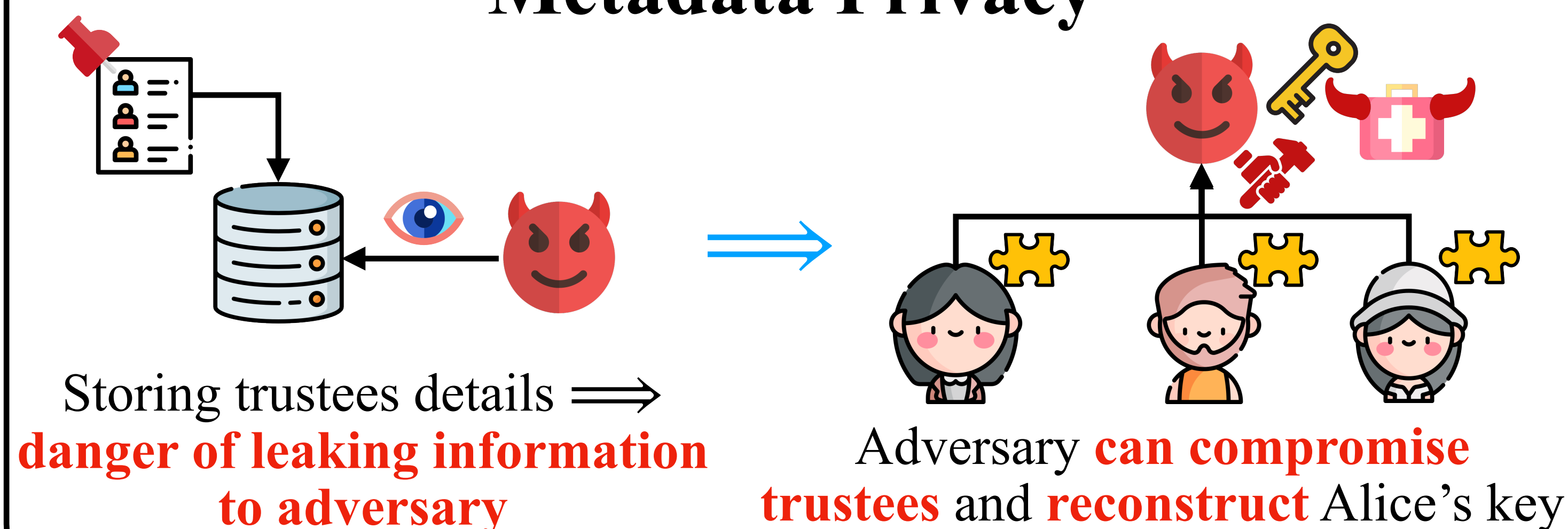
Dealing with the worst-case scenario



Solved by Shamir's Secret Sharing²?

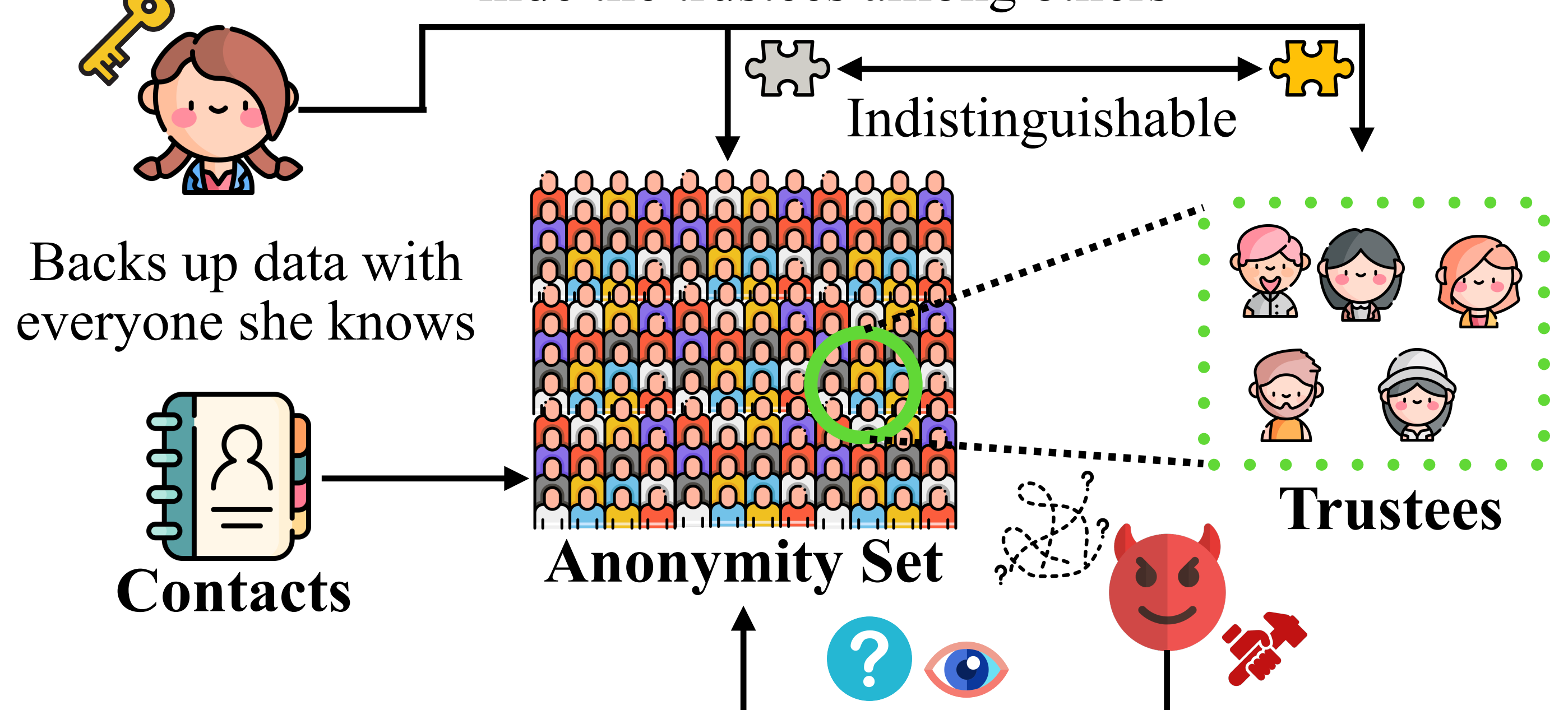


Metadata Privacy



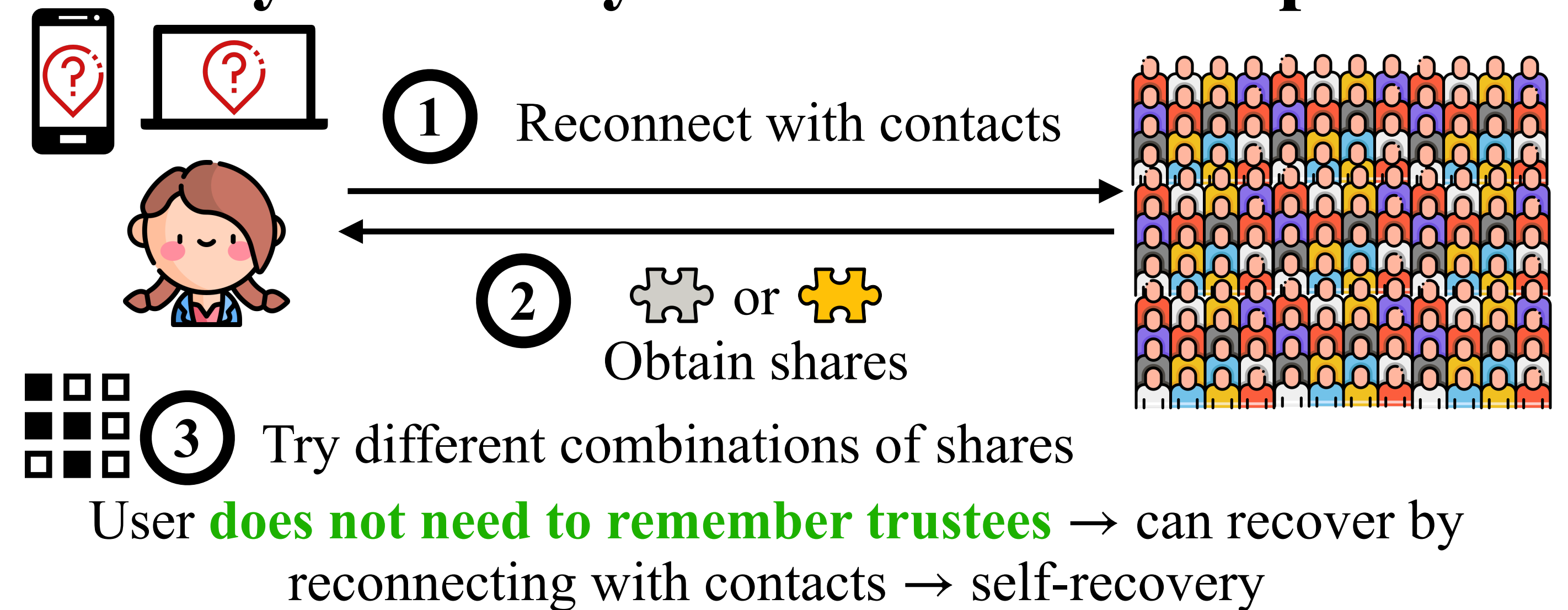
Self-recovery with metadata privacy

Core idea: Alice knows many more people than just her trustees $\rightarrow$ hide the trustees among others



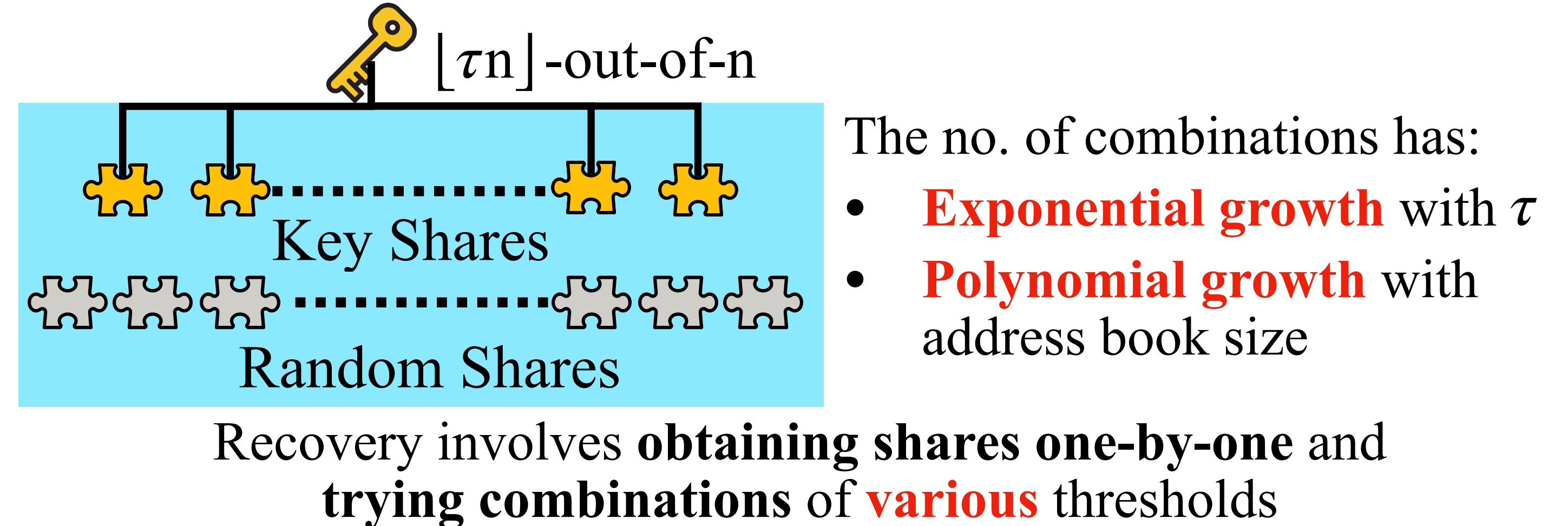
- Key shares (🔑) $\rightarrow$ relevant for recovery $\rightarrow$ trustees
 - Random shares (🔑) $\rightarrow$ irrelevant for recovery $\rightarrow$ non-trustees
- Shares are **indistinguishable** $\Rightarrow$ Trustees are **hidden among non-trustees** $\Rightarrow$ Adversary **has to compromise many** to obtain enough key shares

Key Recovery Procedure with Apollo

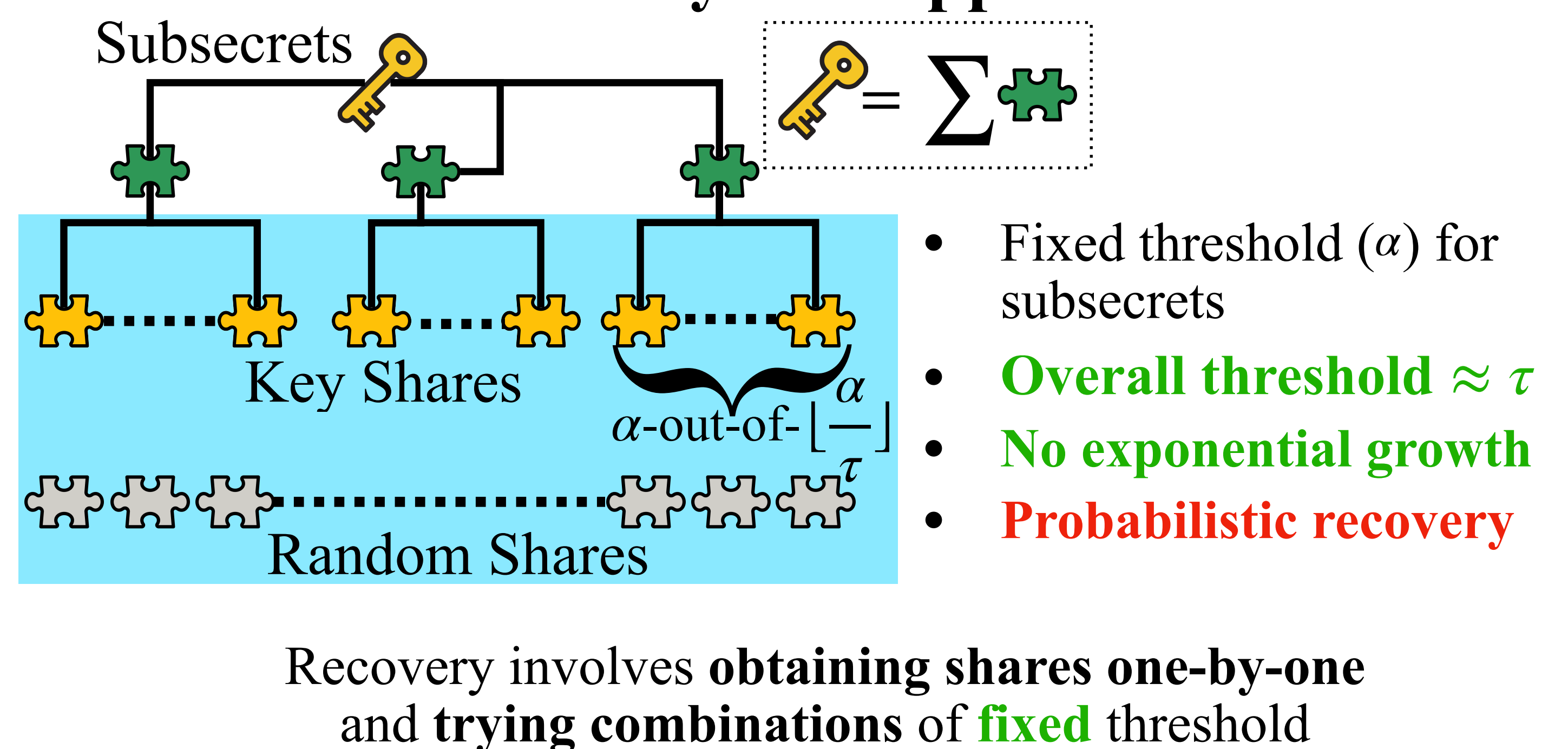


Key Reconstruction

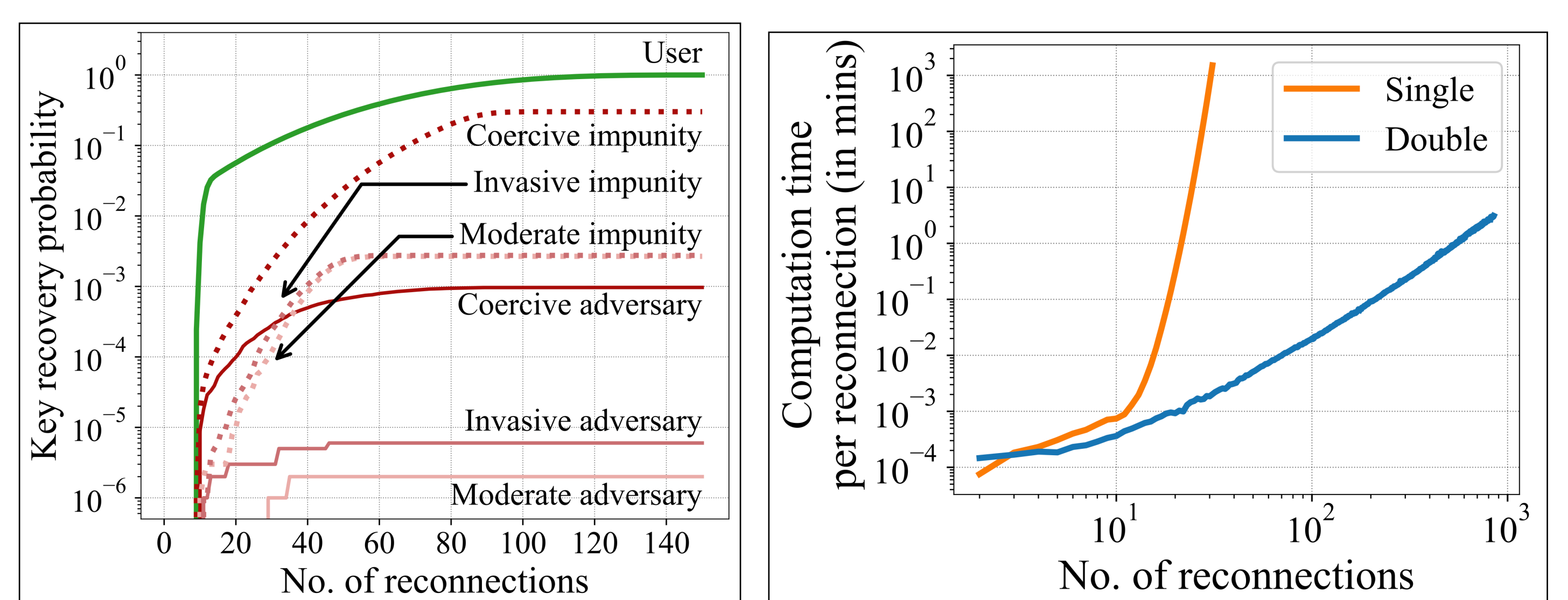
Single-layered Approach



Double-layered Approach



Results

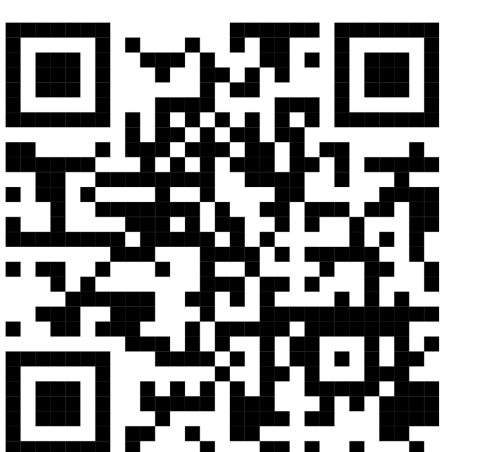


Apollo reduces the chances of malicious recovery

Reduction in computation with added layer

Conclusion

- Vaults are necessary for digital valuables' backup
- Usual solutions pose **memorability** and **privacy** issues



Apollo

Anonymity Set

Hides trustees and makes coercion difficult

Double-layered approach

Makes recovery using anonymity set practical

References

- Gao, X., Yang, Y., Liu, C., Mitropoulos, C., Lindqvist, J., and Oulasvirta, A. Forgetting of passwords: Ecological theory and data, USENIX Security 18.
- Shamir, A. How to Share a Secret. Communications of the ACM 22, 11 (1979).
- Schechter, S., Egelman, S., and Reeder, R. W. It's Not What You Know, But Who You Know: A social approach to last-resort authentication, ACM SIGCHI '09.