Vuvuzela Reimplementation

Sam Ginzburg Benjamin Kuykendall

Key idea

- Message metadata is important to protect
- Any change in user behavior can leak information
- An NSA-style attacker can observe *all* intermediate traffic

"We kill people based on metadata"

Michael Hayden, former Director of the NSA

High level overview

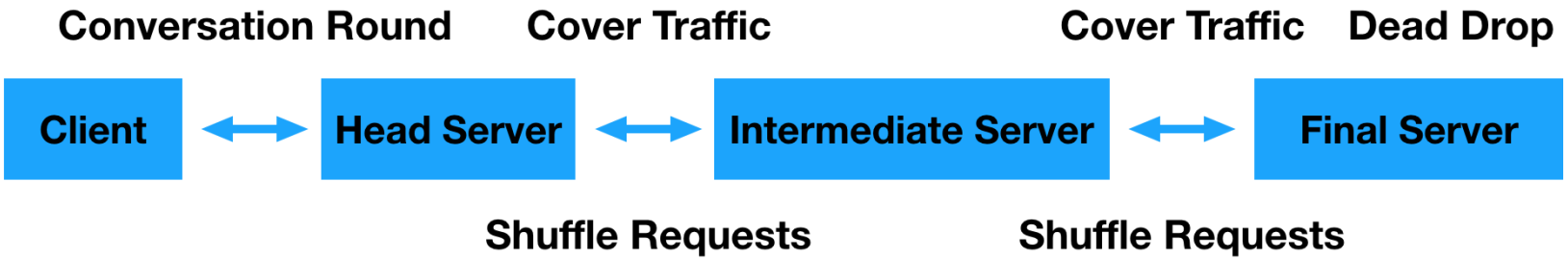
- Messaging system that conceals metadata from MITM attacks
- Messages are sent/received during predefined time periods
- When the servers communicate, noise added to provide privacy

Key challenges

- Security guarantees (formal & systems)
- Scaling the system up
- Modifying the protocol to handle n-way communication

Technical details

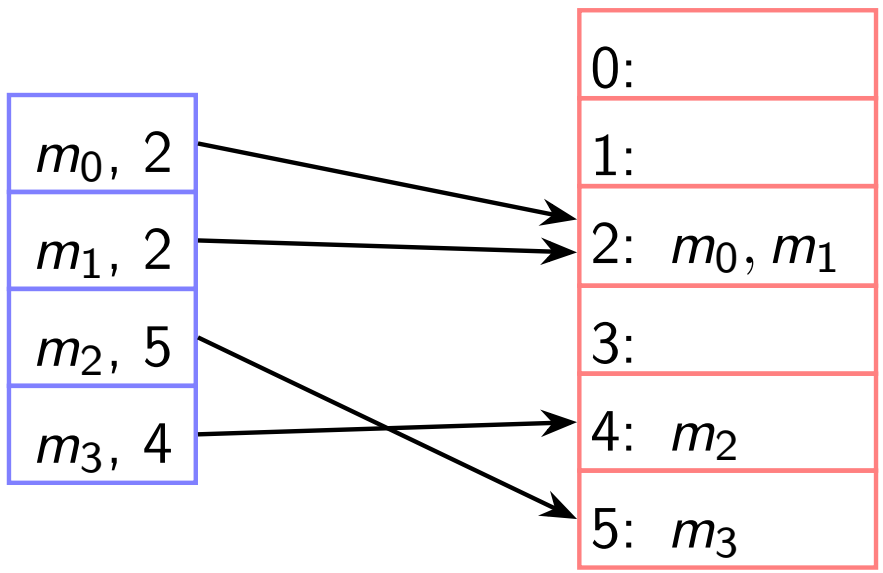
System architecture



- Client has simple put and get API with first server
- Cover traffic and shuffling between servers
- Dead drop phase happens only on the last server

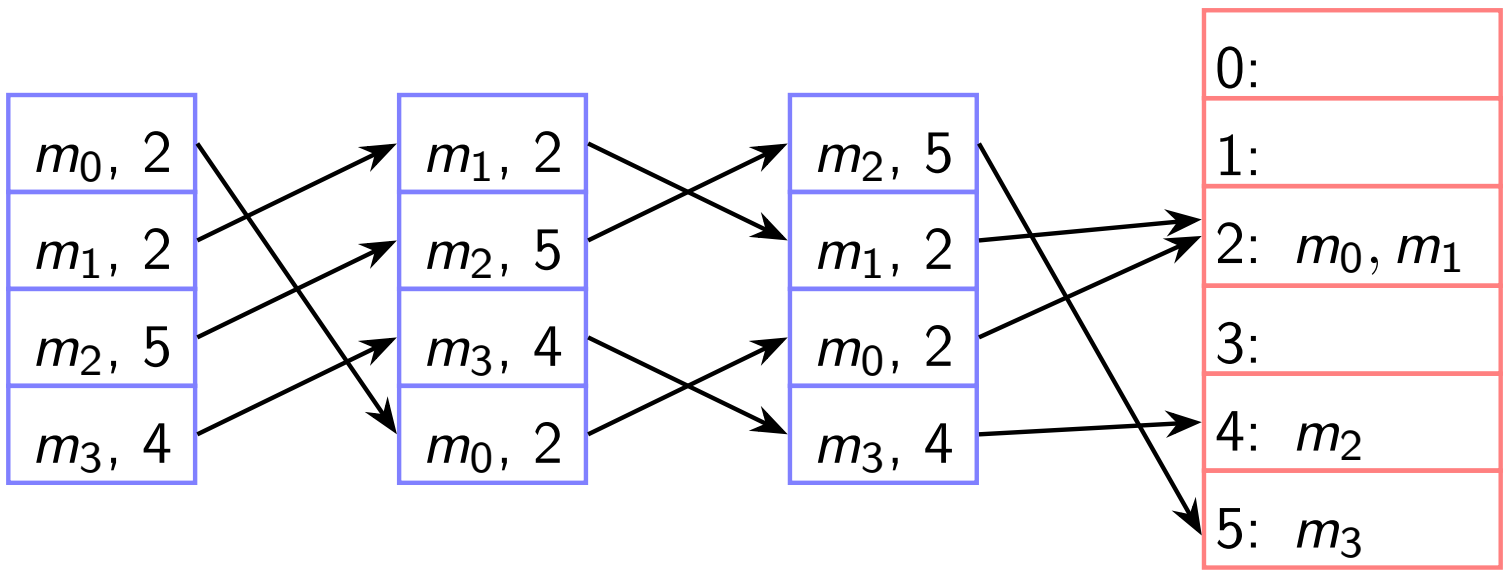
Deaddrops

- Conversants generate shared secret *deaddrop location*
- Messages tagged with deaddrop location
- Final server swaps the messages in each deaddrop



Mixing

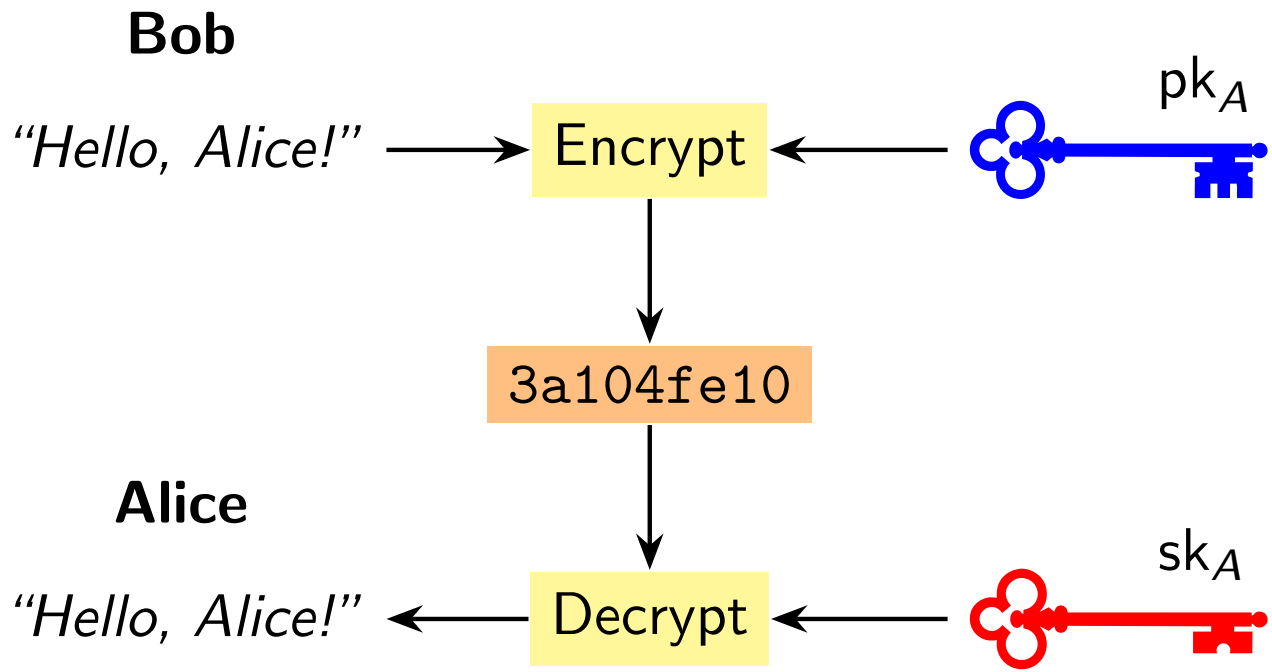
- Mixing hides who is using which deaddrop
- Each server randomly permutes list of messages
- Applies inverse permutation on return route



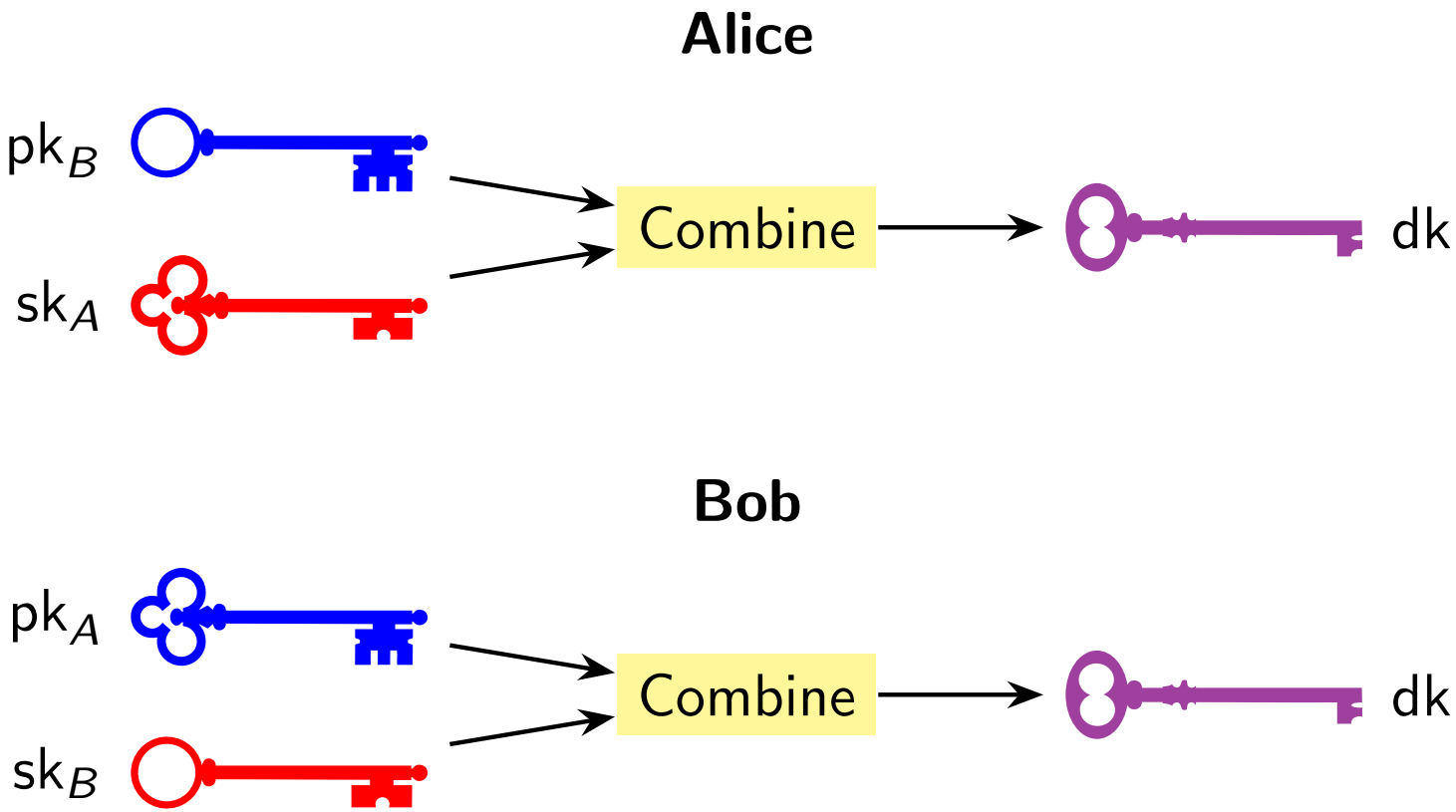
Additional security measures

- Special form of encryption to hide messages
- Cover traffic to hide start and end of conversations

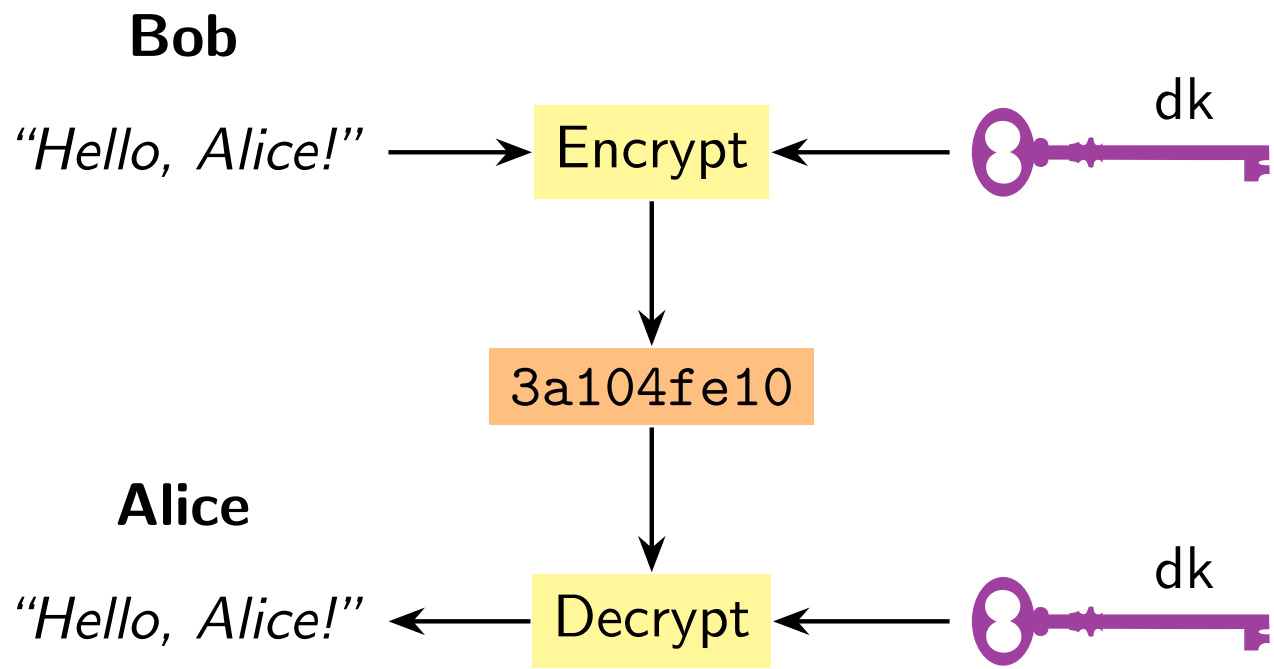
Asymmetric encryption



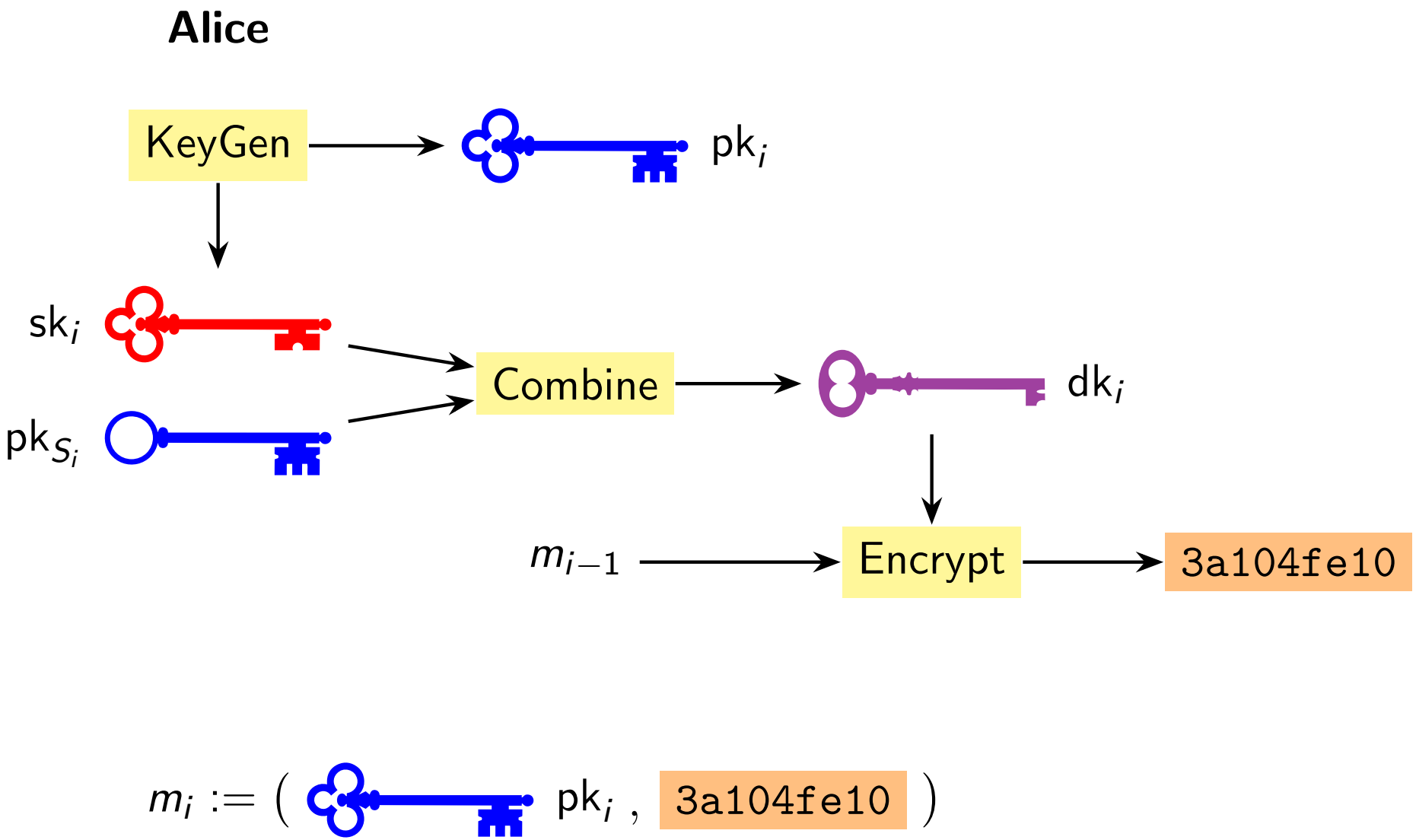
Key exchange



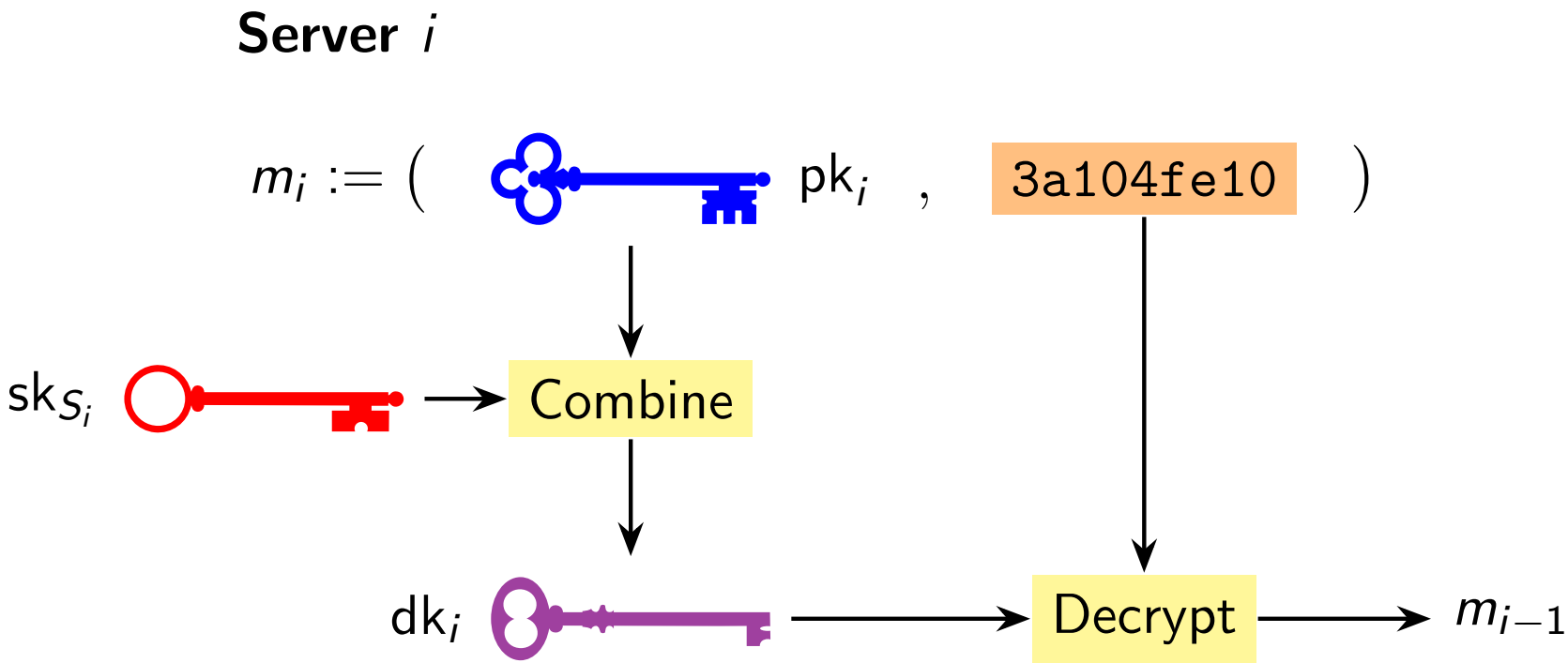
Symmetric encryption



Onion encryption

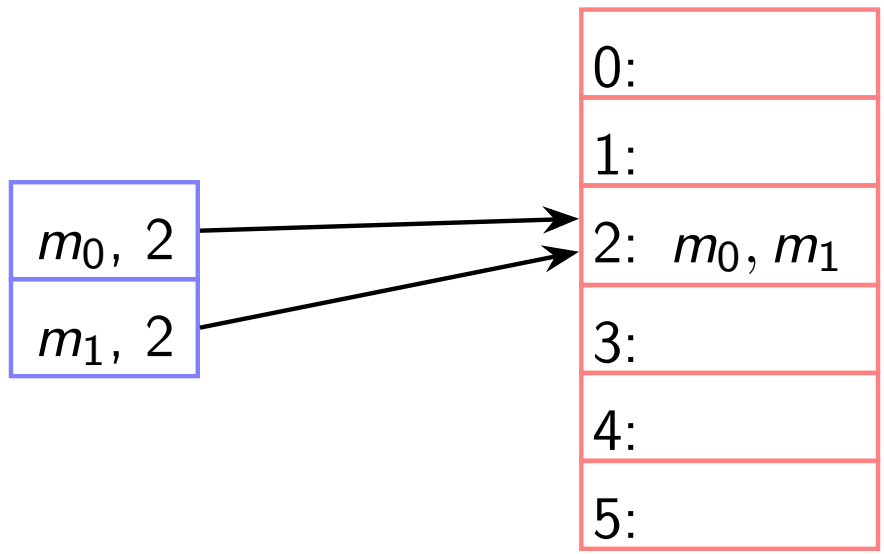


Onion decryption



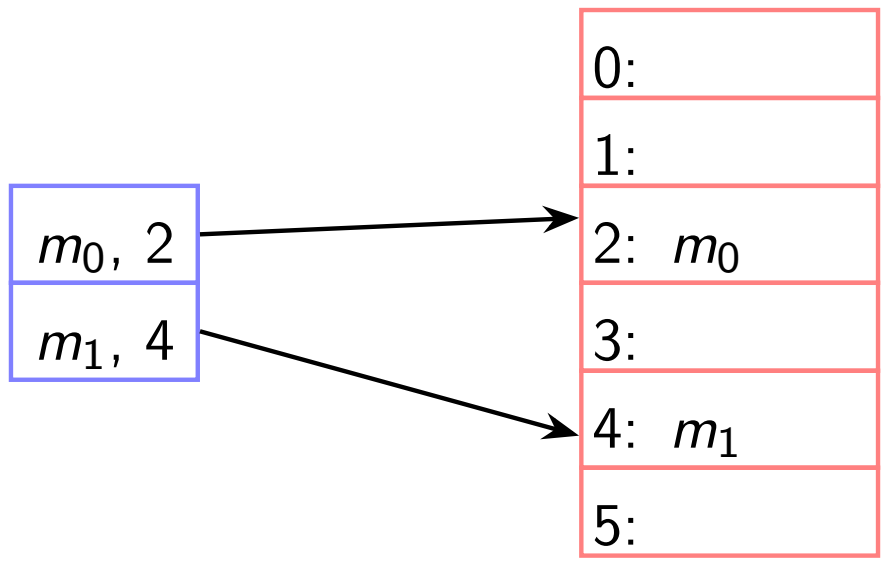
Leakage

Actively communicating:

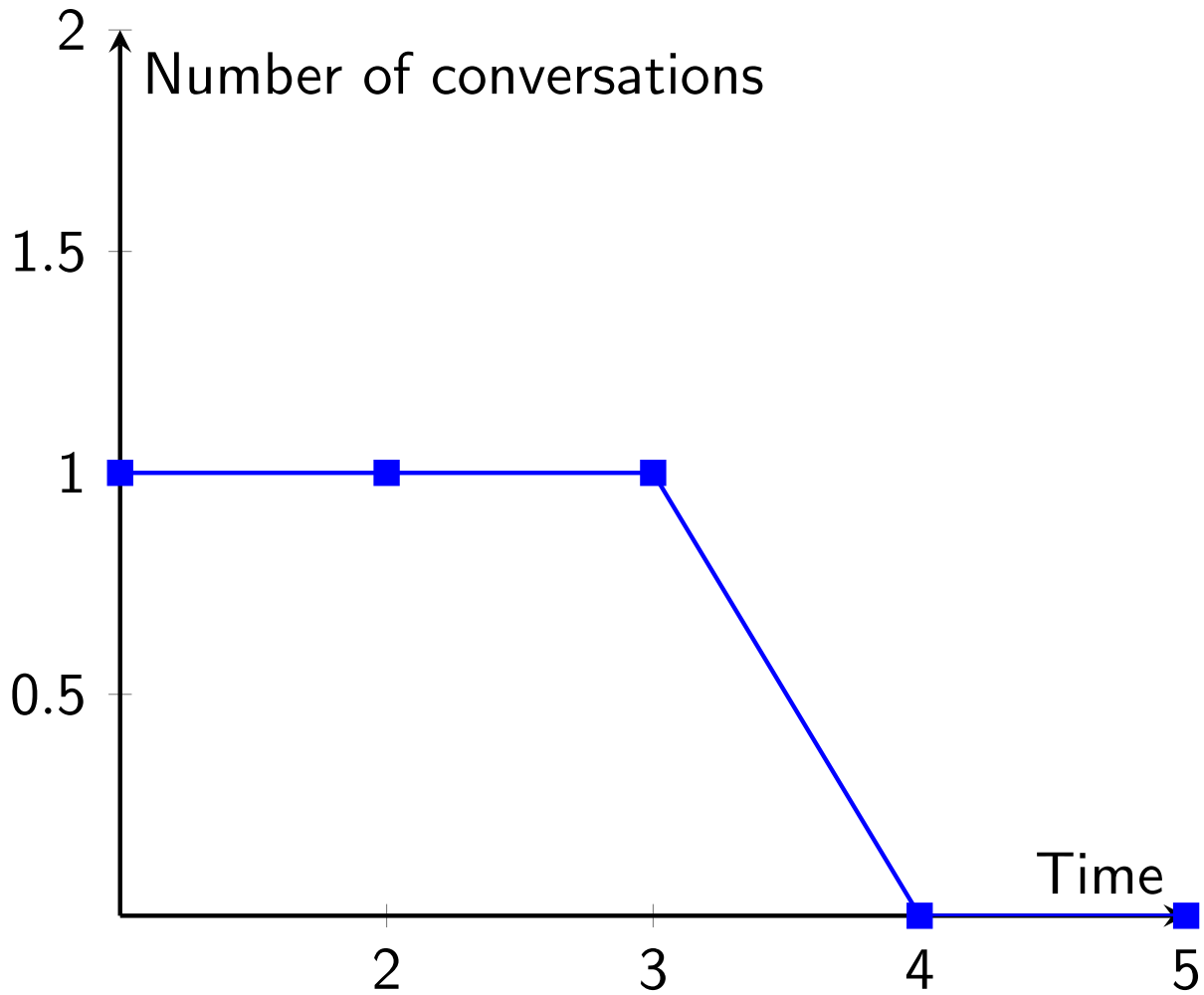


Leakage

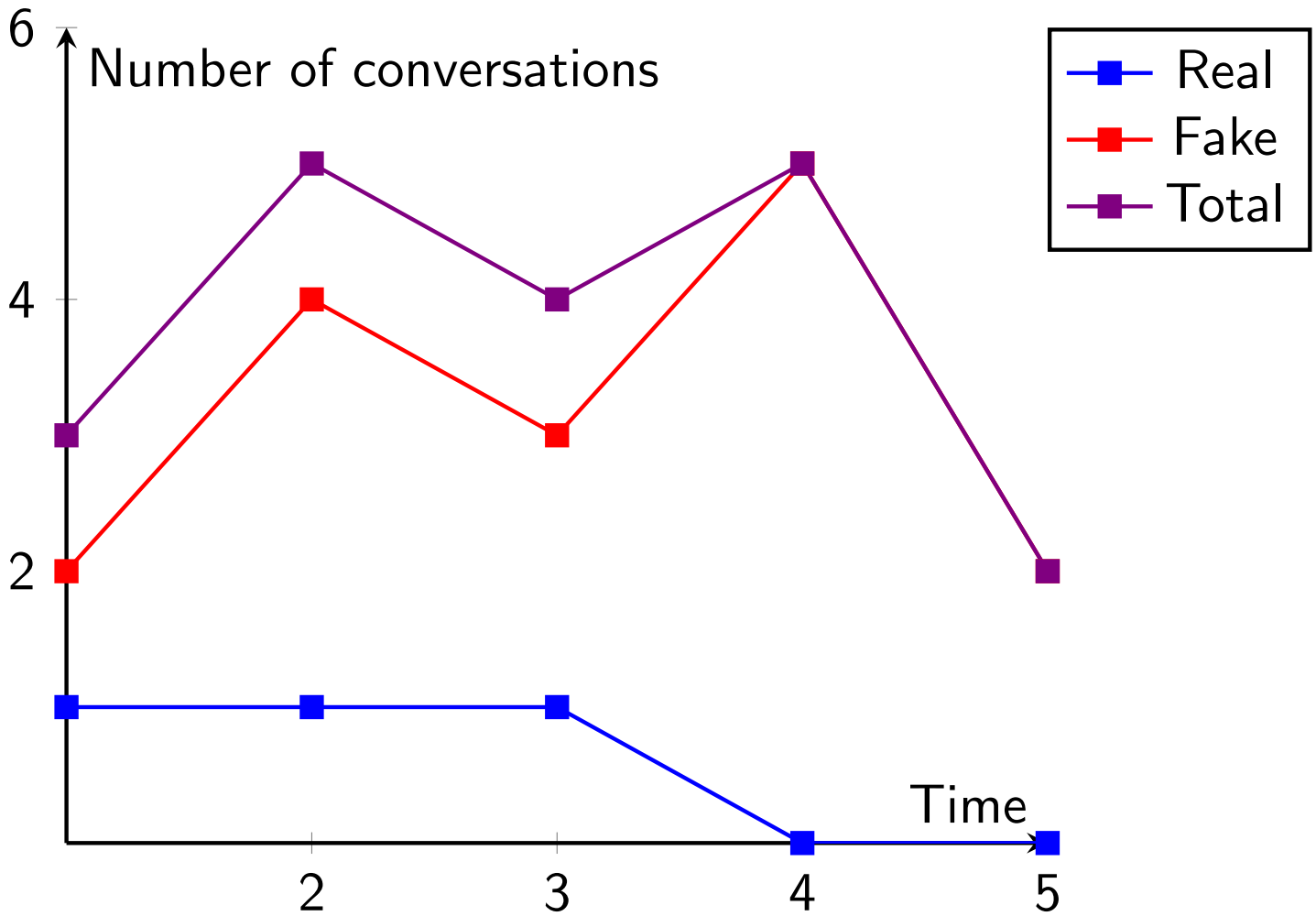
Not communicating:



Leakage



Differential privacy



Implementation status

- Working on it
- Client starting to take shape
- Lots of work left on the server

Evaluation

- Focus on replicating $O(n)$ scaling
- Experiments will be conducted using local servers
  - Bandwidth overhead negligible for clients, huge for servers ($10k/mo on AWS to run!)
- Hope to take advantage of the Princeton SNS cluster
- Otherwise can demonstrate the system with less cover traffic
  - Even with no cover traffic, can still demonstrate $O(n)$ scaling
  - Since cover traffic is easily tuneable, with less computational power we can run the system at a lower security level

Plan for final month

- System implementation completely finished by May 1st
- Make sure we have access to the SNS cluster before then
- Write evaluation scripts
- Perform evaluation with at least 1 final week remaining, dedicated to only writing the report

References

Jelle van den Hooff, David Lazar, Matei Zaharia, and Nickolai Zeldovich.

Vuvuzela: Scalable private messaging resistant to traffic analysis.

In *Proceedings of the 25th Symposium on Operating Systems Principles*, SOSP '15, pages 137–152. ACM, 2015.