Out-of-Band Authentication in Group Messaging: Computational, Statistical, Optimal

Lior Rotem Gil Segev

Hebrew University

Major Effort: E2E-Encrypted Messaging

- Government surveillance and/or coercion
- Untrusted or corrupted messaging servers

Key challenge:
Detecting **man-in-the-middle attacks** when setting up E2E-encrypted channels

Man-in-the-Middle Attacks

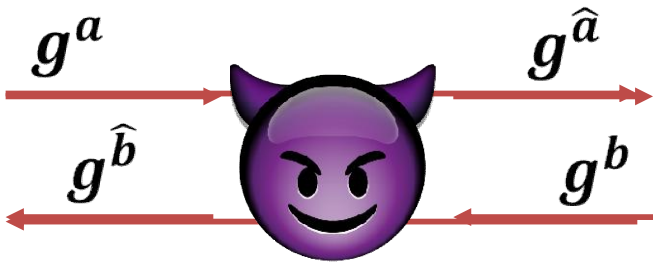
Alice's phone

Bob's phone

Man-in-the-Middle Attacks

- Impossible to detect without any setup

Alice's phone



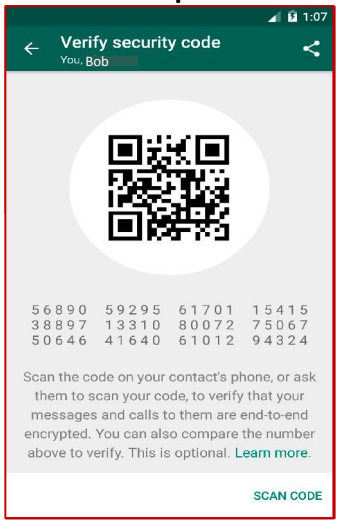
Bob's phone

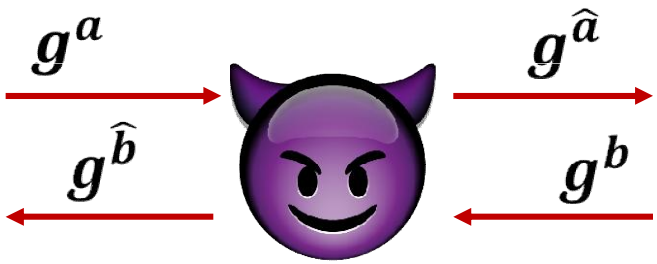
Impractical to assume a trusted PKI in messaging platforms…

Out-of-Band Authentication

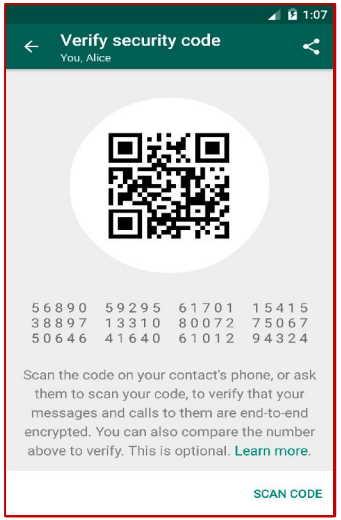
Practical to assume: Users can “out-of-band” authenticate one short value

Alice’s phone





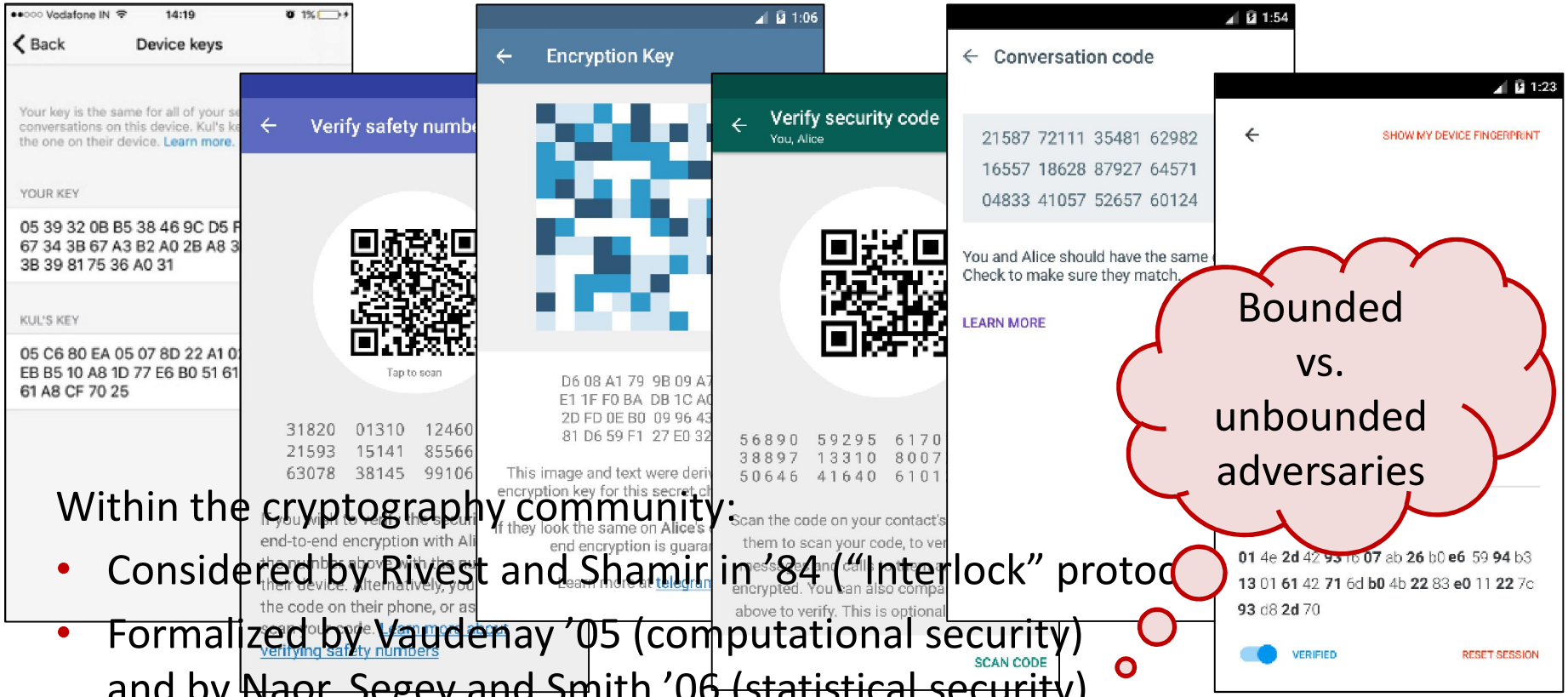
Bob’s phone



- Users can compare a short string displayed on their devices
- Assuming that they recognize each other’s voice, this is a low-bandwidth authenticated channel

Out-of-Band Authentication

Out-of-Band Authentication



Within the cryptography community:

- Considered by Rivest and Shamir in ’84 (“Interlock” protoc
- Formalized by Vaudenay ’05 (computational security) and by Naor, Segev and Smith ’06 (statistical security)

The User-to-User Setting

- An equivalent problem: Detecting MitM attacks in message authentication

Alice's phone

m

$\hat{m}$

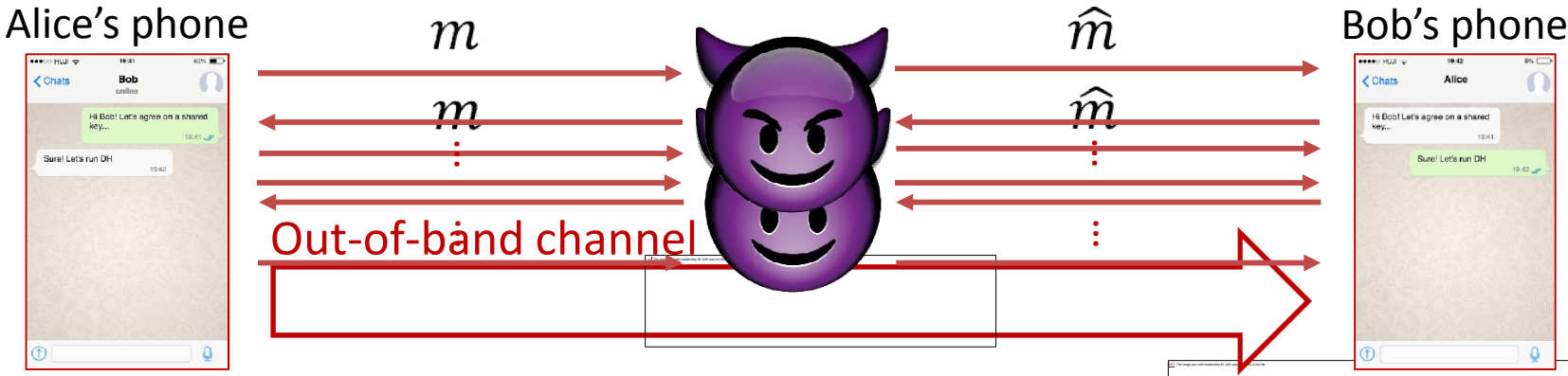
Bob's phone

Detect with prob. $1 - \epsilon$ whenever $\hat{m} \neq m$

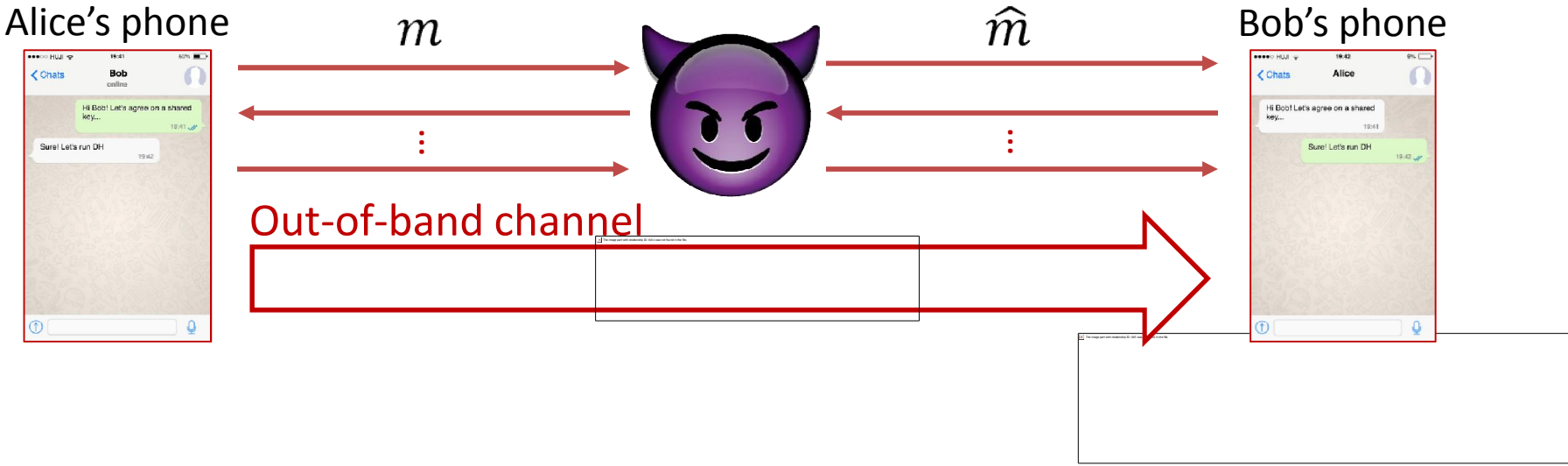
$\Rightarrow$ Given a shared key: MAC the message

$\Leftarrow$ Given a message authentication protocol: Run any key exchange protocol and authenticate the transcript

The User-to-User Setting



The User-to-User Setting



Minimize user effort ⟷ **Maximize security**

User-to-User Bounds

	Protocols	Lower Bounds
Computational Security [Vau05, PV06]	$\log(1/\epsilon)$	$\log(1/\epsilon) - O(1)$
Statistical Security [NSS06]	$2\log(1/\epsilon) + O(1)$	$2\log(1/\epsilon) - O(1)$

This Talk: The Group Setting

User-to-User Setting

✓ Tightly characterized

✓ Practical protocols deployed

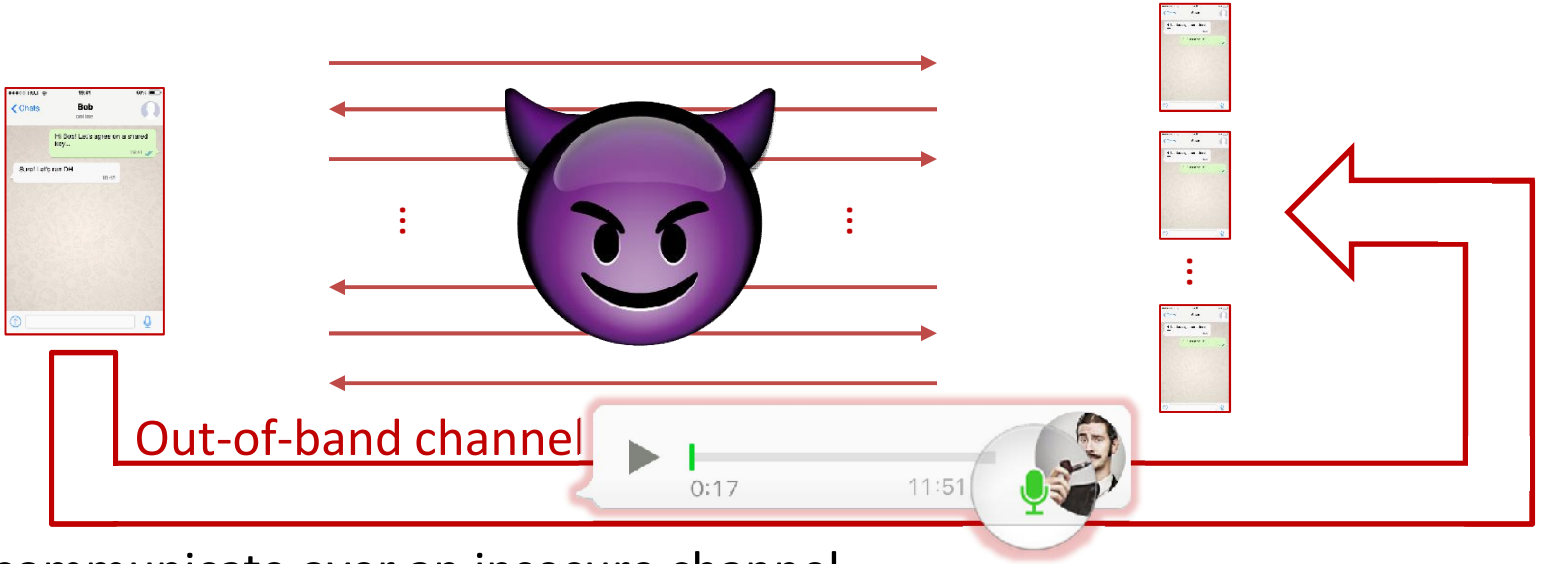
Group Setting

? Not yet studied

✗ Impractical protocols deployed

Our Contributions

A framework modeling out-of-band authentication in the group setting



- Users communicate over an insecure channel
- Group administrator can out-of-band authenticate one short value to all users
- Consistent with and supported by existing messaging platforms

Our Contributions

A framework modeling out-of-band authentication in the group setting

Tight bounds for out-of-band authentication in the group setting

	Protocols	Lower Bounds
Computational Security	$\log(1/\epsilon)$	

k – number of receivers

Our computationally-secure protocol is practically relevant,
and substantially improves the currently-deployed protocols:

E.g., $k = 32$ and $\epsilon = 2^{-80}$: $32 \times 85 = 2720$ bits vs. 85 bits!!

Talk Outline

- Communication model & notions of security
- The naïve protocol
- Our protocols & lower bounds

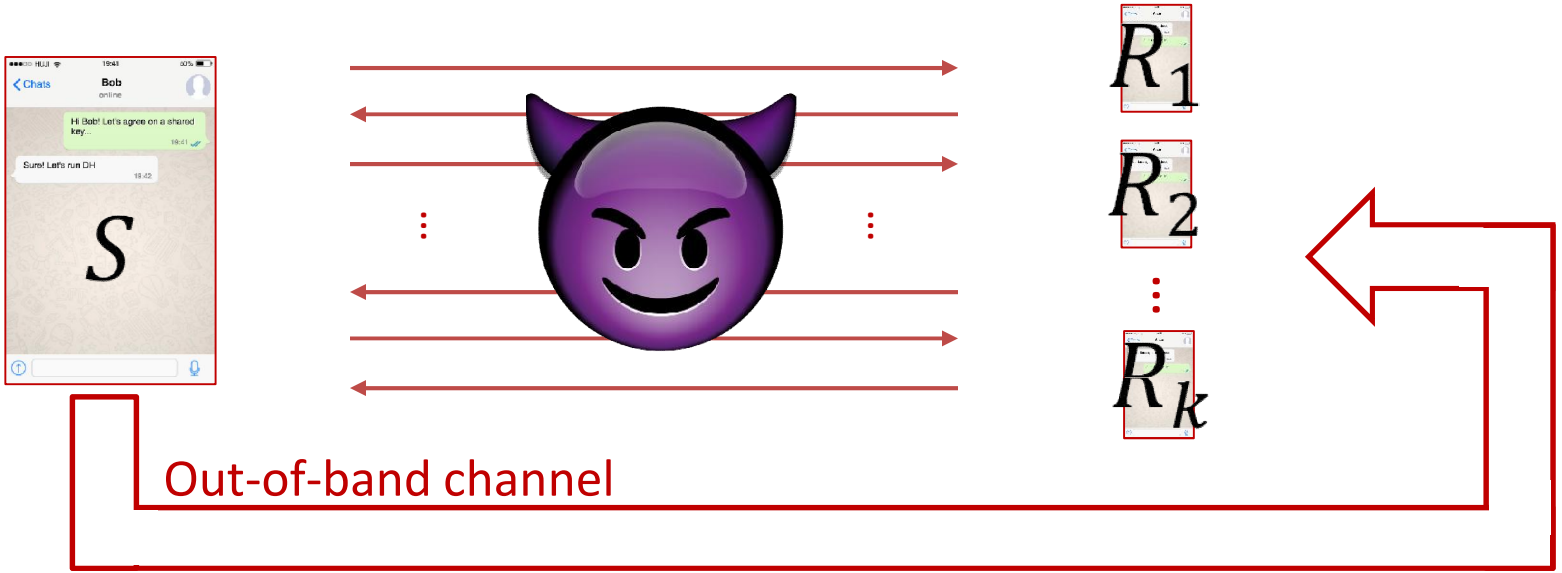
	Protocols	Lower Bounds
Computational Security	$\log(1/\epsilon)$	
Statistical Security	$(k+1)\cdot\left(\log(1/\epsilon)\right.$	

Talk Outline

- Communication model & notions of security
- The naïve protocol
- Our protocols & lower bounds

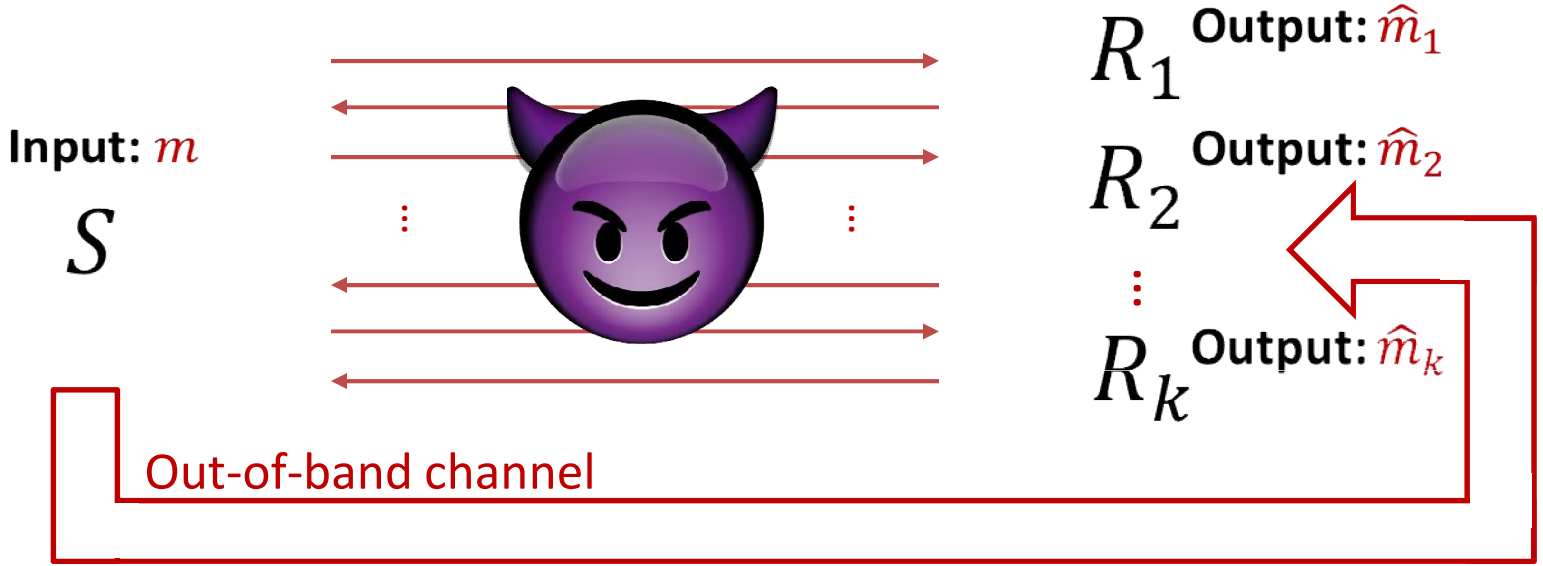
	Protocols	Lower Bounds
Computational Security	$\log(1/\epsilon)$	
Statistical Security	$(k+1)\cdot\left(\log(1/\epsilon)\right.$	

Communication Model



- Insecure channel: Adversary can read, remove and insert messages
- Out-of-band channel:
  Adversary can read, remove and delay messages, for all or for some of the users
  Adversary cannot modify messages/insert new ones in an undetectable manner

Correctness & Security



- **Correctness:** In an honest execution $\forall i\colon \hat{m}_i = m$
- **Unforgeability:** $\Pr[\exists i\colon \hat{m}_i \notin \{m, \perp\}] \leq \epsilon + \nu(\lambda)$
- Computational vs. statistical security

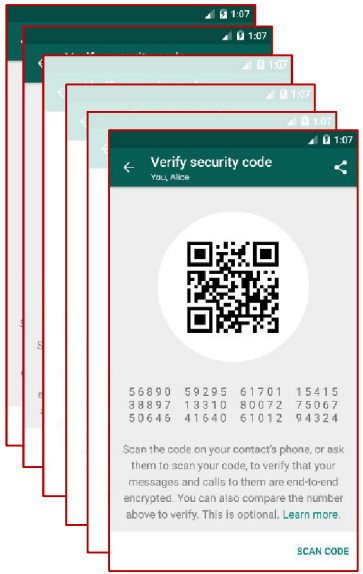
Talk Outline

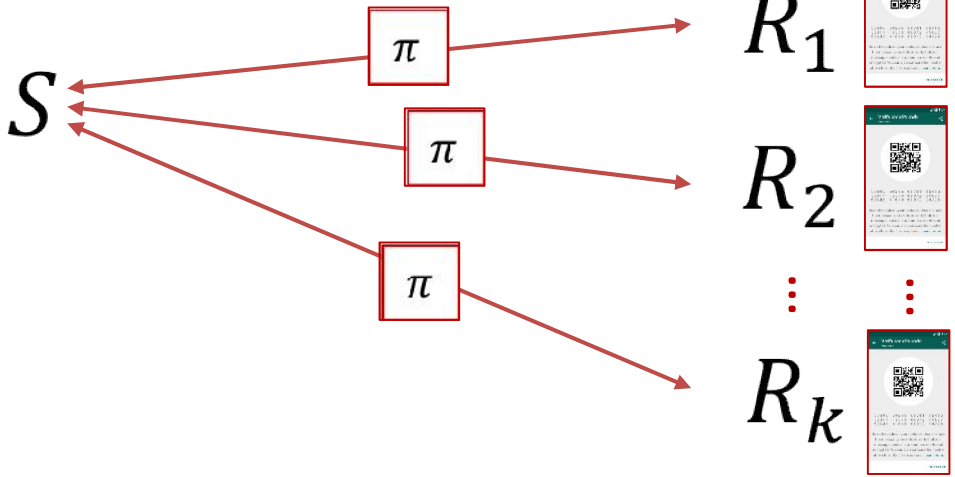
- Communication model & notions of security
- The naïve protocol
- Our protocols & lower bounds

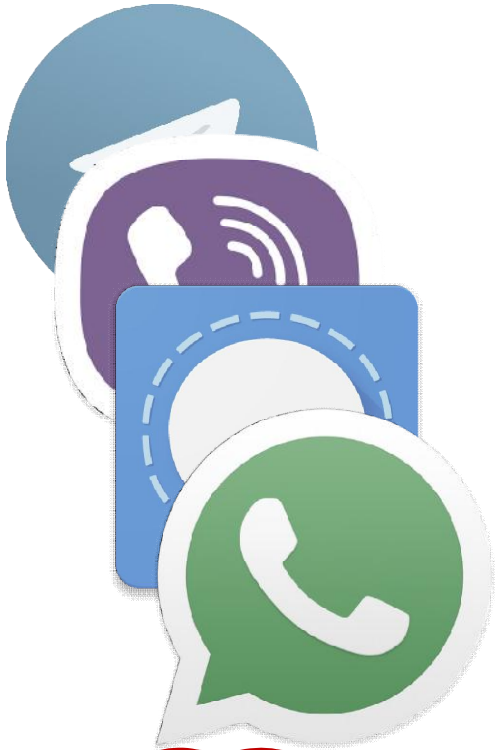
	Protocols	Lower Bounds
Computational Security	$\log(1/\epsilon)$	
Statistical Security	$(k+1)\cdot\left(\log(1/\epsilon)\right.$	

The Naïve Protocol

- Independently invoke a user-to-user protocol π with each R_i







- S out-of-band authenticates at least $k \cdot \log(k/\epsilon)$ bits
- E.g., $k = 32$ and $\epsilon = 2^{-80}$: $2{,}720$ bits
  $k = 2^{10}$ and $\epsilon = 2^{-80}$: $92{,}160$ bits

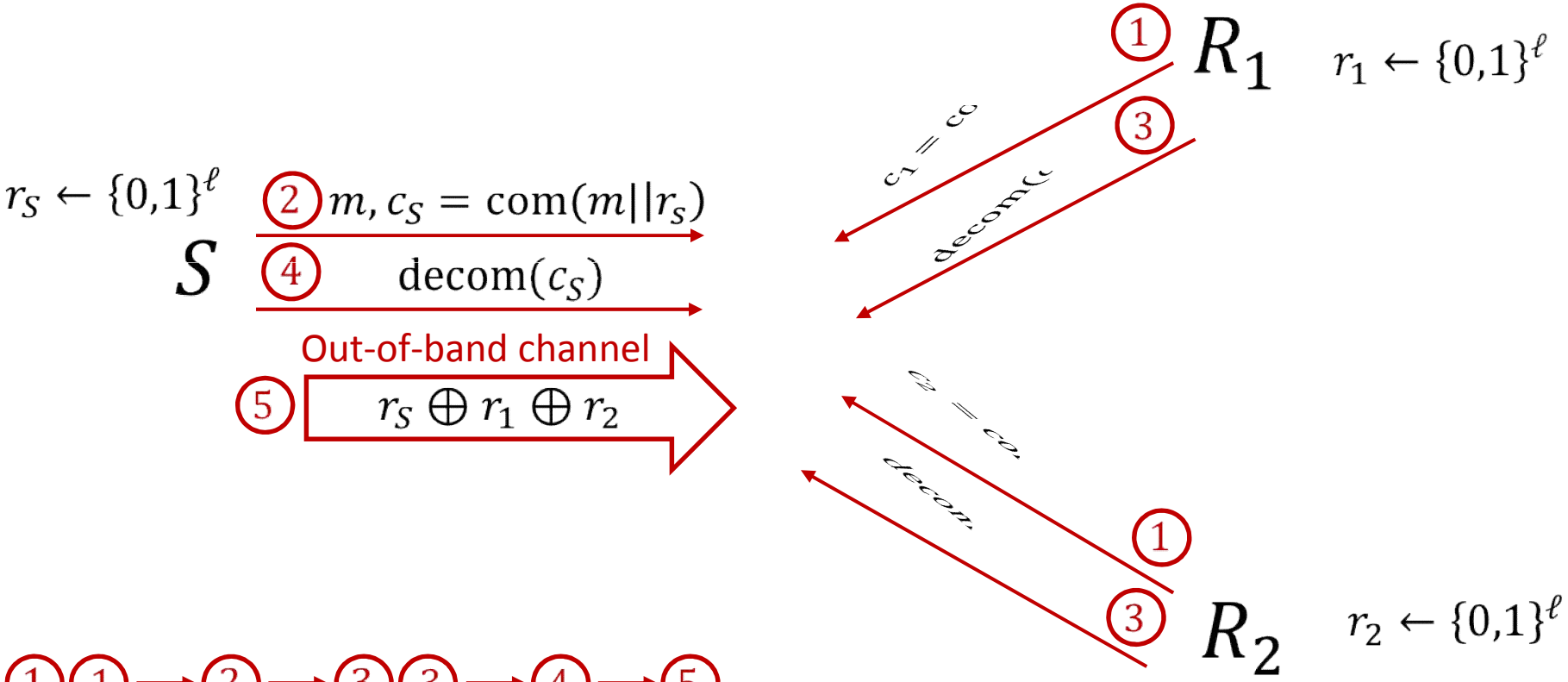
Seems impractical…

Talk Outline

- Communication model & notions of security
- The naïve protocol
- Our protocols & lower bounds

	Protocols	Lower Bounds
Computational Security	$\log(1/\epsilon)$	
Statistical Security	$(k+1)\cdot\left(\log(1/\epsilon)\right.$	

Our Computationally-Secure Protocol



1 1 → 2 → 3 3 → 4 → 5

Our Computationally-Secure Protocol

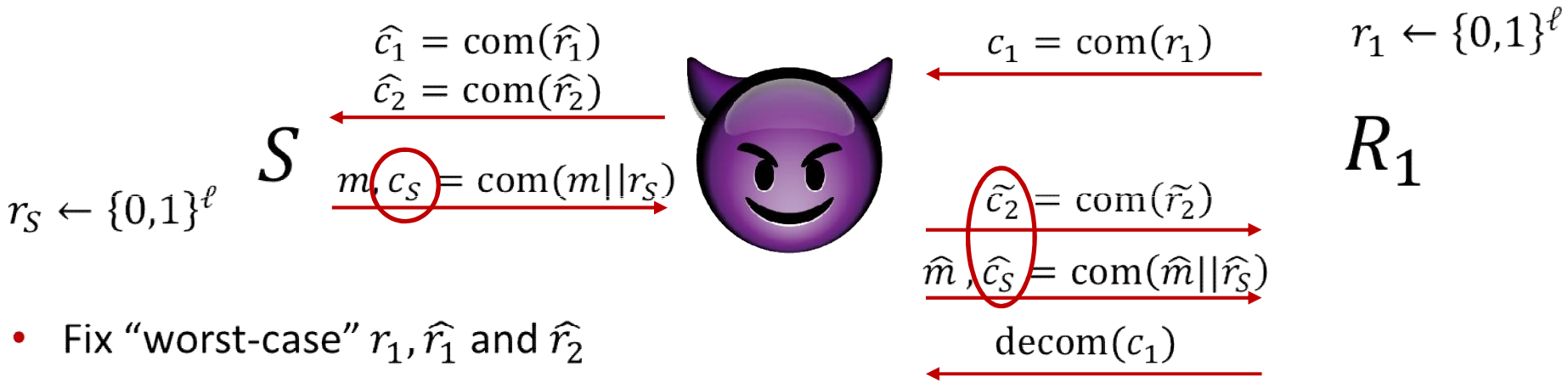
Theorem:
If $(\mathrm{com}, \mathrm{decom})$ is statistically-binding & concurrent non-malleable, then for any $k, \ell \in \mathbb{N}$ it holds that $\epsilon = k \cdot 2^{-\ell}$

Proof sketch:

- Focus individually on each receiver R_i
- Consider all possible synchronizations of a MitM attack
  - Today: Exemplify one notable attack
- Reduce each one to the security of the commitment scheme
  - Statistical binding or concurrent non-malleability

Example: One Possible Attack

- S chooses r_S before R_1 decommits

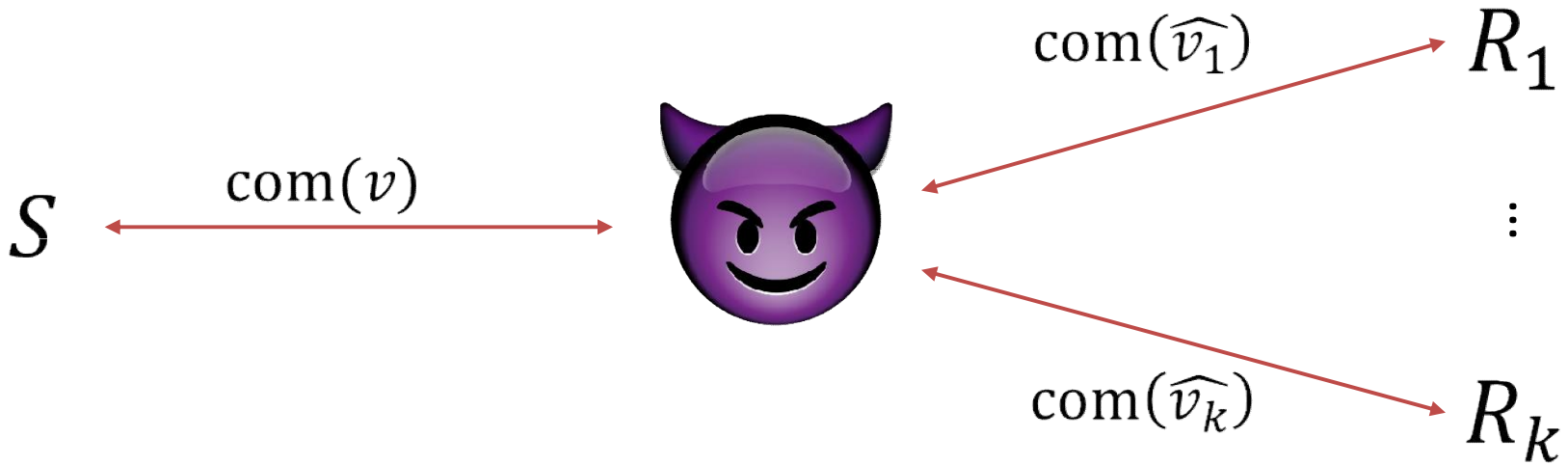


- Fix "worst-case" $r_1, \widehat{r_1}$ and $\widehat{r_2}$
- Attacker gets $\mathrm{com}(m||r_S)$ and needs to output $\mathrm{com}(\widetilde{r_2})$ and $\mathrm{com}(\widehat{m}||\widehat{r_S})$ such that $r_s \oplus \widehat{r_1} \oplus \widehat{r_2} = \widehat{r_S} \oplus r_1 \oplus \widetilde{r_2}$
- Concurrent non-malleability implies that either $m = \widehat{m}$ or

$$\Pr[r_s \oplus \widehat{r_1} \oplus \widehat{r_2} = \widehat{r_S} \oplus r_1 \oplus \widetilde{r_2}] = 2^{-\ell} + \nu(\lambda)$$

Concurrent Non-Malleable Commitments

- Infeasible to “non-trivially correlate” concurrent executions



- Extensive research leading to constant-round schemes from any one-way function [DDN91, …, PR05, PR06, LPV08, LP11, Goy11, GRRV14, GPR16, COSV17, …]
- Simple, efficient and non-interactive in the random-oracle model

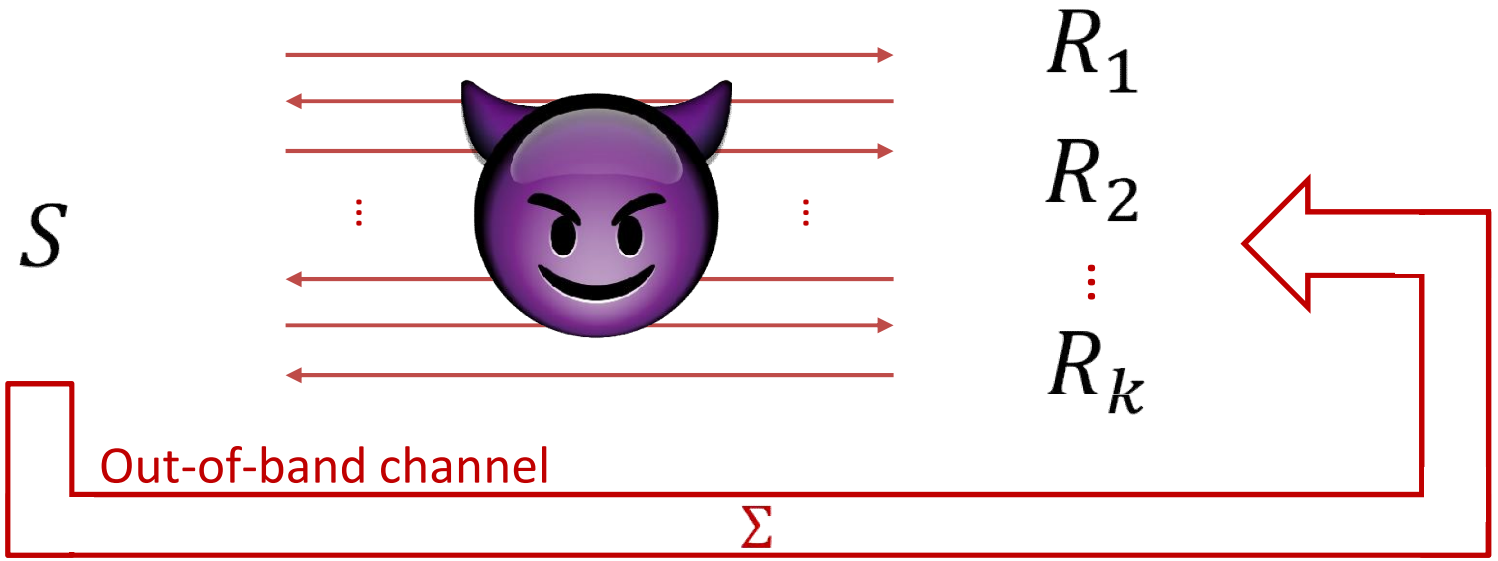
$$\mathrm{com}(v;r) = \mathrm{Hash}(v||r)$$

Talk Outline

- Communication model & notions of security
- The naïve protocol
- Our protocols & lower bounds

	Protocols	Lower Bounds
Computational Security	$\log(1/\epsilon)$	
Statistical Security	$(k+1)\cdot\left(\log(1/\epsilon)\right)$	

Our Statistical Lower Bound

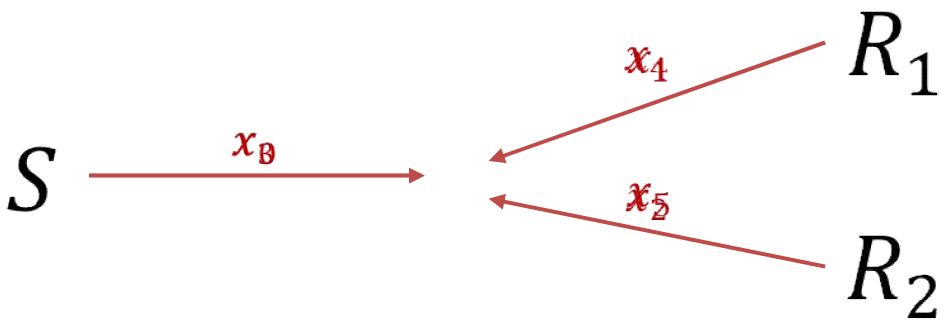


- Denote by Σ the out-of-band value in an honest execution with a random m
- During any execution Σ's Shannon entropy decreases from $H(\Sigma)$ to 0
- **Intuition [NSS06]:** Each party must "independently reduce" at least $\log(1/\epsilon)$ bits from $H(\Sigma)$

$k = \Rightarrow H(\Sigma) \geq (k+1) \cdot \log(1/\epsilon)$

Protocol Structure

- Assume that the protocol has t rounds over the insecure channel
- In each round i a single party is "active" and sends a message x_i
  - If $i \equiv 0 \bmod (k+1)$ then S is active
  - Otherwise, $R_{i \bmod (k+1)}$ is active



Understanding $H(\Sigma)$

- Random variables $M, X_0, \dots, X_{t-1}, \Sigma$
- Split $H(\Sigma)$ according to the marginal contribution of each round:

$$H(\Sigma) = H(\Sigma) - H(\Sigma|M, X_0) + H(\Sigma|M, X_0) - H(\Sigma|M, X_0, X_1) + H(\Sigma|M, X_0, X_1)$$
$$- \dots - H(\Sigma|M, X_0, \dots, X_{t-1}) + H(\Sigma|M, X_0, \dots, X_{t-1})$$

$$= I(\Sigma; M, X_0) + \sum_{j \in [t]: j \equiv 0 \bmod (k+1)} I(\Sigma; X_j | M, X_0, \dots, X_{j-1}) + \sum_{i \in [k]} \sum_{j \equiv i \bmod (k+1)} I(\Sigma; X_j | M, X_0, \dots, X_{j-1}) + H(\Sigma|M, X_0, \dots, X_{t-1})$$

Entropy reduction by S

Entropy reduction by R_i

Understanding $H(\Sigma)$

Lemma 1:
There exists a man-in-the-middle attacker that succeeds with probability

$$\epsilon_0 \geq 2^{-\left(I(\Sigma;M,X_0)+\sum_{j\equiv 0 \bmod (k+1)} I\left(\Sigma;X_j\middle|M,X_0,\ldots,X_{j-1}\right)+H(\Sigma|M,X_0,\ldots,X_{t-1})\right)}$$

Lemma 2:
For every $i \in [k]$ there exists a man-in-the-middle attacker that succeeds with probability

$$\epsilon_i \geq 2^{-\sum_{j\equiv i \bmod (k+1)} I\left(\Sigma;X_j\middle|M,X_0,\ldots,X_{j-1}\right)}$$

Lower Bounding $H(\Sigma)$

- We present $k+1$ attacks that succeed with probabilities $\epsilon_0, \ldots, \epsilon_k$ such that

$$2^{-H(\Sigma)-k} \leq \prod_{i=0}^{k} \epsilon_i$$

- The security of the protocol guarantees that

$$\prod_{i=0}^{k} \epsilon_i \leq \epsilon^{k+1}$$

$$\Downarrow$$

$$H(\Sigma) \geq (k+1) \cdot \log(1/\epsilon) - k$$

Summary

A framework modeling out-of-band authentication in the group setting

Tight bounds for out-of-band authentication in the group setting

	Protocols	Lower Bounds
Computational Security	$\log(1/\epsilon)$	
Statistical Security	$(k+1)\cdot\left(\log(1/\epsilon)\right.$	

Thank You!

https://eprint.iacr.org/2018/493