Multi-party Off-the-Record Messaging

Ian Goldberg* Berkant Ustaoğlu†
Matthew D. Van Gundy‡ Hao Chen‡

*University of Waterloo

†NTT Information Sharing Platform Laboratories

‡University of California, Davis

16th ACM Conference on Computer and Communications Security

The Chicago Outfit

Boss

Al **Capone**

Bootlegging

Bugs Moran

Gambling

Paul **Ricca**

Extortion

Machine Gun **Mc Gurn**

The Chicago Outfit

The Law

Eliot **Ness**

Boss

Al **Capone**

Bootlegging

Bugs Moran

Gambling

Paul **Ricca**

Extortion

Machine Gun **Mc Gurn**

The Chicago Outfit

The Law

Eliot **Ness**

Boss

Al **Capone**

Bootlegging

Bugs Moran

Gambling

Paul **Ricca**

Extortion

Machine Gun **Mc Gurn**

The *Secret* Life of the American Stool Pigeon

Bugs

Ricca

Capone

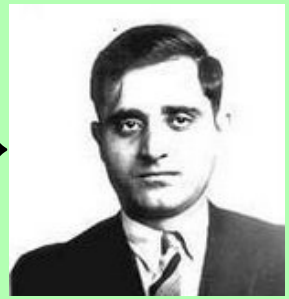
Ness

McGurn

The *Secret* Life of the American Stool Pigeon

Bugs

M



Ricca

Capone

M

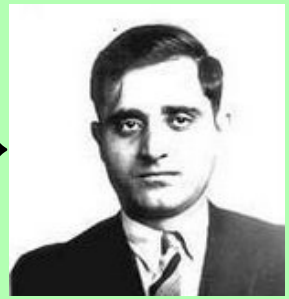
Ness

McGurn

The *Secret* Life of the American Stool Pigeon

Bugs

M



Ricca

Bugs: M

Capone

M

Bugs: M

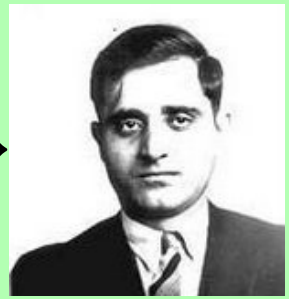
Ness

McGurn

The *Secret* Life of the American Stool Pigeon

Bugs

M



Ricca

Bugs: M

Capone

M

Bugs: M

Ness

McGurn

Bugs: M

The *Secret* Life of the American Stool Pigeon

Bugs

Ricca

Capone

Ness here.

Ness here.

Ness

McGurn

The *Secret* Life of the American Stool Pigeon

Bugs

Ricca

Capone

And, . . .

Capone. . .

Ness

McGurn

The *Secret* Life of the American Stool Pigeon

Bugs

Ricca

Capone

Protect me

Ness

McGurn

The *Secret* Life of the American Stool Pigeon

Bugs

Ricca

Capone

Protect me

Protect my family

Ness

McGurn

The *Secret* Life of the American Stool Pigeon

Bugs

Ricca

Capone

Only you

Only you

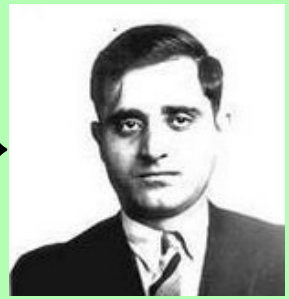
Ness

McGurn

The *Secret* Life of the American Stool Pigeon

Bugs

Ness: Protect family



Ricca

Capone

Only you

Only you

Ness

McGurn

The *Secret* Life of the American Stool Pigeon

Bugs

Ricca

Capone

Ok

Ok

Ness

McGurn

The *Secret* Life of the American Stool Pigeon

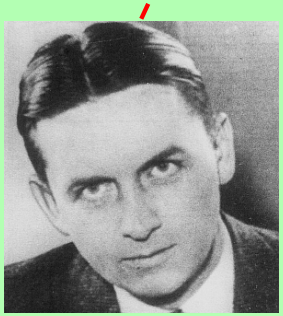
$x \wedge \neg y$

Bugs

Ricca

$\neg x \wedge y$

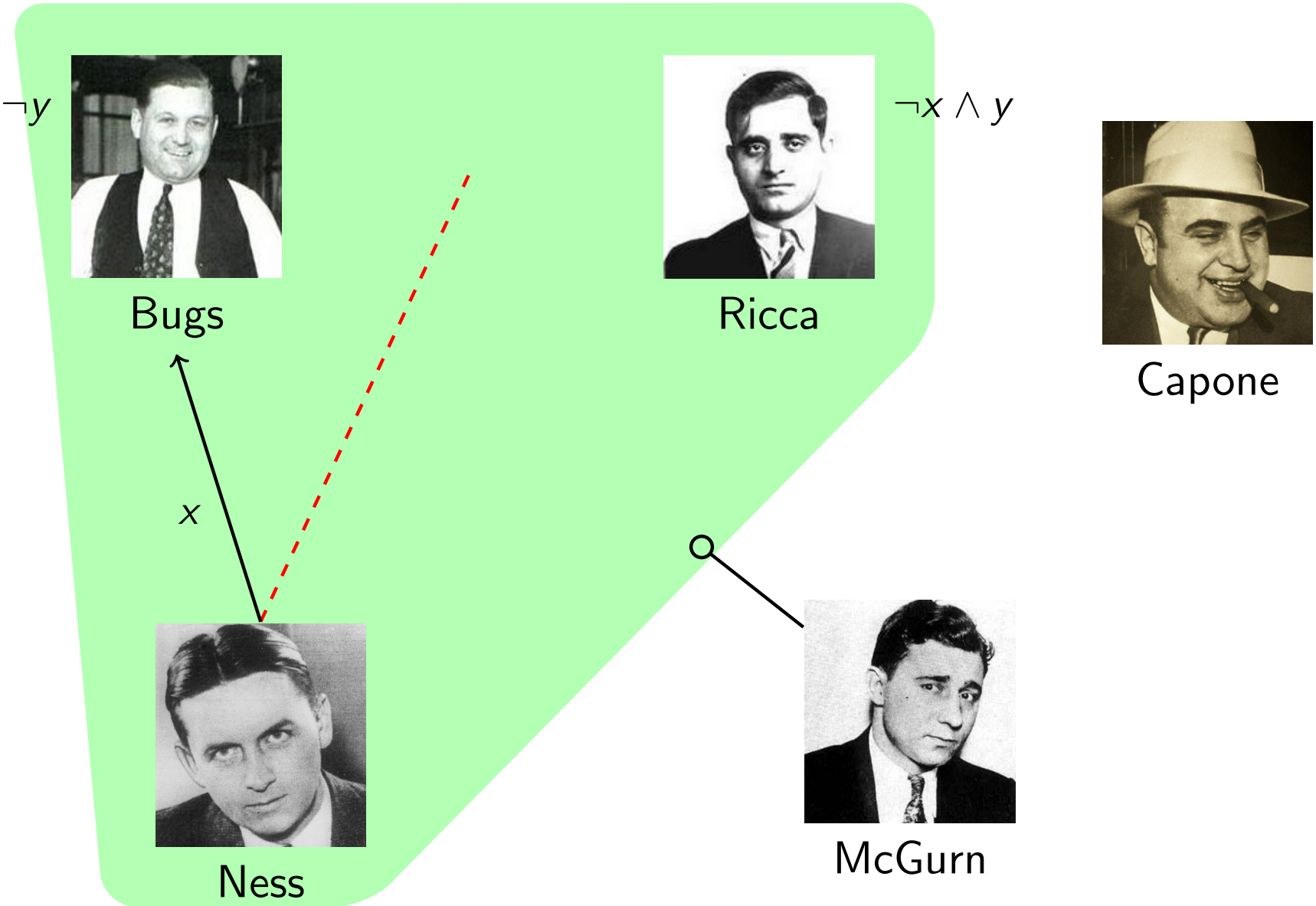
Capone



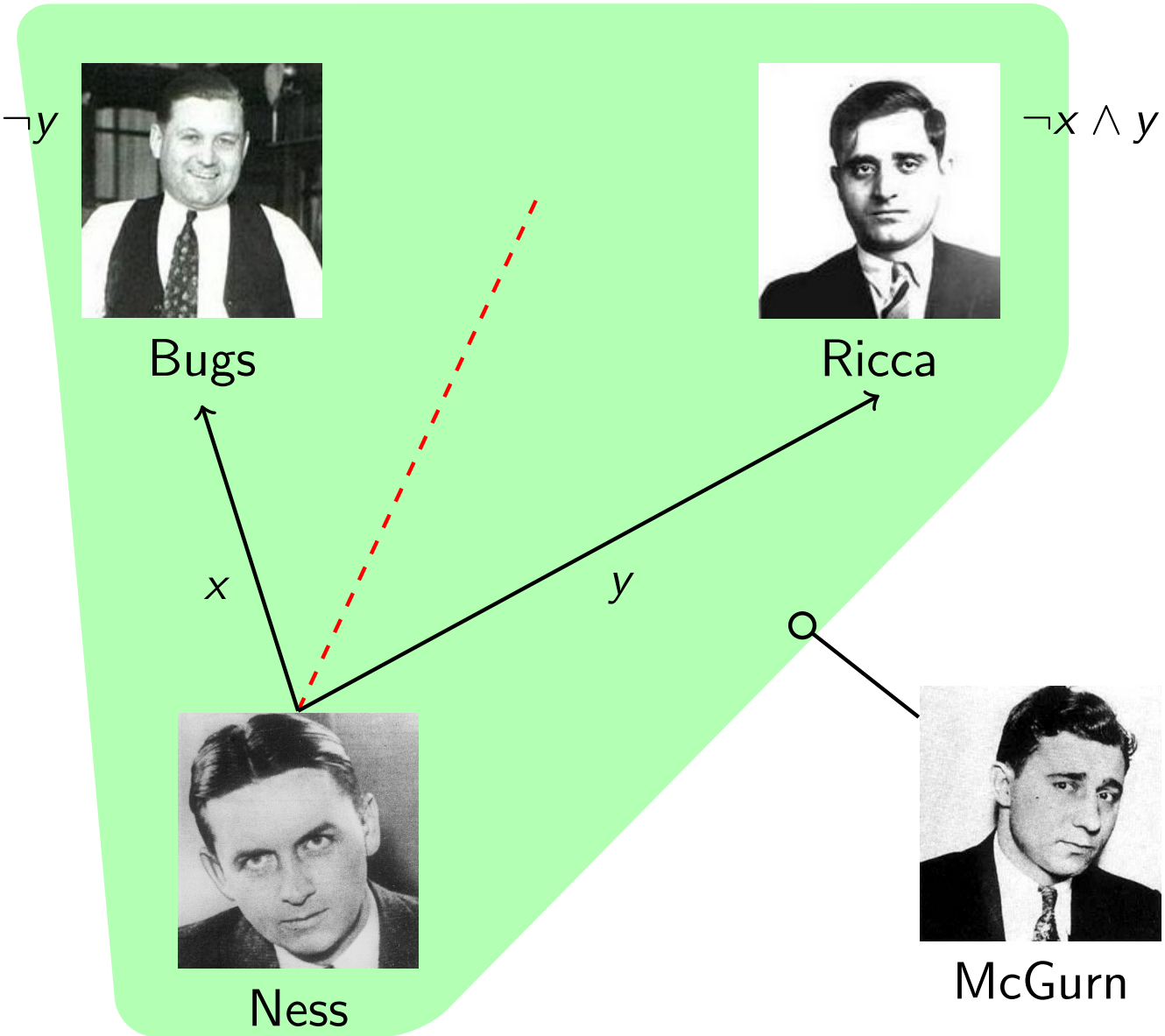
Ness

McGurn

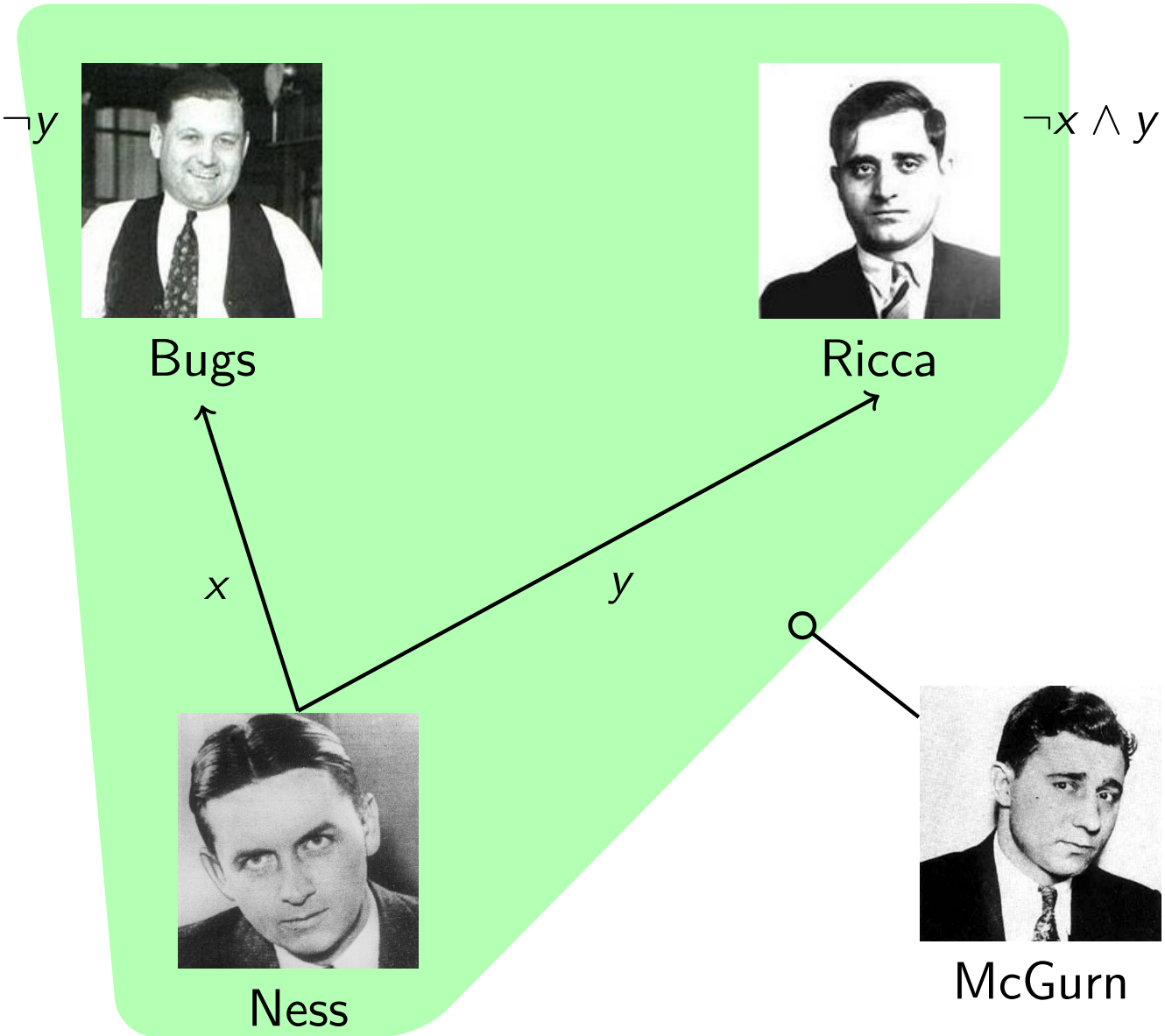
The *Secret* Life of the American Stool Pigeon



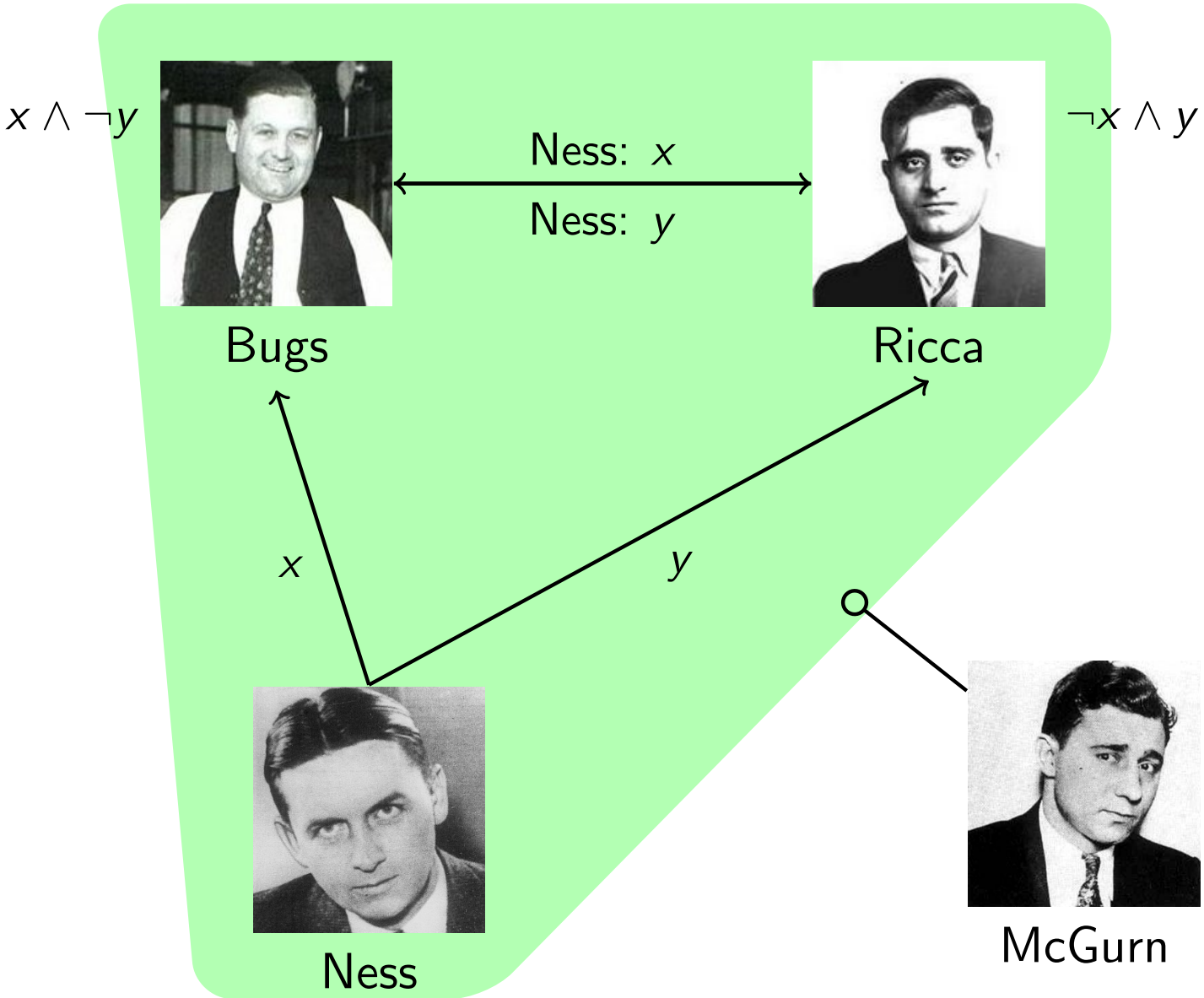
The *Secret* Life of the American Stool Pigeon



The *Secret* Life of the American Stool Pigeon



The *Secret* Life of the American Stool Pigeon



The *Secret* Life of the American Stool Pigeon

Bugs

Ricca

Capone

M

M'

Ness

McGurn

The *Secret* Life of the American Stool Pigeon

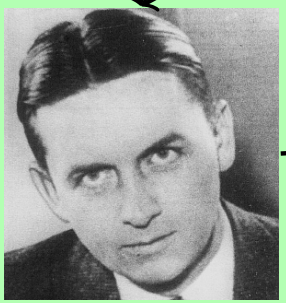
Bugs

Ricca

Capone

M

M'



Ness

Bugs: M
Ricca: M'

McGurn

The *Secret* Life of the American Stool Pigeon

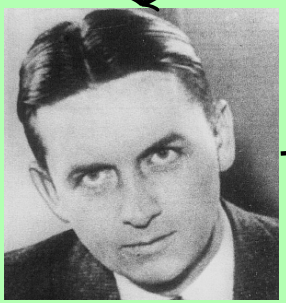
Bugs

Ricca

Capone

M

M'



Ness

Bugs: M
Ricca: M'

McGurn

Bugs: M
Ricca: M'

The *Secret* Life of the American Stool Pigeon

Bugs

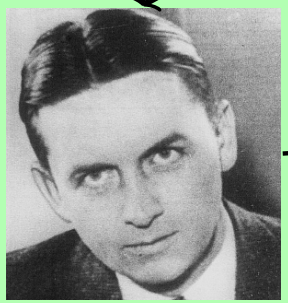
Ricca

Bugs: M
Ricca: M'

Capone

M

M'



Ness

Bugs: M
Ricca: M'

McGurn

Bugs: M
Ricca: M'

The *Secret* Life of the American Stool Pigeon

Bugs

Ricca

Bugs: M
Ricca: M'

Capone

Ness

McGurn

The *Secret* Life of the American Stool Pigeon

Bugs

Ricca

Bugs: M
Ricca: M'

Capone

Ness

McGurn

Bugs: Z
Ricca: Z'

The *Secret* Life of the American Stool Pigeon

Bugs

Ricca

Bugs: M
Ricca: M'

Bugs: Z
Ricca: Z'

Capone

Ness

McGurn

Bugs: Z
Ricca: Z'

The *Secret* Life of the American Stool Pigeon

Bugs

Ricca

Bugs: M
Ricca: M'

Bugs: Z
Ricca: Z'

Capone

Ness

McGurn

Bugs: M
Ricca: Z'

The *Secret* Life of the American Stool Pigeon

Bugs

Ricca

Bugs: M
Ricca: M'

Bugs: Z
Ricca: Z'

Capone

Bugs: M
Ricca: Z'

Ness

McGurn

Bugs: M
Ricca: Z'

System Requirements and Threat Model

Requirements

- Confidentiality
- Entity Authentication
- Origin Authentication
- Consensus
- (Limited) Non-Repudiation
- Plausible Deniability
  - Forgeability
  - Malleability

The Adversary

- Has full control of the network
- Corrupts up to $n - 1$ participants
- Delivers wire transcripts and corrupt participant state to the Judge

The Judge

- Distinguishes legitimate transcripts from forgeries
- Given: transcript, corrupt participant state, all long-lived

Partial Solutions

- PGP
  - Employs digital signatures for non-repudiation
  - Allows proving authorship to a third-party
- Two-party Off-the-Record Communication
  - All confidentiality and authenticity based on shared secret
  - Symmetric capabilities allow impersonation

Overview

We achieve Multi-party Off-the-Record Messaging through:

- Generate per-session ephemeral signing keys
- Deniable signature key exchange (DSKE)
- Generate shared group encryption key
- Until membership change:
  - Communicate via authenticated encryption
- Detect consensus violations

Deniable Signature Key Exchange (DSKE)

Guarantees Bugs (respectively Ricca) that:

- He is indeed talking to Ricca
- Ricca has chosen PK_R as ephemeral signature key for session *sid*
- Ricca knows private key SK_R corresponding to PK_R
- A corrupt Ricca cannot prove to Capone that PK_B is Bugs's key

Given

- Deniable Key Exchange (Di Raimondo and Gennaro CCS 2006)
- Authenticated Encryption
- Secure Public-Key Signature Scheme

Deniable Signature Key Exchange (DSKE)

B: PK_B, SK_B

Deniable Signature Key Exchange (DSKE)

B: PK_B, SK_B
R: PK_R, SK_R

Deniable Signature Key Exchange (DSKE)

$$
\begin{array}{rl}
\text{B:} & PK_B, SK_B \\
\text{R:} & PK_R, SK_R \\
\text{B} \leftrightarrow \text{R:} & k \leftarrow DKA(B, R)
\end{array}
$$

Deniable Signature Key Exchange (DSKE)

	B:	PK_B, SK_B
	R:	PK_R, SK_R
B $\leftrightarrow$ R:		$k \leftarrow DKA(B, R)$
B $\rightarrow$ R:		$AE_k(sid, B, R, PK_B)$

Deniable Signature Key Exchange (DSKE)

	B:	PK_B, SK_B
	R:	PK_R, SK_R
B $\leftrightarrow$ R:		$k \leftarrow DKA(B, R)$
B $\rightarrow$ R:		$AE_k(sid, B, R, PK_B)$
R $\rightarrow$ B:		$AE_k(sid, R, B, PK_R)$

Deniable Signature Key Exchange (DSKE)

$$
\begin{array}{rl}
\text{B:} & PK_B, SK_B \\
\text{R:} & PK_R, SK_R \\
\text{B} \leftrightarrow \text{R:} & k \leftarrow DKA(B, R) \\
\text{B} \rightarrow \text{R:} & AE_k(sid, B, R, PK_B) \\
\text{R} \rightarrow \text{B:} & AE_k(sid, R, B, PK_R) \\
\text{B} \rightarrow \text{R:} & AE_k(\ Sign_{SK_B}(sid, B, R, PK_R)\ )
\end{array}
$$

Deniable Signature Key Exchange (DSKE)

$$
\begin{array}{rl}
\text{B:} & PK_B, SK_B \\
\text{R:} & PK_R, SK_R \\
\text{B} \leftrightarrow \text{R:} & k \leftarrow DKA(B, R) \\
\text{B} \rightarrow \text{R:} & AE_k(sid, B, R, PK_B) \\
\text{R} \rightarrow \text{B:} & AE_k(sid, R, B, PK_R) \\
\text{B} \rightarrow \text{R:} & AE_k(\ Sign_{SK_B}(sid, B, R, PK_R)\ ) \\
\text{R} \rightarrow \text{B:} & AE_k(\ Sign_{SK_R}(sid, R, B, PK_B)\ )
\end{array}
$$

Deniable Signature Key Exchange (DSKE)

B: PK_B, SK_B

R: PK_R, SK_R

B $\leftrightarrow$ R: $k \leftarrow DKA(B, R)$

B $\rightarrow$ R: $AE_k(sid, B, R, PK_B)$

R $\rightarrow$ B: $AE_k(sid, R, B, PK_R)$

B $\rightarrow$ R: $AE_k(\ Sign_{SK_B}(sid, B, R, PK_R)\ )$

R $\rightarrow$ B: $AE_k(\ Sign_{SK_R}(sid, R, B, PK_B)\ )$

B: Upon validating values from R:

associate PK_R to Ricca for *sid*

Deniable Signature Key Exchange (DSKE)

	B:	PK_B, SK_B
	R:	PK_R, SK_R
B $\leftrightarrow$ R:		$k \leftarrow DKA(B, R)$
B $\rightarrow$ R:		$AE_k(sid, B, R, PK_B)$
R $\rightarrow$ B:		$AE_k(sid, R, B, PK_R)$
B $\rightarrow$ R:		$AE_k(\ Sign_{SK_B}(sid, B, R, PK_R)\ )$
R $\rightarrow$ B:		$AE_k(\ Sign_{SK_R}(sid, R, B, PK_B)\ )$
	B:	Upon validating values from R:
		associate PK_R to Ricca for *sid*
	R:	Upon validating values from B:
		associate PK_B to Bugs for *sid*

Session Initiation

Guarantees to each participant

- The identity of every other participant
- The ephemeral pubic key PK_* of each other participant
- A shared symmetric encryption key gk
- The protocol parameters negotiated before session initiation
- Consensus all of the above

Session Initiation

Bugs

Ricca

Ness

Session Initiation

PK_B

Bugs

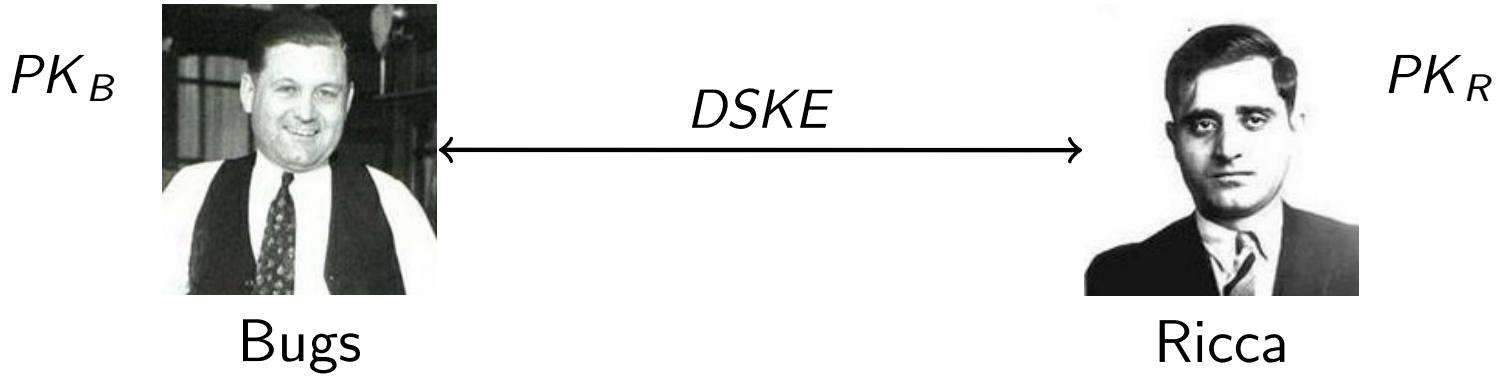
PK_R

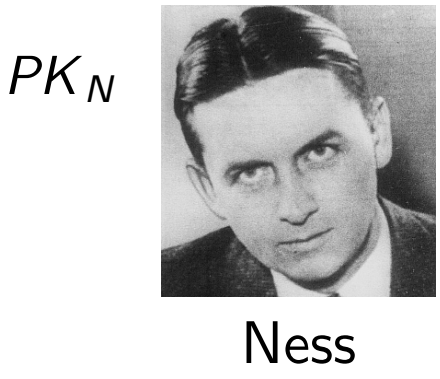
Ricca

PK_N

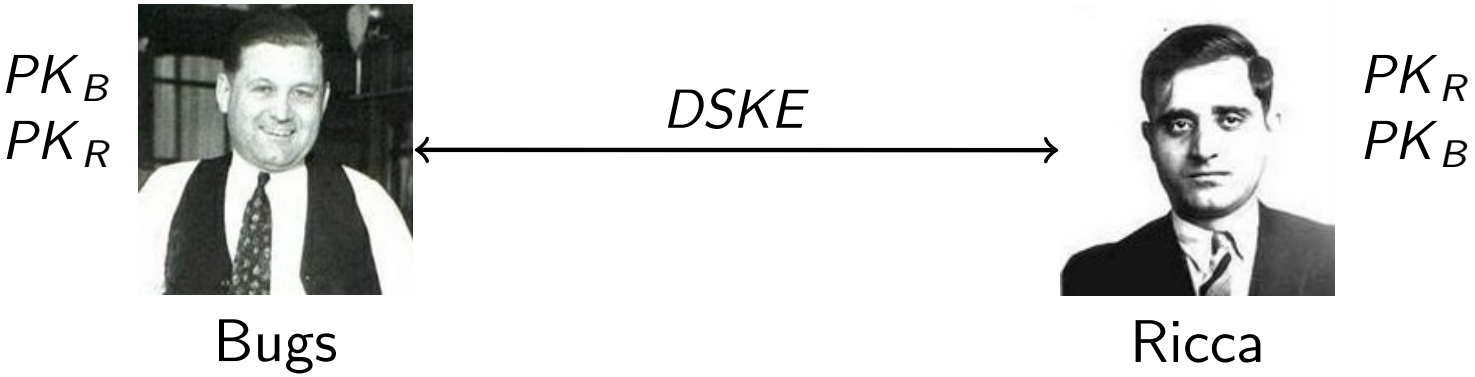
Ness

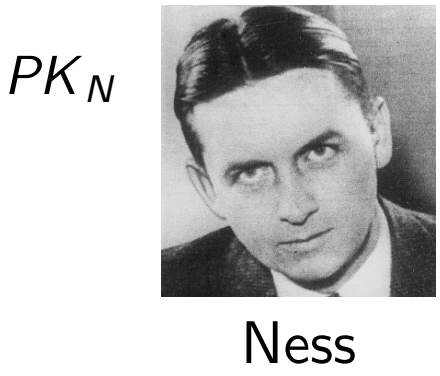
Session Initiation





Session Initiation





Session Initiation

PK_B
PK_R

Bugs

PK_R
PK_B

Ricca

$DSKE$

PK_N

Ness

Session Initiation

PK_B
PK_R, PK_N

Bugs

Ricca

PK_R
PK_B

DSKE

PK_N
PK_B

Ness

Session Initiation

PK_B
PK_R, PK_N

Bugs

PK_R
PK_B

Ricca

DSKE

PK_N
PK_B

Ness

Session Initiation

PK_B
PK_R, PK_N

Bugs

Ricca

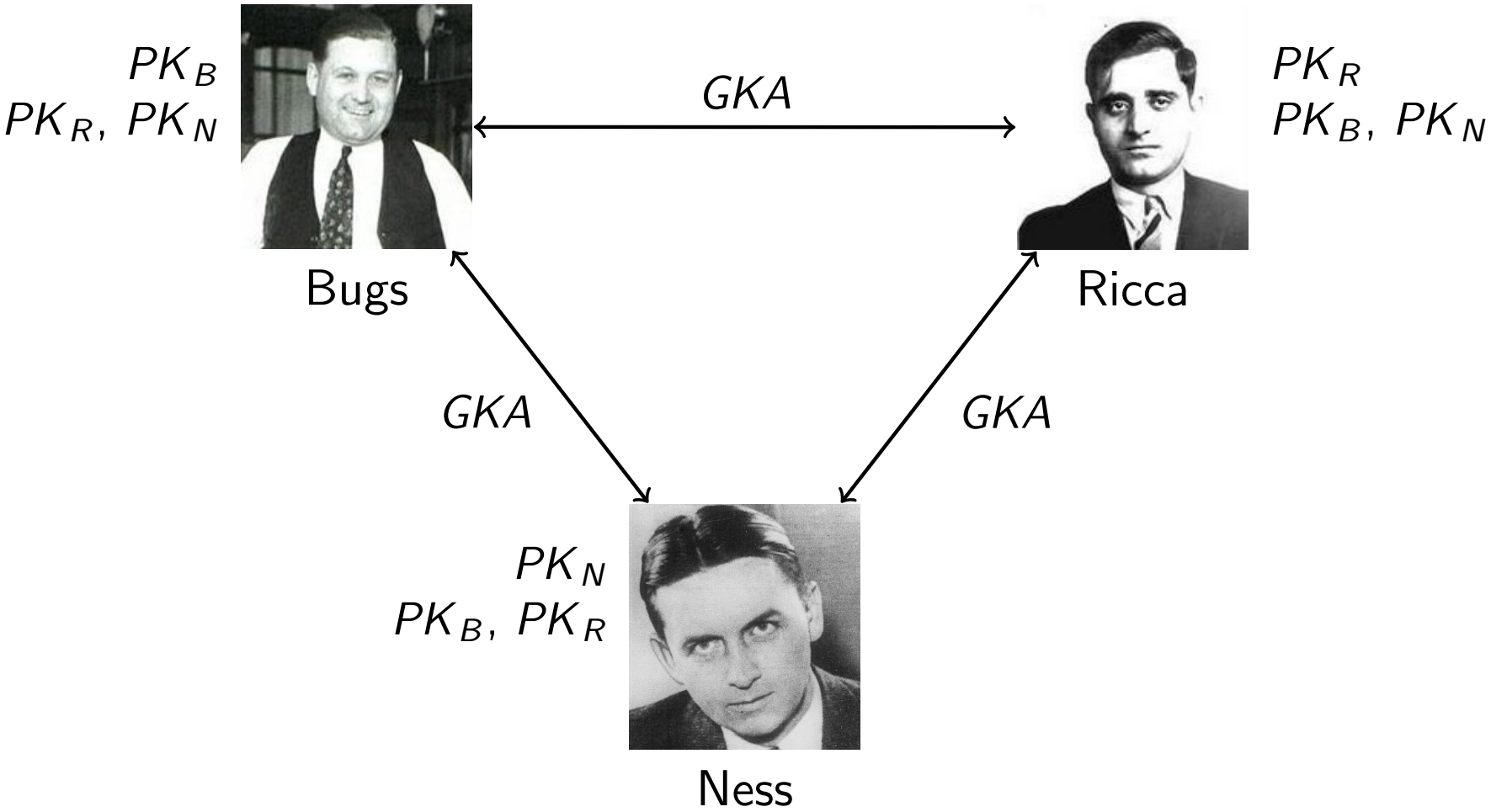
PK_R
PK_B, PK_N

DSKE

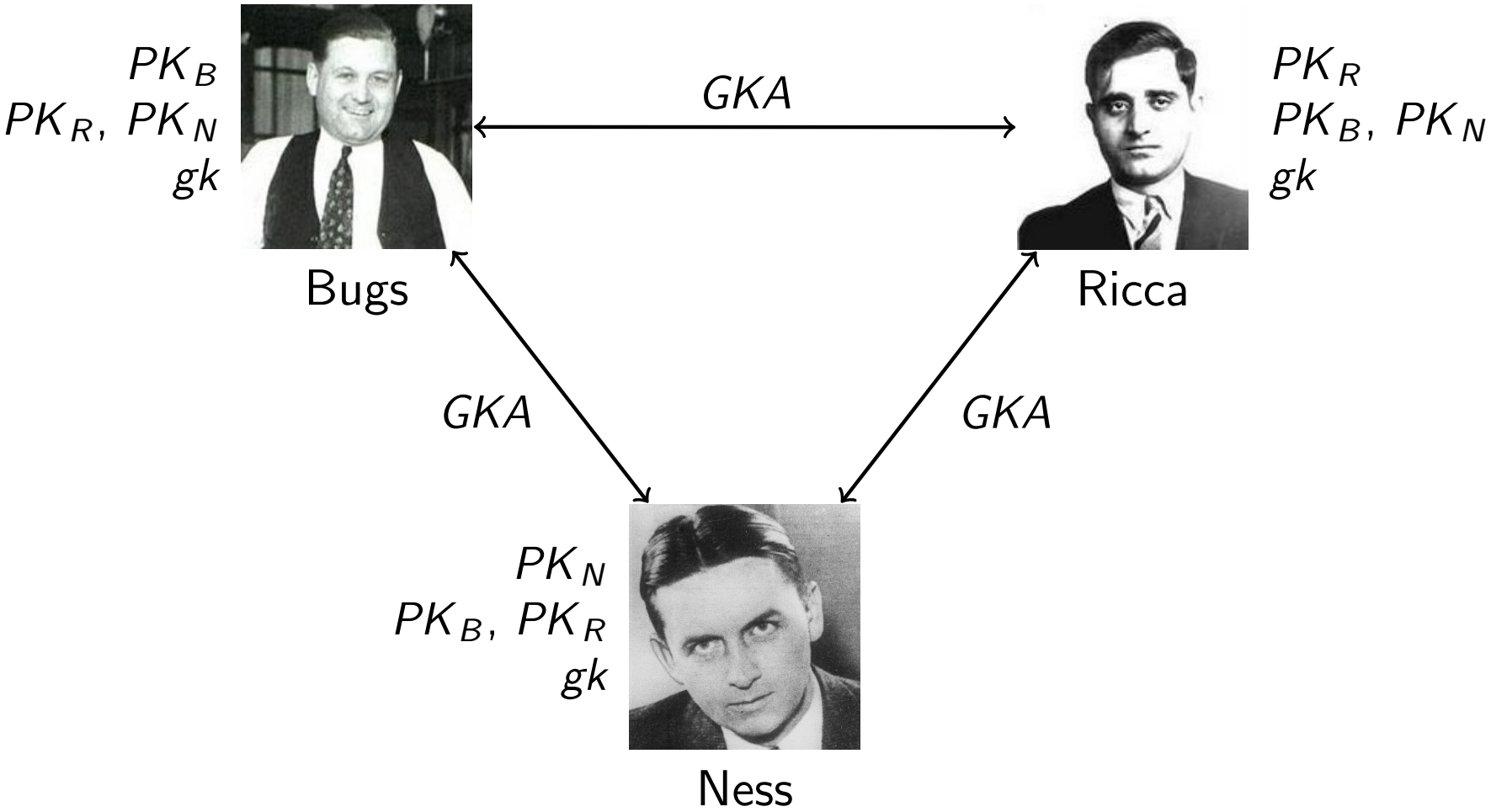
PK_N
PK_B, PK_R

Ness

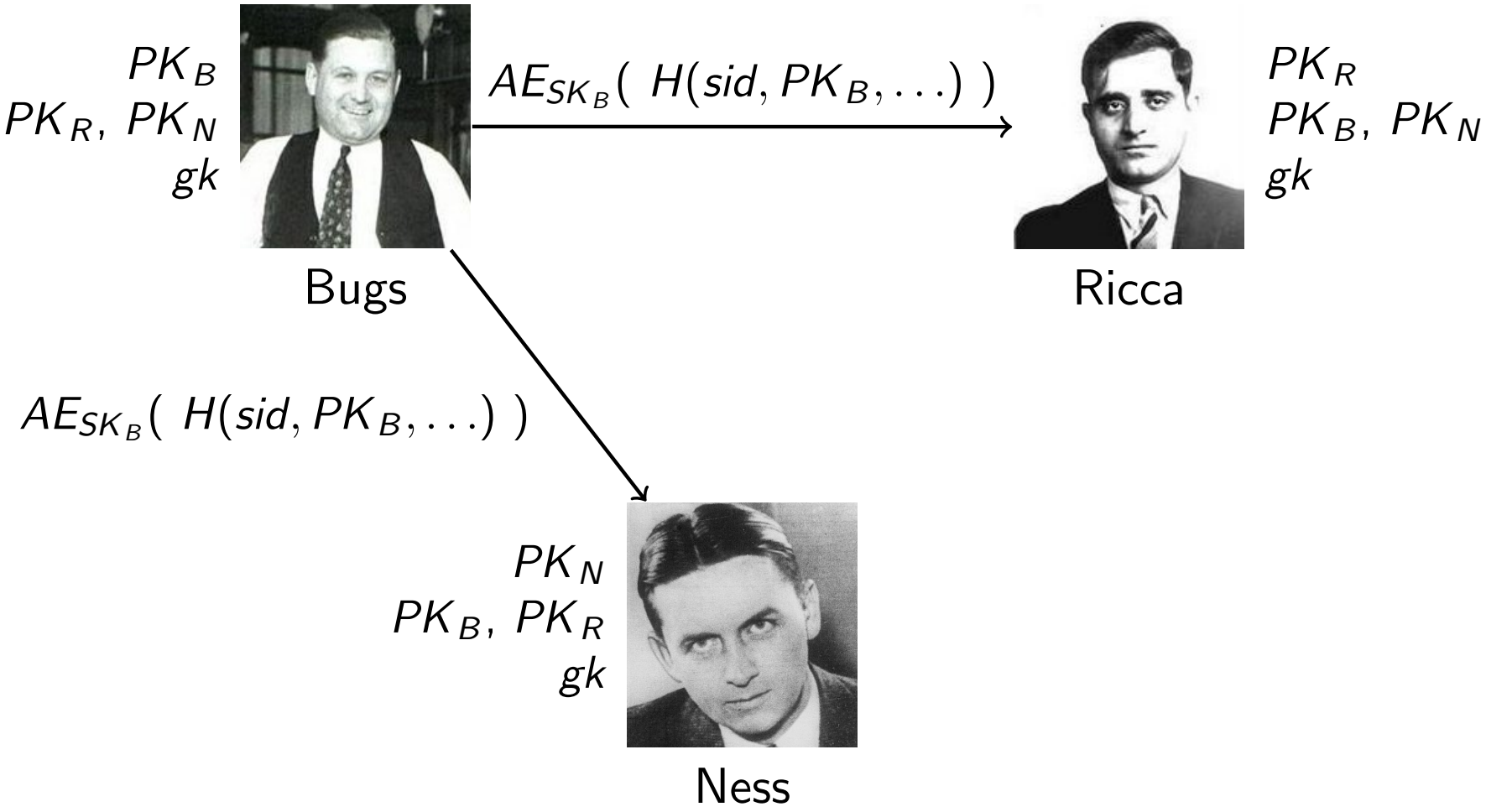
Session Initiation



Session Initiation



Session Initiation



Session Initiation

Guarantees to each participant

- The identity of every other participant
- The ephemeral pubic key PK_* of each other participant
- A shared symmetric encryption key gk
- The protocol parameters negotiated before session initiation
- Consensus all of the above

Session Initiation

Guarantees to each participant

- The identity of every other participant DSKE
- The ephemeral pubic key PK_* of each other participant DSKE
- A shared symmetric encryption key gk
- The protocol parameters negotiated before session initiation
- Consensus all of the above

Session Initiation

Guarantees to each participant

- The identity of every other participant — DSKE
- The ephemeral pubic key PK_* of each other participant — DSKE
- A shared symmetric encryption key gk — GKA
- The protocol parameters negotiated before session initiation
- Consensus all of the above

Session Initiation

Guarantees to each participant

- The identity of every other participant — DSKE
- The ephemeral pubic key PK_* of each other participant — DSKE
- A shared symmetric encryption key gk — GKA
- The protocol parameters negotiated before session initiation — Attest
- Consensus all of the above — Attest

Session Initiation

Guarantees to each participant

- The identity of every other participant — DSKE
- The ephemeral pubic key PK_* of each other participant — DSKE
- A shared symmetric encryption key gk — GKA
- The protocol parameters negotiated before session initiation — Attest
- Consensus all of the above — Attest

Performance

- DSKE: $O(n^2)$
- GKA: $O(n)$
- Attest: $O(n)$

Sending Messages

Guarantees to the recipient

- Confidentiality
- Origin Authentication

PK_B, PK_N, PK_R, gk

Bugs

Performance

- One symmetric key encryption
- One public key signature

PK_R, PK_N, PK_B, gk

Ricca

PK_N, PK_B, PK_R, gk

Ness

Sending Messages

Guarantees to the recipient

- Confidentiality
- Origin Authentication

PK_B, PK_N, PK_R, gk
Bugs: M

Bugs

Performance

- One symmetric key encryption
- One public key signature

PK_R, PK_N, PK_B, gk

Ricca

PK_N, PK_B, PK_R, gk

Ness

Sending Messages

Guarantees to the recipient

- Confidentiality
- Origin Authentication

PK_B, PK_N, PK_R, gk
Bugs: M
$\mathcal{C} \leftarrow Encrypt_{gk}(M)$

Bugs

Performance

- One symmetric key encryption
- One public key signature

PK_R, PK_N, PK_B, gk

Ricca

PK_N, PK_B, PK_R, gk

Ness

Sending Messages

Guarantees to the recipient

- Confidentiality
- Origin Authentication

PK_B, PK_N, PK_R, gk
Bugs: M
$\mathcal{C} \leftarrow Encrypt_{gk}(M)$
$\sigma \leftarrow Sign_{SK_B}(sid, \mathcal{C})$

Bugs

Performance

- One symmetric key encryption
- One public key signature

PK_R, PK_N, PK_B, gk

Ricca

PK_N, PK_B, PK_R, gk

Ness

Sending Messages

Guarantees to the recipient

- Confidentiality
- Origin Authentication

Performance

- One symmetric key encryption
- One public key signature

PK_B, PK_N, PK_R, gk
Bugs: M
$\mathcal{C} \leftarrow Encrypt_{gk}(M)$
$\sigma \leftarrow Sign_{SK_B}(sid, \mathcal{C})$

Bugs

$sid, \mathcal{C}, \sigma$

Ricca

PK_R, PK_N, PK_B, gk

$sid, \mathcal{C}, \sigma$

Ness

PK_N, PK_B, PK_R, gk

Sending Messages

Guarantees to the recipient

- Confidentiality
- Origin Authentication

Performance

- One symmetric key encryption
- One public key signature

PK_B, PK_N, PK_R, gk
Bugs: M
$\mathcal{C} \leftarrow Encrypt_{gk}(M)$
$\sigma \leftarrow Sign_{SK_B}(sid, \mathcal{C})$

Bugs

$sid, \mathcal{C}, \sigma$

Ricca

PK_R, PK_N, PK_B, gk
if $Verify_{PK_B}(sid, \mathcal{C}, \sigma)$:

$sid, \mathcal{C}, \sigma$

Ness

PK_N, PK_B, PK_R, gk
if $Verify_{PK_B}(sid, \mathcal{C}, \sigma)$:

Sending Messages

Guarantees to the recipient

- Confidentiality
- Origin Authentication

Performance

- One symmetric key encryption
- One public key signature

PK_B, PK_N, PK_R, gk
Bugs: M
$\mathcal{C} \leftarrow Encrypt_{gk}(M)$
$\sigma \leftarrow Sign_{SK_B}(sid, \mathcal{C})$

Bugs

$sid, \mathcal{C}, \sigma$

Ricca

PK_R, PK_N, PK_B, gk
if $Verify_{PK_B}(sid, \mathcal{C}, \sigma)$:
$M \leftarrow Decrypt_{gk}(\mathcal{C})$

$sid, \mathcal{C}, \sigma$

Ness

PK_N, PK_B, PK_R, gk
if $Verify_{PK_B}(sid, \mathcal{C}, \sigma)$:
$M \leftarrow Decrypt_{gk}(\mathcal{C})$

Sending Messages

Guarantees to the recipient

- Confidentiality
- Origin Authentication

Performance

- One symmetric key encryption
- One public key signature

PK_B, PK_N, PK_R, gk
Bugs: M
$\mathcal{C} \leftarrow Encrypt_{gk}(M)$
$\sigma \leftarrow Sign_{SK_B}(sid, \mathcal{C})$

Bugs

$sid, \mathcal{C}, \sigma$

Ricca

PK_R, PK_N, PK_B, gk
if $Verify_{PK_B}(sid, \mathcal{C}, \sigma)$:
$M \leftarrow Decrypt_{gk}(\mathcal{C})$
Bugs: M

$sid, \mathcal{C}, \sigma$

Ness

PK_N, PK_B, PK_R, gk
if $Verify_{PK_B}(sid, \mathcal{C}, \sigma)$:
$M \leftarrow Decrypt_{gk}(\mathcal{C})$
Bugs: M

Ending a Session

Guarantees to each participant

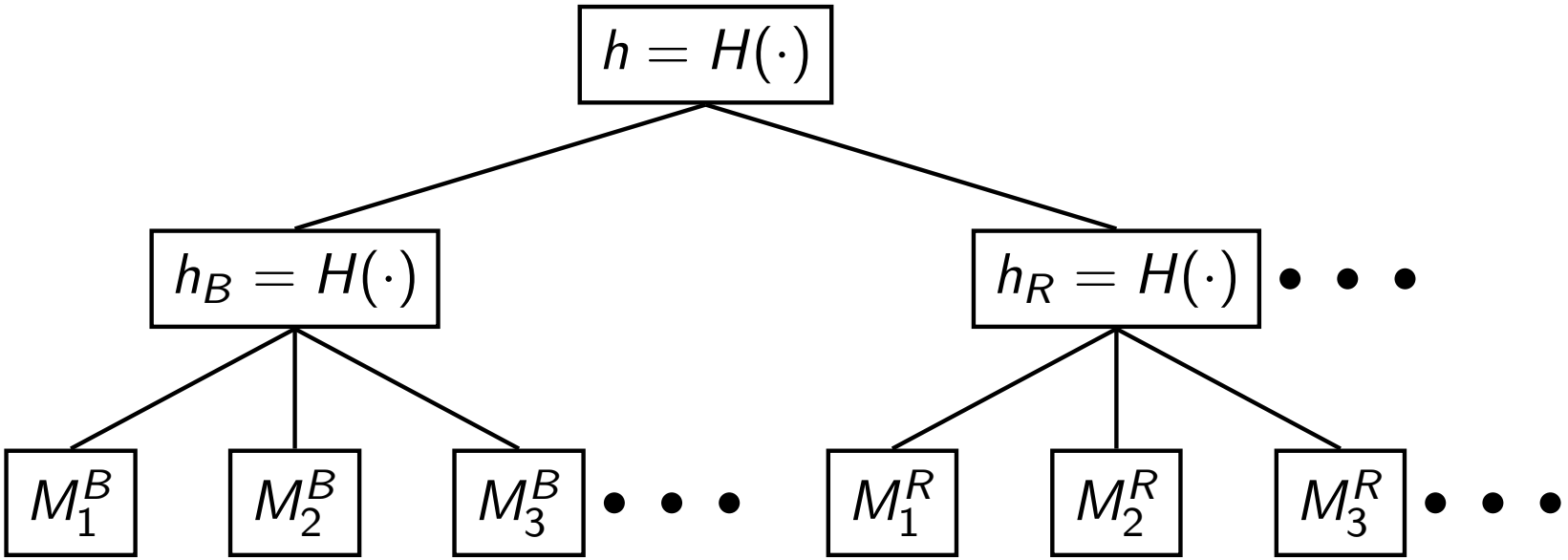
- Confidentiality of previous messages
- Confidentiality of subsequent messages
- Detection of consensus violations
- Publication of ephemeral signature keys

Procedure

- Each participant calculates a digest over all messages (h)
- Participants exchange digests using authenticated encryption
- Publish ephemeral signing key if digests received from all other participants

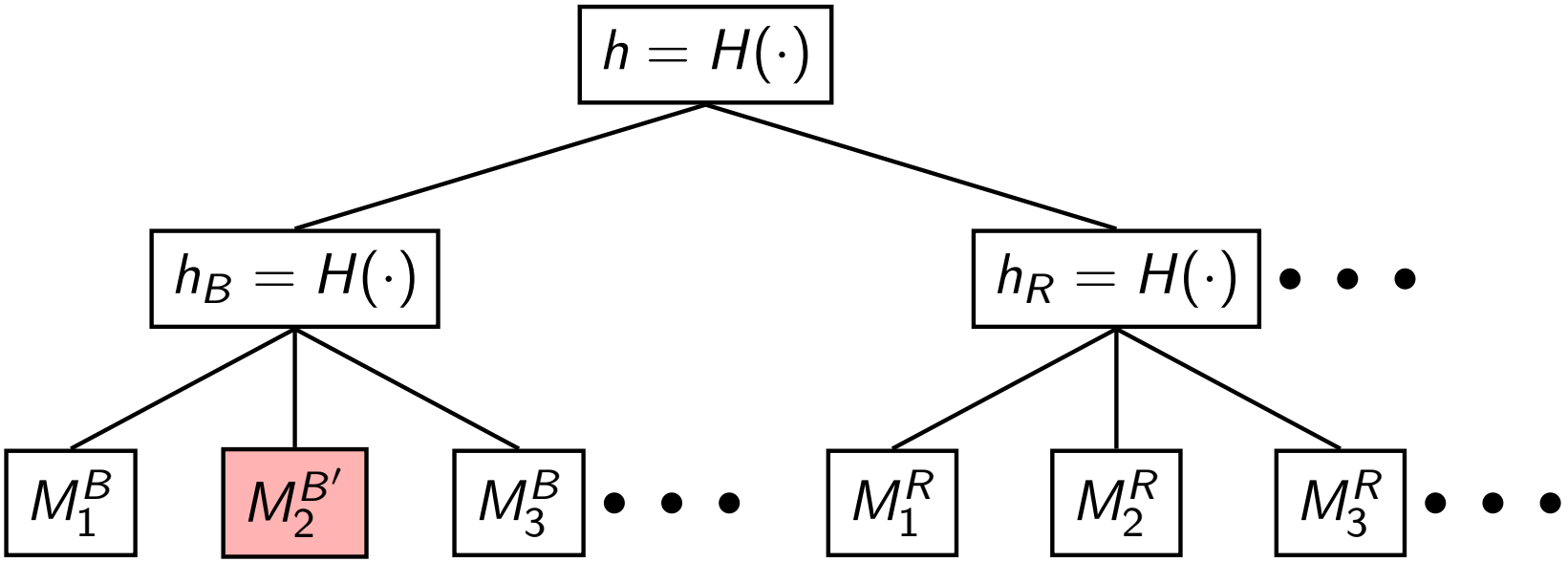
Detecting Consensus Violations

Each participant forms a Merkle hash tree over all messages:



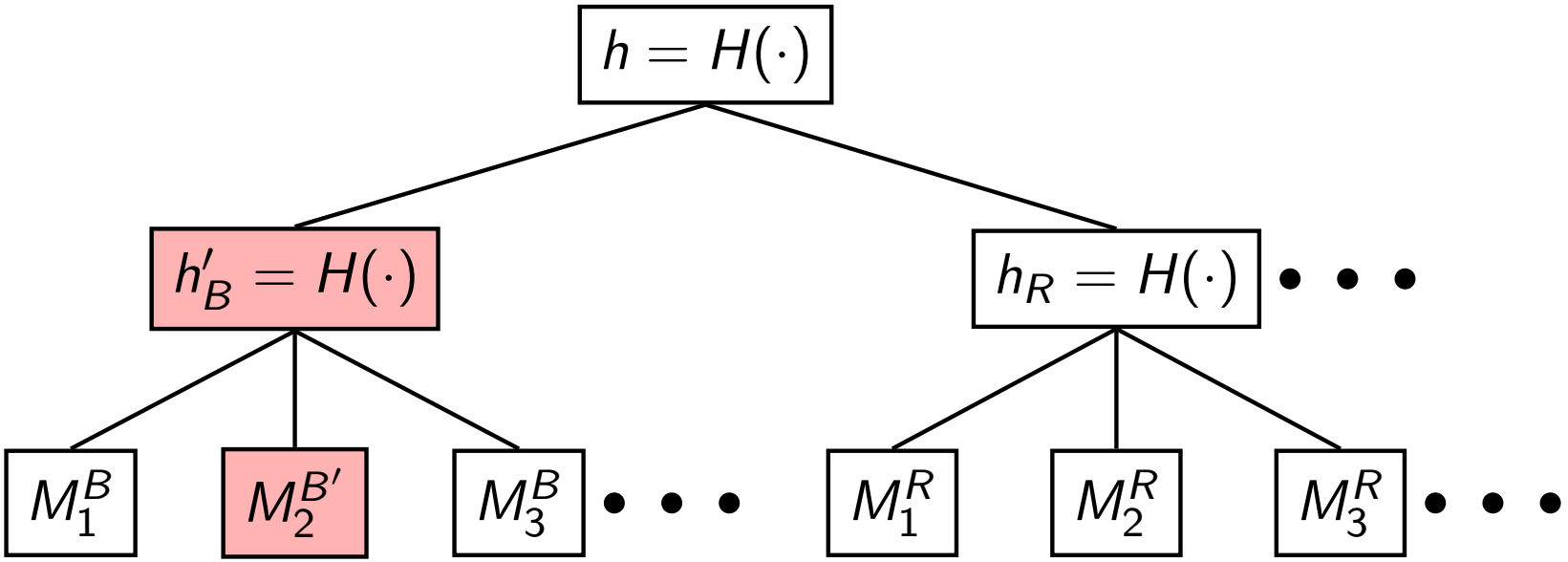
Detecting Consensus Violations

Each participant forms a Merkle hash tree over all messages:



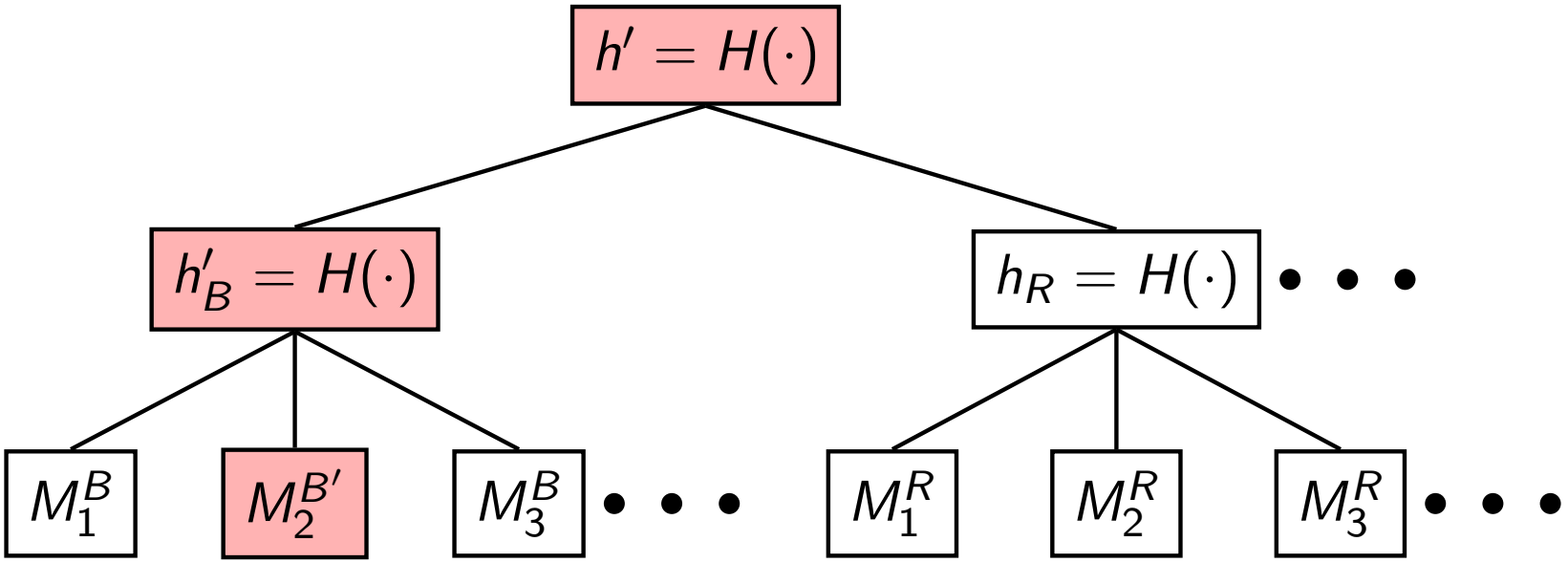
Detecting Consensus Violations

Each participant forms a Merkle hash tree over all messages:



Detecting Consensus Violations

Each participant forms a Merkle hash tree over all messages:



Weakening Assumptions

- Ensuring consensus incrementally
- Robustness to network interruption
- *n*-party primitives

Related Work

- Two-party Off-the-Record Communication (Borisov et al. WPES 2004)
- Group OTR (GOTR) (Bian et al. IRI 2007)
- Deniable Encryption (Canetti et al. CRYPTO 1997)
- Deniable Authentication and Key Exchange (Di Raimondo and Gennaro CCS 2006)

Conclusion

- Given requirements for off-the-record communication in a multi-party setting
- Given new primitive for Deniable Signature Key Exchange
- Leveraged DSKE to get deniable n-party interactive communication

Questions anyone?