Consistent Synchronous Group Off-The-Record Messaging with SYM-GOTR

Mike Schliep[1], Eugene Vasserman[2], and Nicholas Hopper[1]
[1]University of Minnesota, [2]Kansas State University

Security Goals

Message Confidentiality/Integrity/Authentication

Forward/Backward Secrecy

Security Goals

Message Confidentiality/Integrity/Authentication

Forward/Backward Secrecy

Deniability

Security Goals

Message Confidentiality/Integrity/Authentication

Forward/Backward Secrecy

Deniability

Participant Consistency

Transcript Consistency

System Model

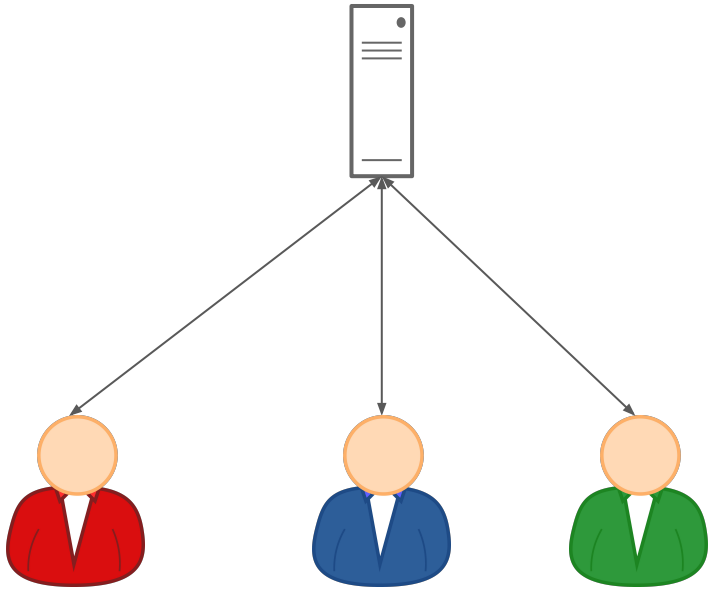
Instant Messaging

System Model

Instant Messaging

Server (XMPP)

Online Participants



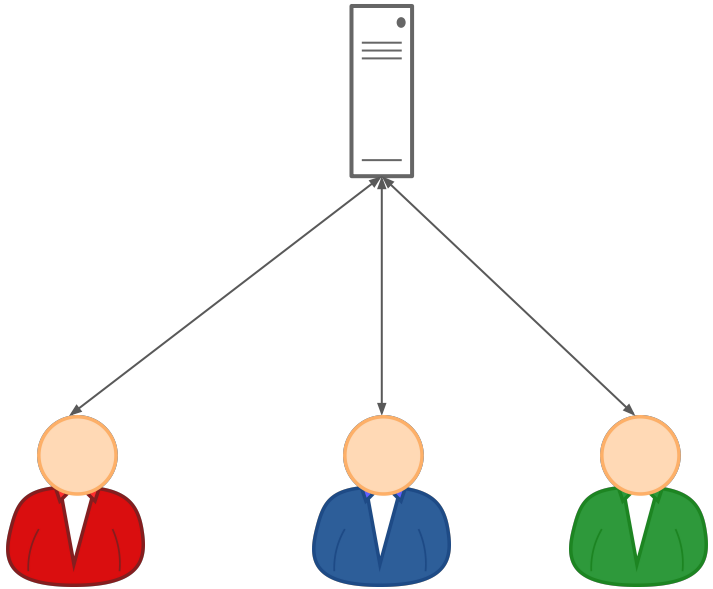
System Model

Instant Messaging

Server (XMPP)

Online Participants

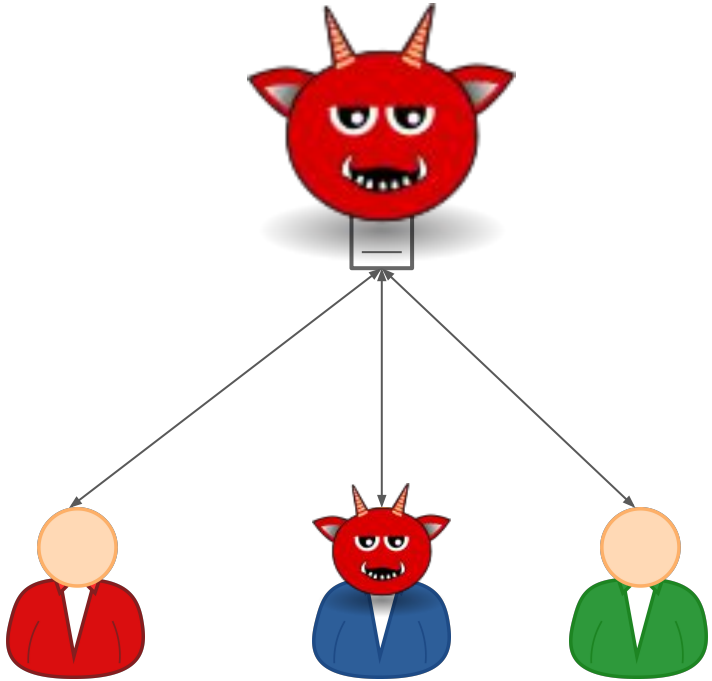
- Setup
- Add/Remove
- Broadcast



Threat Model

Compromised Server

Compromised Participants



Existing Applications

Signal

WhatsApp

Threema

Literature

Schliep, Kariniemi, Hopper (WPES’17)

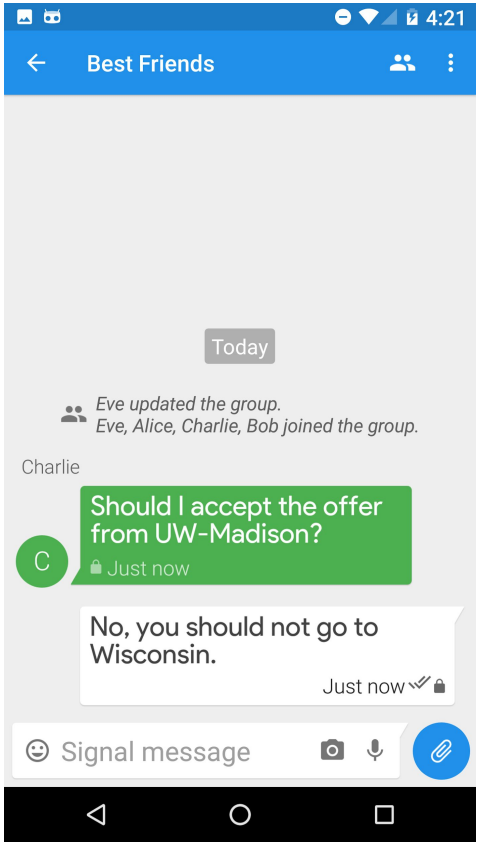
Rösler, Mainka, Schwenk (EuroS&P’18)

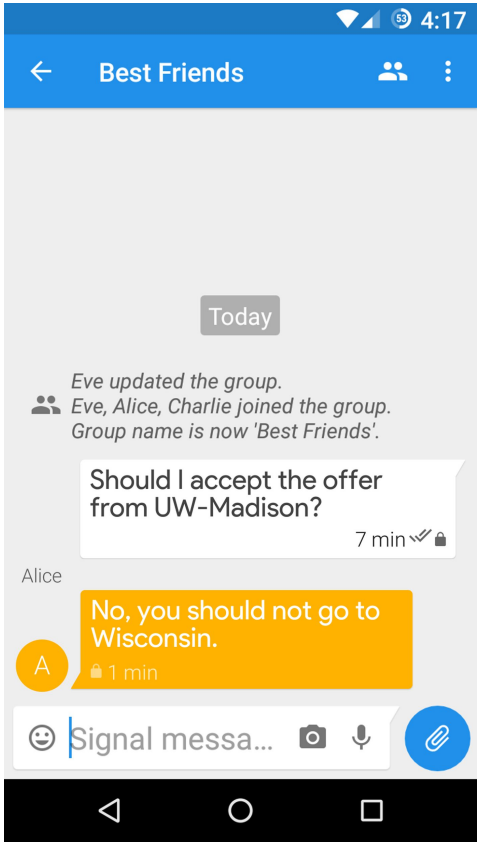
Literature

Schliep, Kariniemi, Hopper (WPES'17)

Rösler, Mainka, Schwenk (EuroS&P'18)

Participant Inconsistency



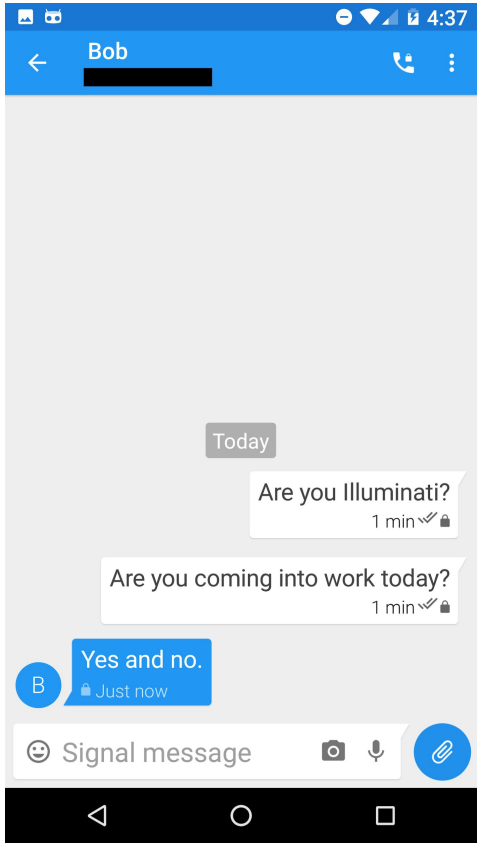


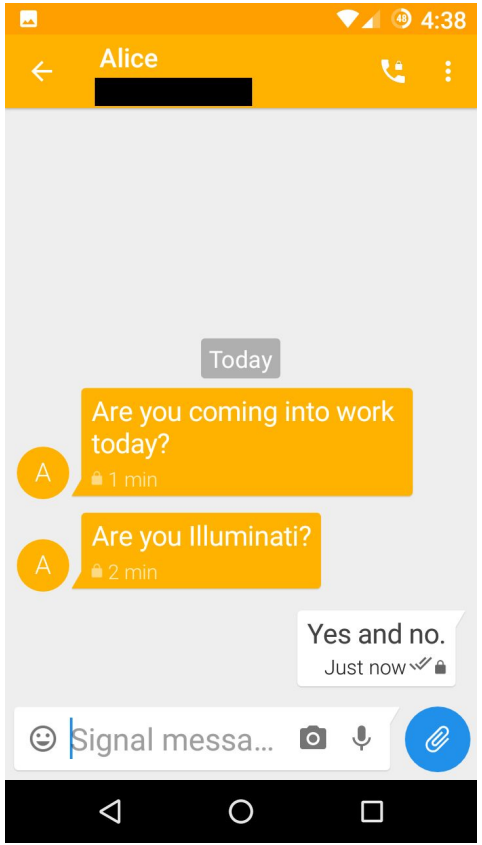
Literature

Schliep, Kariniemi, Hopper (WPES'17)

Rösler, Mainka, Schwenk (EuroS&P'18)

Transcript Inconsistency





Literature

Schliep, Kariniemi, Hopper (WPES’17)

Rösler, Mainka, Schwenk (EuroS&P’18)

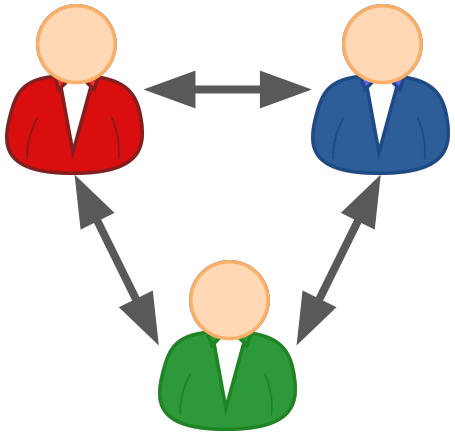
mpOTR - Goldberg, Ustaoğlu, Gundy, Chen (CCS’09)

GOTR - Liu, Vasserman, Hopper (WPES’13)

SYM-GOTR Overview

SYM-GOTR Overview

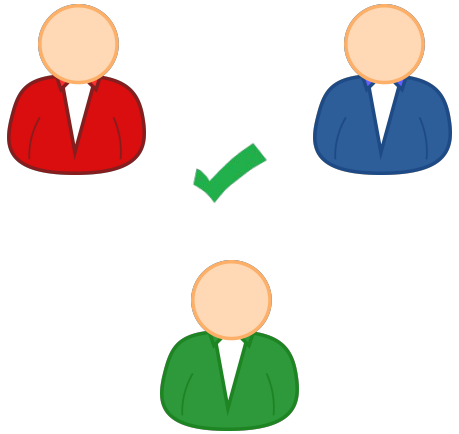
Secure 2-party channel between all participants



SYM-GOTR Overview

Secure 2-party channel between all participants

Participant consistency check (symmetric key material)

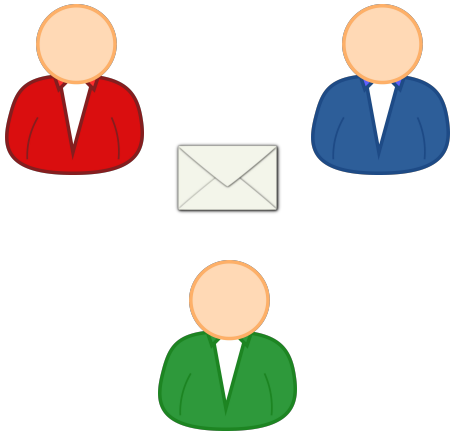


SYM-GOTR Overview

Secure 2-party channel between all participants

Participant consistency check (symmetric key material)

Broadcast message



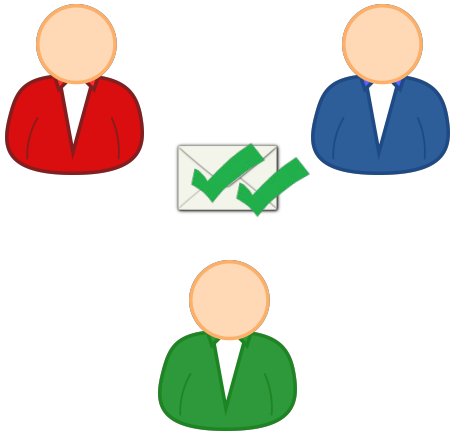
SYM-GOTR Overview

Secure 2-party channel between all participants

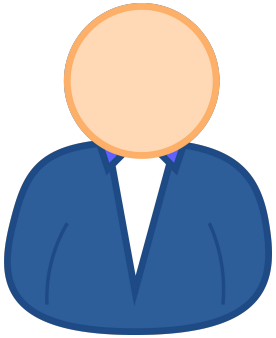
Participant consistency check (symmetric key material)

Broadcast message

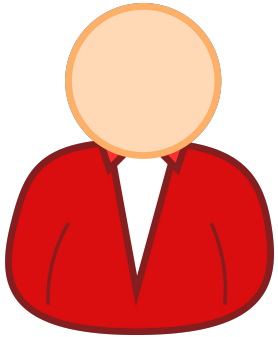
2-part message consistency check



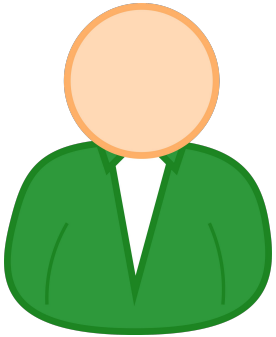
SYM-GOTR Setup



Bob

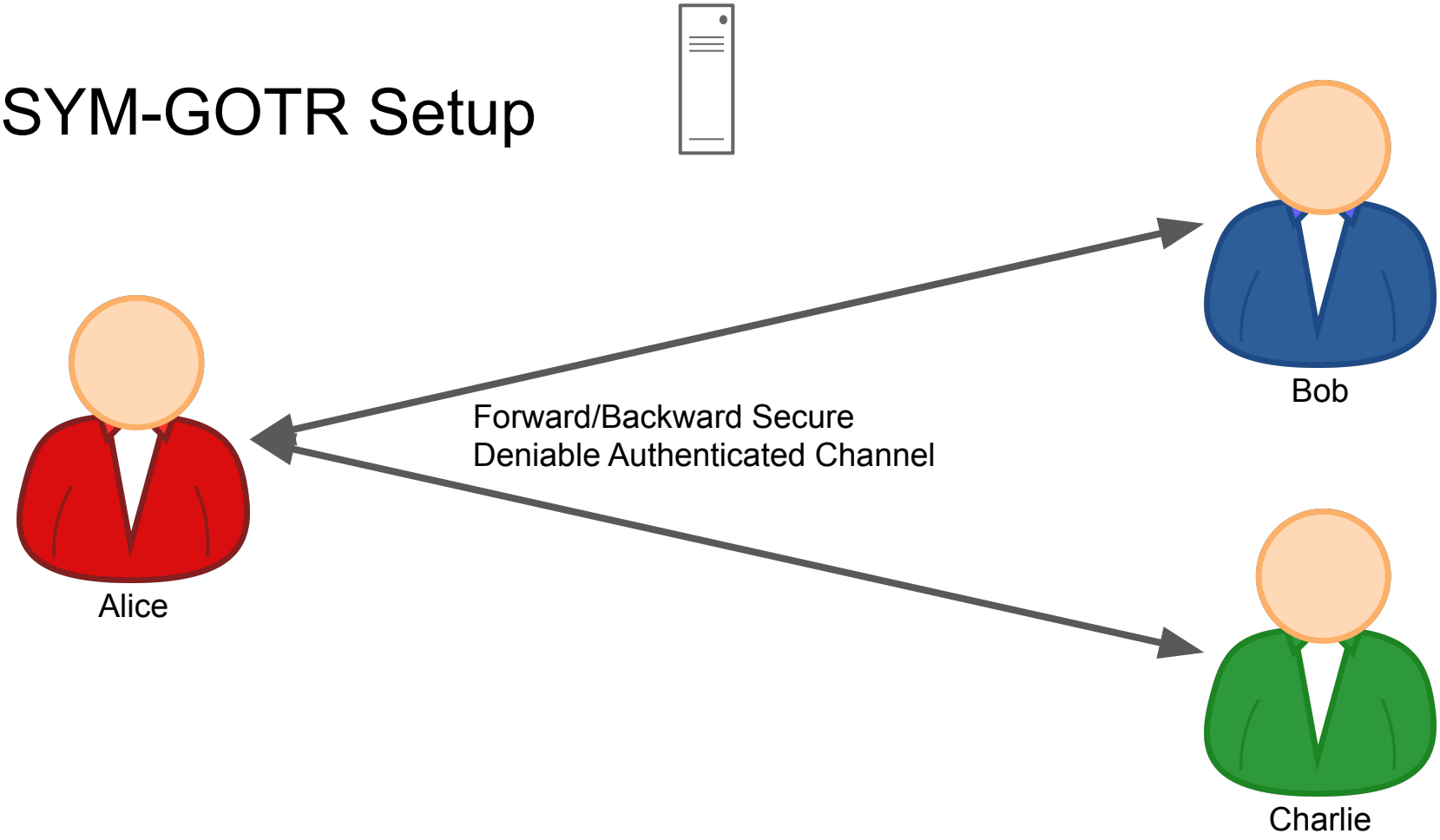


Alice

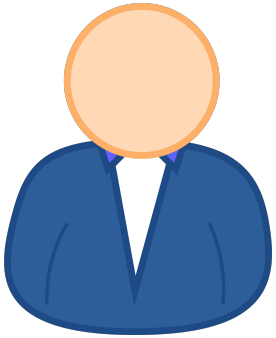


Charlie

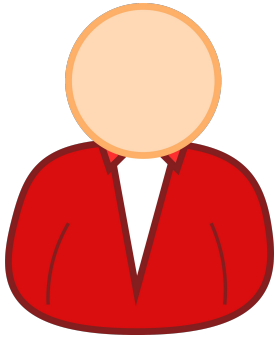
SYM-GOTR Setup



SYM-GOTR Setup

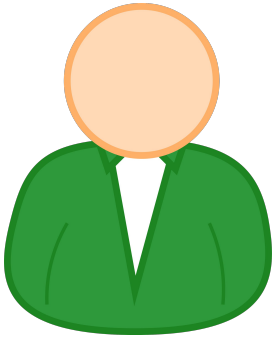


Bob



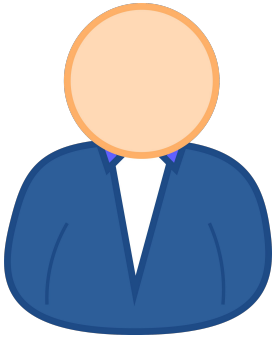
Alice

$s_a \leftarrow \{0,1\}^l$

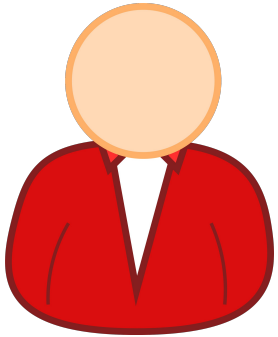


Charlie

SYM-GOTR Setup

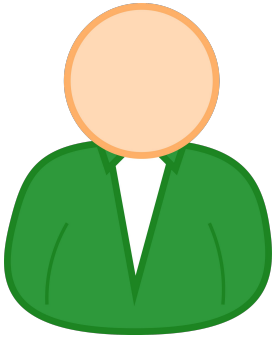


Bob



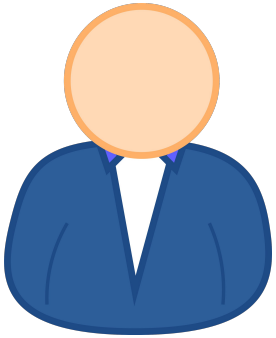
Alice

$$s_a \leftarrow \{0,1\}^l$$
$$sk_a, vk_a \leftarrow \text{GEN}()$$

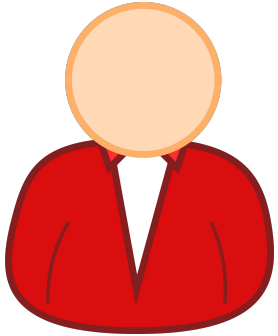


Charlie

SYM-GOTR Setup

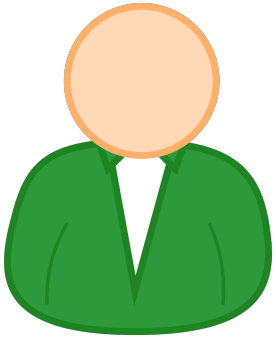


Bob



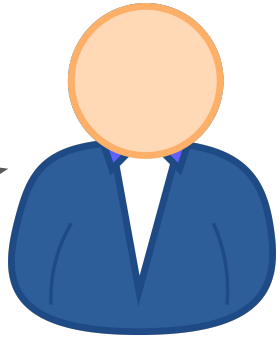
Alice

$$s_a \leftarrow \{0,1\}^l$$
$$sk_a, vk_a \leftarrow \textsc{Gen}()$$
$$gv_a \leftarrow H_2(Sid, U)$$



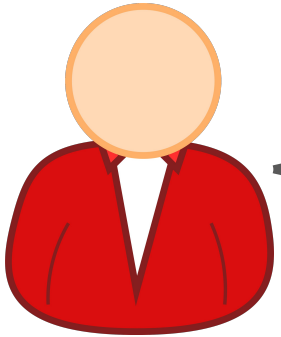
Charlie

SYM-GOTR Setup



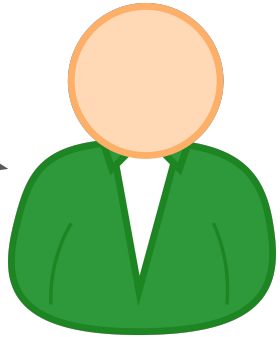
Bob

s_a, vk_a, gv_a



Alice

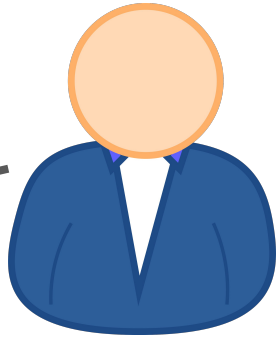
s_a, vk_a, gv_a



Charlie

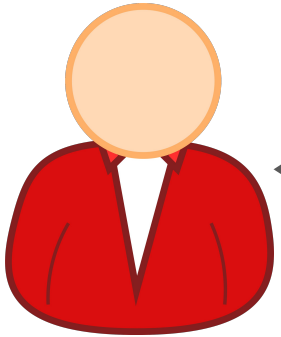
$s_a \leftarrow \{0,1\}^l$
$sk_a, vk_a \leftarrow \text{GEN}()$
$gv_a \leftarrow H_2(Sid, U)$

SYM-GOTR Setup



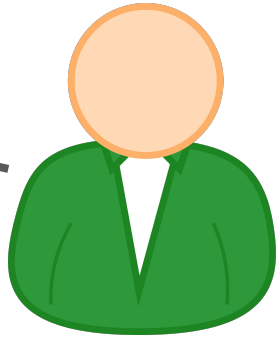
Bob

s_b, vk_b, gv_b



Alice

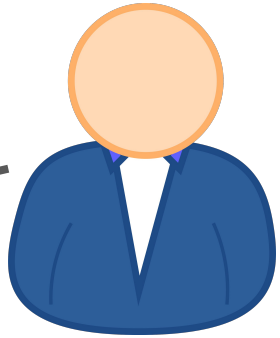
s_c, vk_c, gv_c



Charlie

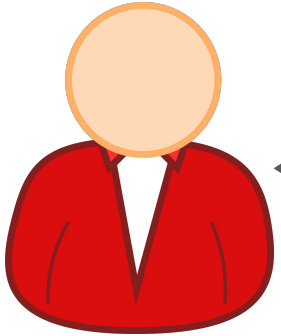
$s_a \leftarrow \{0,1\}^l$
$sk_a, vk_a \leftarrow \text{GEN}()$
$gv_a \leftarrow H_2(Sid, U)$

SYM-GOTR Setup



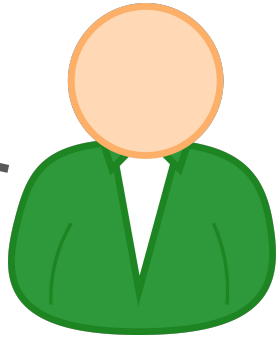
Bob

s_b, vk_b, gv_b



Alice

s_c, vk_c, gv_c

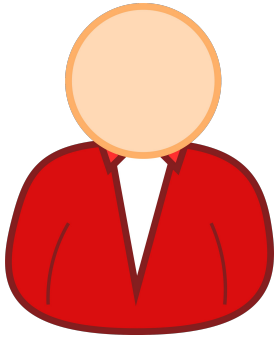


Charlie

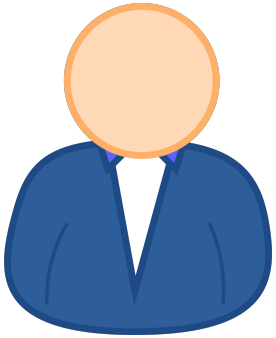
$s_a \leftarrow \{0,1\}^l$
$sk_a, vk_a \leftarrow \text{GEN}()$
$gv_a \leftarrow H_2(Sid, U)$

$gv_a = gv_b = gv_c$

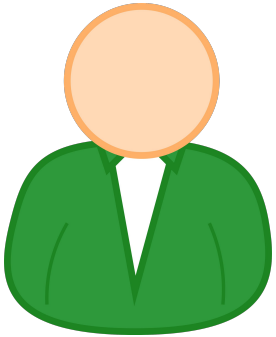
Broadcast



Alice

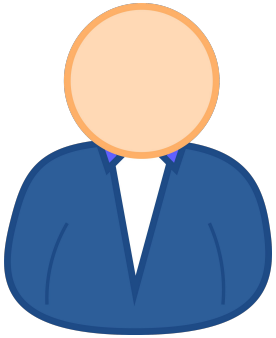


Bob

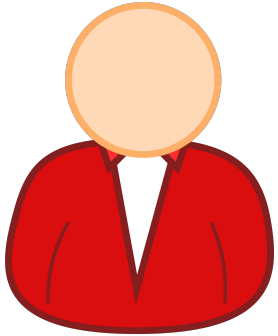


Charlie

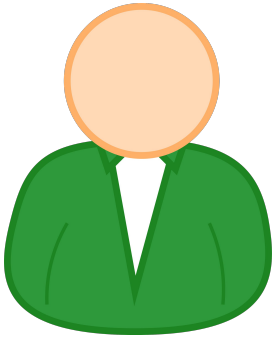
Broadcast



Bob



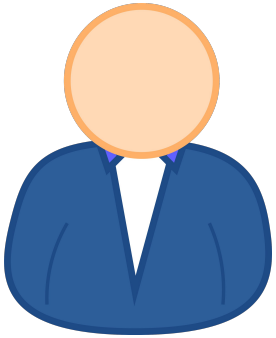
Alice



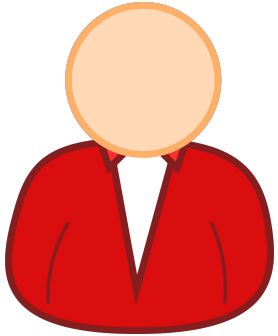
Charlie

$$k \leftarrow \mathrm{KDF}_3(Sid, (\text{“Alice”}, s_a), (\text{“Alice”}, s_a))(\text{“Bob”}, s_b), (\text{“Charlie”}, s_c))$$

Broadcast

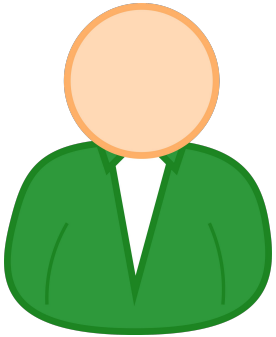


Bob



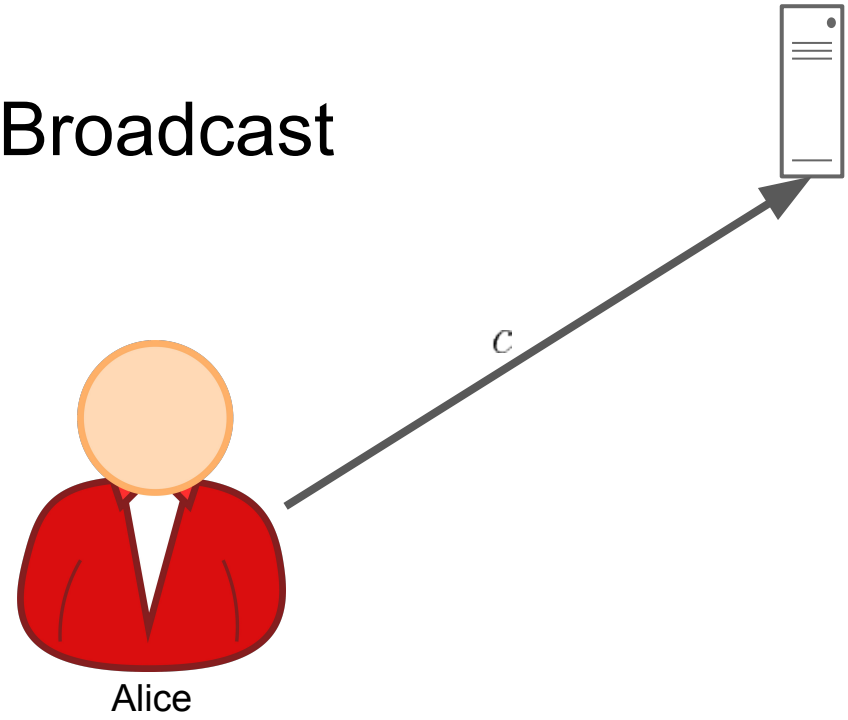
Alice

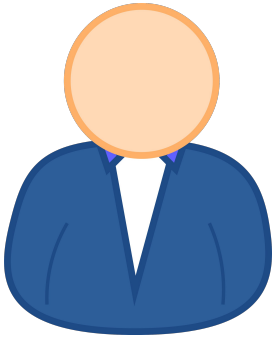
$$k \leftarrow \mathrm{KDF}_3(Sid, (\text{“Alice”}, s_a), (\text{“Alice”}, s_a))(\text{“Bob”}, s_b), (\text{“Charlie”}, s_c))$$
$$c \leftarrow \mathrm{AEnc}_k(m)$$

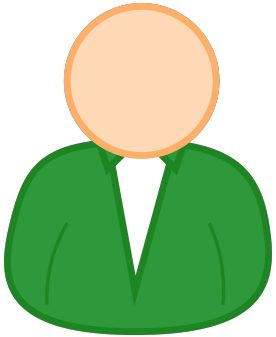


Charlie

Broadcast

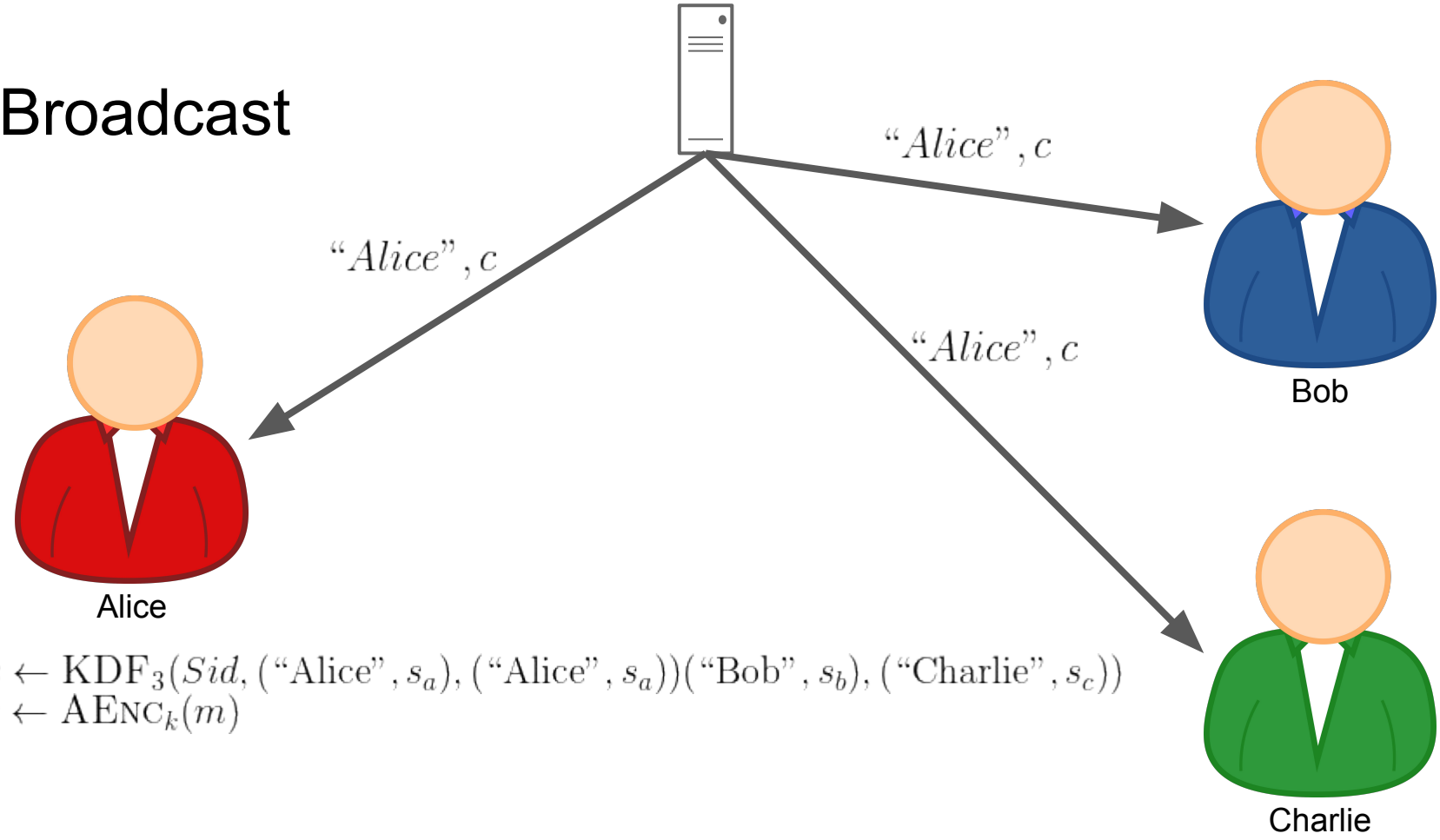






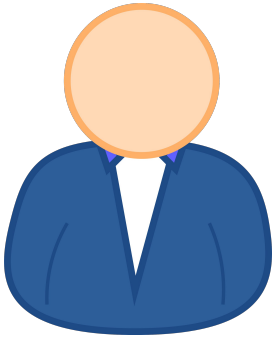
$$k \leftarrow \mathrm{KDF}_3(Sid, (\text{“Alice”}, s_a), (\text{“Alice”}, s_a))(\text{“Bob”}, s_b), (\text{“Charlie”}, s_c))$$
$$c \leftarrow \mathrm{AEnc}_k(m)$$

Broadcast

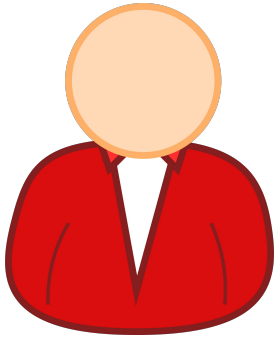


$k \leftarrow \mathrm{KDF}_3(Sid, (\text{“Alice”}, s_a), (\text{“Alice”}, s_a))(\text{“Bob”}, s_b), (\text{“Charlie”}, s_c))$
$c \leftarrow \mathrm{AEnc}_k(m)$

Consistency Check

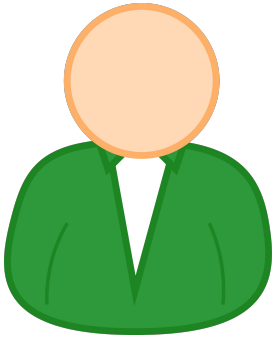


Bob



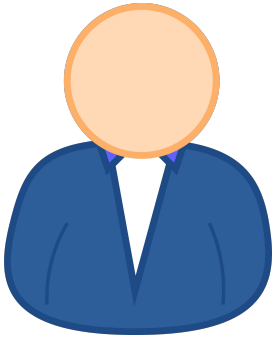
Alice

$c \leftarrow \mathrm{AEnc}_k(m)$

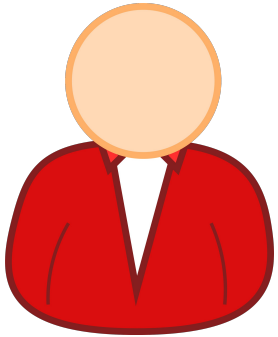


Charlie

Consistency Check

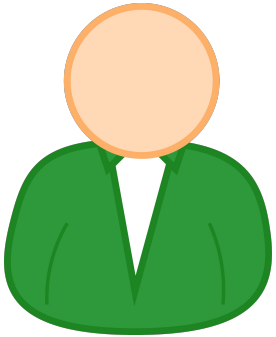


Bob



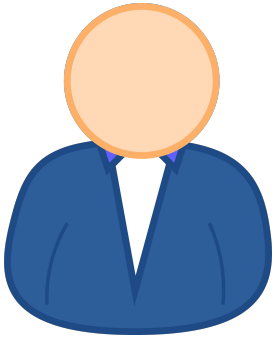
Alice

$$c \leftarrow \mathrm{AEnc}_k(m)$$
$$d_a \leftarrow \mathrm{H}_3(\text{“accept”})|\mathrm{H}_3(\text{“reject”}, c)$$

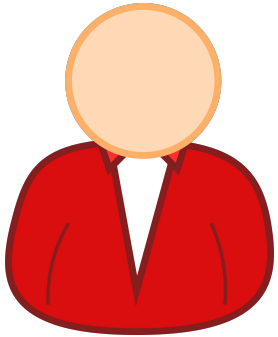


Charlie

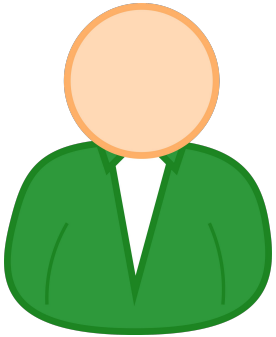
Consistency Check



Bob



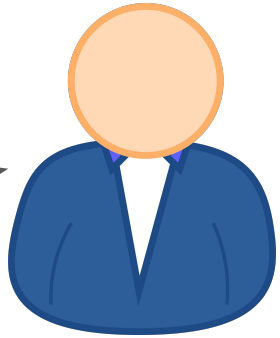
Alice



Charlie

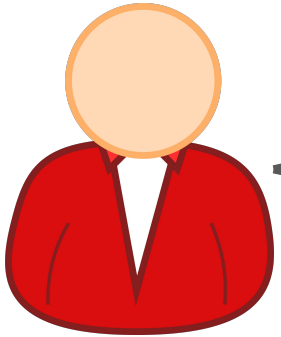
$c \leftarrow \mathrm{AENC}_k(m)$
$d_a \leftarrow \mathrm{H}_3(\text{“accept”})|\mathrm{H}_3(\text{“reject”}, c)$
$sig_a \leftarrow \mathrm{SIGN}_{sk_a}(d_a)$

Consistency Check



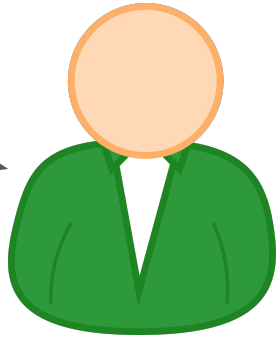
Bob

d_a, sig_a



Alice

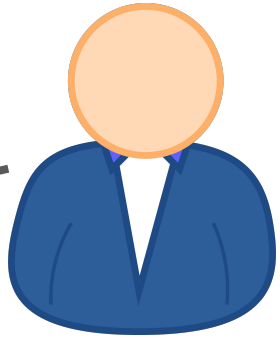
d_a, sig_a



Charlie

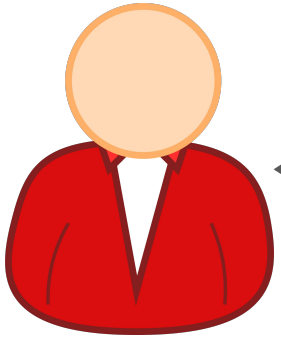
$c \leftarrow \text{AENC}_k(m)$
$d_a \leftarrow \text{H}_3(\text{“accept”})|\text{H}_3(\text{“reject”}, c)$
$sig_a \leftarrow \text{SIGN}_{sk_a}(d_a)$

Consistency Check



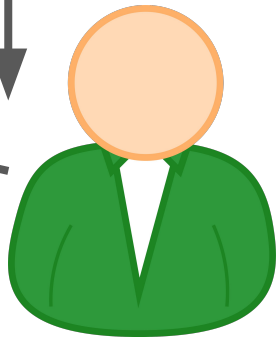
Bob

d_b, sig_b



Alice

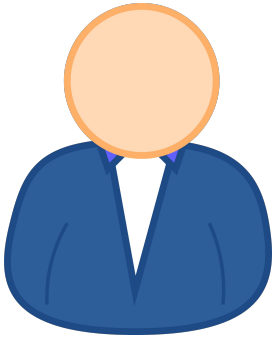
d_c, sig_c



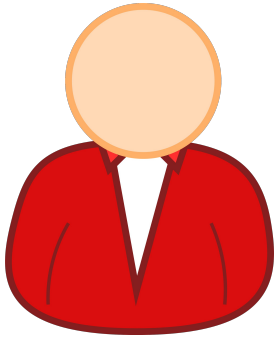
Charlie

$c \leftarrow \text{AENC}_k(m)$
$d_a \leftarrow \text{H}_3(\text{“accept”})|\text{H}_3(\text{“reject”}, c)$
$sig_a \leftarrow \text{SIGN}_{sk_a}(d_a)$

Consistency Check

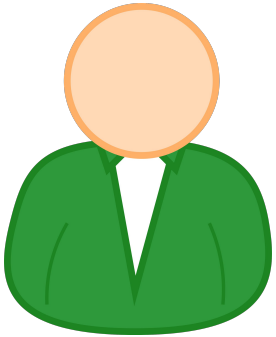


Bob



Alice

$$d_a = d_b = d_c$$
$$\text{VERIFY}_{vk_a}(d_a)$$
$$\text{VERIFY}_{vk_b}(d_b)$$
$$\text{VERIFY}_{vk_c}(d_c)$$

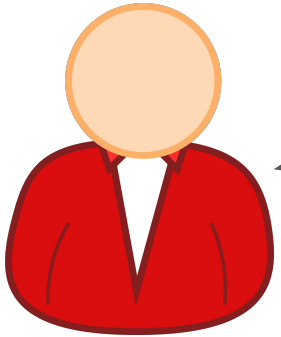


Charlie

Consistency Check

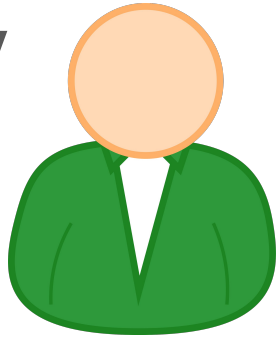
Bob

accept



Alice

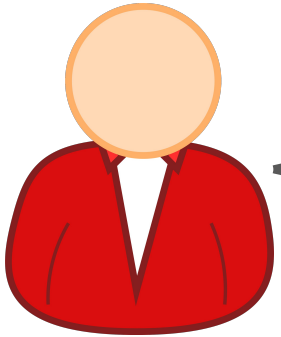
reject



Charlie

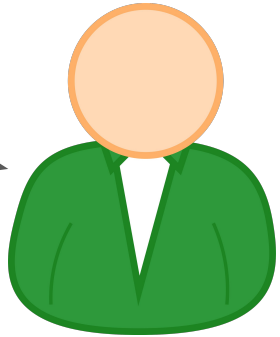
Signature Check

Bob



Alice

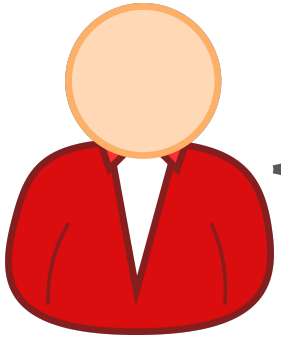
$(\text{“}Bob\text{”}, sig_b), (\text{“}Charlie\text{”}, sig_c)$



Charlie

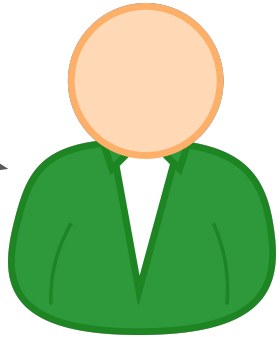
Signature Check

Bob



Alice

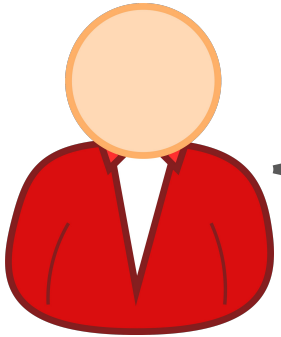
$$H_4((U_{accept}, sig_{accept}), \ldots), (U_{reject}, sig_{reject})$$



Charlie

Signature Check

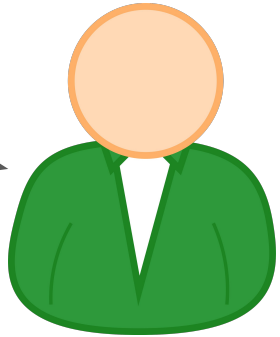
Bob



Alice

$H_4((U_{accept}, sig_{accept}), ...), (U_{reject}, sig_{reject})$

s'_a, vk'_a



Charlie

Implementation

Java Library

Jitsi Plugin

Implementation

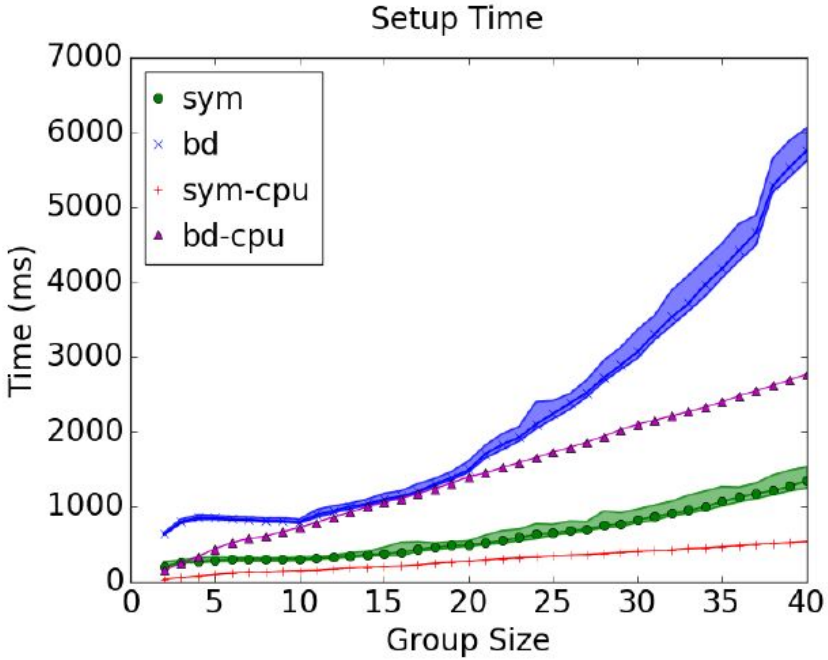
Java Library

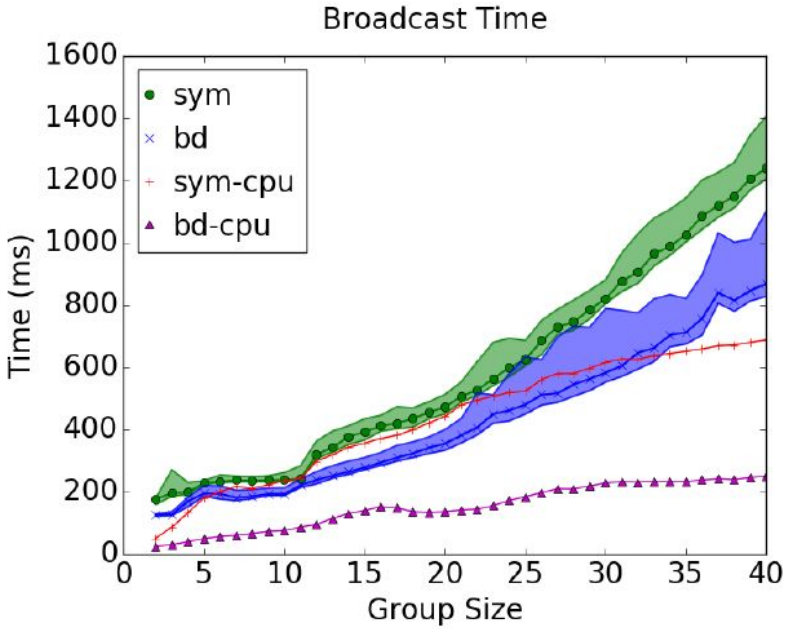
Jitsi Plugin

$5/month Linode Server (ejabberd)

40 clients across 8 university machines

Compared to WPES’13 (BD-GOTR)


Setup Time
Time (ms)
Group Size
sym
bd
sym-cpu
bd-cpu
0
1000
2000
3000
4000
5000
6000
7000
0
5
10
15
20
25
30
35
40

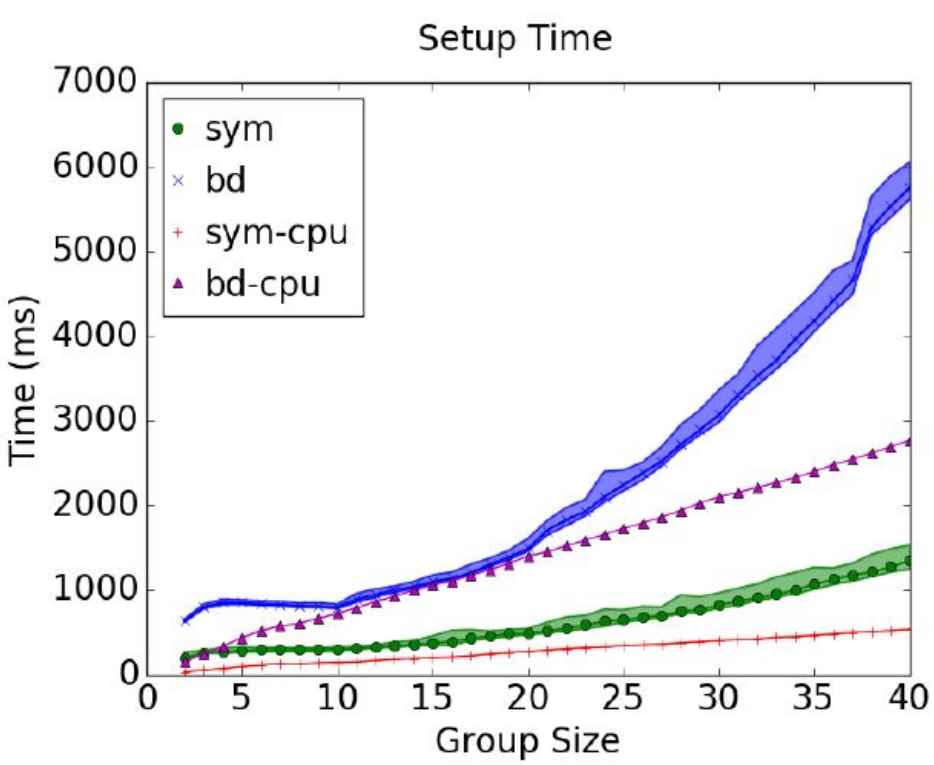

Broadcast Time
Time (ms)
Group Size
sym
bd
sym-cpu
bd-cpu
0
200
400
600
800
1000
1200
1400
1600
0
5
10
15
20
25
30
35
40

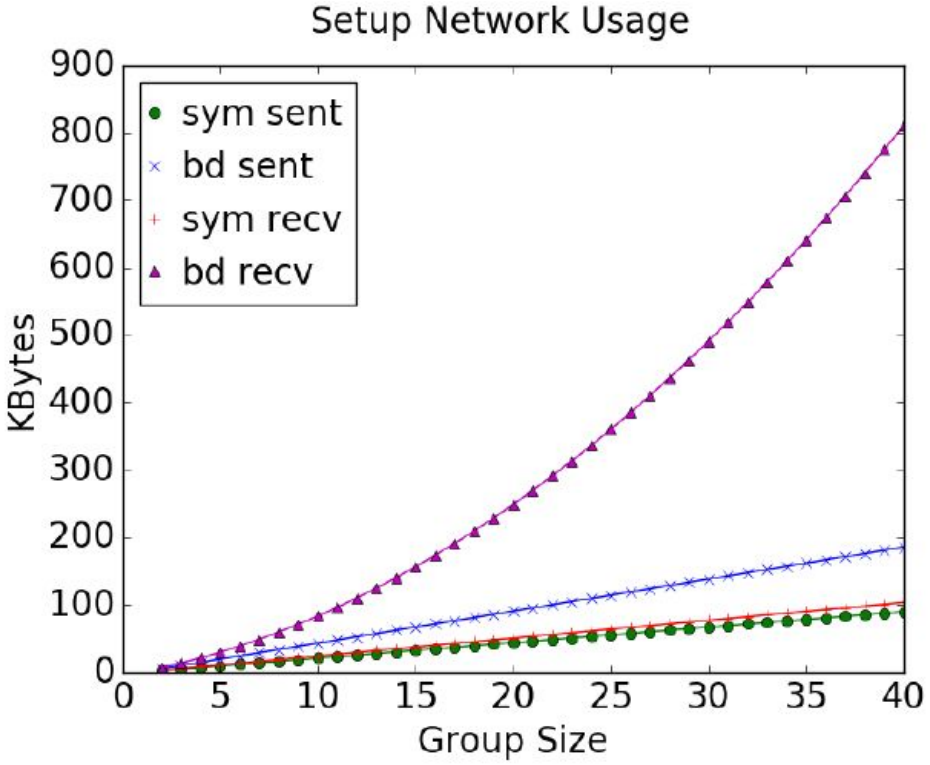
Take Away

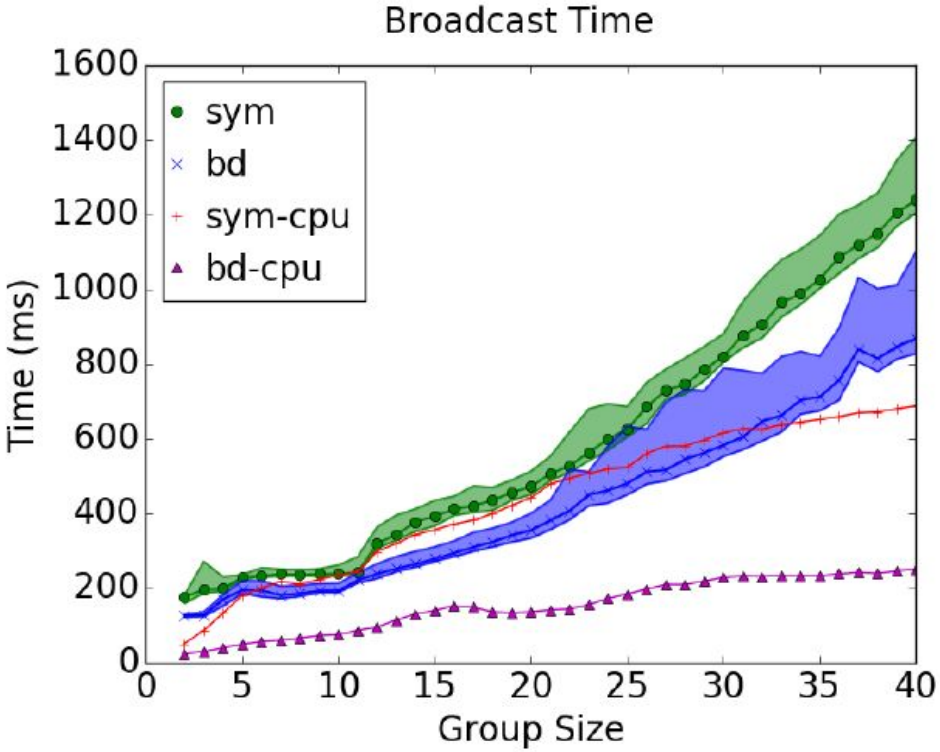
SYM-GOTR is a secure messaging protocol with strong consistency properties.

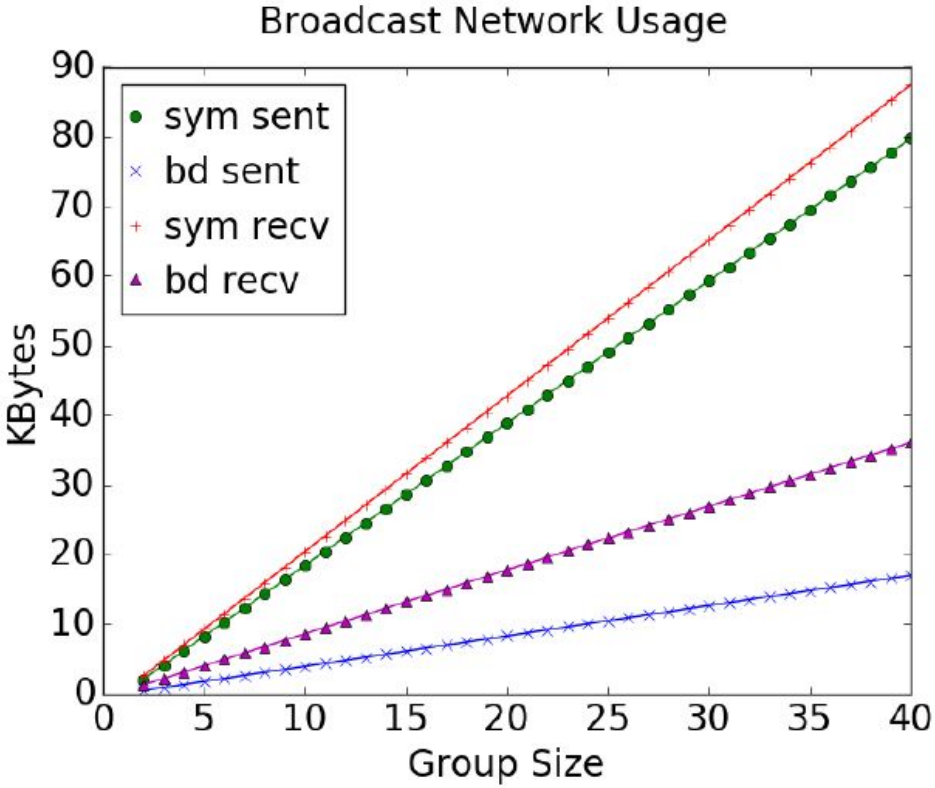
- Participant Consistency Check
- 2-part Message Consistency Check

Practical with our Java implementation.


Setup Time
Time (ms)
Group Size
sym
bd
sym-cpu
bd-cpu
0
1000
2000
3000
4000
5000
6000
7000
0
5
10
15
20
25
30
35
40


Setup Network Usage
KBytes
Group Size
sym sent
bd sent
sym recv
bd recv
0
100
200
300
400
500
600
700
800
900
0
5
10
15
20
25
30
35
40


Broadcast Time
Time (ms)
Group Size
sym
bd
sym-cpu
bd-cpu
0
200
400
600
800
1000
1200
1400
1600
0
5
10
15
20
25
30
35
40


Broadcast Network Usage
KBytes
Group Size
sym sent
bd sent
sym recv
bd recv
0
10
20
30
40
50
60
70
80
90
0
5
10
15
20
25
30
35
40