Fingerprint Scheduling

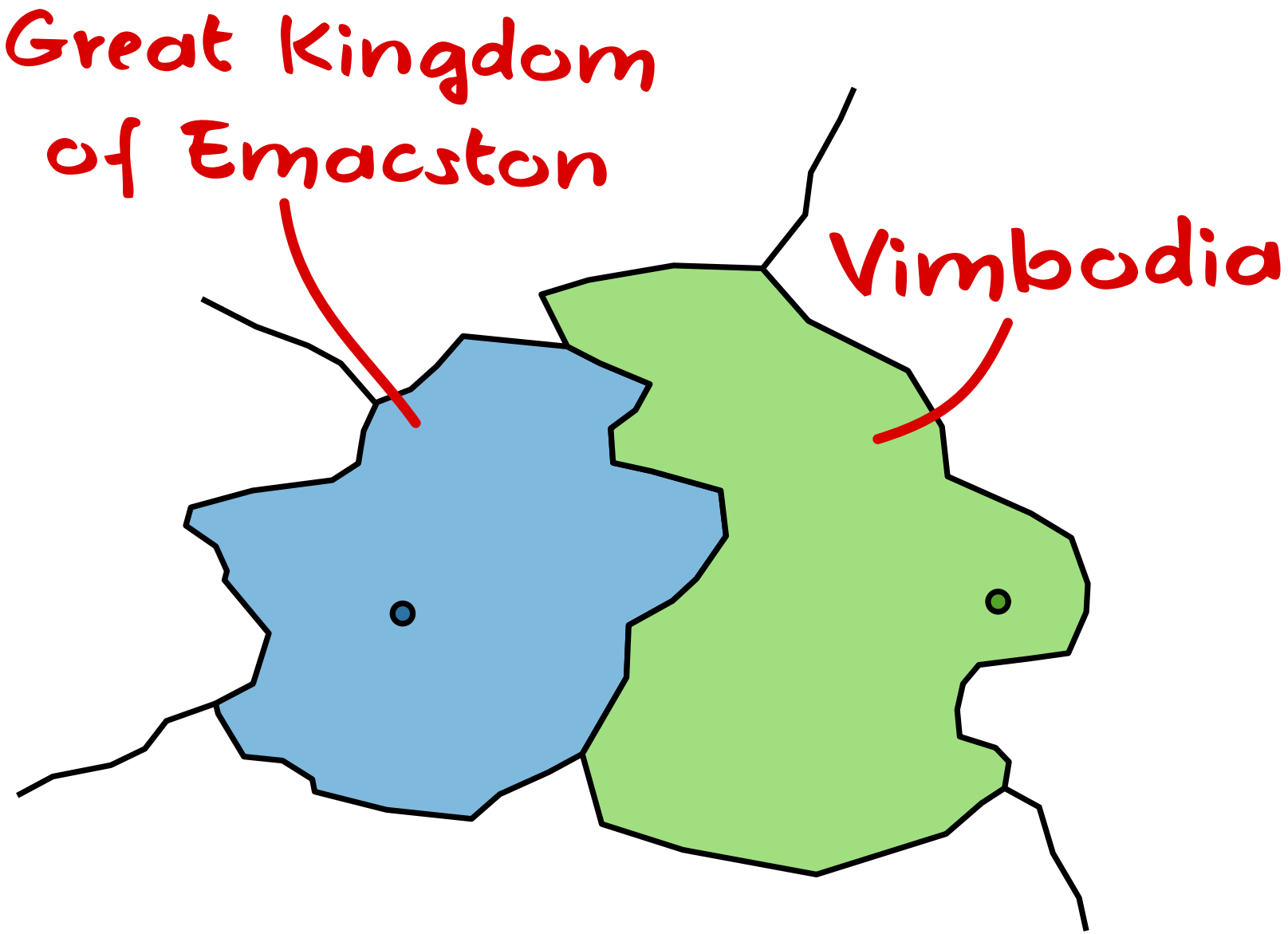
for dining-cryptographer networks

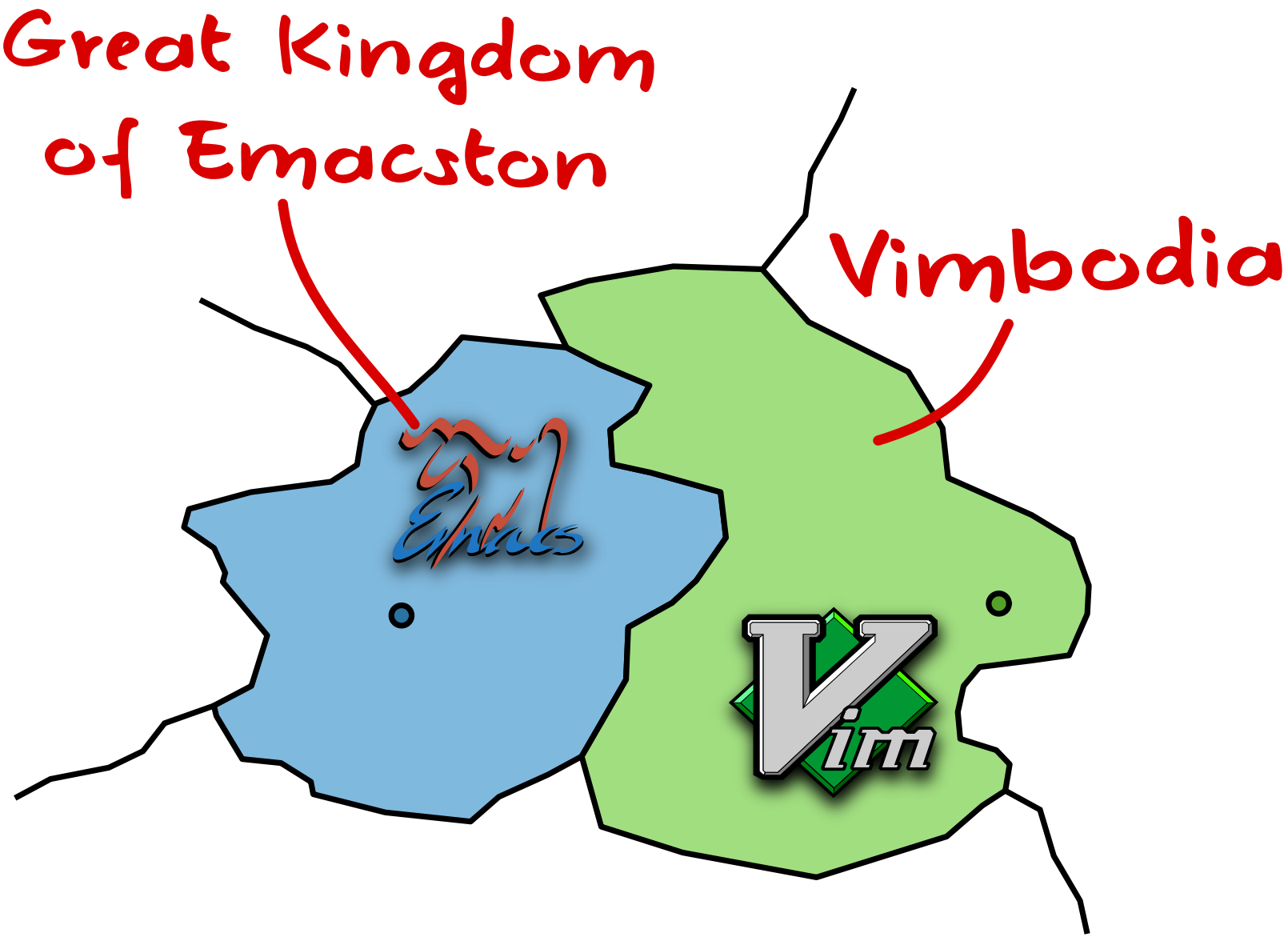
Radboud Universiteit Nijmegen

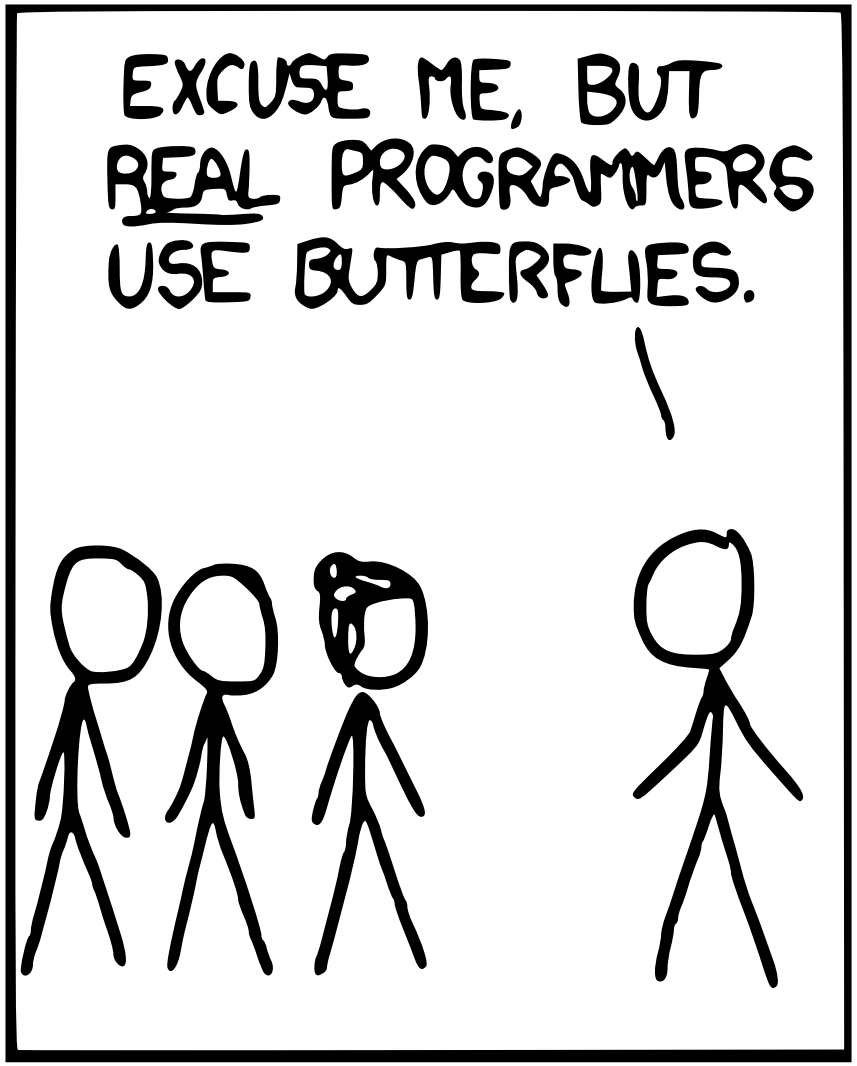
Peter Schwabe
peter@cryptojedi.org

Moritz Neikes
m.neikes@student.ru.nl

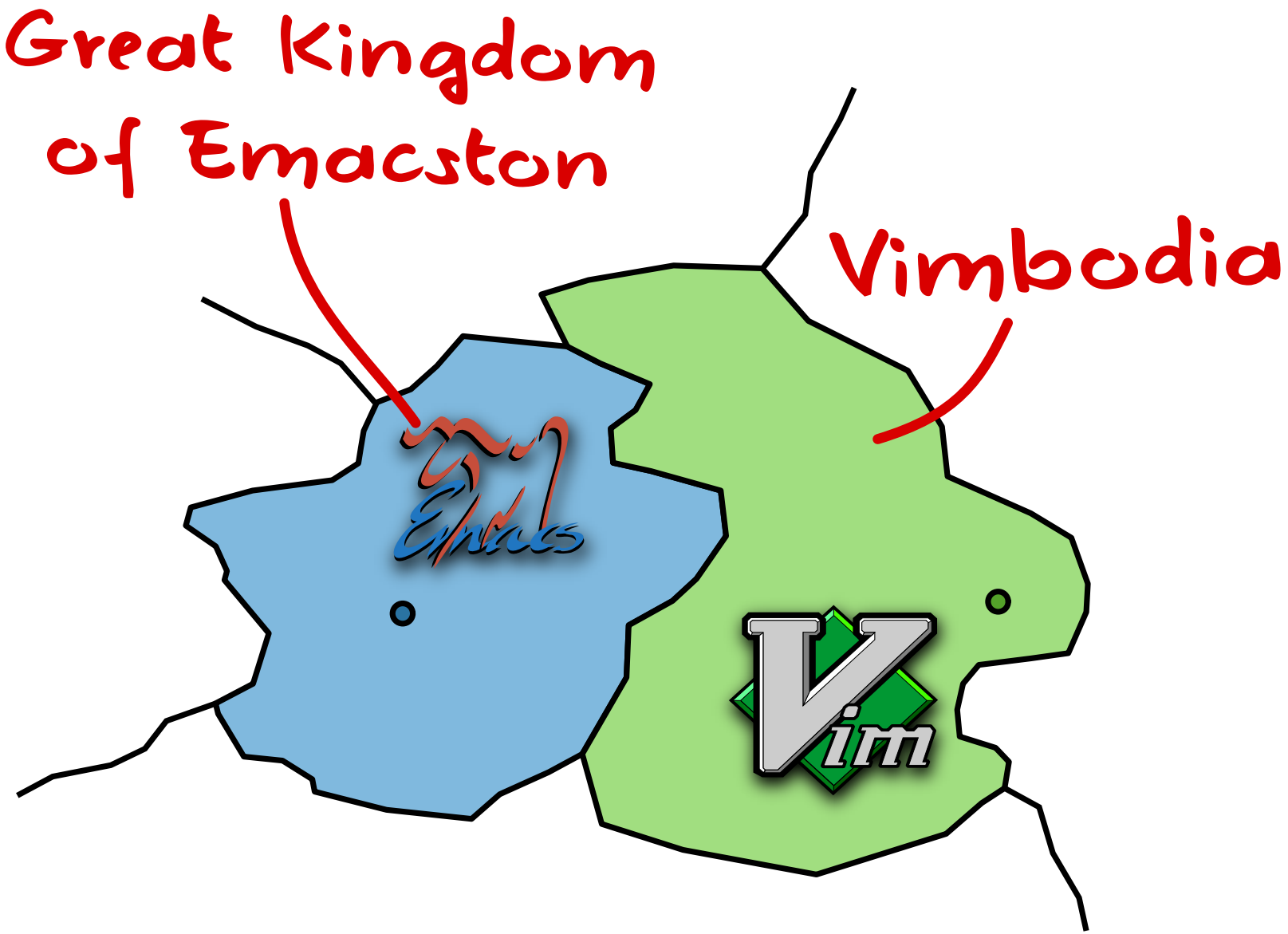
Anna Krasnova
anna@mechanical-mind.org

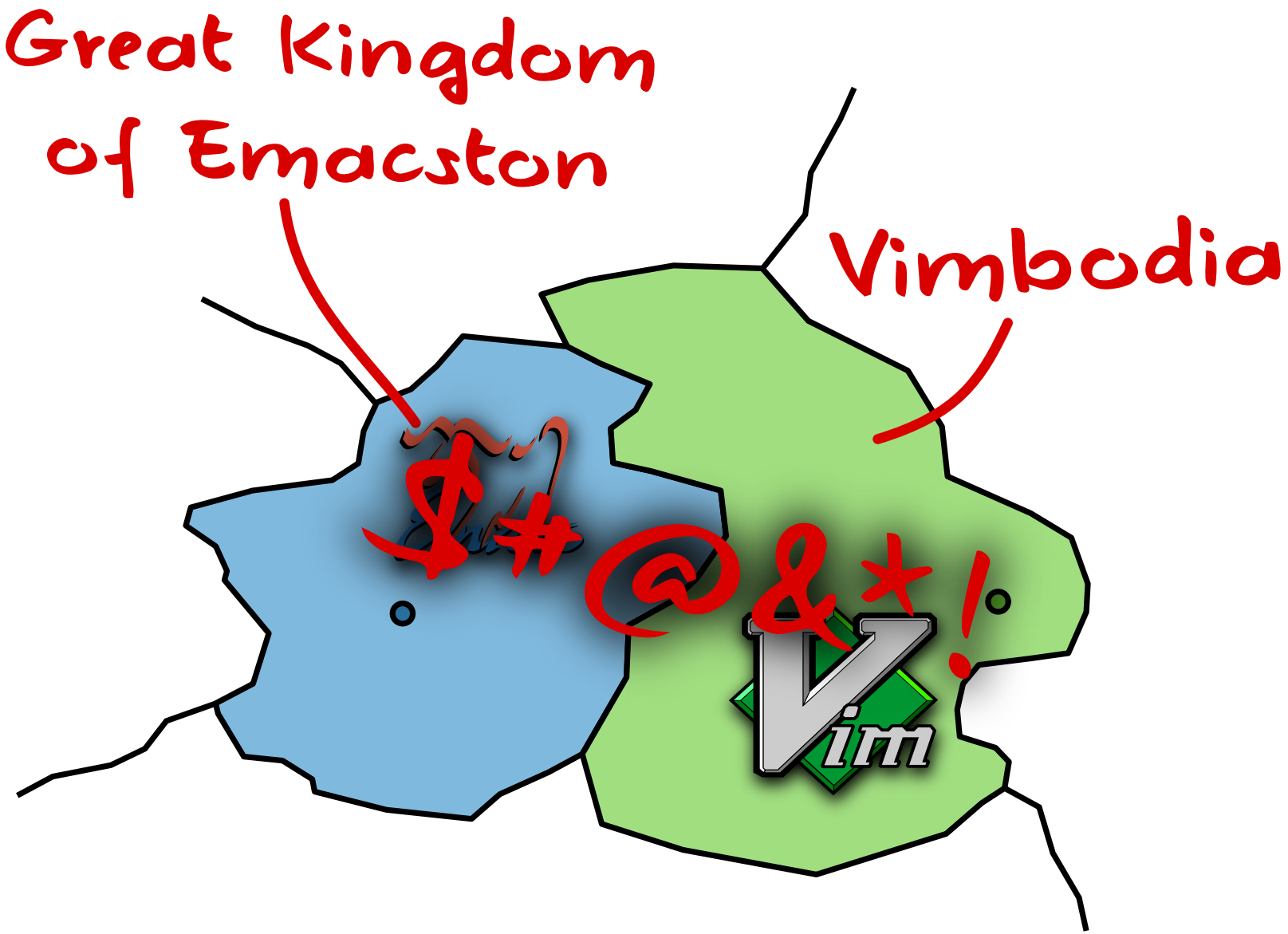

Great Kingdom
of Emacston
Vimbodia


Great Kingdom
of Emacston
Vimbodia



https://xkcd.com/378/


Great Kingdom
of Emacston
Vimbodia
Emacs
Vim


Great Kingdom
of Emacston
Vimbodia
$#@&*!
Vim

Problem

Anonymous communication

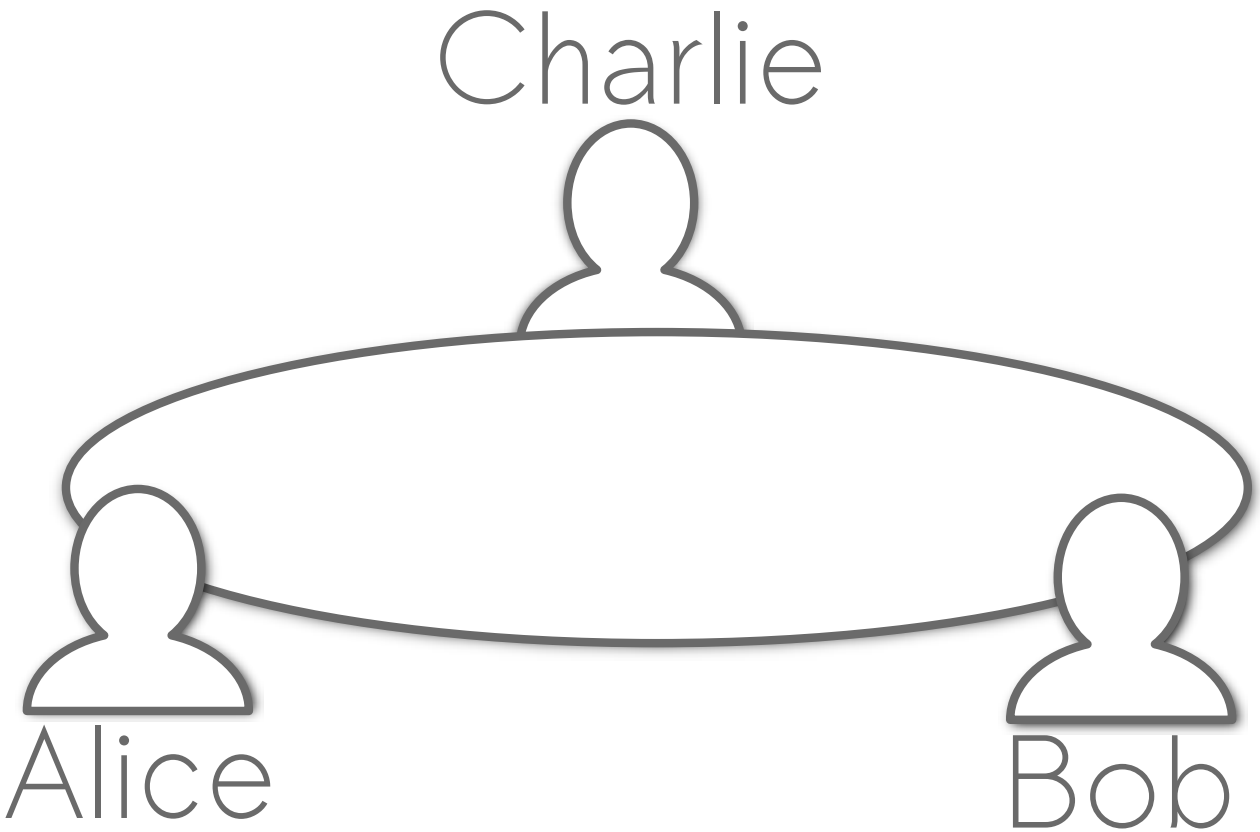
- even against very strong adversaries

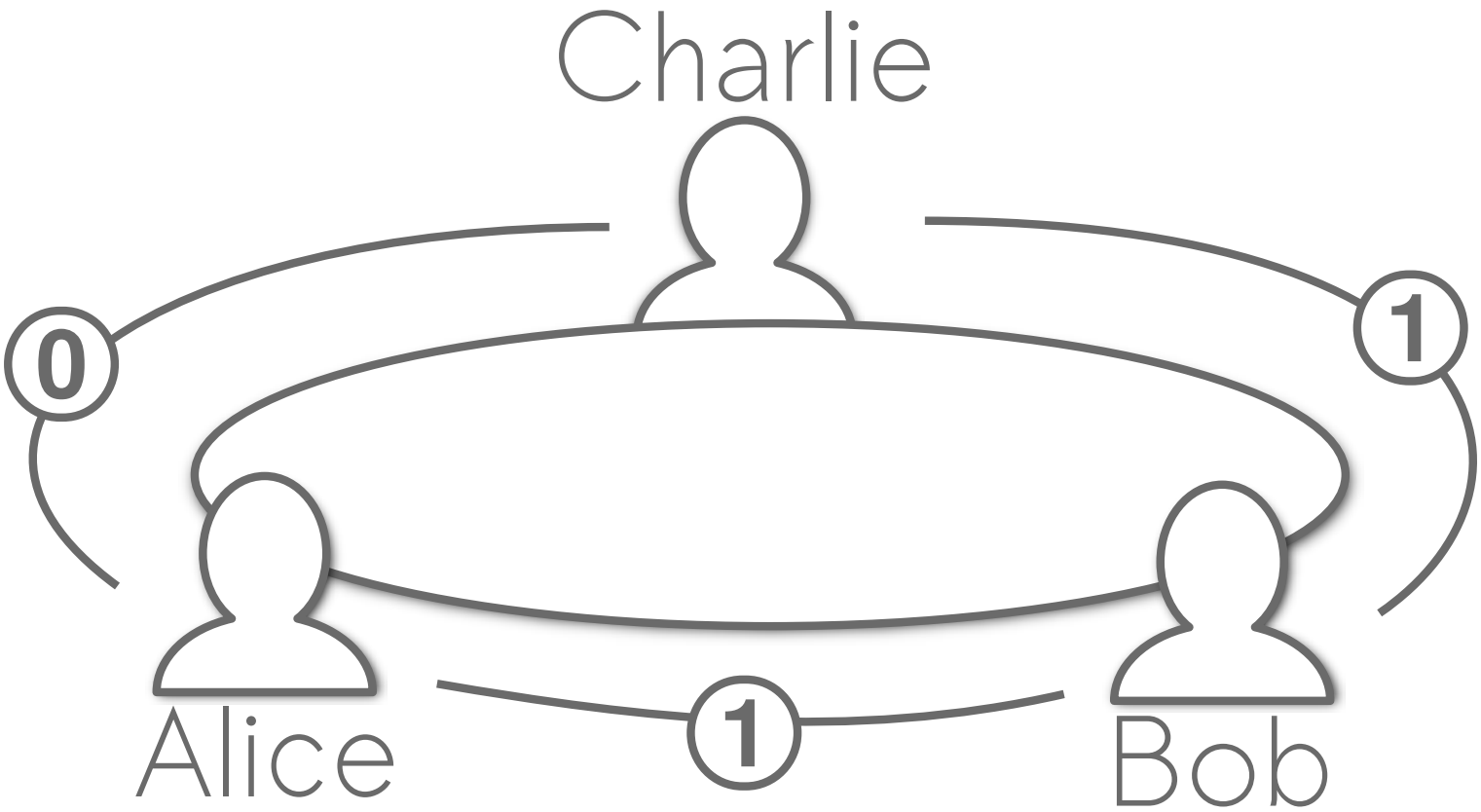
Many users

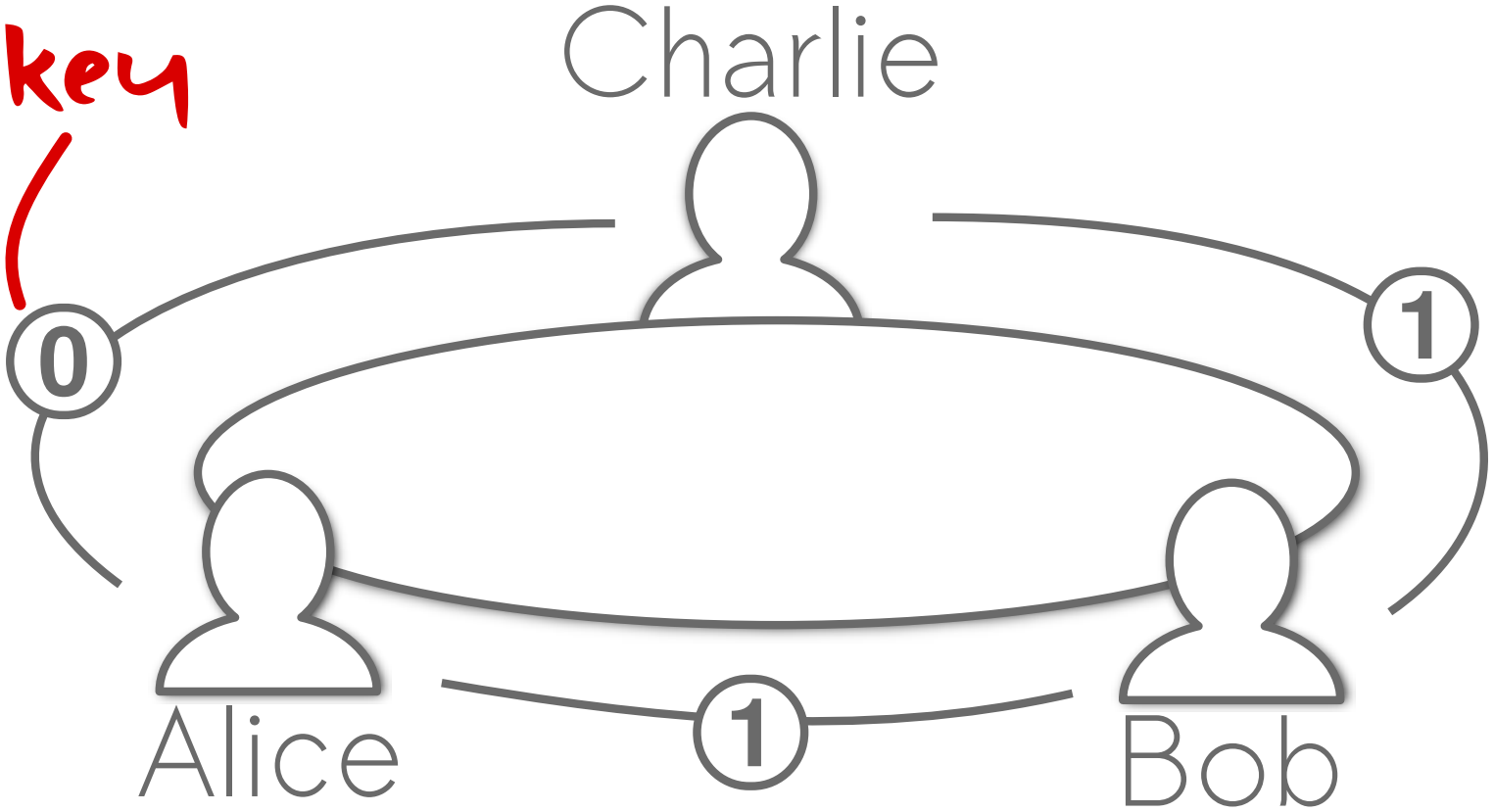
Unstable connections

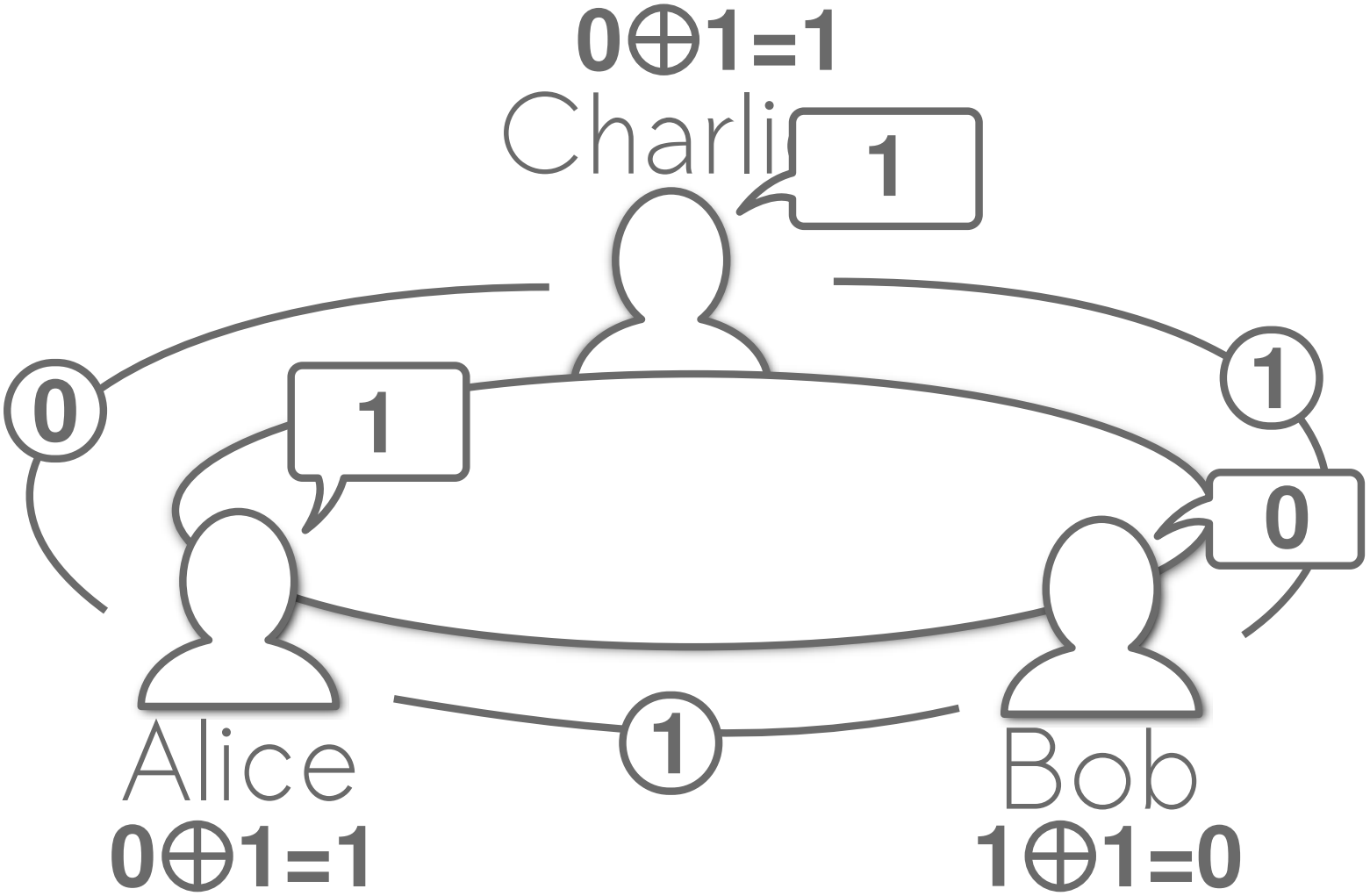
DC networks

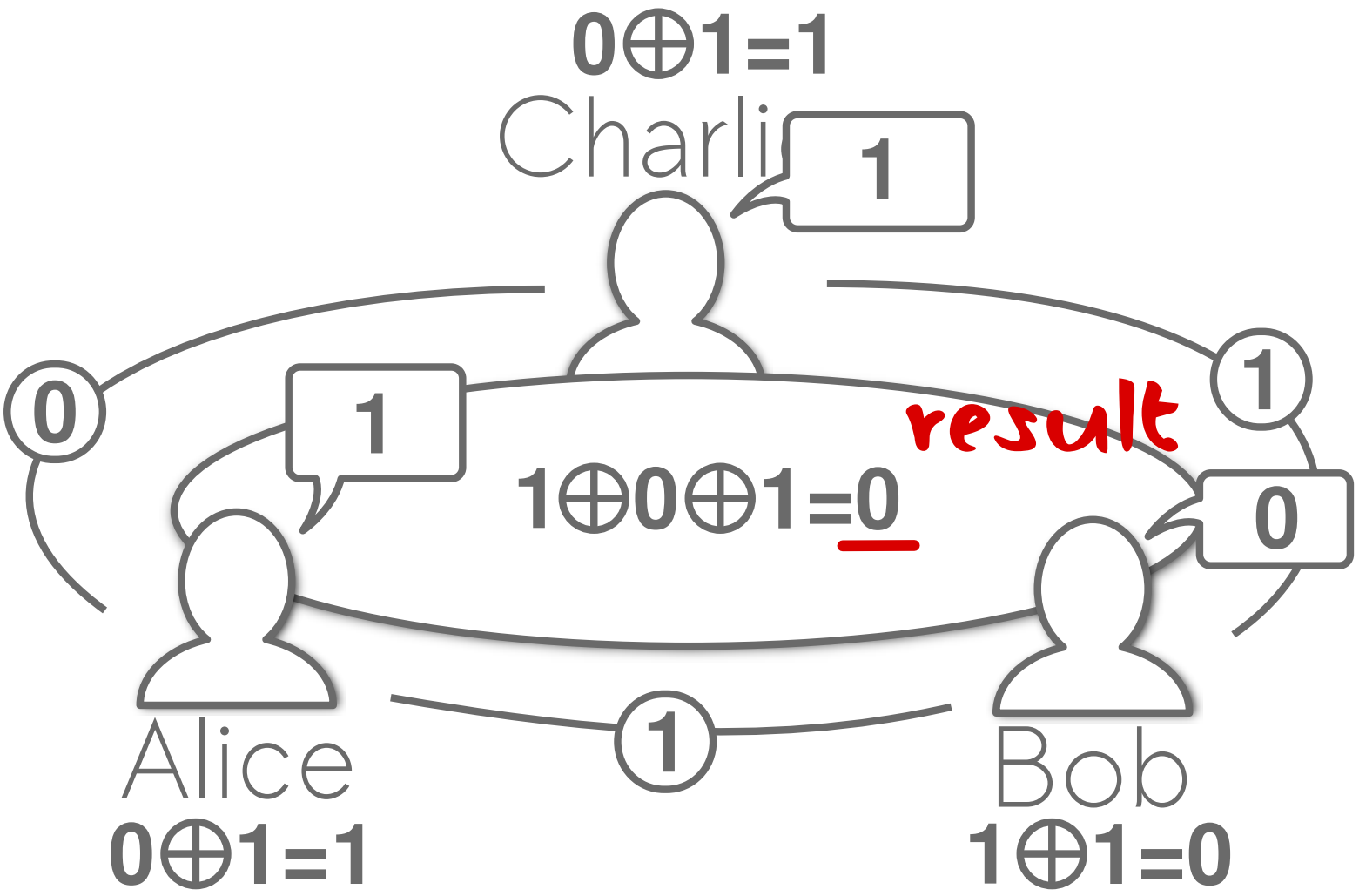
(Chaum, 1988)

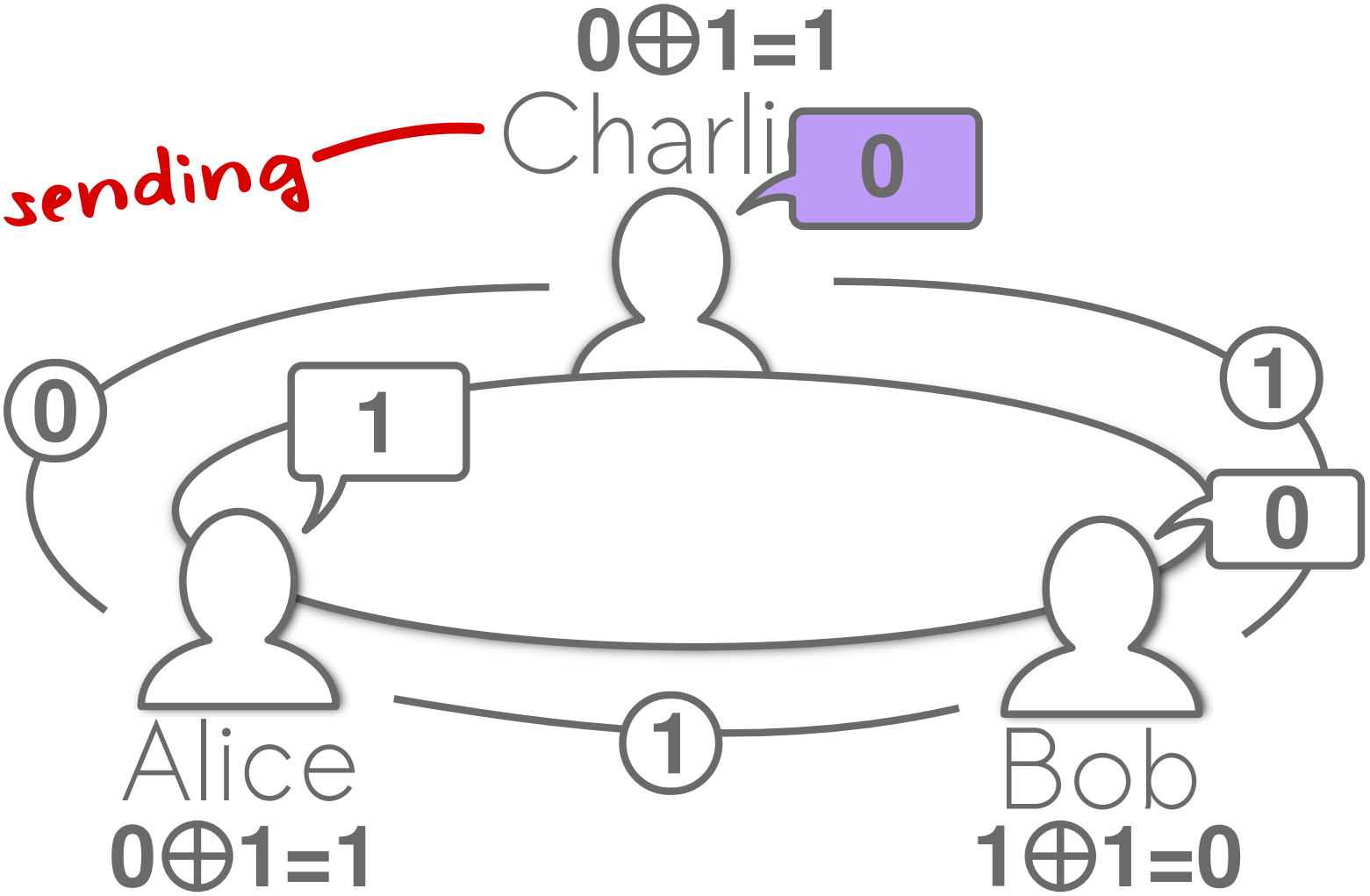

Charlie
Alice
Bob

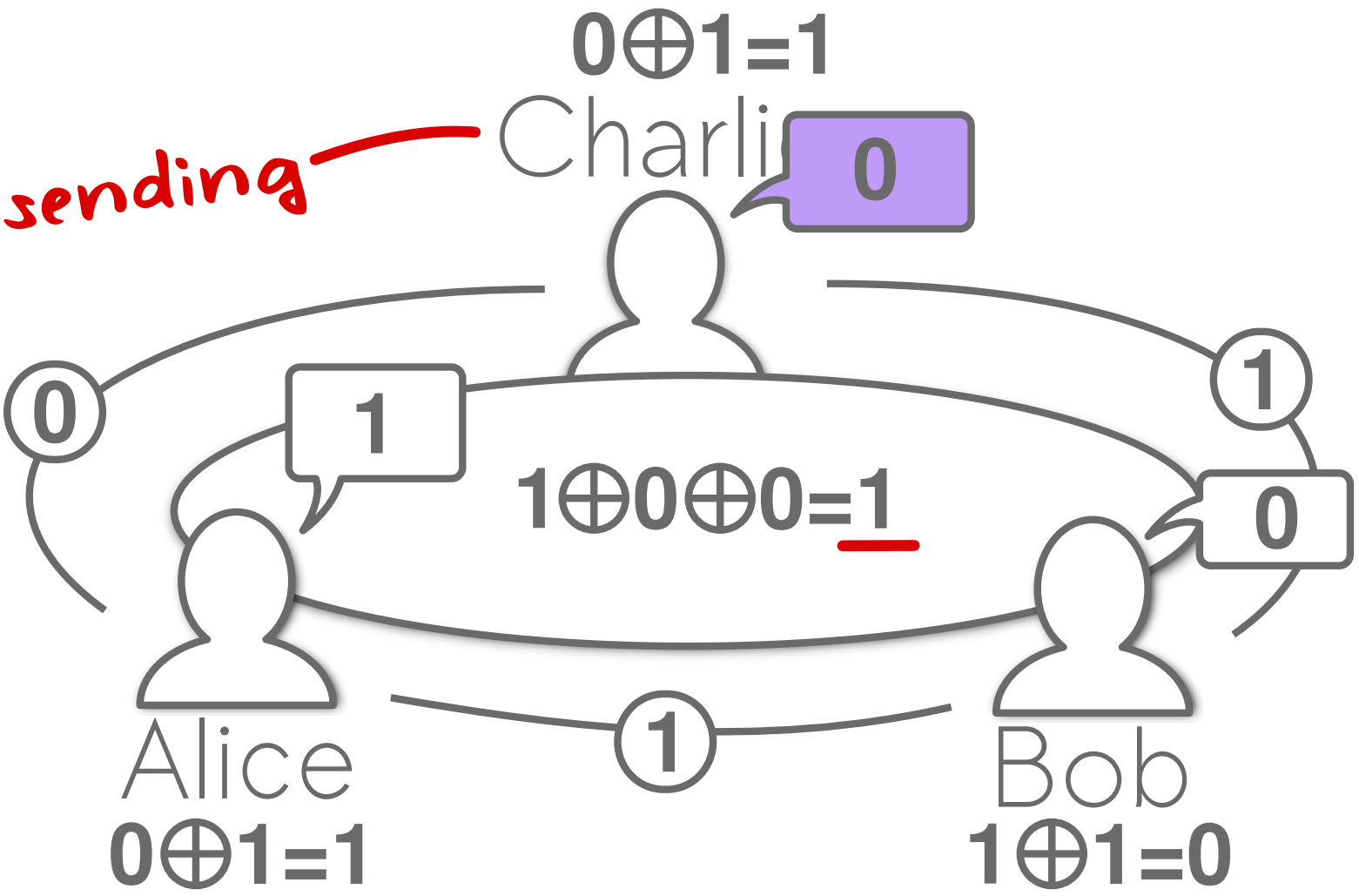

Charlie
0
1
Alice
1
Bob


key
Charlie
0
1
Alice
1
Bob

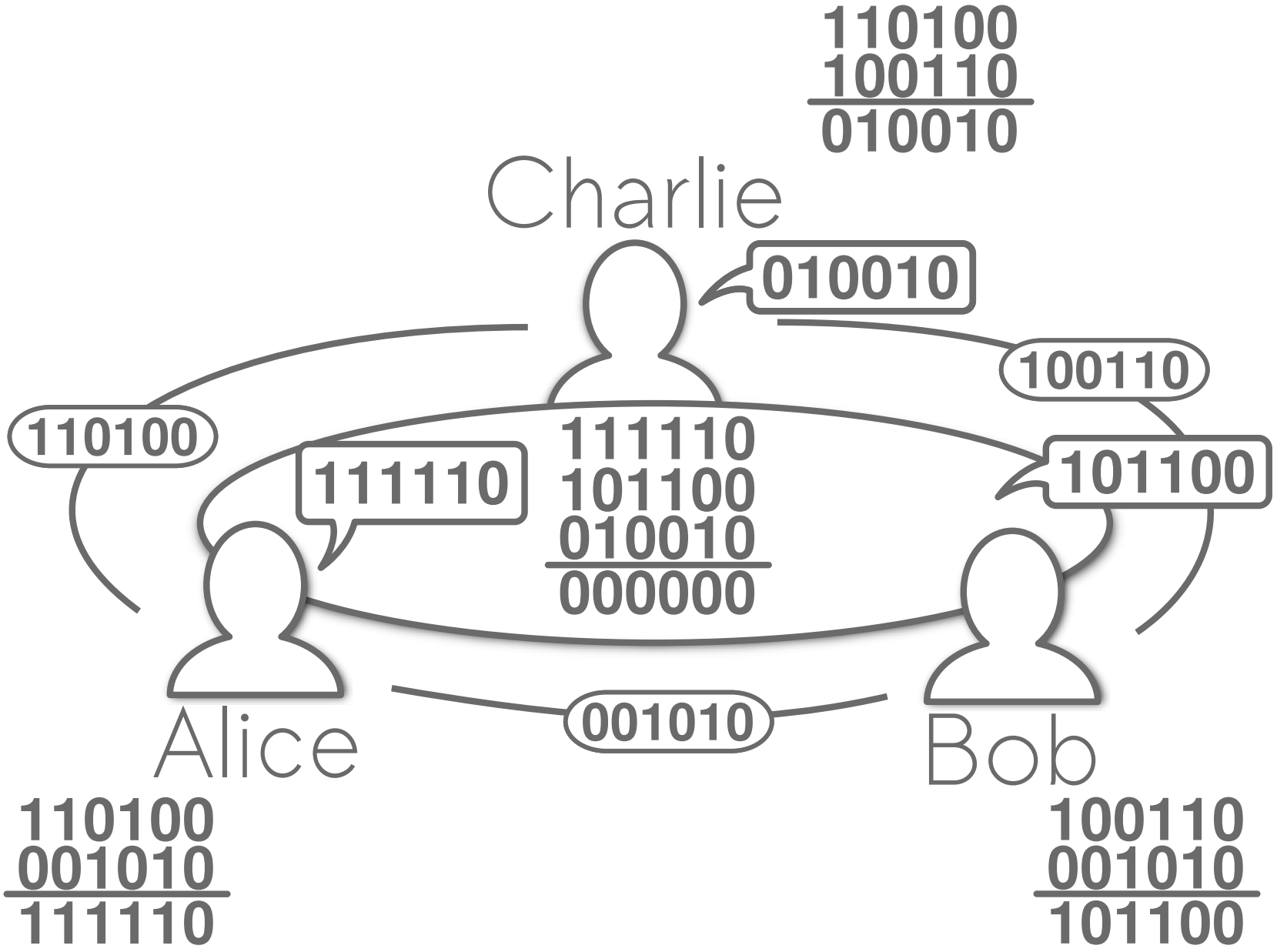

0⊕1=1
Charli
1
0
1
1
0
1
Alice
0⊕1=1
Bob
1⊕1=0

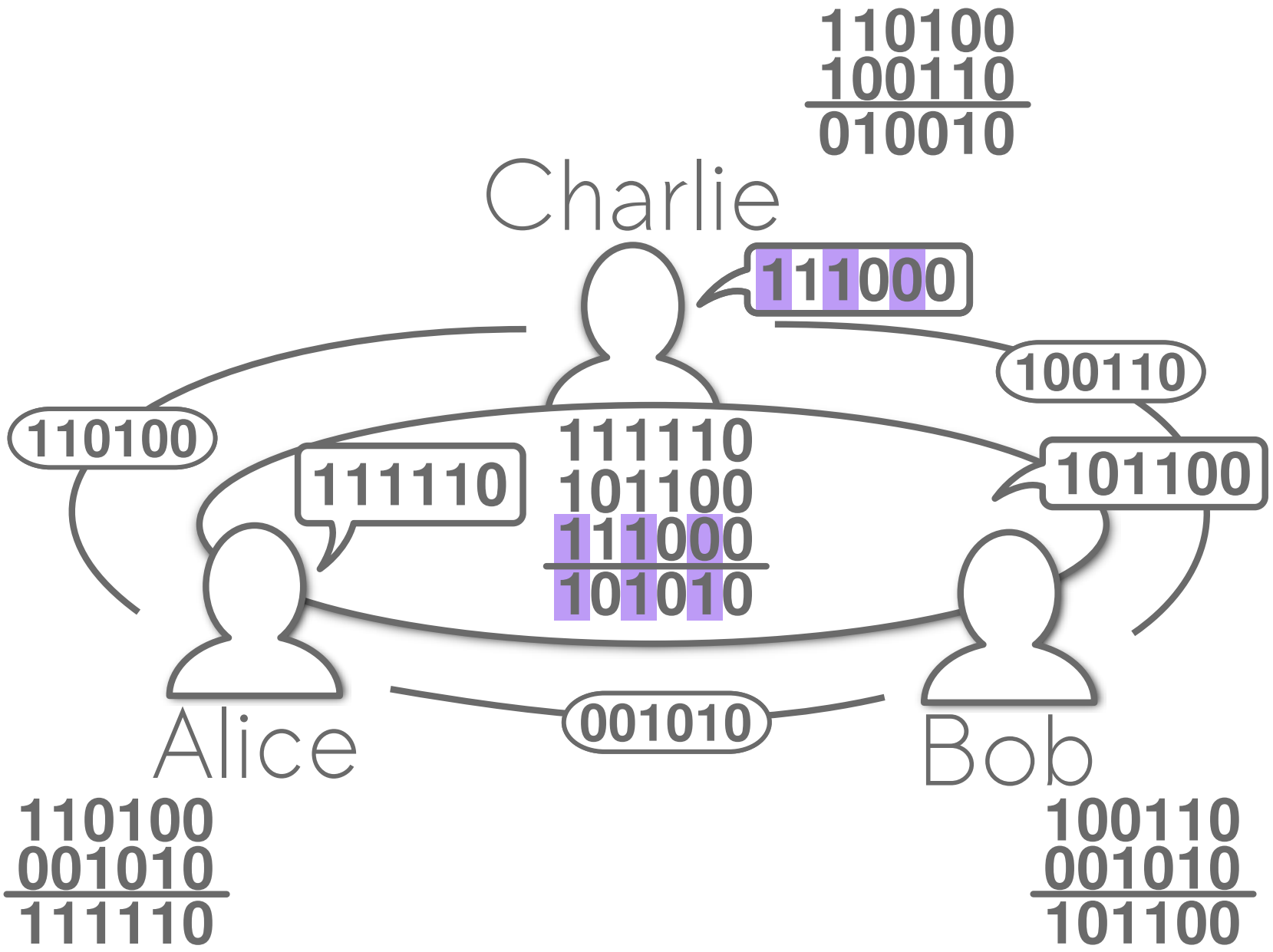

0⊕1=1
Charli
1
0
1
1
result
1⊕0⊕1=0
0
1
Alice
0⊕1=1
Bob
1⊕1=0

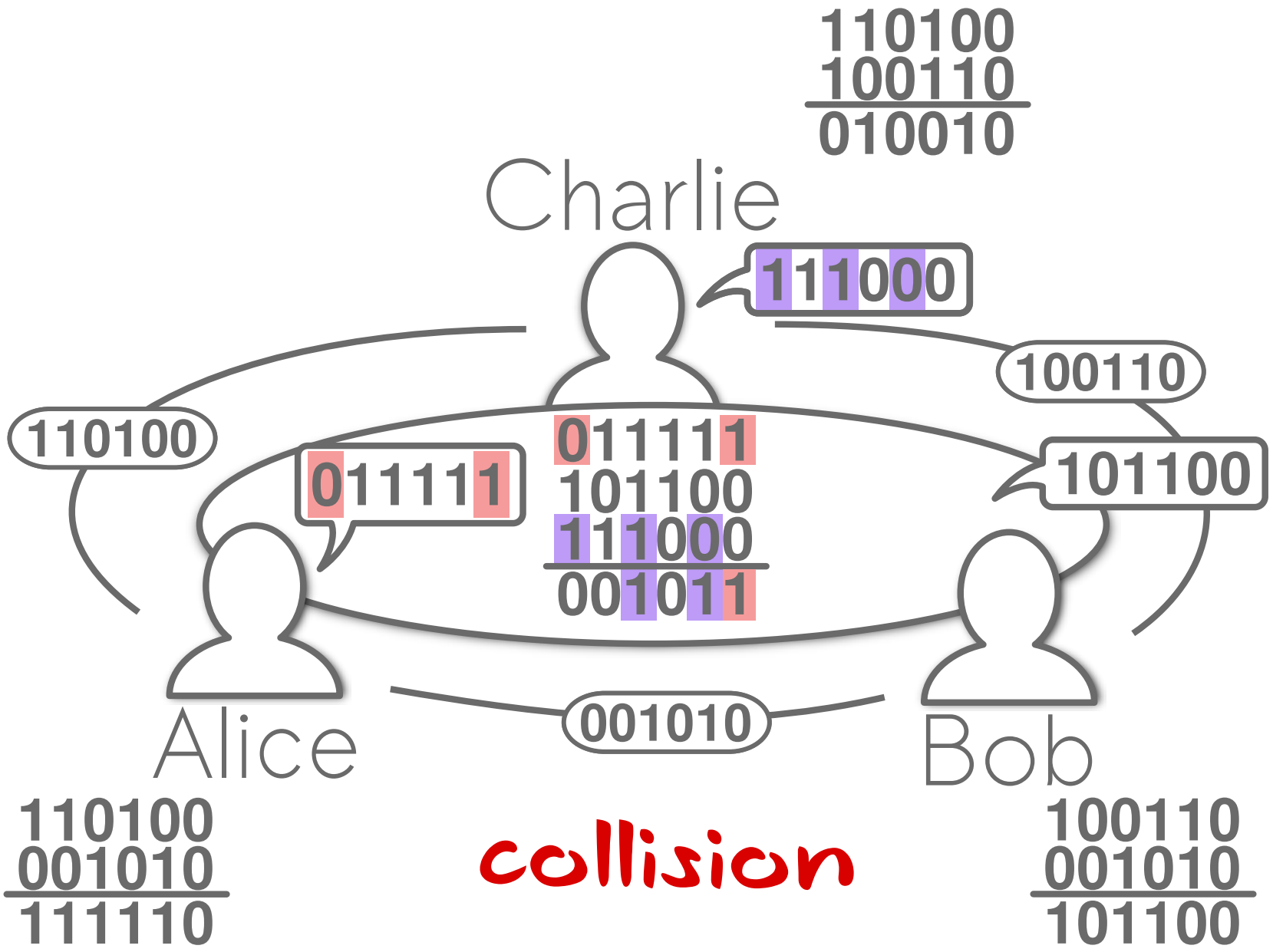

0⊕1=1
Charlie
sending
0
0
1
1
0
1
Alice
0⊕1=1
Bob
1⊕1=0


0⊕1=1
Charlie
sending
0
0
1
1
1⊕0⊕0=1
0
1
Alice
0⊕1=1
Bob
1⊕1=0

More Bits


110100
100110
010010
Charlie
010010
100110
110100
111110
101100
010010
000000
111110
101100
Alice
001010
Bob
110100
001010
111110
100110
001010
101100


110100
100110
010010
Charlie
111000
100110
110100
111110
101100
111110
101100
111000
101010
Alice
001010
Bob
110100
001010
111110
100110
001010
101100


110100
100110
010010
Charlie
111000
100110
110100
011111
101100
011111
101100
111000
001011
Alice
001010
Bob
110100
001010
111110
collision
100110
001010
101100

Collisions

Multiple senders → Collision
Corruption → Retransmission
Wasted traffic → Inefficient

Collisions

Multiple senders → Collision
Corruption → Retransmission
Wasted traffic → Inefficient

BAD

Collisions

More users → More collisions
→ More corruption
→ More traffic waste

WORSE

Recap

DC networks:

Unconditional anonymity

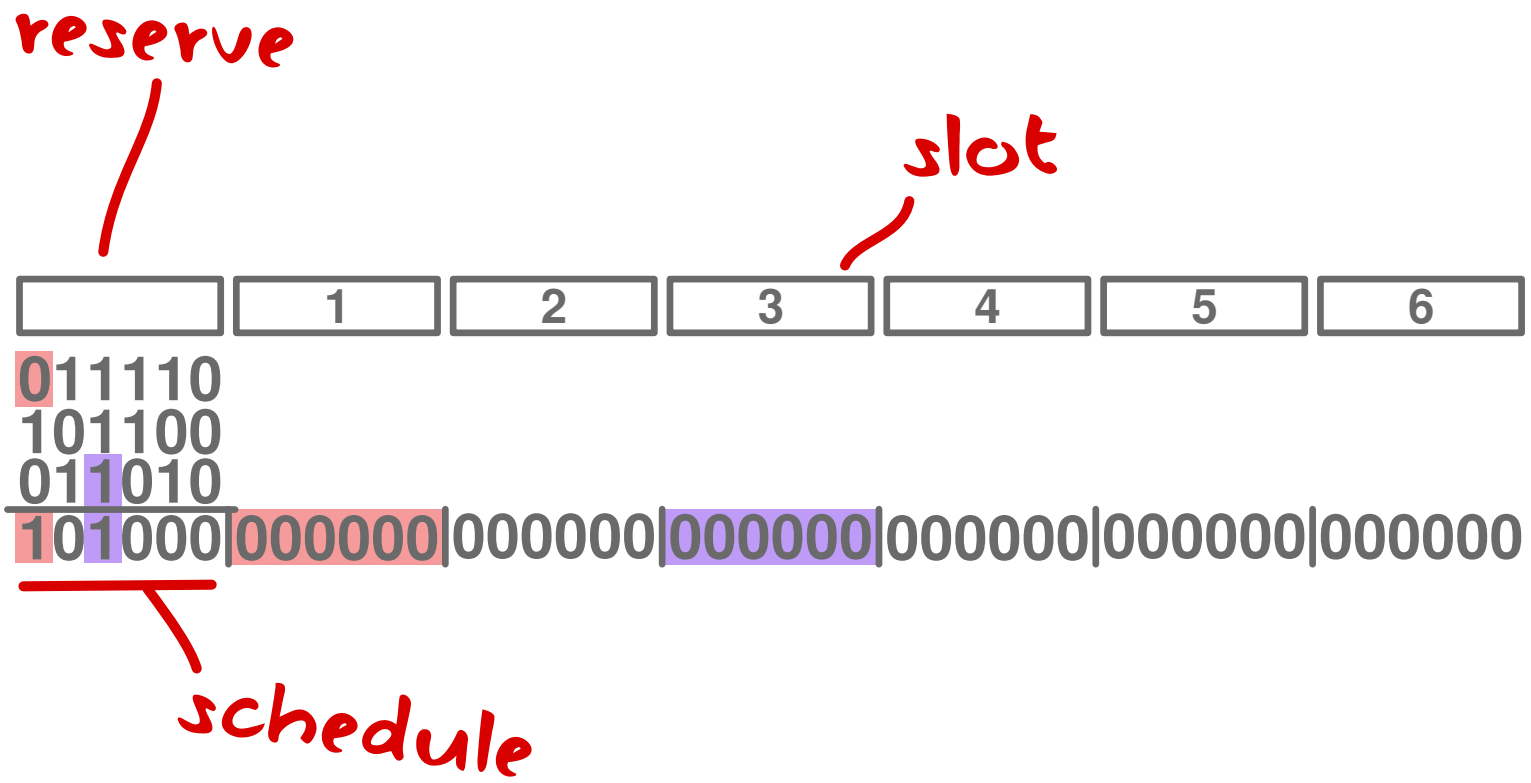
Arbitrary messages

Many participants

High traffic load

Collisions

Scheduling


reserve
slot
1
2
3
4
5
6
011110
101100
011010
101000|000000|000000|000000|000000|000000|000000
schedule

Collisions during reservation?

Detectable

```
110110
101100
011010
------
000000
```

Undetectable

```
110110
100100
011010
------
001000
```

More slots! → Herbivore

Herbivore

Goel, Robson, Polte, Sirer 2003

More Slots!

~1000 × #users

doesn't scale

Inactive users:

more slots than needed

Disconnected users:

not relevant

Divide-and-conquer

small sub-nets

small anonymity set ☹

http://www.cs.cornell.edu/People/egs/papers/herbivore-tr.pdf

~~Herbivore~~ doesn't scale

Goel, Robson, Polte, Sirer 2003

Tree-like collision resolution with superposed receiving

Andreas Pfitzmann, 1990

http://dud.inf.tu-dresden.de/sirene/publ/Pfit_88_0.pdf … _6.pdf

Pfitzmann's algorithm

Andreas Pfitzmann, 1990

Pick slot

Slot index through DC-net

Finite field addition

http://dud.inf.tu-dresden.de/sirene/publ/Pfit_88_0.pdf … _6.pdf

slots **1...12**

Alice:	**3**	**1**
Bob:	**7**	**1**
Charlie:	**2**	**1**
	12	**3**

slots **1...12**

Alice:	**3**	**1**
Bob:	**7**	**1**
Charlie:	**2**	**1**
	12	**3**

$$\lfloor 12/3 \rfloor = 4$$

slots **1...12**

Alice:	**3**	**1**	**3**	**1**
Bob:	**7**	**1**	**0**	**0**
Charlie:	**2**	**1**	**2**	**1**
	12	**3**	**5**	**2**

$\lfloor 12/3 \rfloor = 4$

slots **1...12**

Alice:	**3**	**1**	**3**	**1**	**0**	**0**
Bob:	**7**	**1**	**0**	**0**	**0**	**0**
Charlie:	**2**	**1**	**2**	**1**	**2**	**1**
	12	**3**	**5**	**2**	**2**	**1**
	$\lfloor 12/3 \rfloor = 4$		$\lfloor 5/2 \rfloor = 2$			

slots **1...12**

Alice:	**3**	**1**	**3**	**1**	**0**	**0**
Bob:	**7**	**1**	**0**	**0**	**0**	**0**
Charlie:	**2**	**1**	**2**	**1**	**2**	**1**
	12	**3**	**5**	**2**	**2**	**1**
	$\lfloor 12/3 \rfloor = 4$		$\lfloor 5/2 \rfloor = 2$			

public

2

slots **1...12**

Alice:	**3**	1	**3**	1	**0**	0
Bob:	**7**	1	**0**	0	**0**	0
Charlie:	**2**	1	**2**	1	**2**	1
	12	3	**5**	2	**2**	1

public

$\lfloor 12/3 \rfloor = 4$ $\lfloor 5/2 \rfloor = 2$

2	3	7

slots **1...12**

collision

Alice:	3	1	3	1	3	1
Bob:	3	1	3	1	3	1
Charlie:	11	1	0	0	0	0
	17	3	6	2	6	2
	$\lfloor 17/3 \rfloor = 5$		$\lfloor 6/2 \rfloor = 3$			

3	11

Pfitzmann's algorithm

Andreas Pfitzmann, 1990

Utilizes message collisions

No undetectable conflicts

Inactive users:

- no additional costs

http://dud.inf.tu-dresden.de/sirene/publ/Pfit_88_0.pdf … _6.pdf

unstable
connections
Emacs
Vim

Pfitzmann's algorithm

Andreas Pfitzmann, 1990

Utilizes message collisions

No undetectable conflicts

Inactive users:

- no additional costs

Disconnected users:

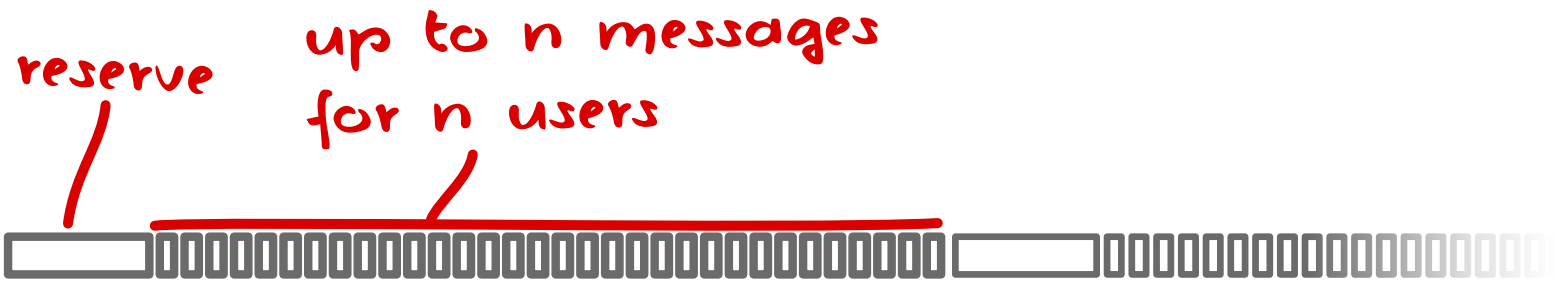
- breaks protocol

http://dud.inf.tu-dresden.de/sirene/publ/Pfit_88_0.pdf … _6.pdf

slots **1...12**

Alice:	**3**	**1**	**3**	**1**	**0**	**0**
Bob:	**7**	**1**	**0**	**0**	**0**	**0**
Charlie:	**2**	**1**	**2**	**1**	**2**	**1**
	12	**3**	**5**	**2**	**2**	**1**
	$\lfloor 12/3 \rfloor = 4$		$\lfloor 5/2 \rfloor = 2$			

Joining delay



linear in # users

~~Herbivore~~ doesn't scale

Goel, Robson, Polte, Sirer 2003

~~Pfitzmann's algorithm~~

Andreas Pfitzmann, 1990

breaks on disconnect

Dissent

Corrigan-Gibbs, Ford 2010

Anonymity by shuffle

Accountable

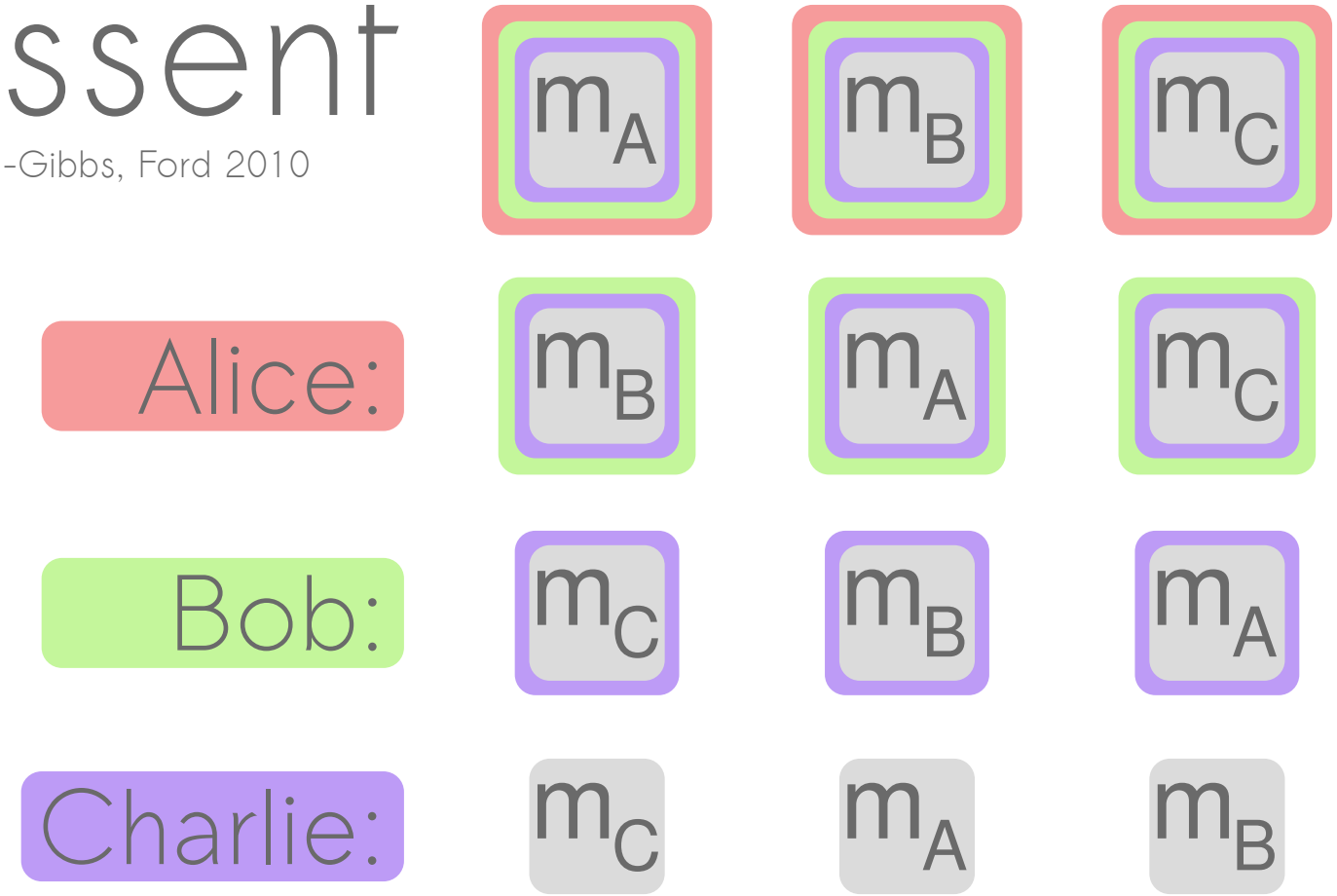
Two modes:

- shuffle
- bulk

http://dedis.cs.yale.edu/dissent/files/dissent.pdf

Dissent

Corrigan-Gibbs, Ford 2010



(simplified!)

http://dedis.cs.yale.edu/dissent/files/dissent.pdf

Dissent

Corrigan-Gibbs, Ford 2010

Guaranteed sending

Shuffle

- fixed message length

Bulk

- variable message length
- big computational overhead

side-channel

http://dedis.cs.yale.edu/dissent/files/dissent.pdf

~~Herbivore~~ doesn't scale

Goel, Robson, Polte, Sirer 2003

~~Pfitzmann's algorithm~~

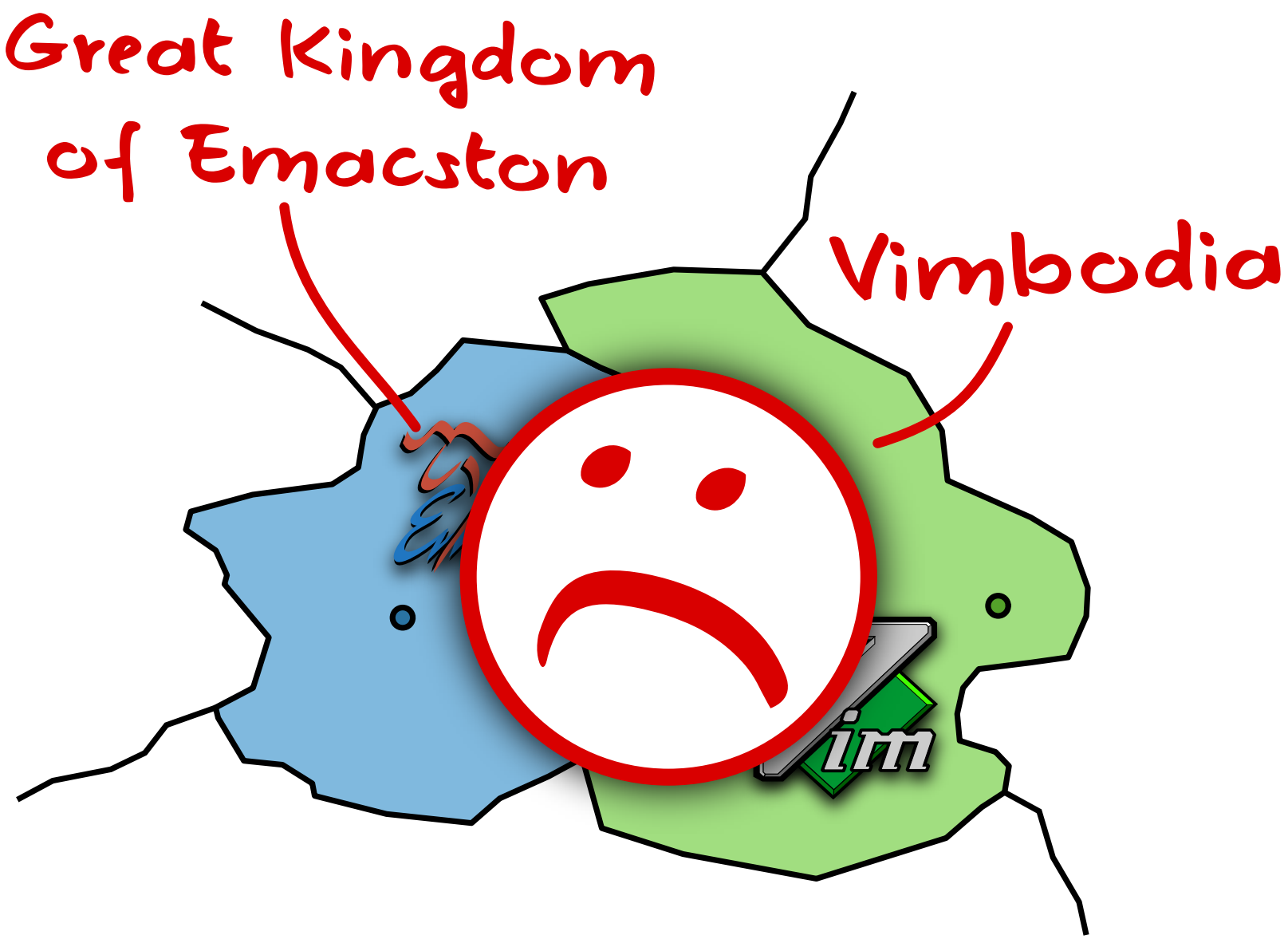
Andreas Pfitzmann, 1990

breaks on disconnect

~~Dissent~~ hard to implement

Corrigan-Gibbs, Ford 2010

breaks on disconnect


Great Kingdom
of Emacston
Vimbodia
Vim

Collisions during reservation?

Detectable

```
110110
101100
011010
------
000000
```

Undetectable

```
110110
100100
011010
------
001000
```

More slots!

More bits! → Fingerprint scheduling

Fingerprint scheduling

- More bits per slot
  - 2 bits for now
- More choices
  - Flip left / right / both bit(s)
  - → detect more collisions

fingerprint

Alice: **10**
Bob: **11**
Charlie: **01**

11.01.10
10.00.00
00.00.10

01.01.00

3 slots

Alice: **10**
Bob: **11**
Charlie: **01**

11.01.10
10.00.00
00.00.10
01.01.00

taken

free

II.

Alice: **01**
Bob: **11**
Charlie: **11**

11.10.00
01.11.11
01.01.01

11.00.10

01.01.00

previously

III.

Alice: **10**
Bob: **10**
Charlie: **01**

01.11.01
10.10.10
10.11.01

01.10.10

11.00.10
01.01.00 previously

III.

converged!

Alice: **10**
Bob: **10**
Charlie: **01**

01.11.01
10.10.10
10.11.01

01.10.10

11.00.10
01.01.00 previously

III. converged!

Alice: **10**
Bob: **10**
Charlie: **01**

01.11.01
10.10.10
10.11.01

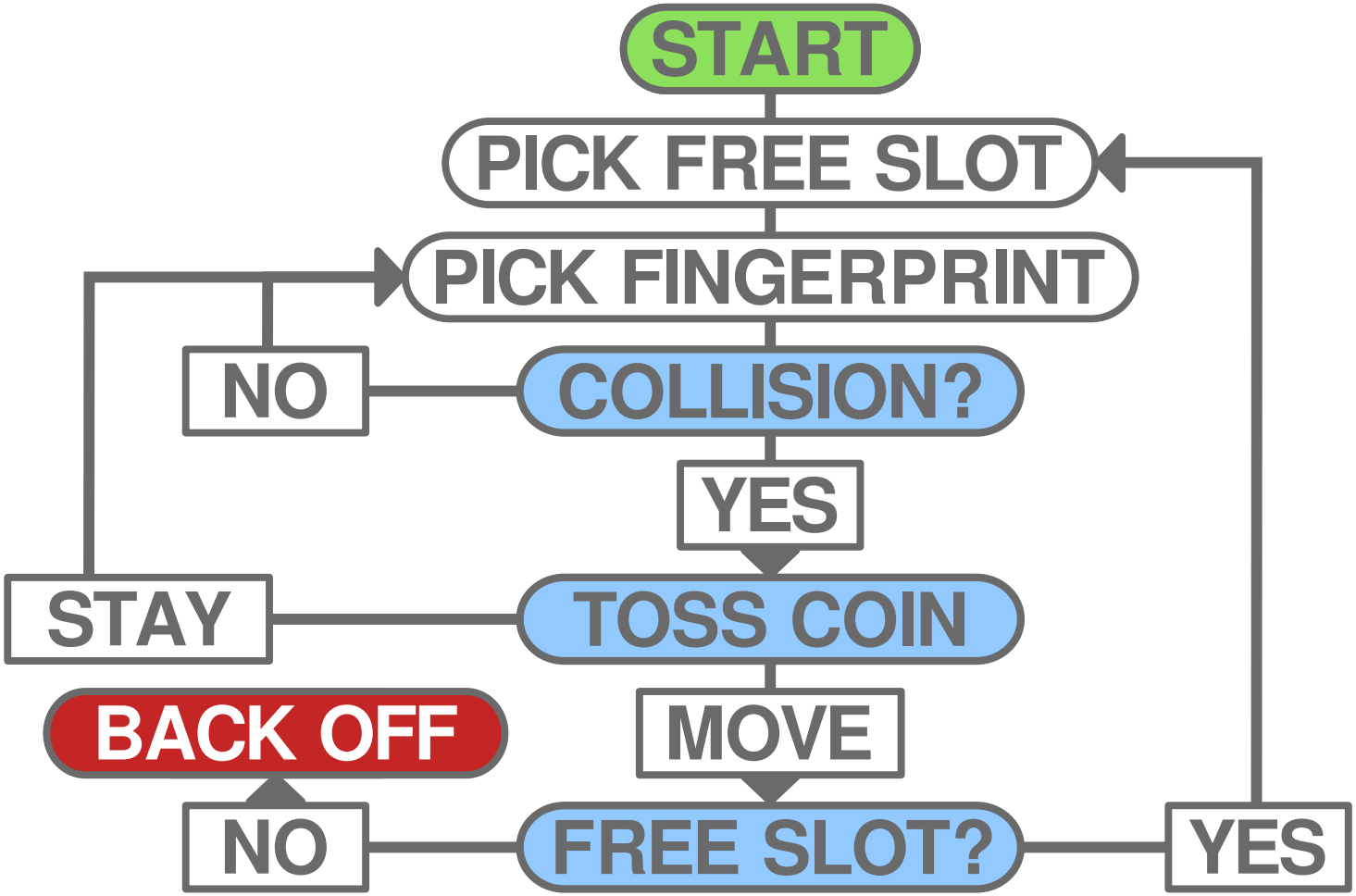
01.10.10

11.00.10
01.01.00 previously

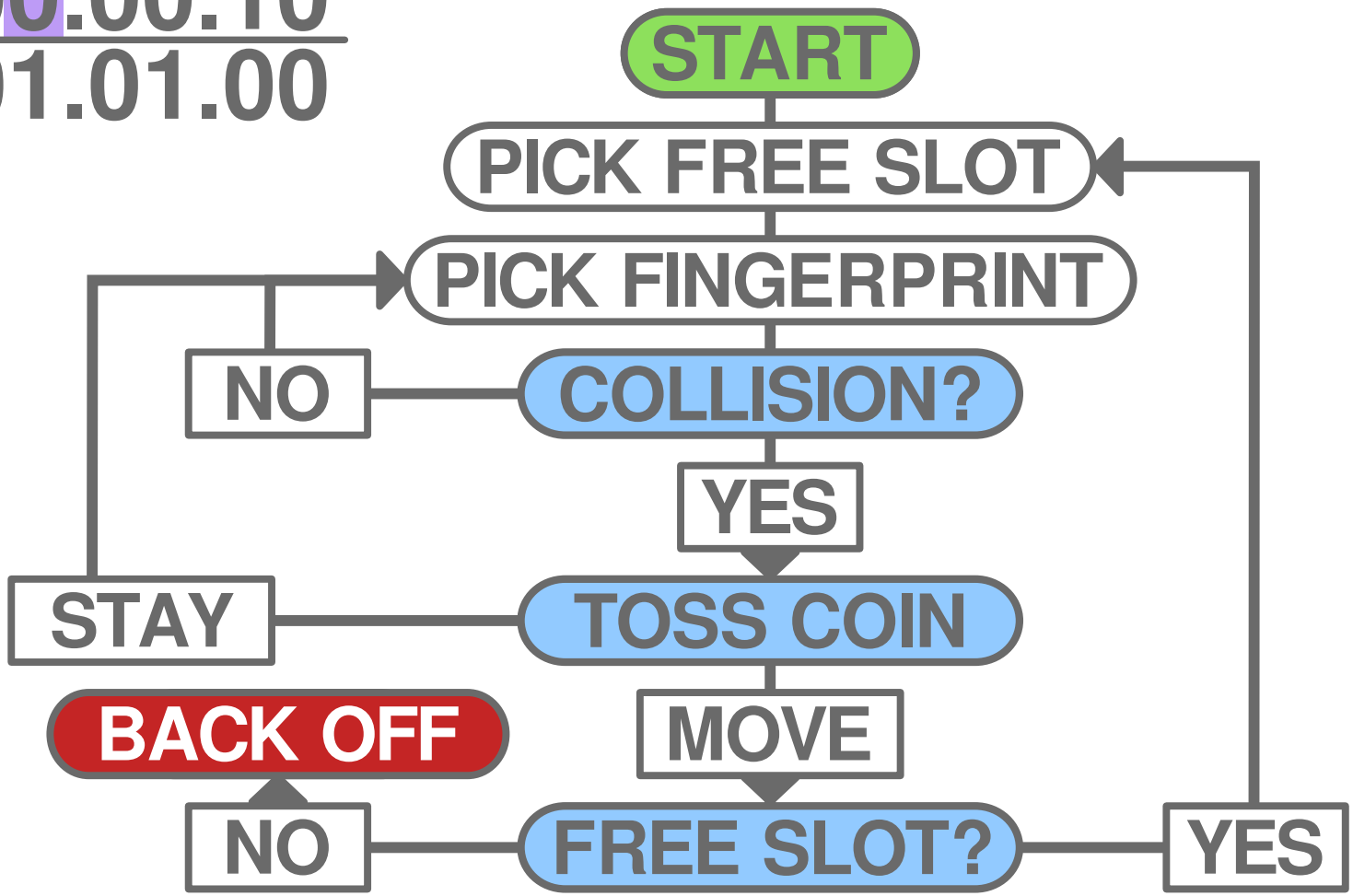
	1	2	3
01.10.10	000000	000000	000000

Fingerprint scheduling

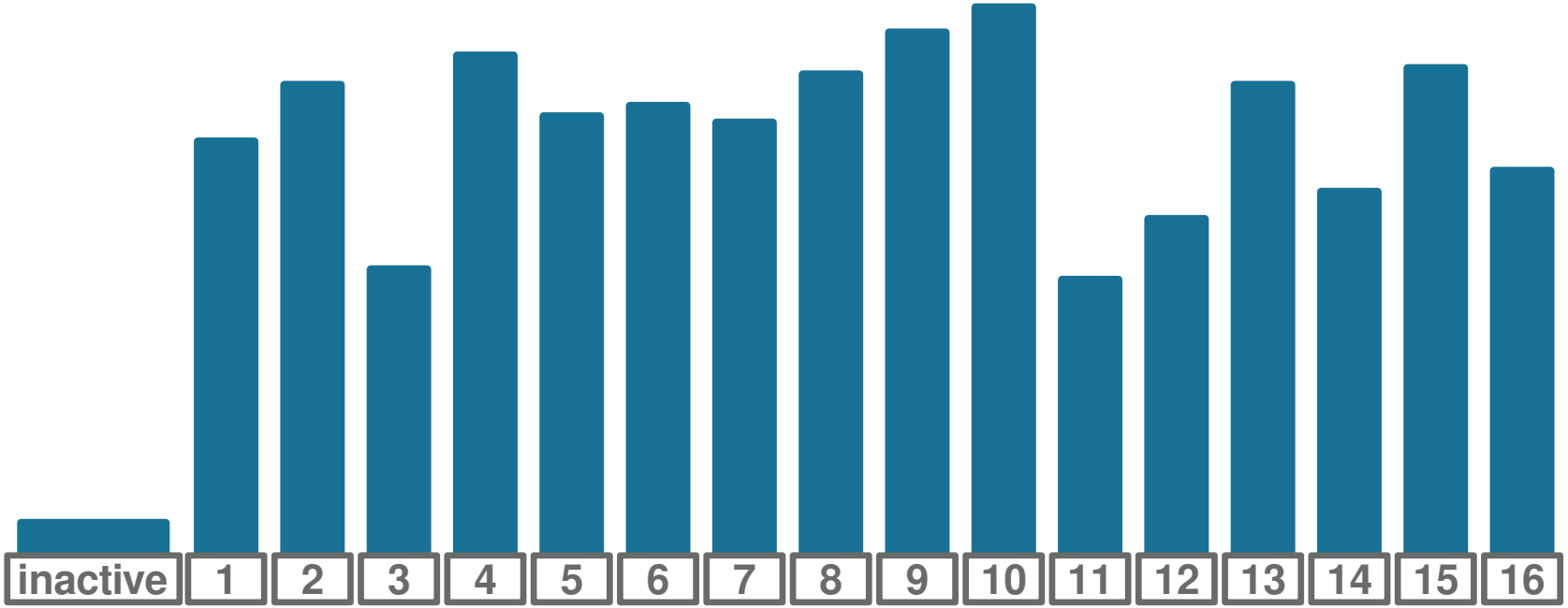
- `s` slots, choose one
- `b` bits
- Iterate
- Discussion


START
PICK FREE SLOT
PICK FINGERPRINT
NO
COLLISION?
YES
STAY
TOSS COIN
BACK OFF
MOVE
NO
FREE SLOT?
YES

11.01.10
10.00.00
00.00.10
01.01.00

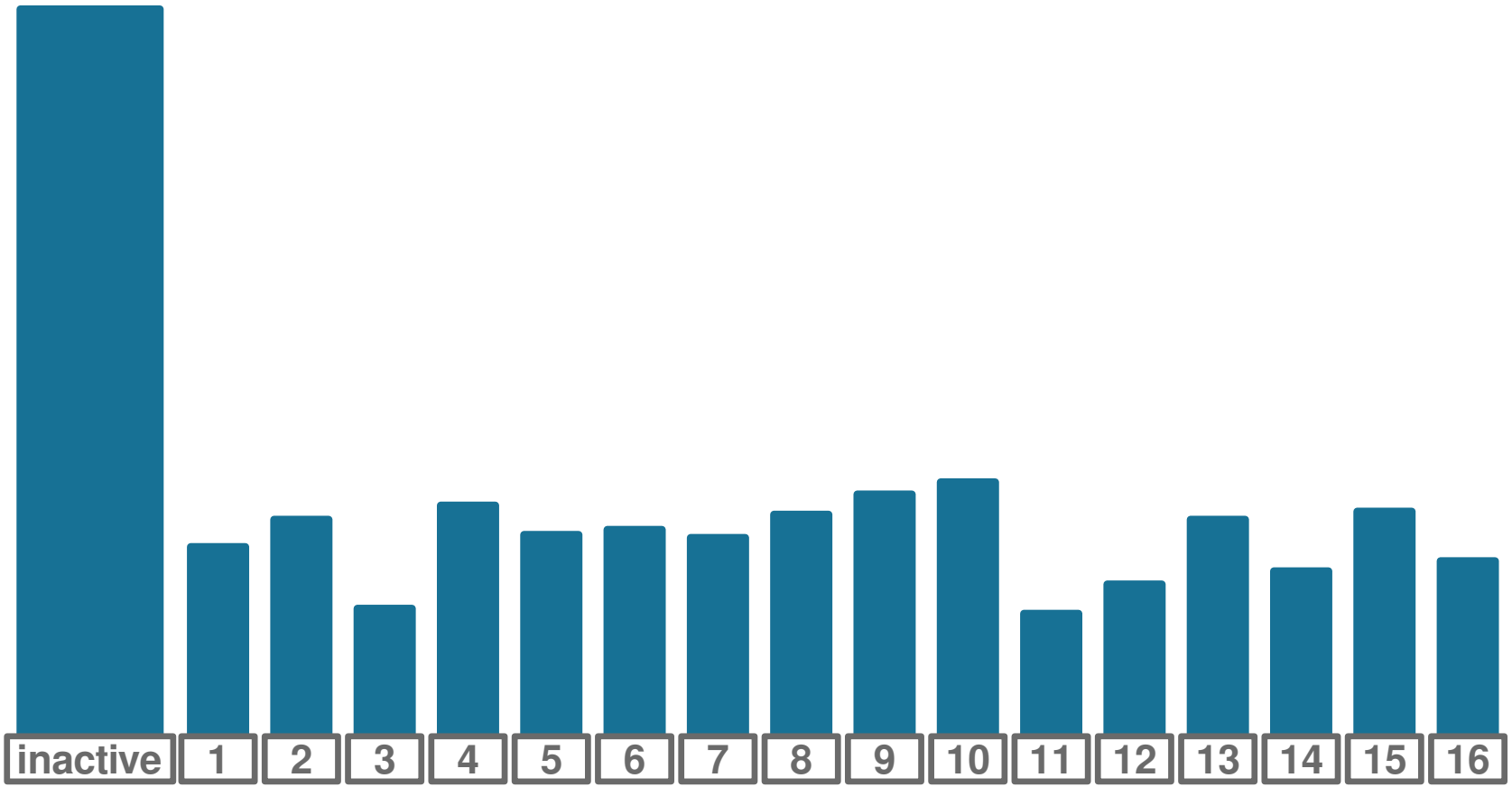


1,000 users



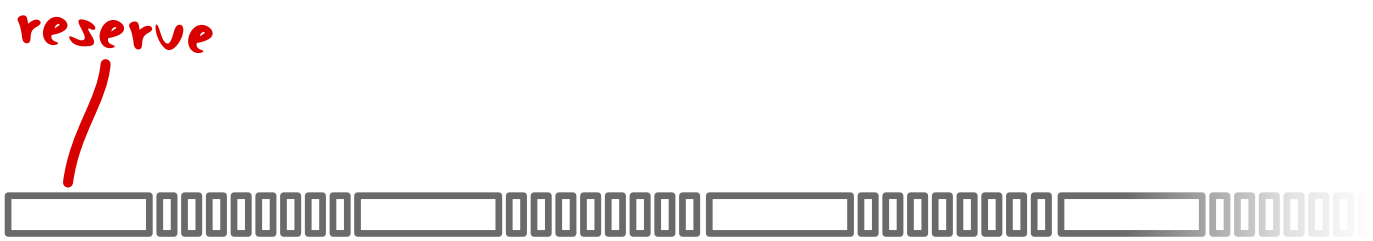
16 slots

1,000 users



16 slots

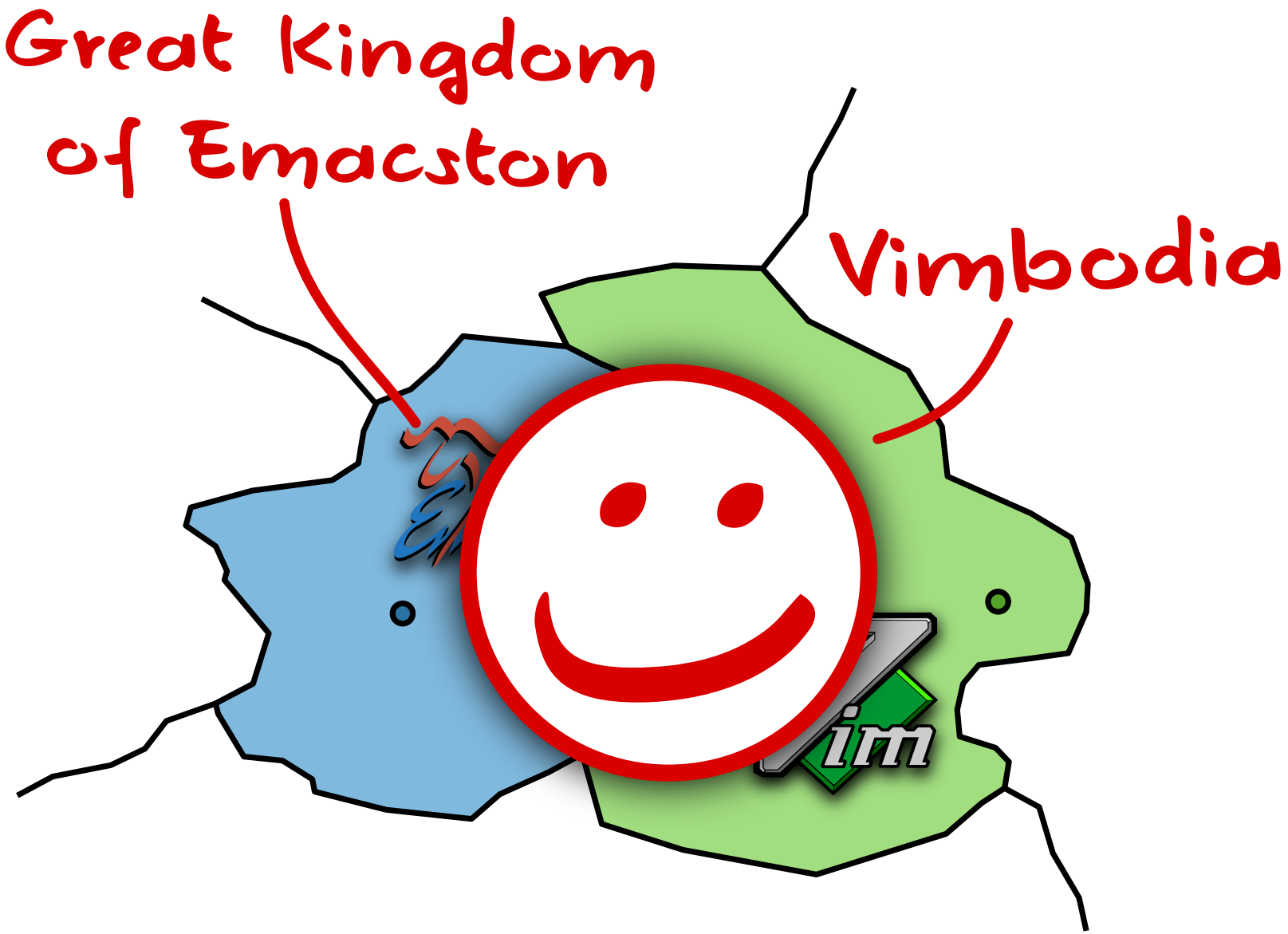
Joining delay



constant

Fingerprint scheduling

- **s** slots, choose one
- **b** bits
- Iterate
- Discussion
- Inactive users:
  - no additional costs
- Disconnected users:
  - compensated immediately


Great Kingdom
of Emacston
Vimbodia

THE VERY INCOMPLETE MATRIX OF DC-NETWORK SOLUTIONS AND THEIR PROPERTIES

	PFITZMANN	HERBIVORE	FINGERPRINT	DISSENT SHUFFLE	DISSENT BULK
Guaranteed Sending	✗	✗	✗	✓	✓
Adapt to load balance	INHERENT	ESTIMATED	INHERENT	✗ MANUAL	✓
Equal throughput	✗	✗	✗	✓	✗
Catch disruptors	EXTERNAL PROTOCOL	EXTERNAL PROTOCOL	EXTERNAL PROTOCOL	INHERENT	
False accusation				NEVER	
Computational overhead	LITTLE	NONE	LITTLE	LARGE	MASSIVE
Disconnected users	RESTART	IRRELEVANT	COMPENSATED	RESTART	

Fingerprint scheduling

Scales with # active users

Stable under disconnections

Fast, even in large networks

Simple to implement

No computational overhead

No more war about editors

m.neikes@student.ru.nl

Traditional alg.

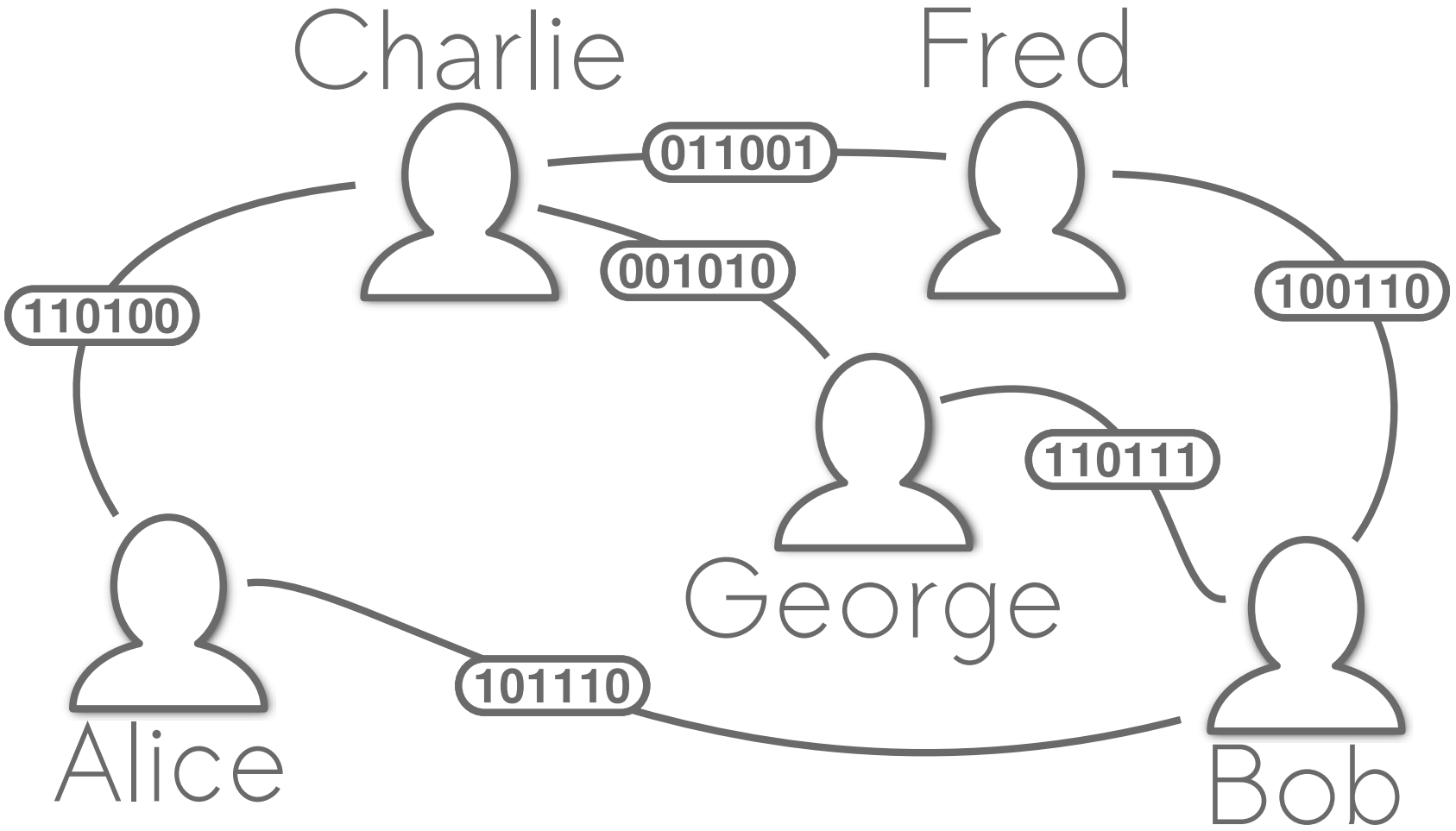
Collision resolution

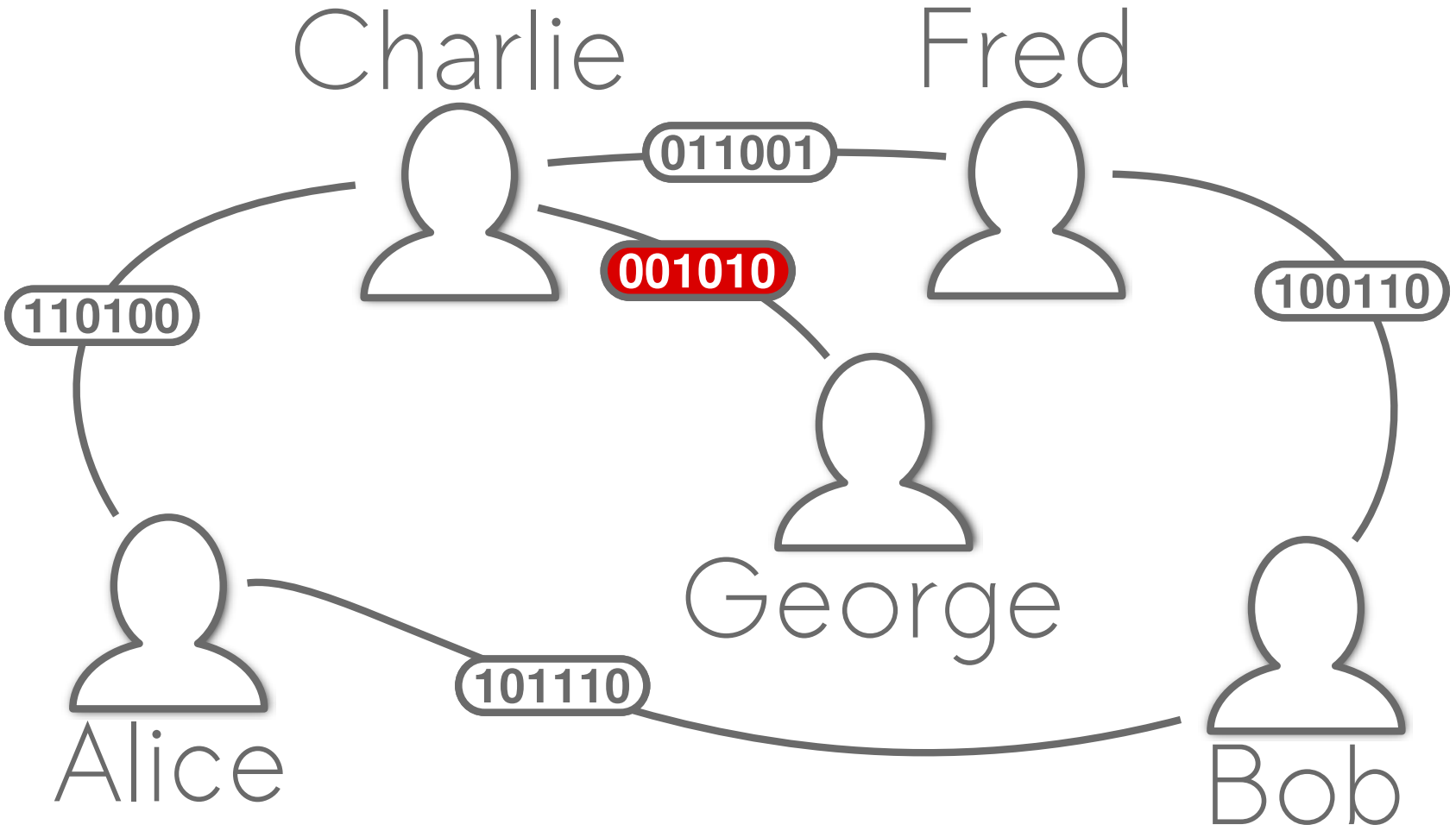
- (slotted) ALOHA — doesn't scale
- CSMA Carrier Sense Multiple Access — inefficient

Collision-free

- Bit-map protocols
- Tokens

no anonymity


Charlie
Fred
011001
001010
110100
100110
110111
George
101110
Alice
Bob


Charlie
Fred
011001
001010
110100
100110
George
101110
Alice
Bob