TECHNISCHE UNIVERSITÄT DRESDEN

PrimeLife

Faculty of Computer Science Institute of Systems Architecture, Chair of Privacy and Data Security

Privacy-Enhanced Event Scheduling

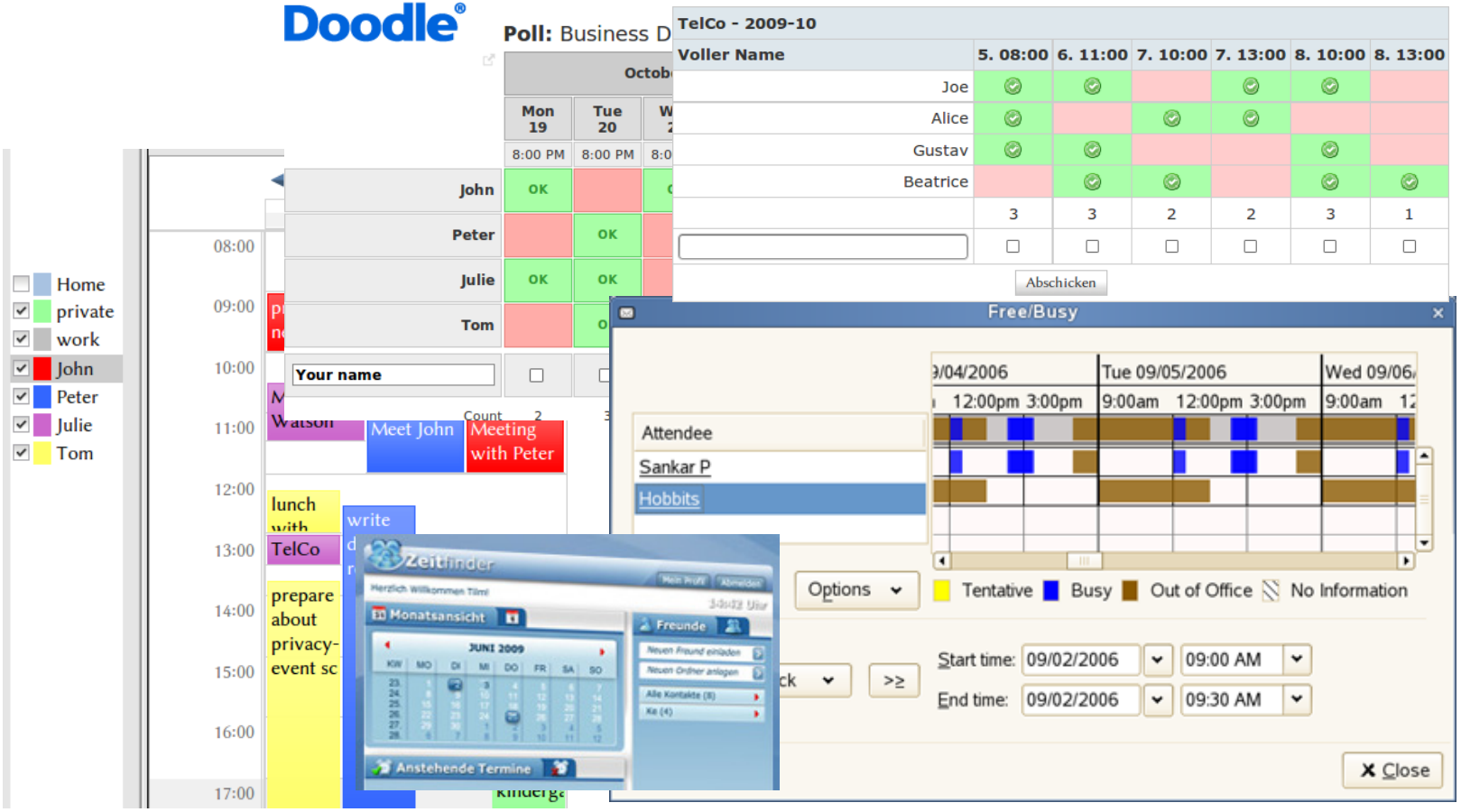
http://dudle.inf.tu-dresden.de

Benjamin.Kellermann@tu-dresden.de
D19E 04A8 8895 020A 8DF6
0092 3501 1A32 491A 3D9C

Berlin, December 29, 2009

PrimeLife is a research project funded by the European Commission's 7th Framework Programme

Event Scheduling



Privacy Problems

Direct Inference

Will my husband vote for the date of our wedding anniversary?

Doodle®

Poll: Business Dinner

	October 2009				
	Mon 19	Tue 20	Wed 21	Thu 22	Fri 23
	8:00 PM	8:00 PM	8:00 PM	8:00 PM	8:00 PM
John	OK		OK	OK	OK
Peter		OK		OK	OK
Julie	OK	OK		OK	
Tom		OK	OK	OK	OK
Your name	☐	☐	☐	☐	☐
Count	2	3	2	4	3

Privacy Problems

Direct Inference

Will my husband vote for the date of our wedding anniversary?

Doodle®

Poll: Business Dinner

	October 2009				
	Mon 19	Tue 20	Wed 21	Thu 22	Fri 23
	8:00 PM	8:00 PM	8:00 PM	8:00 PM	8:00 PM
John	OK		OK	OK	OK
Peter		OK		OK	OK
Julie	OK	OK		OK	
Tom		OK	OK	OK	OK
Your name	☐	☐	☐	☐	☐
Count	2	3	2	4	3

Privacy Problems

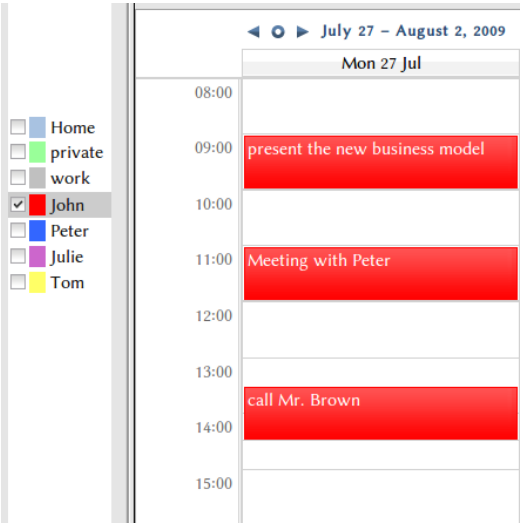
Indirect Inference

The availability pattern of user bunny23 looks suspiciously like the one of my employee John Doe!

Doodle®

Poll: Chat

	July 2009									
	Mon 27									
	8:00 AM	9:00 AM	10:00 AM	11:00 AM	12:00 PM	1:00 PM	2:00 PM	3:00 PM	4:00 PM	5:00 PM
MickeyMouse	OK	OK		OK	OK	OK	OK			
bunny23	OK		OK		OK			OK	OK	OK
superman1970		OK	OK	OK	OK	OK				
Snoopy		OK	OK	OK	OK	OK	OK		OK	OK
little_girl				OK	OK	OK		OK	OK	
Your name	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Count	2	3	3	4	**5**	4	2	2	3	2



Privacy Problems

Indirect Inference

The availability pattern of user bunny23 looks suspiciously like the one of my employee John Doe!

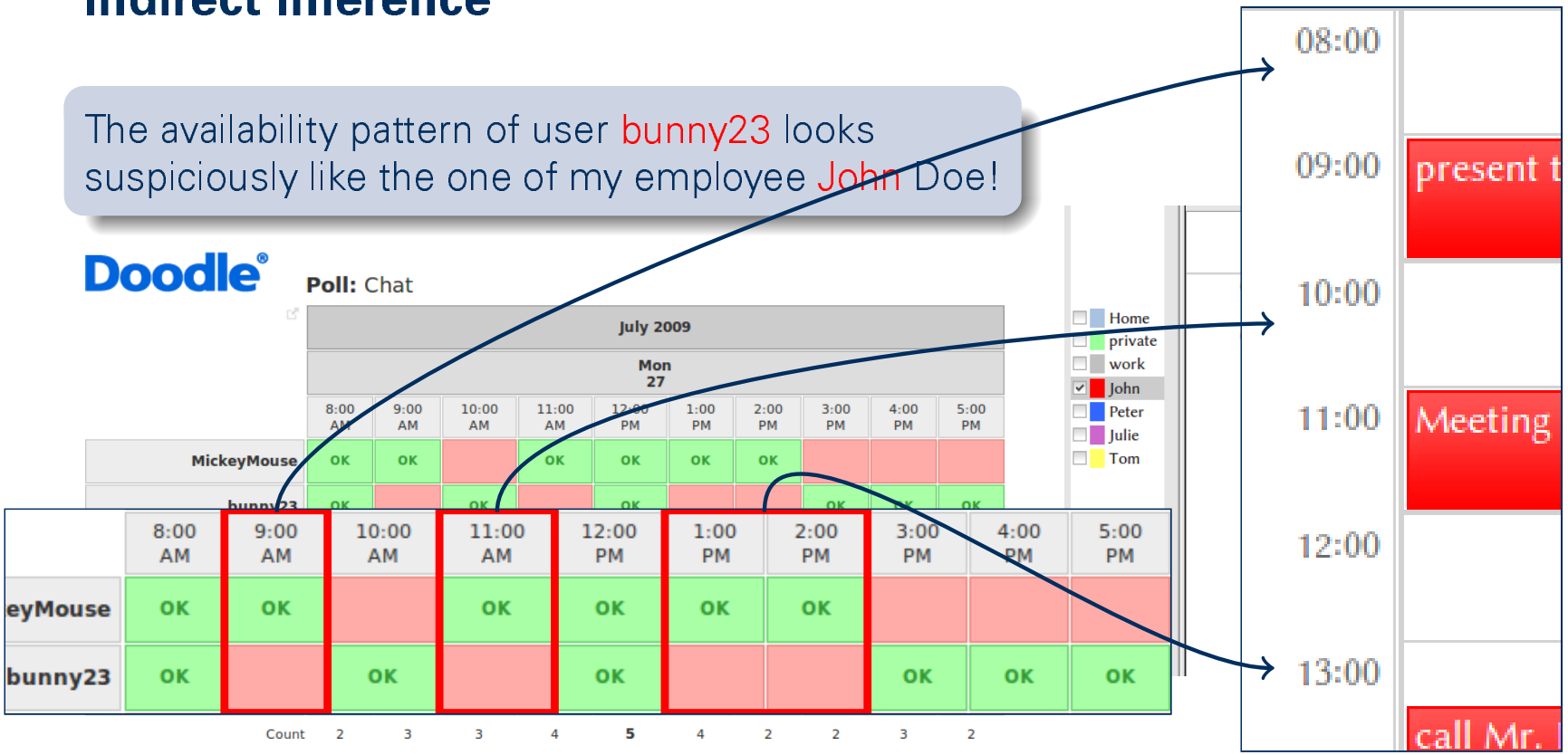


Table of Contents

GFDL Hajotthu

Requirements

- Untrusted Server

Requirements

- Untrusted Server
- Privacy
- Verifiability

Requirements

- Untrusted Server
- Privacy
- Verifiability
- Low Communication Complexity
- Low Computational Complexity

E-Voting vs. Event Scheduling

	Vote
Candidate #1	
Candidate #2	✘
⋮	
Candidate #10	

	Date #1	Date #2	...	Date #320
Yes	✘			✘
No		✘		

one vote per column

E-Voting vs. Event Scheduling

scales

	Vote
Candidate #1	
Candidate #2	✘
⋮	
Candidate #10	

	Date #1	Date #2	...	Date #320
Yes	✘			✘
No		✘		

one vote per column

E-Voting vs. Event Scheduling

scales

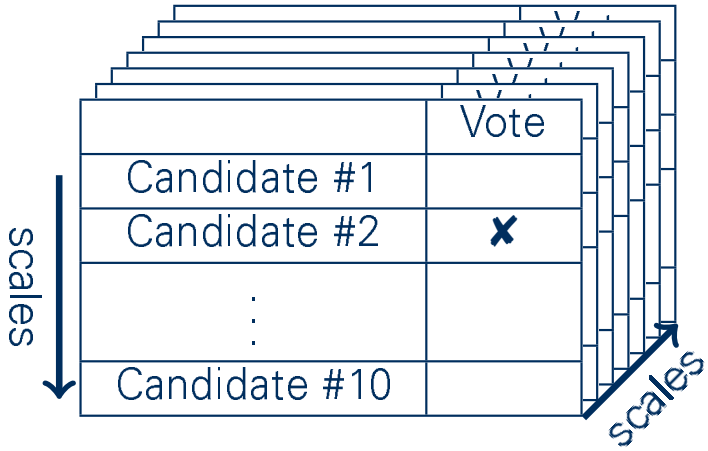
	Vote
Candidate #1	
Candidate #2	✘
⋮	
Candidate #10	

	Date #1	Date #2	...	Date #320
Yes	✘			✘
No		✘		

scales

one vote per column

E-Voting vs. Event Scheduling

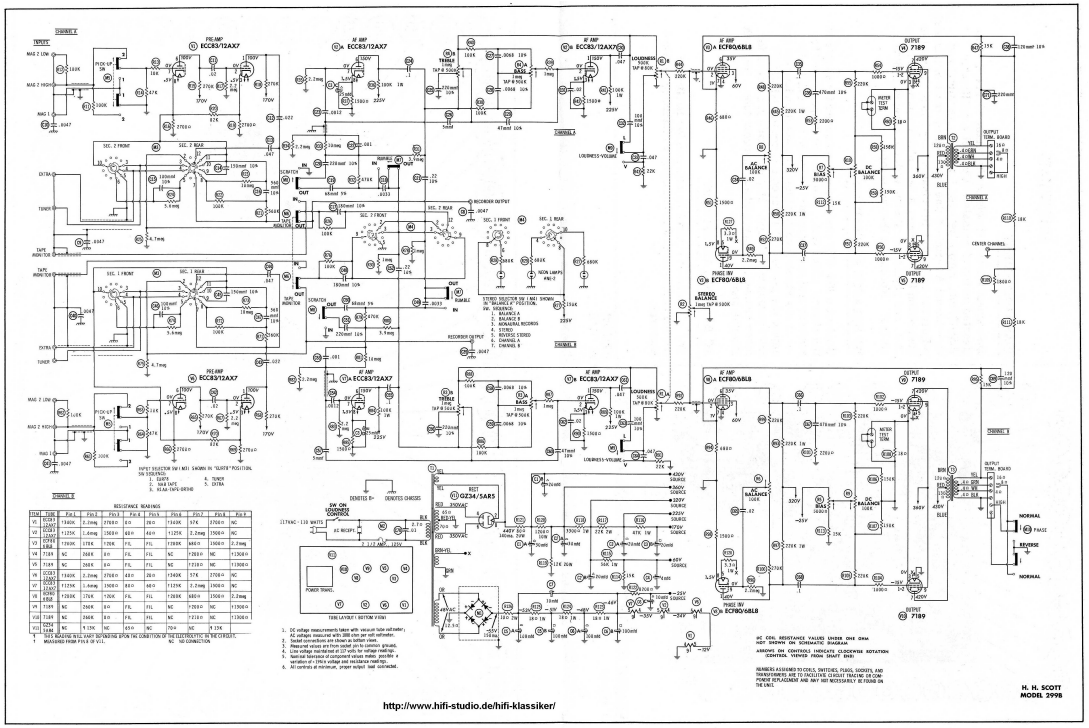


	Date #1	Date #2	...	Date #320
Yes	✘			✘
No		✘		

scales

one vote per column

Scheme



Superposed Sending

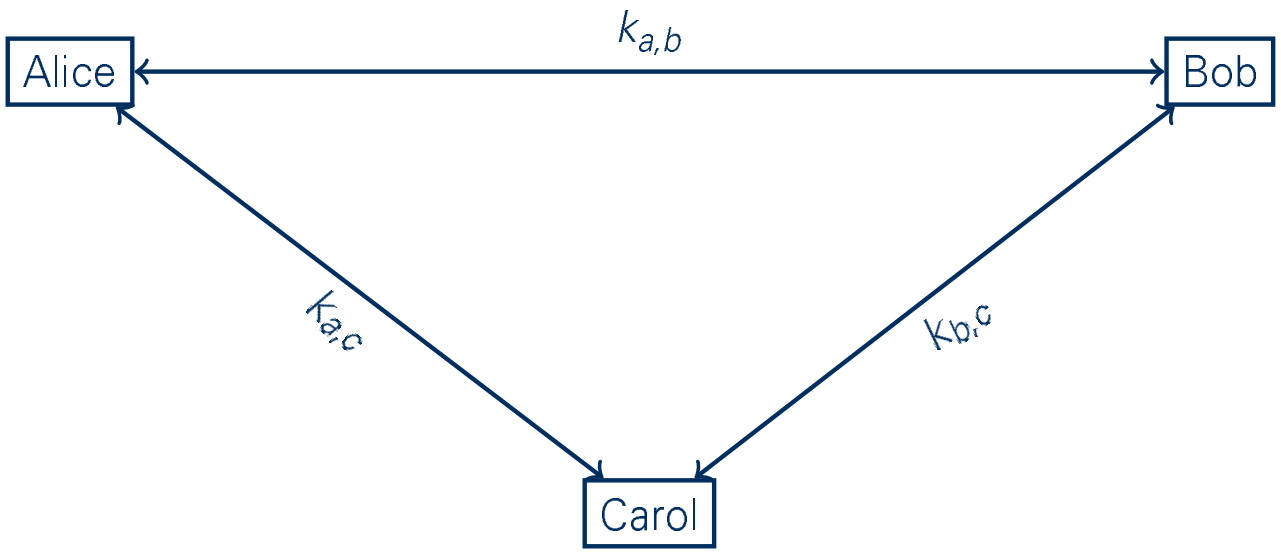
Alice

Bob

Carol

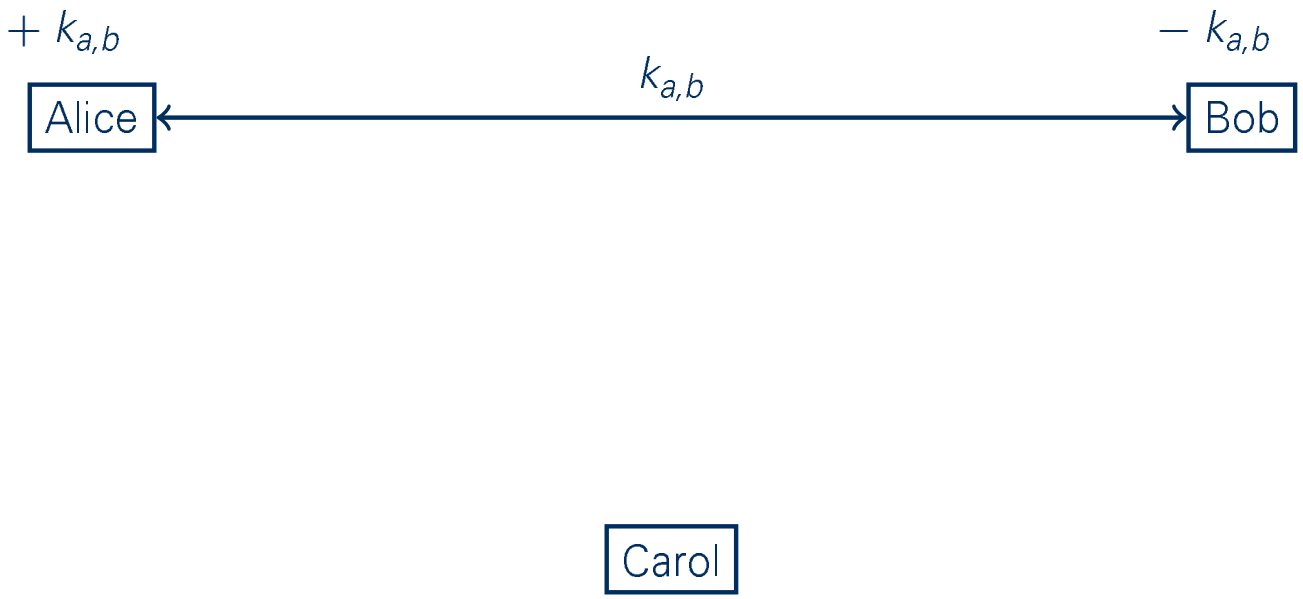
D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

Superposed Sending



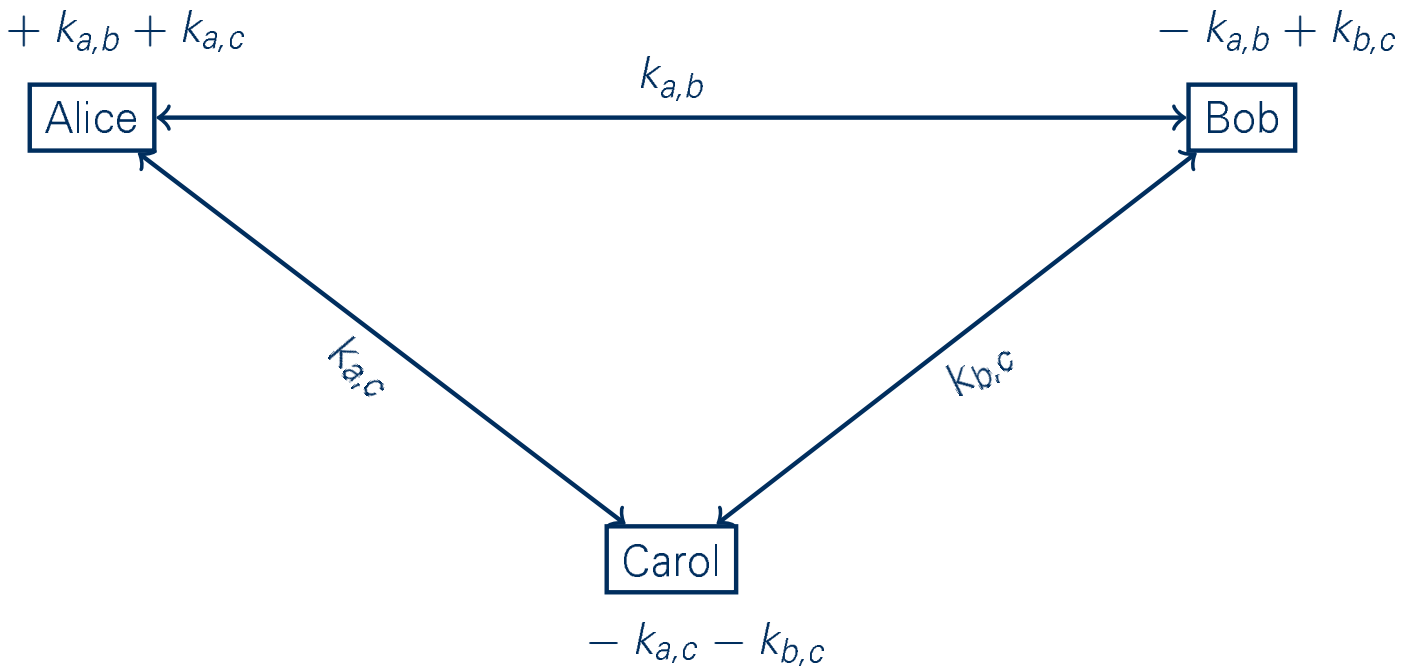
D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

Superposed Sending



D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

Superposed Sending



D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

Superposed Sending

$m_a + k_{a,b} + k_{a,c}$

Alice

$m_b - k_{a,b} + k_{b,c}$

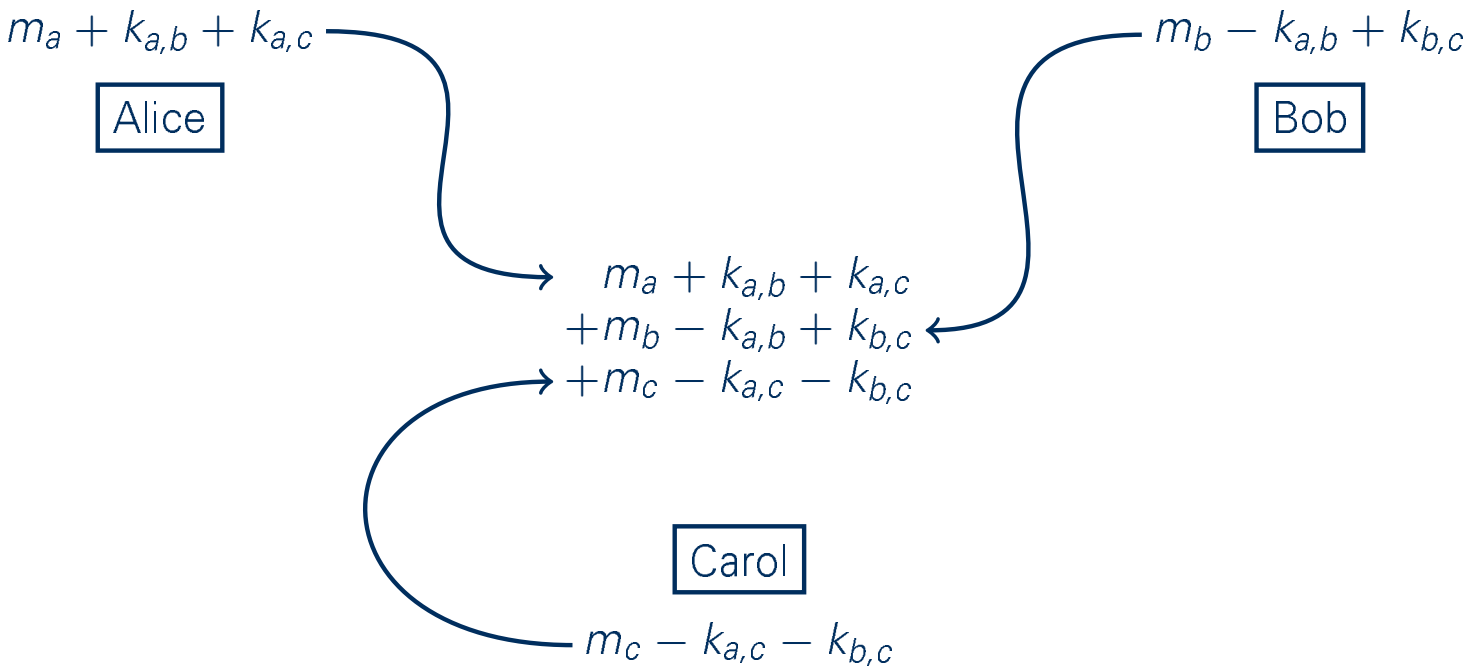
Bob

Carol

$m_c - k_{a,c} - k_{b,c}$

D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

Superposed Sending



D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

Superposed Sending

Alice

Bob

$$
\begin{aligned}
m_a &+ k_{a,b} + k_{a,c} \\
+m_b &- k_{a,b} + k_{b,c} \\
+m_c &- k_{a,c} - k_{b,c}
\end{aligned}
$$

Carol

D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

Superposed Sending

Alice

Bob

$$
\begin{array}{rl}
m_a & + k_{a,c} \\
+m_b & + k_{b,c} \\
+m_c - k_{a,c} & - k_{b,c}
\end{array}
$$

Carol

D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

Superposed Sending

Alice

Bob

$$
\begin{aligned}
& m_a && + k_{a,c} \\
+ & m_b \\
+ & m_c && - k_{a,c}
\end{aligned}
$$

Carol

D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

Superposed Sending

Alice

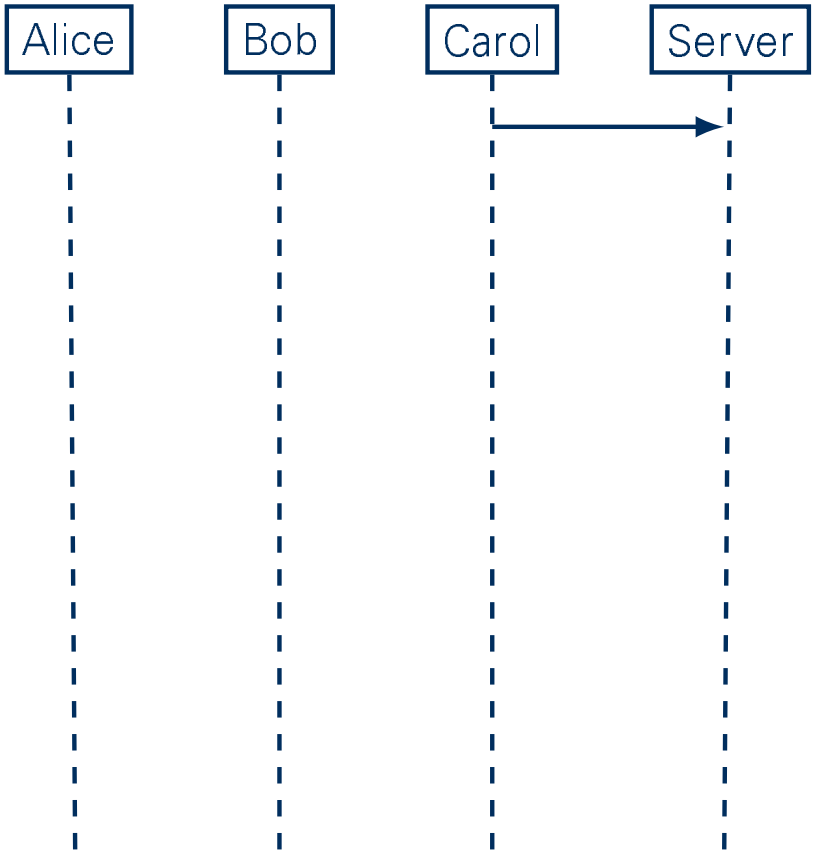
Bob

$$\begin{aligned} & m_a \\ + & m_b \\ + & m_c \end{aligned}$$

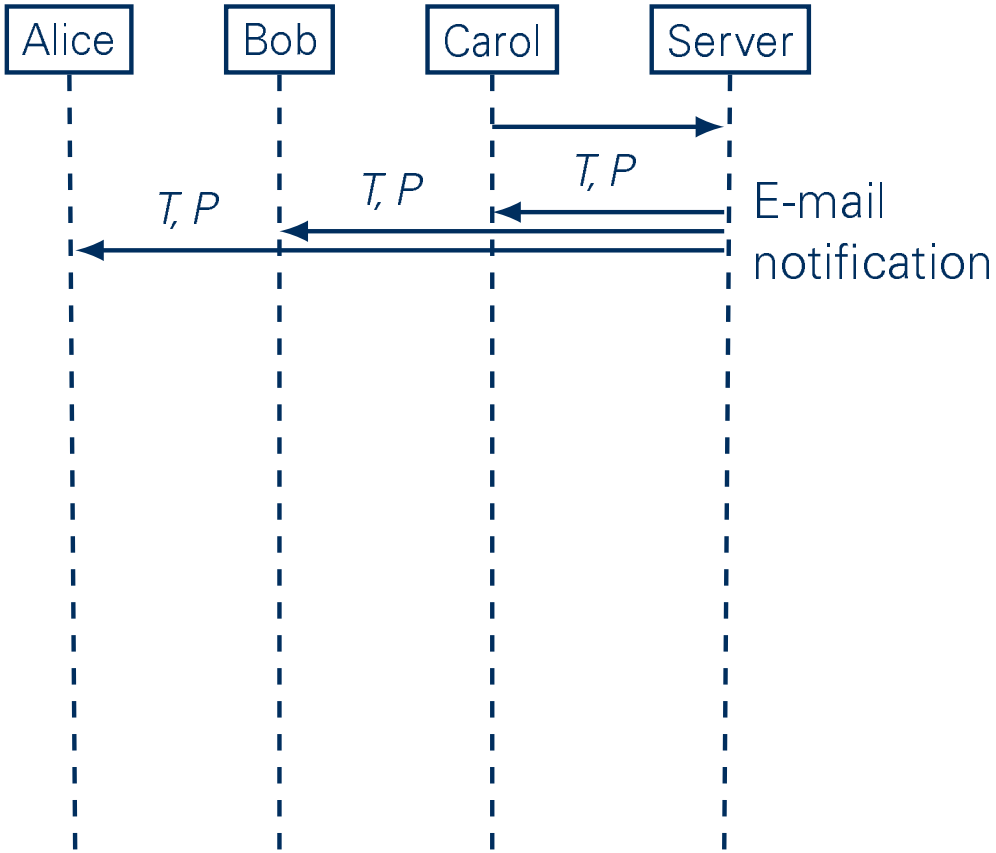
Carol

D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

Poll Initialization

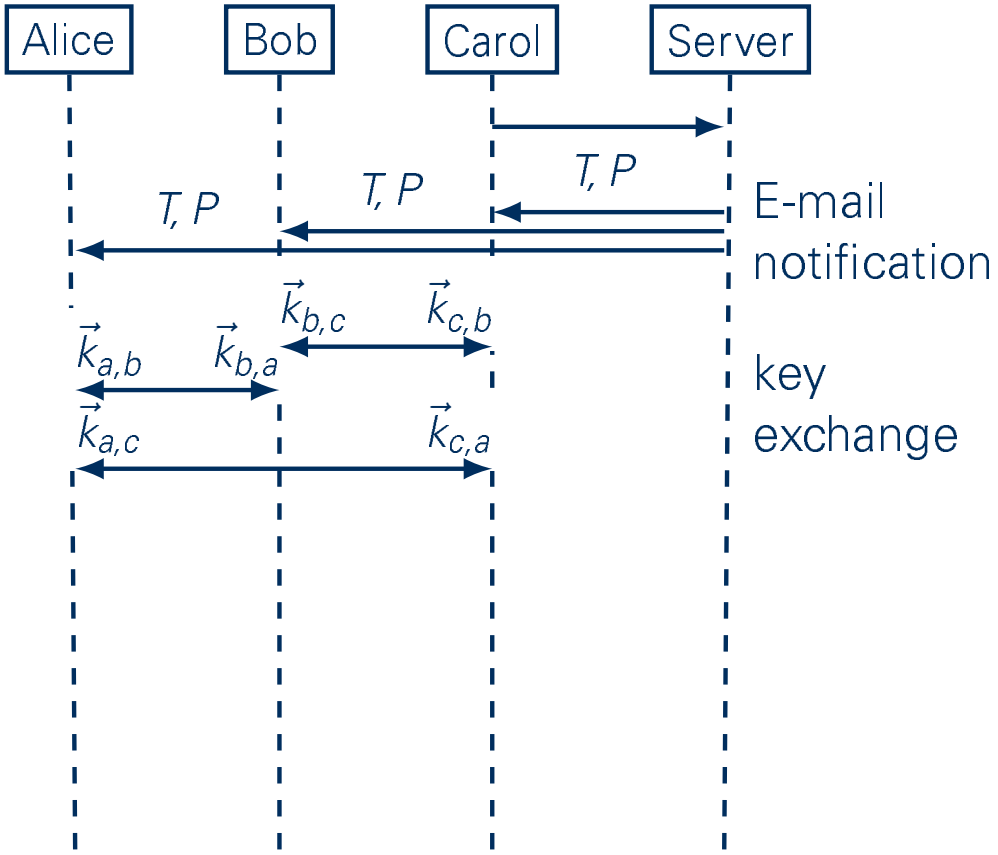


Poll Initialization



T . . . time slots
P . . . voters

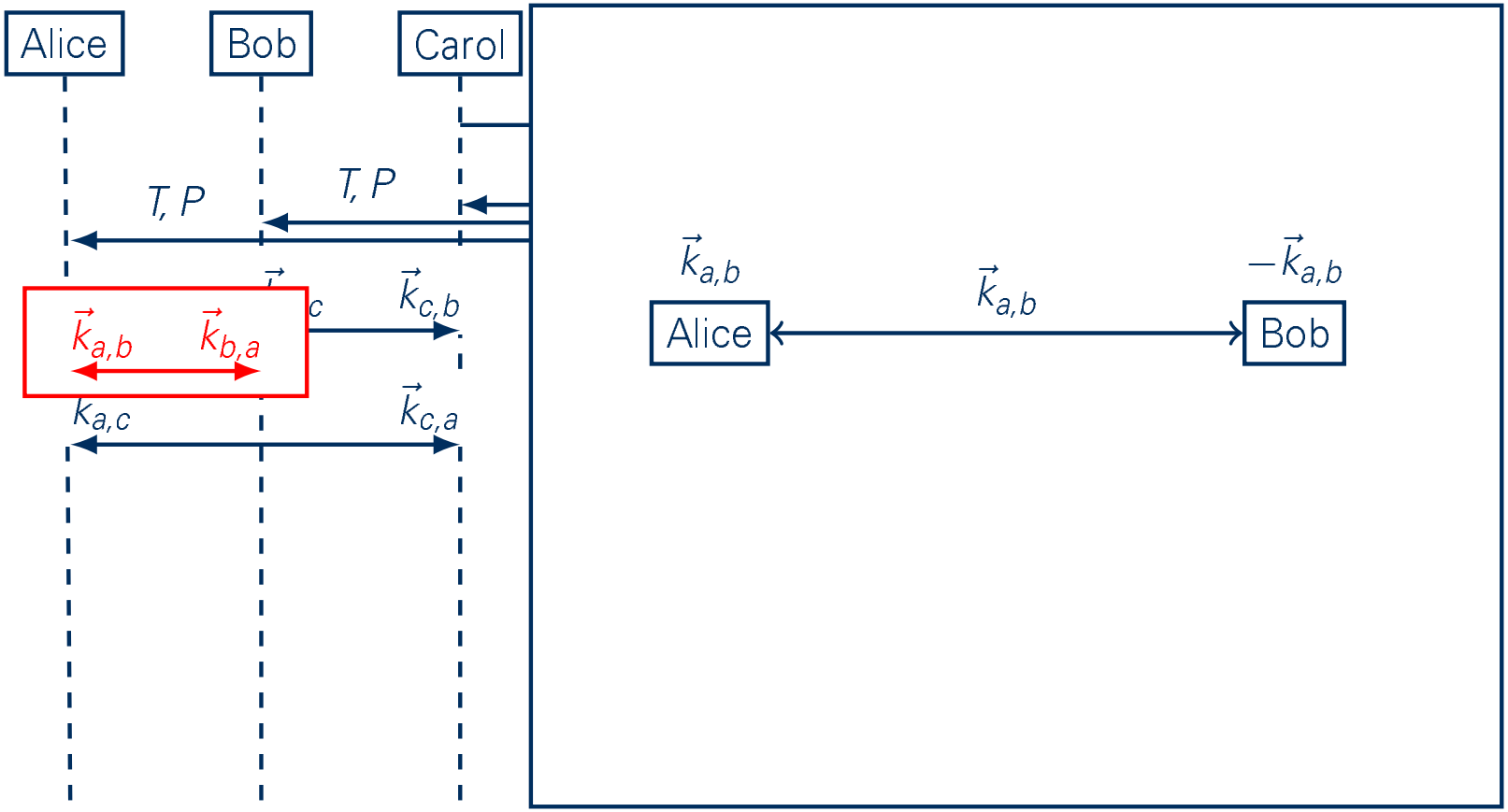
Poll Initialization



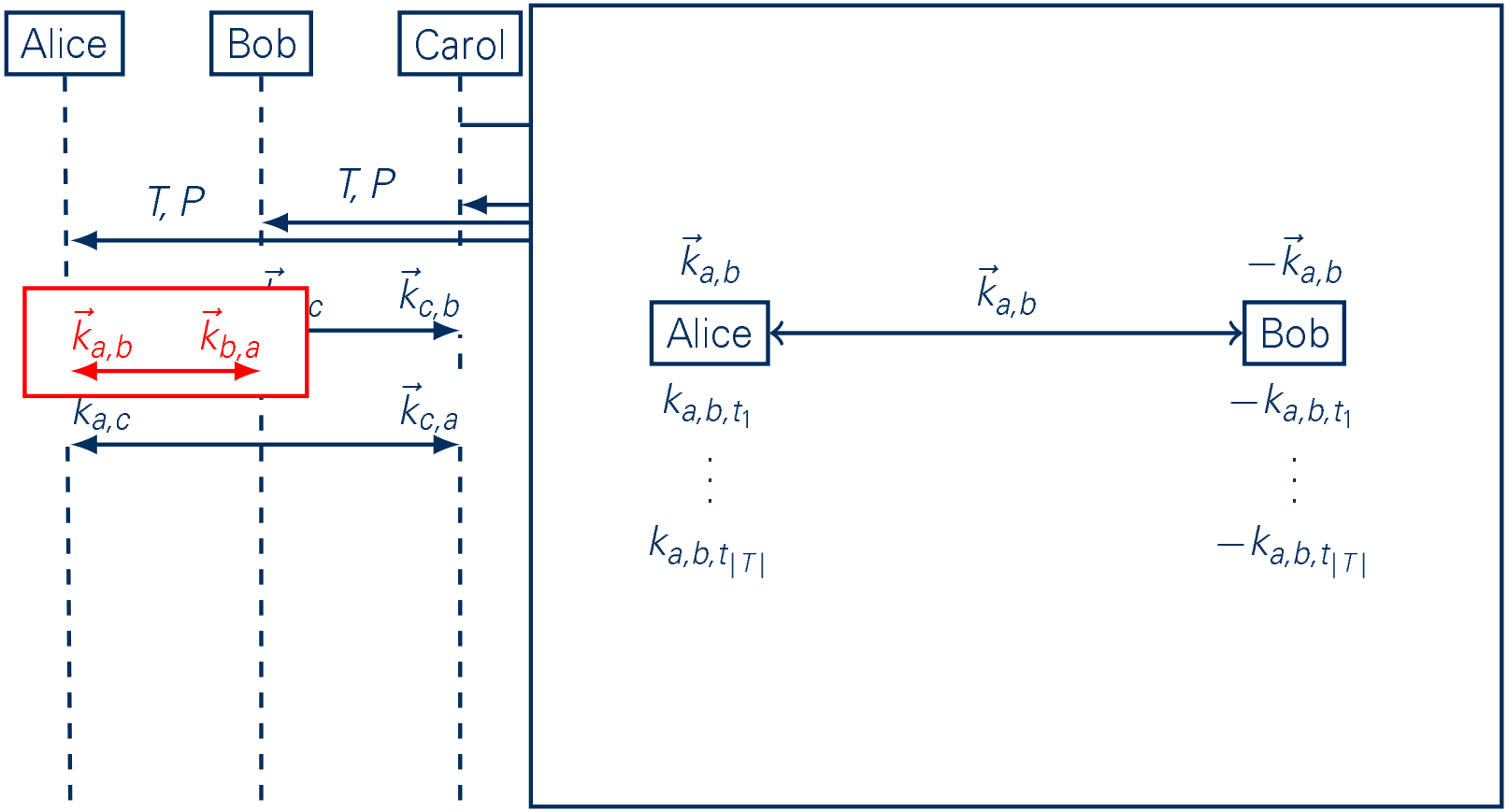
T . . . time slots
P . . . voters

$\vec{k}_{i,j}$ . . . key vector

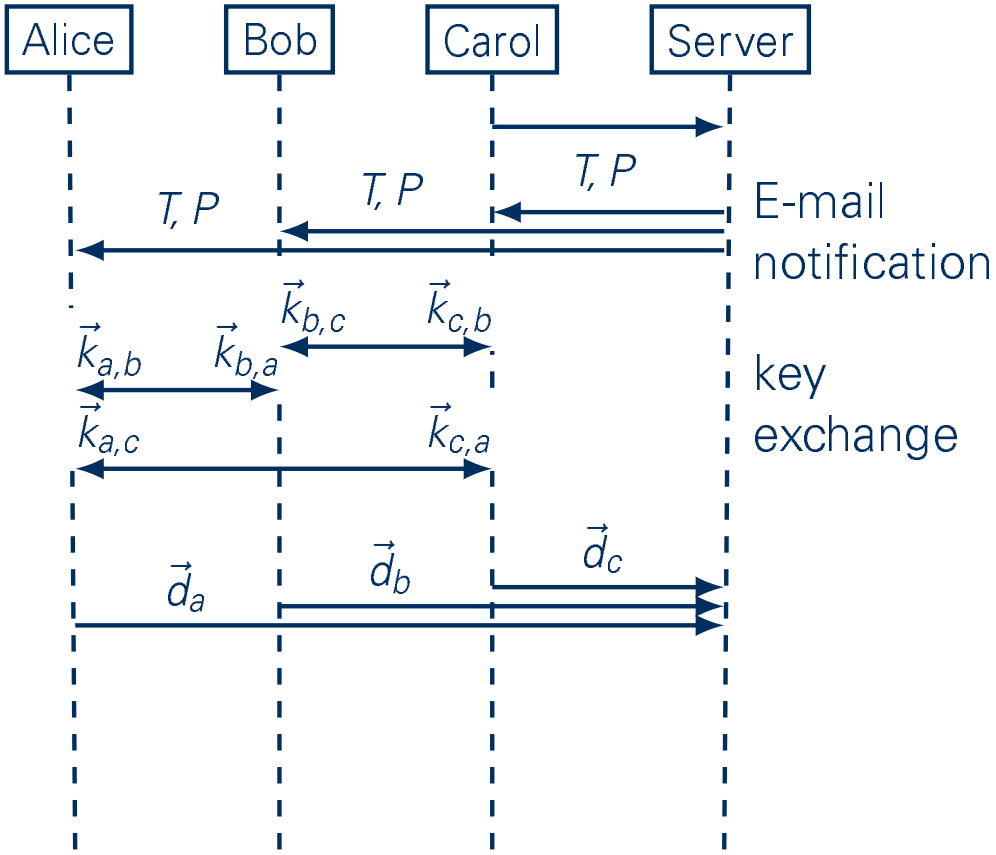
Poll Initialization



Poll Initialization



Casting of Votes

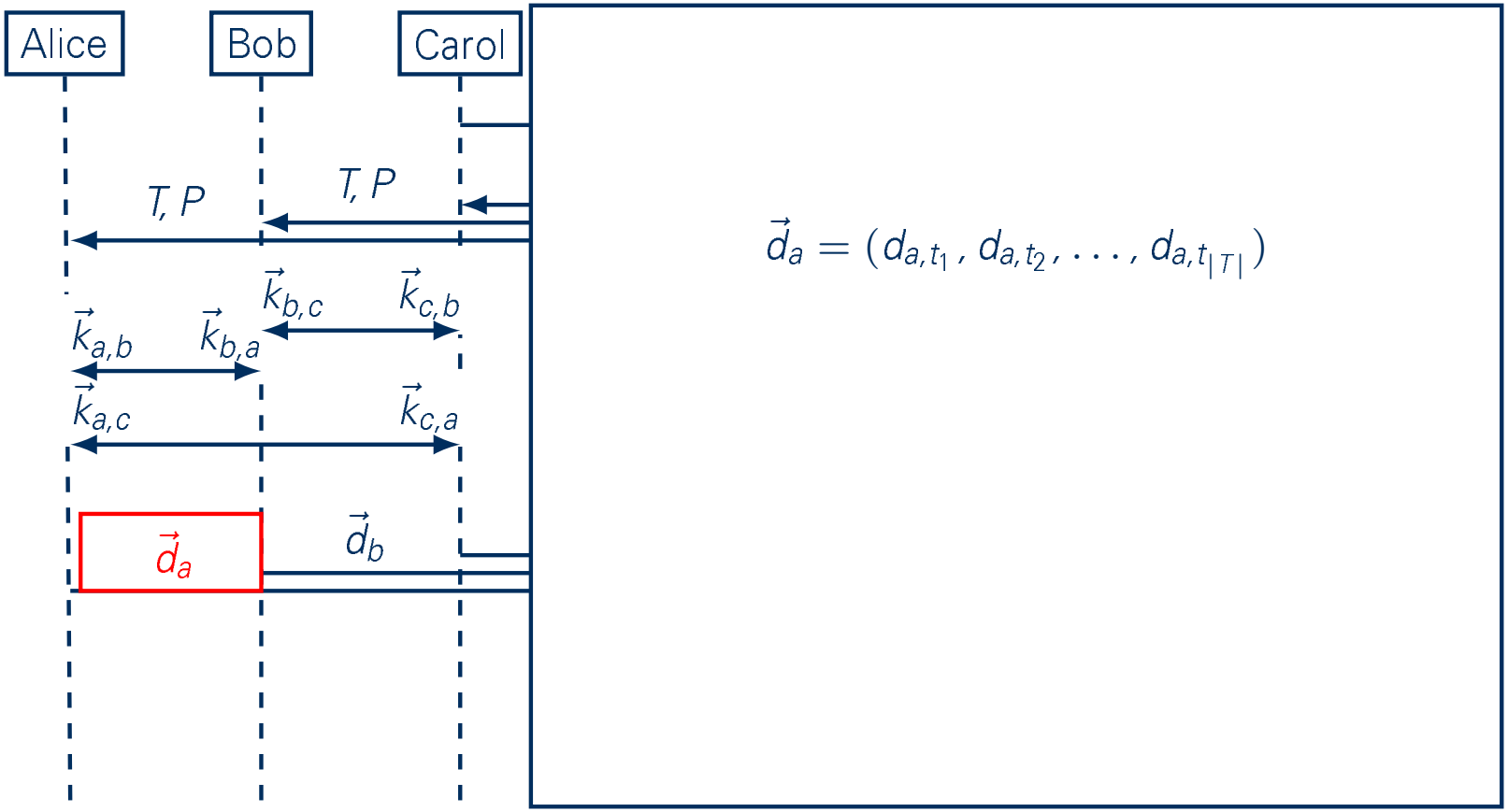


T . . . time slots
P . . . voters

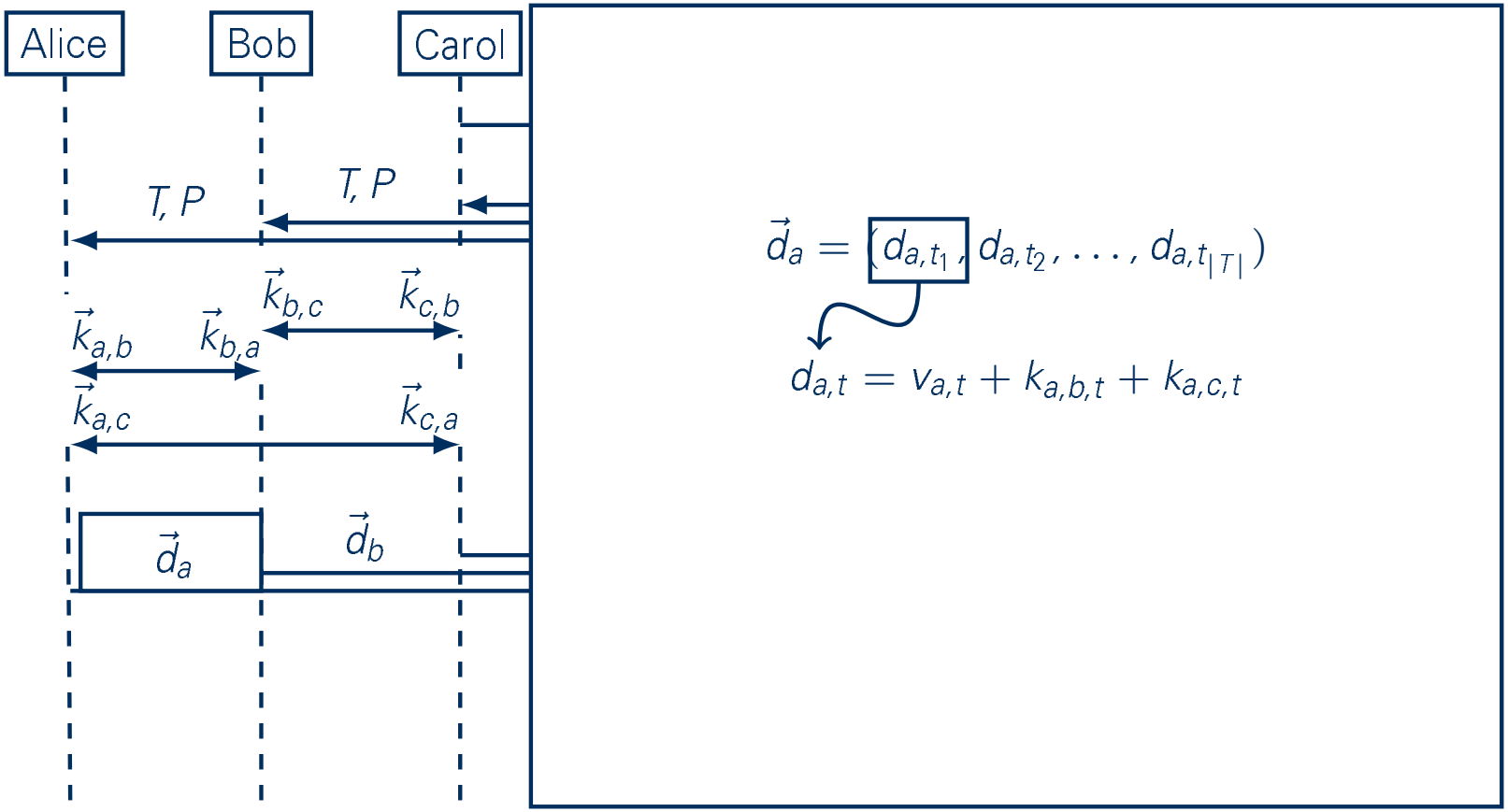
$\vec{k}_{i,j}$ . . . key vector

$\vec{d}$ . . . encrypted votes

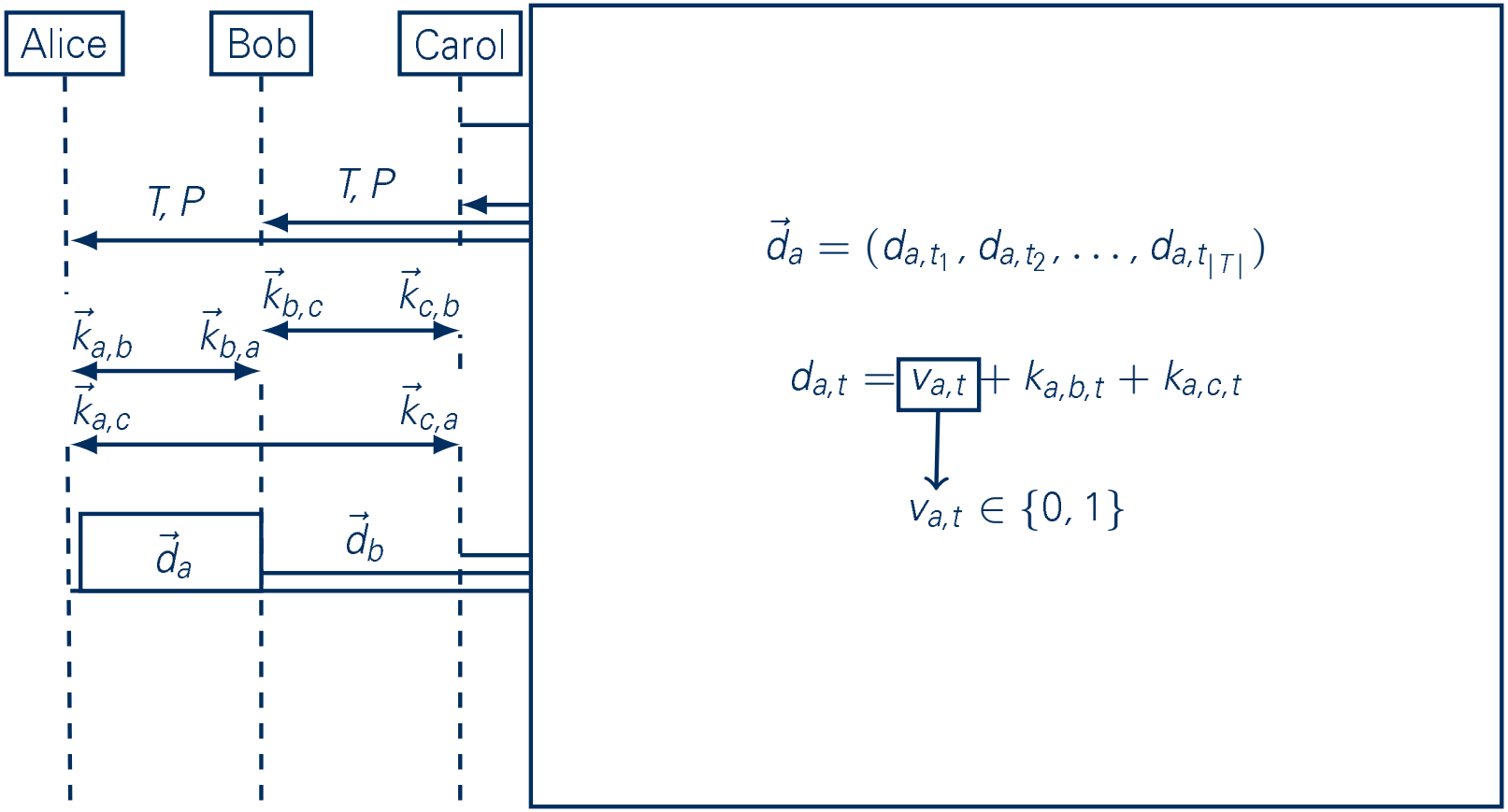
Casting of Votes



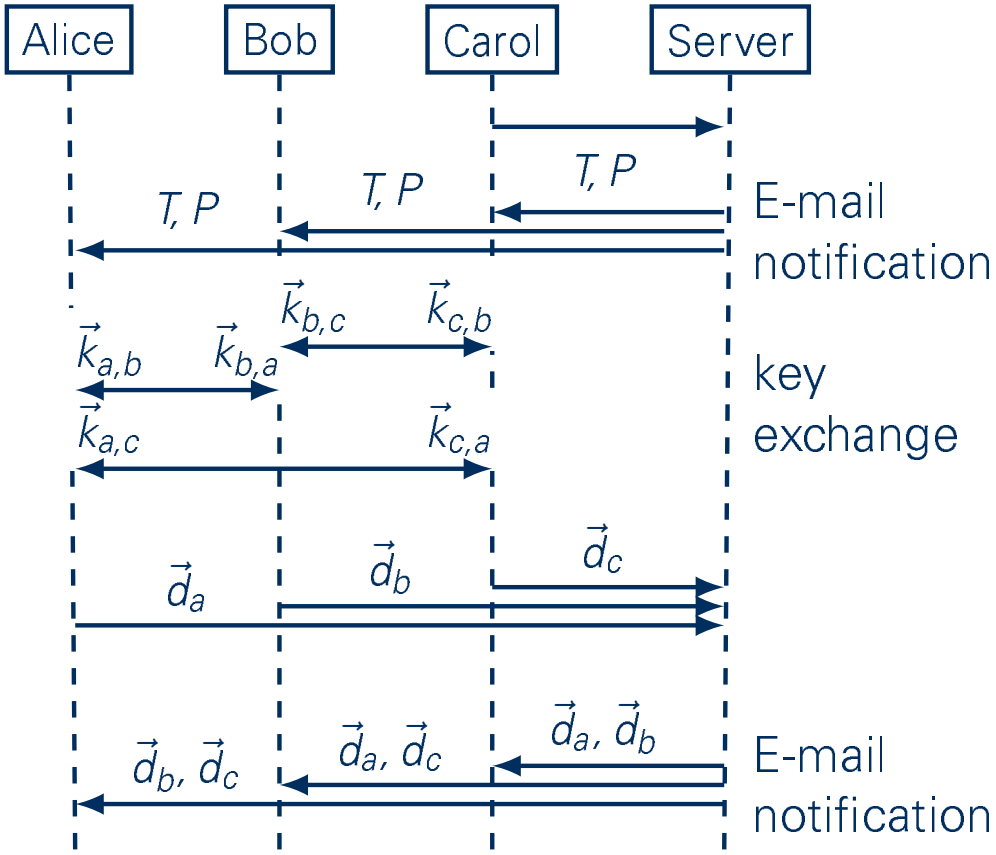
Casting of Votes



Casting of Votes



Result Publication

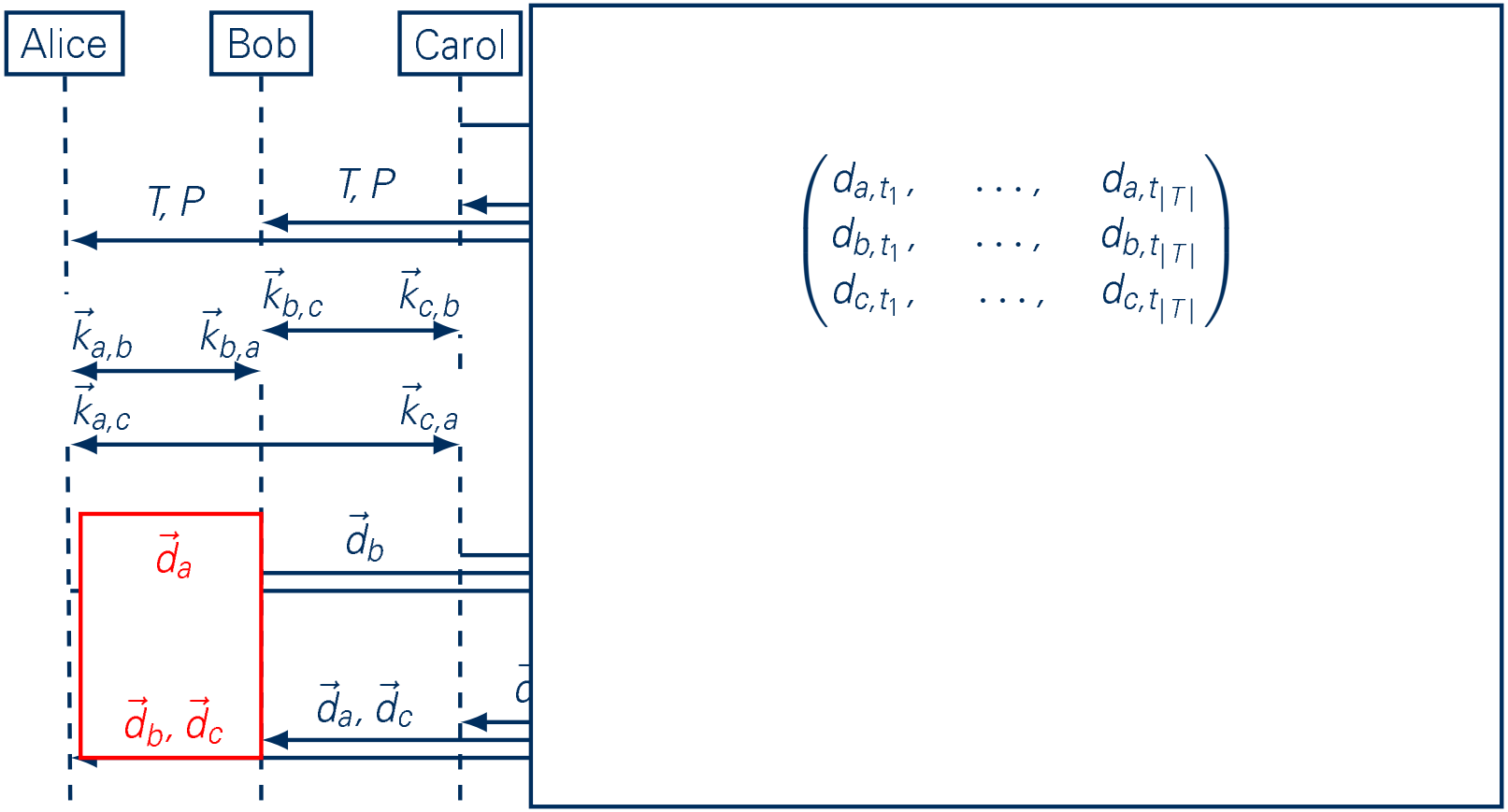


T . . . time slots
P . . . voters

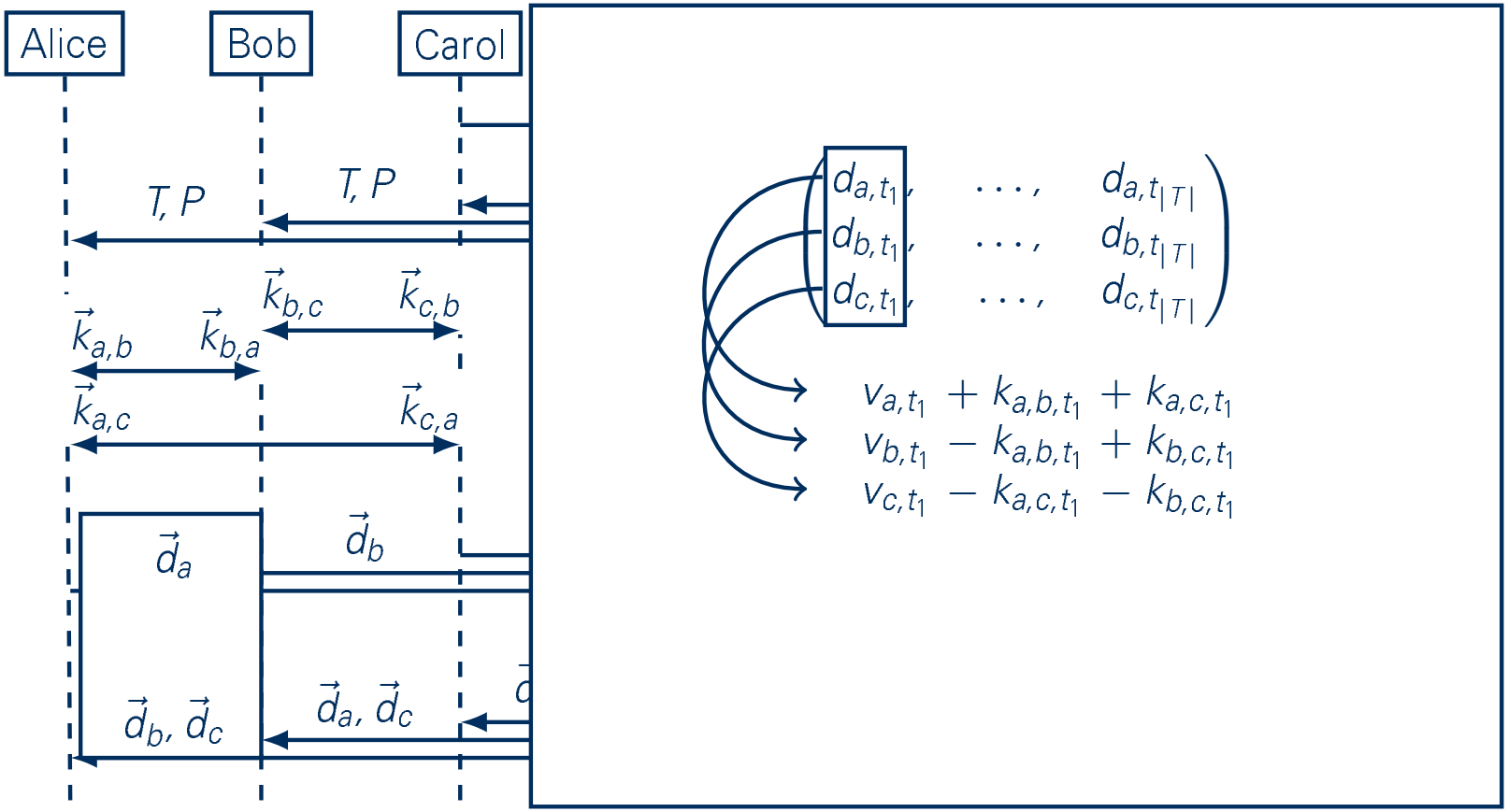
$\vec{k}_{i,j}$ . . . key vector

$\vec{d}$ . . . encrypted votes

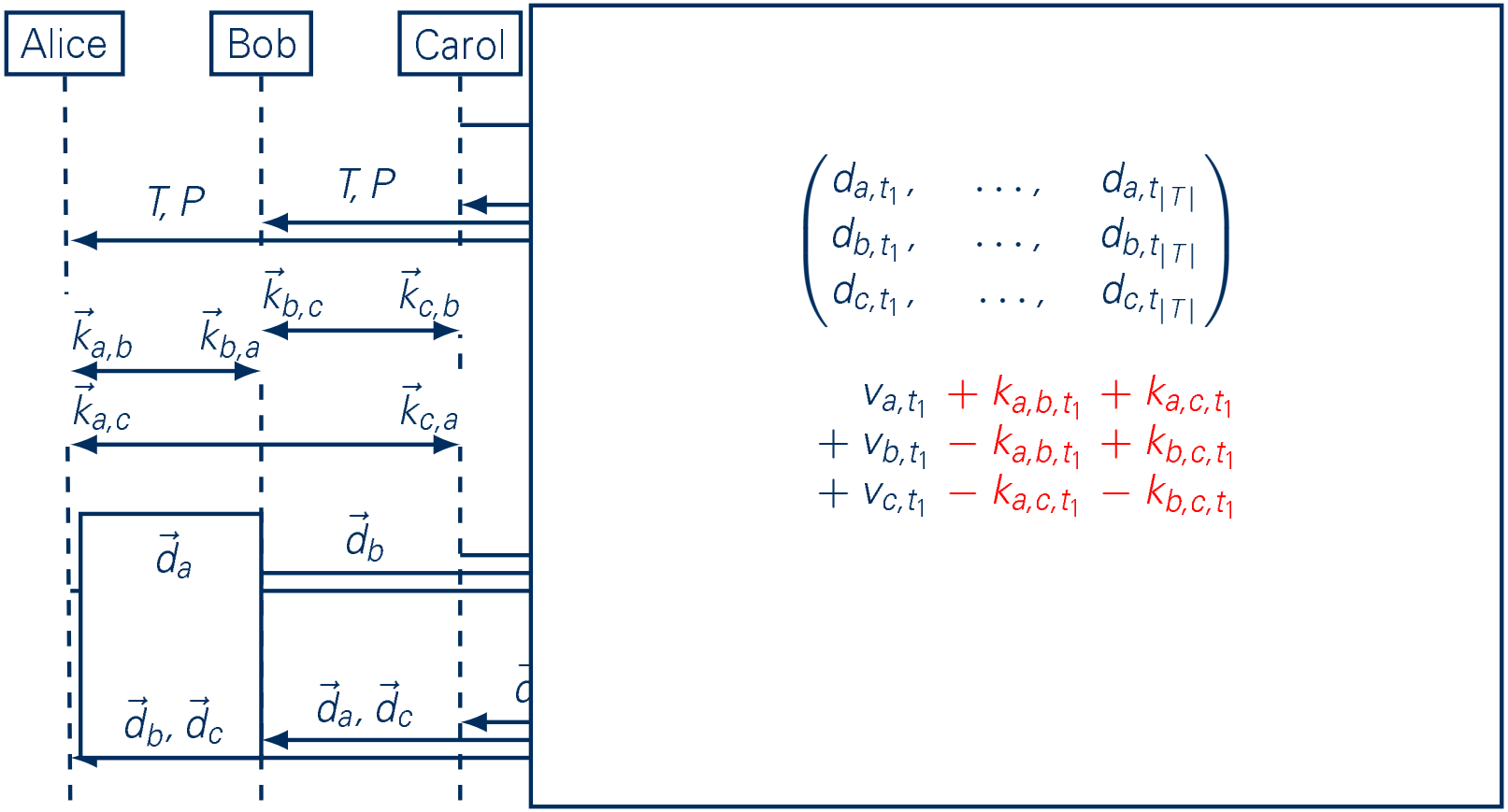
Result Publication



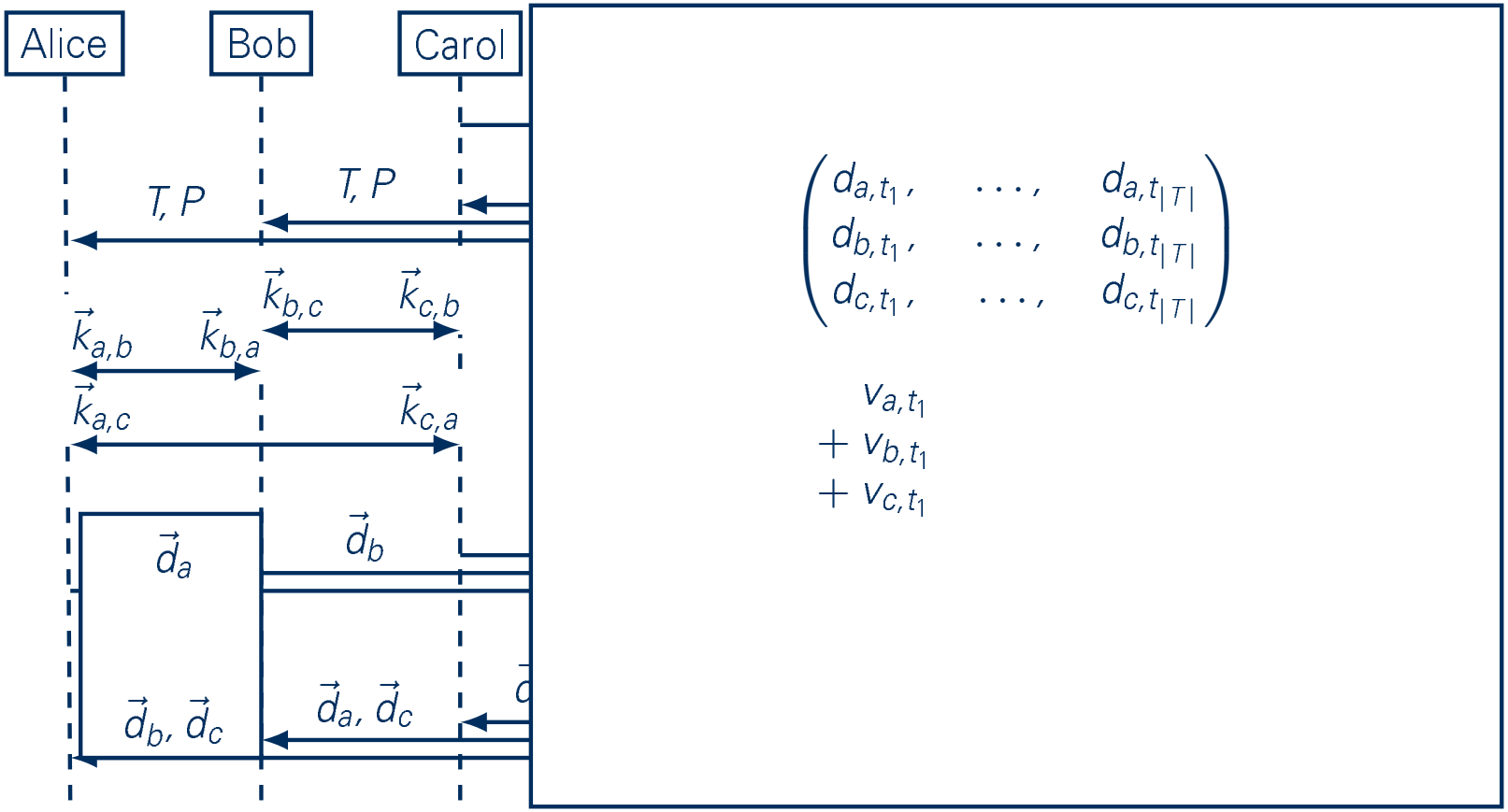
Result Publication



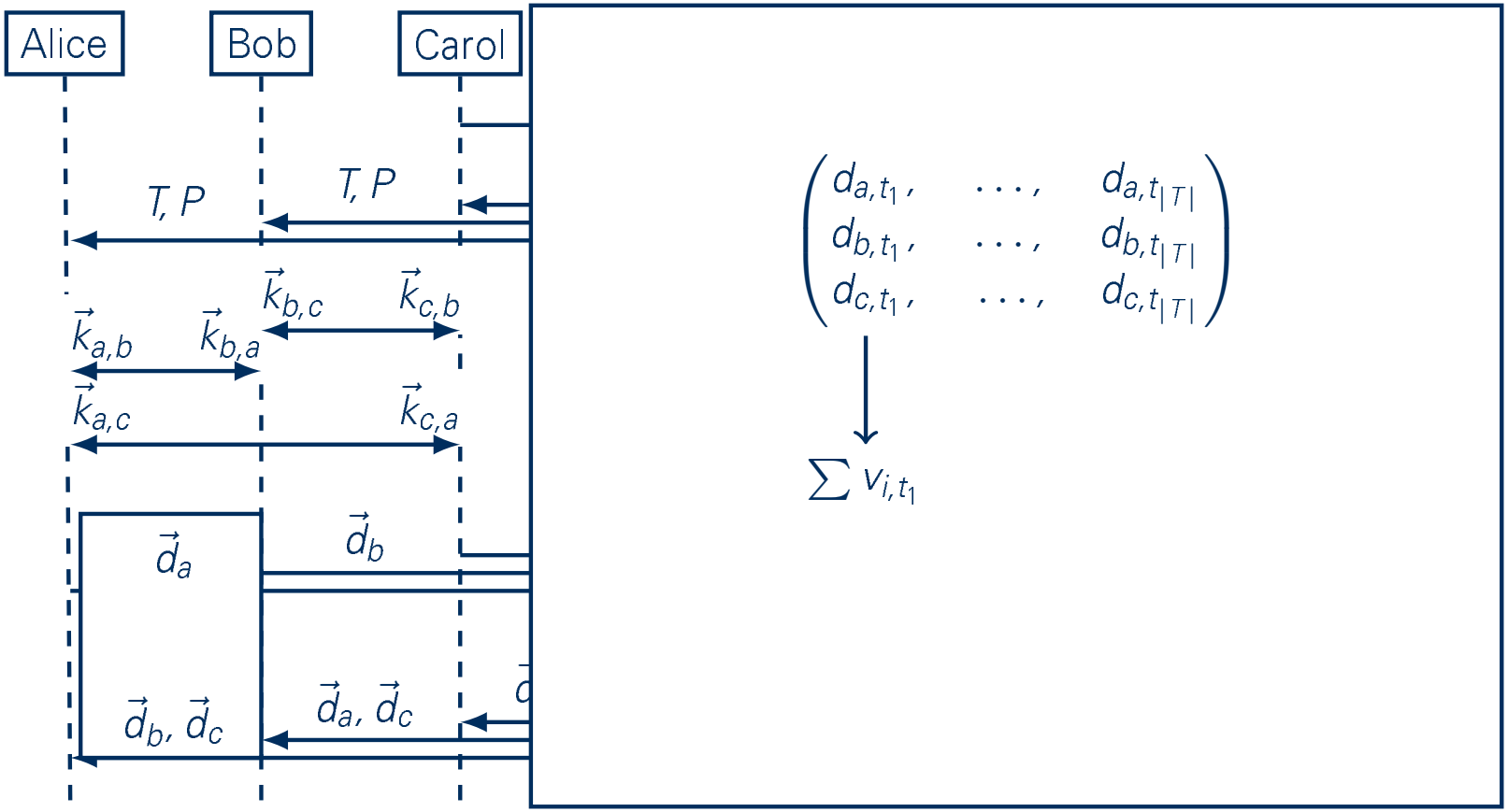
Result Publication



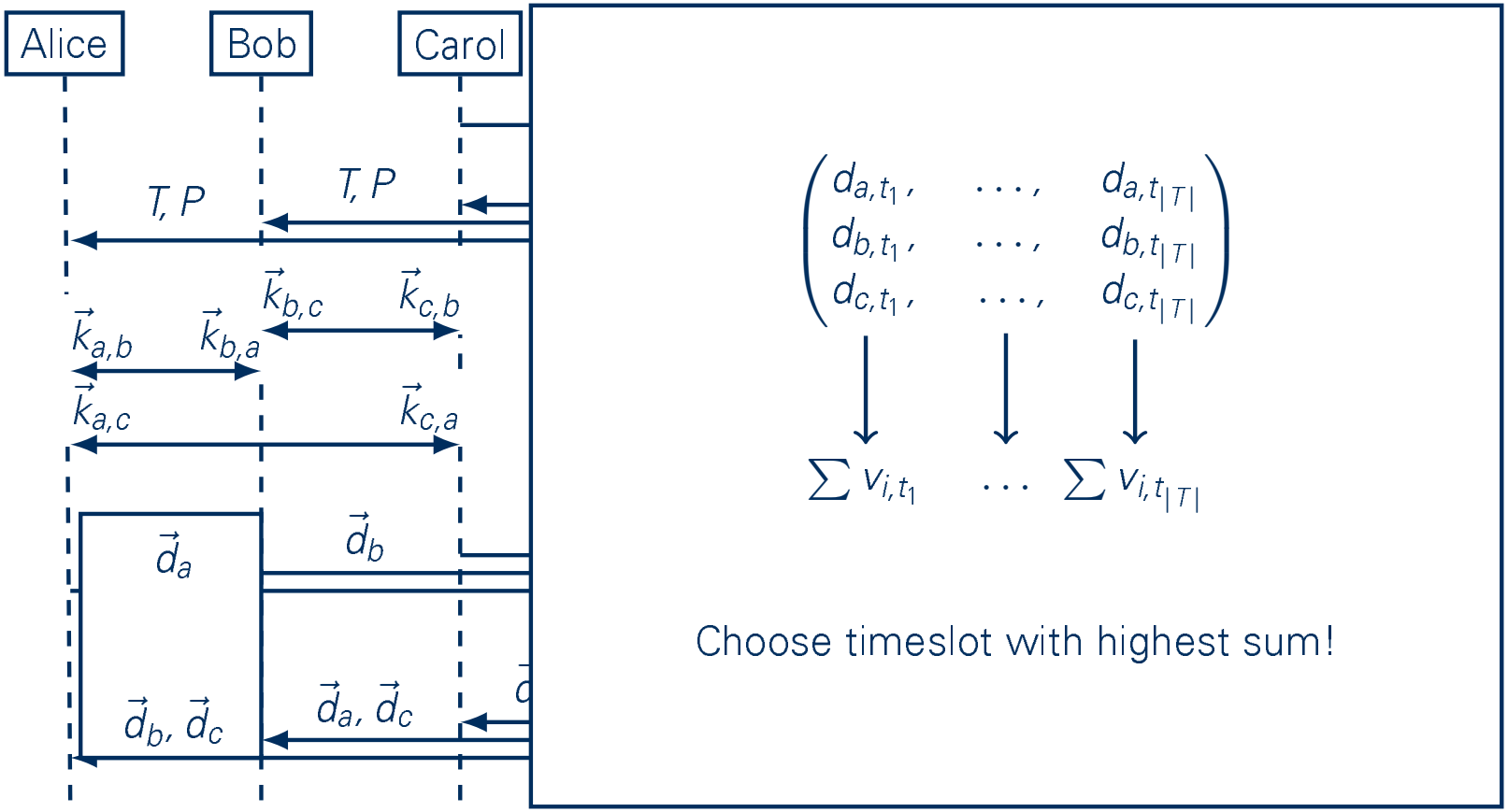
Result Publication



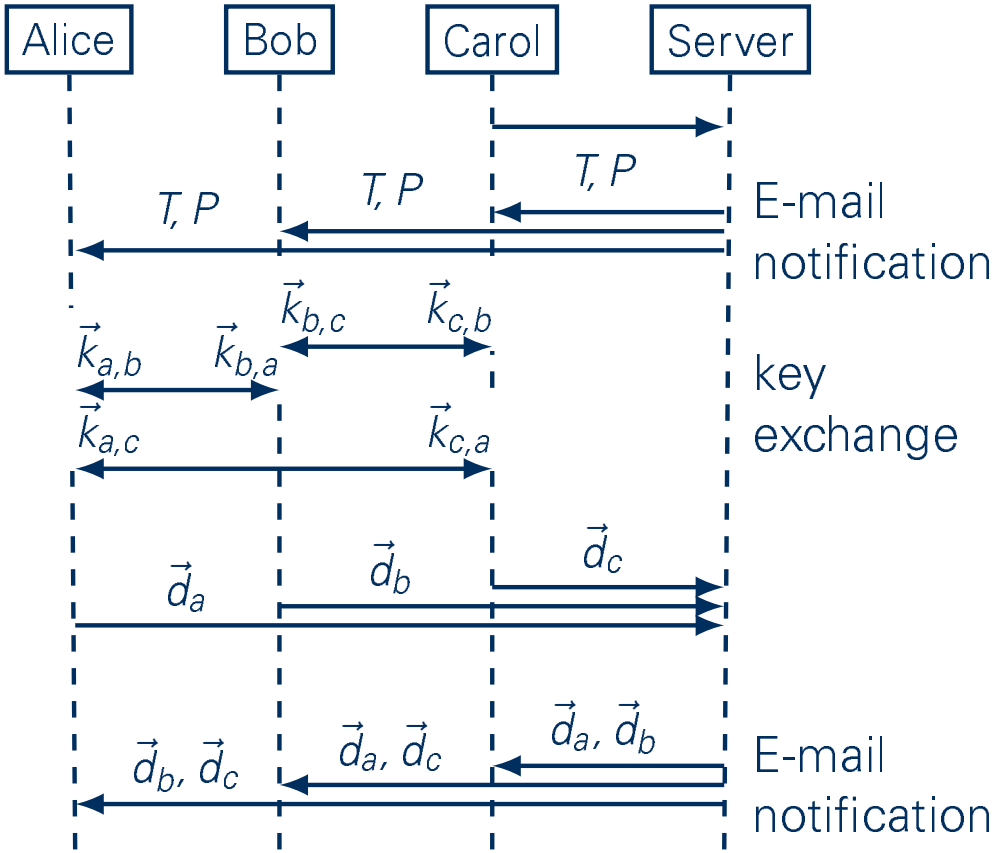
Result Publication



Result Publication



Trying to Cheat

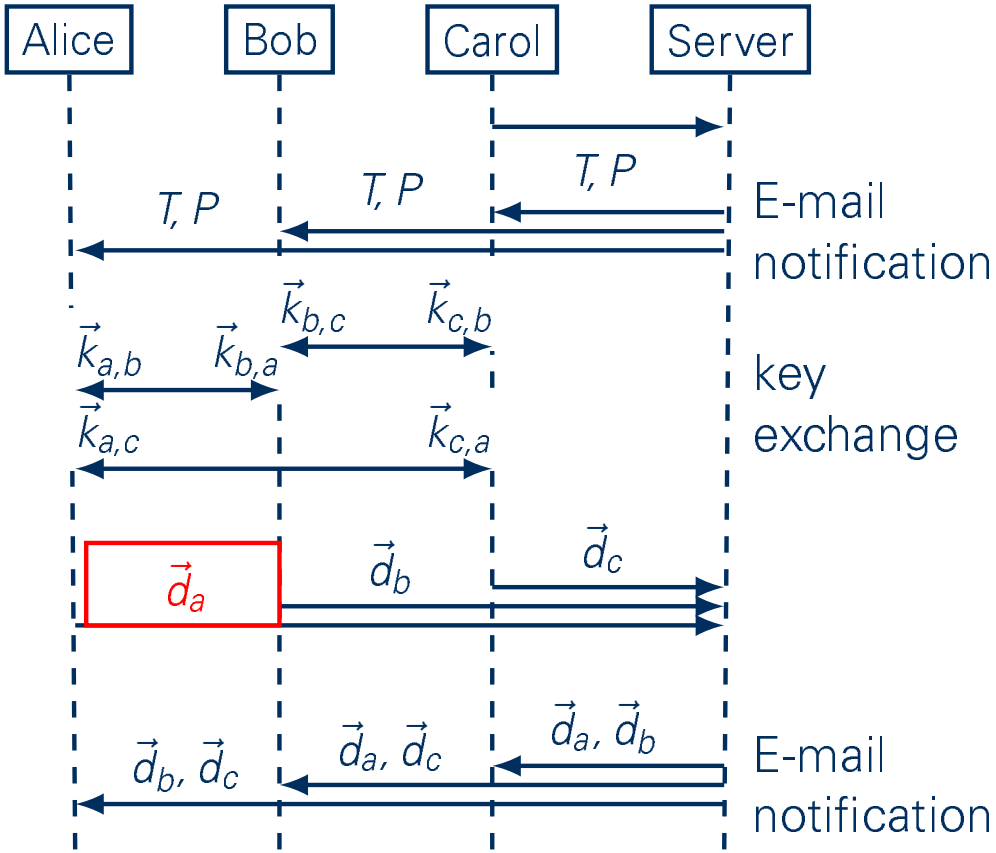


T . . . time slots
P . . . voters

$\vec{k}_{i,j}$ . . . key vector

$\vec{d}$ . . . encrypted votes

Trying to Cheat

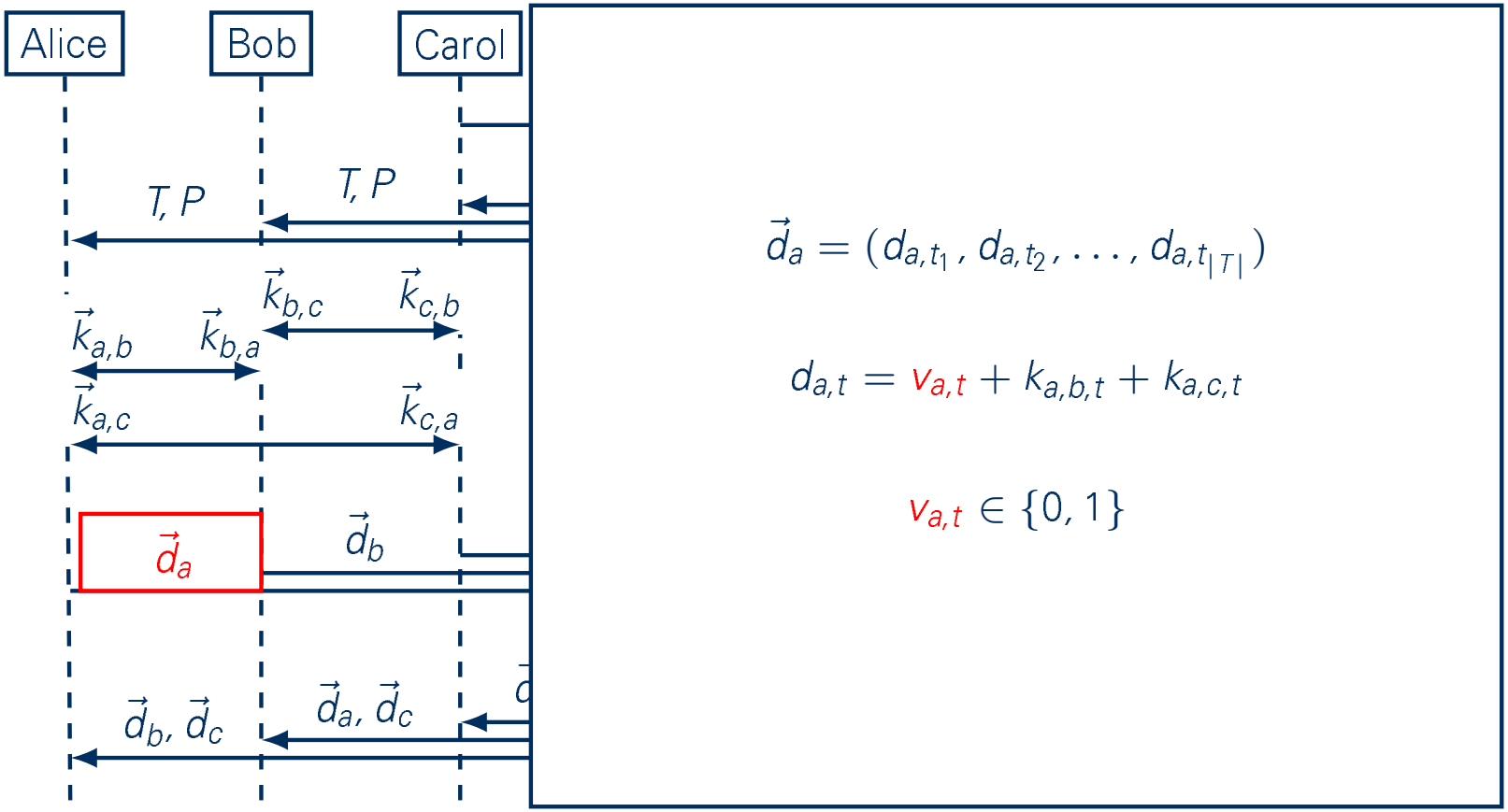


T . . . time slots
P . . . voters

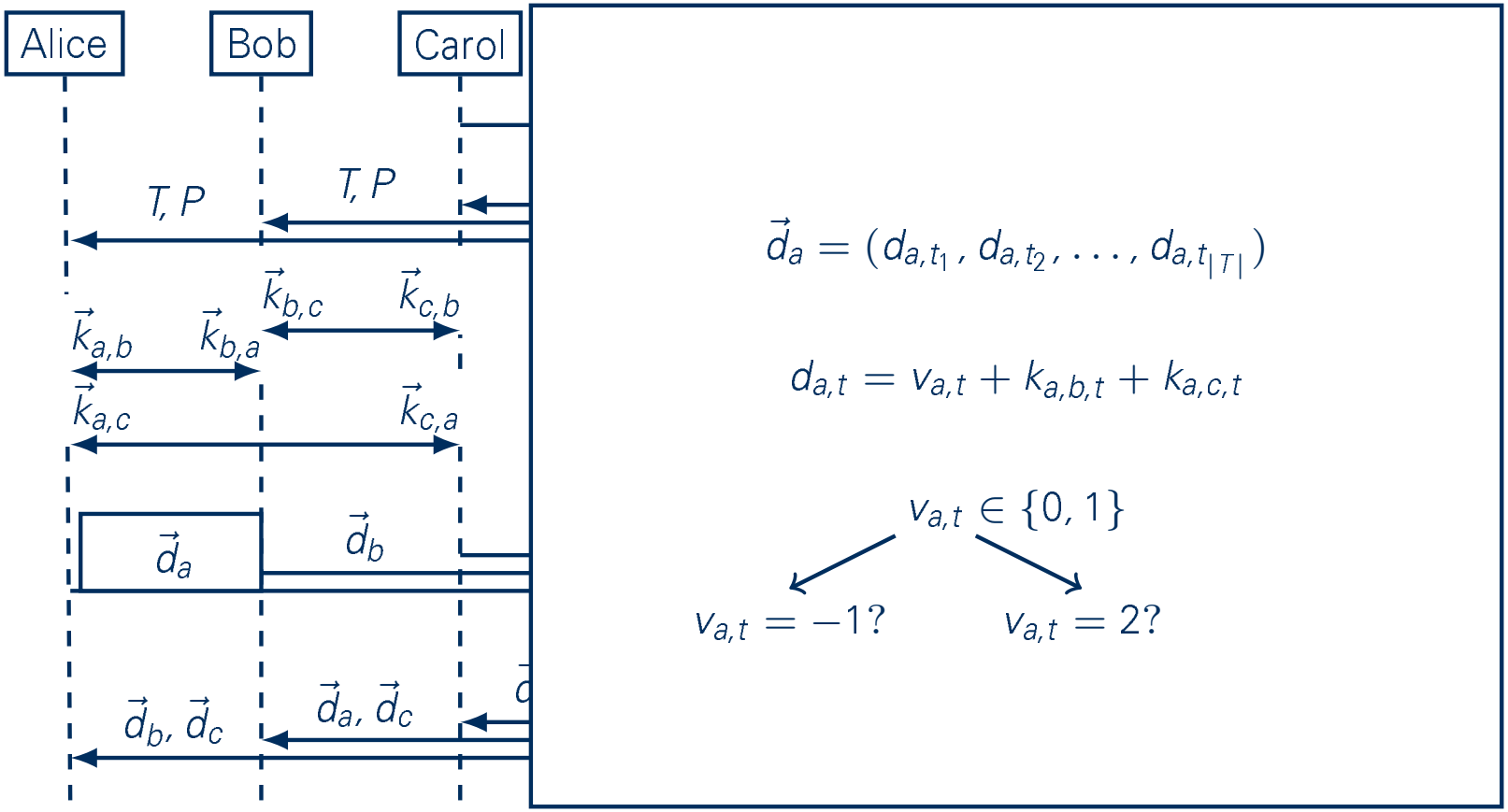
$\vec{k}_{i,j}$ . . . key vector

$\vec{d}$ . . . encrypted votes

Trying to Cheat



Trying to Cheat



Avoid −1 Cheaters

	T1	T2	T3	T4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	0	0	1	0
$\sum$	1	2	2	0

Avoid −1 Cheaters

	T1	T2	T3	T4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	0	0	1	0
$\sum$	1	2	2	0

Avoid −1 Cheaters

	T1	T2	T3	T4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	0	0	1	0
$\sum$	1	2	2	0

Avoid −1 Cheaters

	T1	T2	T3	T4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	−1	−1	1	−1
$\sum$	0	1	2	−1

Avoid −1 Cheaters

	T1	T2	T3	T4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	0	−1	1	0
$\sum$	1	1	2	0

Avoid −1 Cheaters

	T1	T2	T3	T4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	0	−1	1	0
$\sum$	1	1	2	0

Alice	0	0	0	0

Alice	0	1	0	0

Alice	1	0	0	0

$\sum$	1	1	0	0

Avoid −1 Cheaters

	T1	T2	T3	T4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	0	−1	1	0
$\sum$	1	1	2	0

Alice	0	0	0	0
Bob	0	1	0	0

Alice	0	1	0	0
Bob	0	0	0	0

Alice	1	0	0	0
Bob	0	0	1	0

$\sum$	1	2	1	0

Avoid −1 Cheaters

	T1	T2	T3	T4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	0	−1	1	0
$\sum$	1	1	2	0

Alice	0	0	0	0
Bob	0	1	0	0
$\sum$		≥ 0?		
Alice	0	1	0	0
Bob	0	0	0	0
$\sum$		≥ 0?		
Alice	1	0	0	0
Bob	0	0	1	0
$\sum$		≥ 0?		
$\sum$	1	2	1	0

Avoid −1 Cheaters

	T1	T2	T3	T4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	0	−1	1	0
$\sum$	1	1	2	0

Alice	0	0	0	0
Bob	0	1	0	0
Mallory	0	?	0	0
$\sum$		≥ 0?		
Alice	0	1	0	0
Bob	0	0	0	0
Mallory	0	?	0	0
$\sum$		≥ 0?		
Alice	1	0	0	0
Bob	0	0	1	0
Mallory	0	?	1	0
$\sum$		≥ 0?		
$\sum$	1	2	2	0

Avoid +2 Cheaters

	T1	T2	T3	T4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	0	0	2	0
$\sum$	1	2	3	0

Avoid +2 Cheaters

normal poll

	T1	T2	T3	T4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	0	0	2	0
$\sum$	1	2	3	0

inverted poll

	T1	T2	T3	T4
Alice	0			
Bob	1			
Mallory	1			
$\sum$	2			

Avoid +2 Cheaters

normal poll

	T1	T2	T3	T4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	0	0	2	0
$\sum$	1	2	3	0

inverted poll

	T1	T2	T3	T4
Alice	0			
Bob	1			
Mallory	1			
$\sum$	2			

$\sum$	3

Avoid +2 Cheaters

normal poll

	T1	T2	T3	T4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	0	0	2	0
$\sum$	1	2	3	0

inverted poll

	T1	T2	T3	T4
Alice	0	0		
Bob	1	0		
Mallory	1	1		
$\sum$	2	1		

$\sum$	3	3

Avoid +2 Cheaters

normal poll

	T1	T2	T3	T4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	0	0	2	0
$\sum$	1	2	3	0

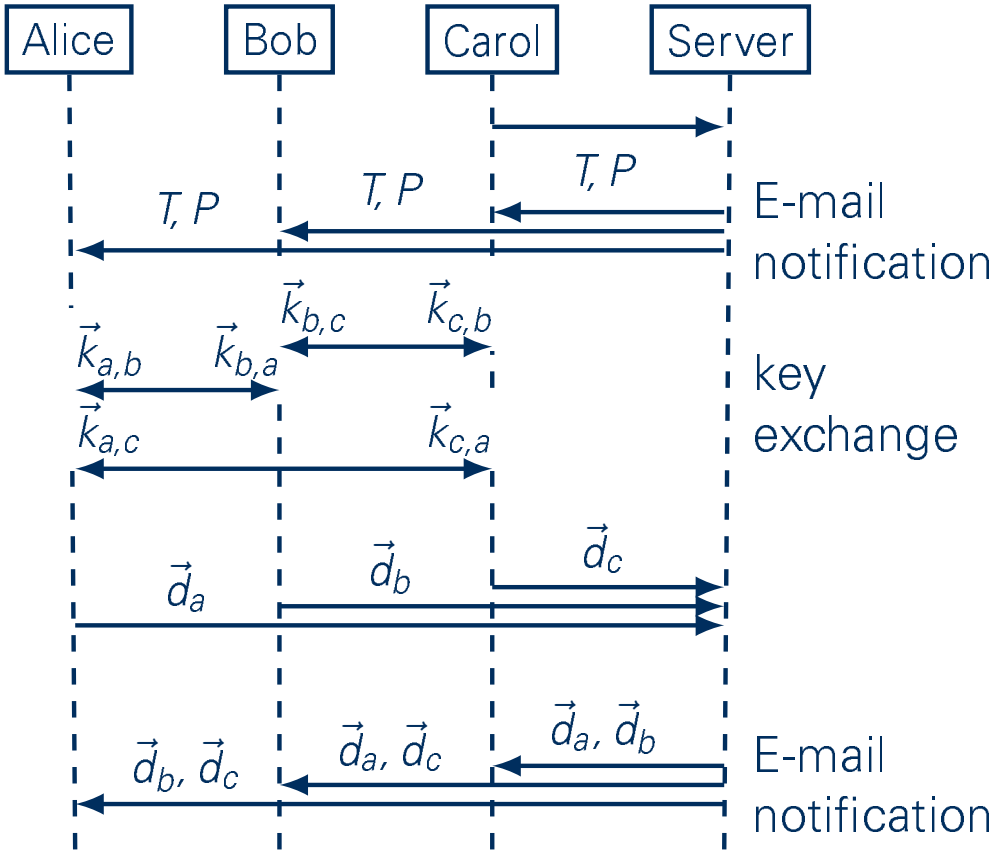
inverted poll

	T1	T2	T3	T4
Alice	0	0	1	
Bob	1	0	0	
Mallory	1	1	−1	
$\sum$	2	1	0	

$\sum$	3	3	3

Extensions

Simplifying the Key Exchange

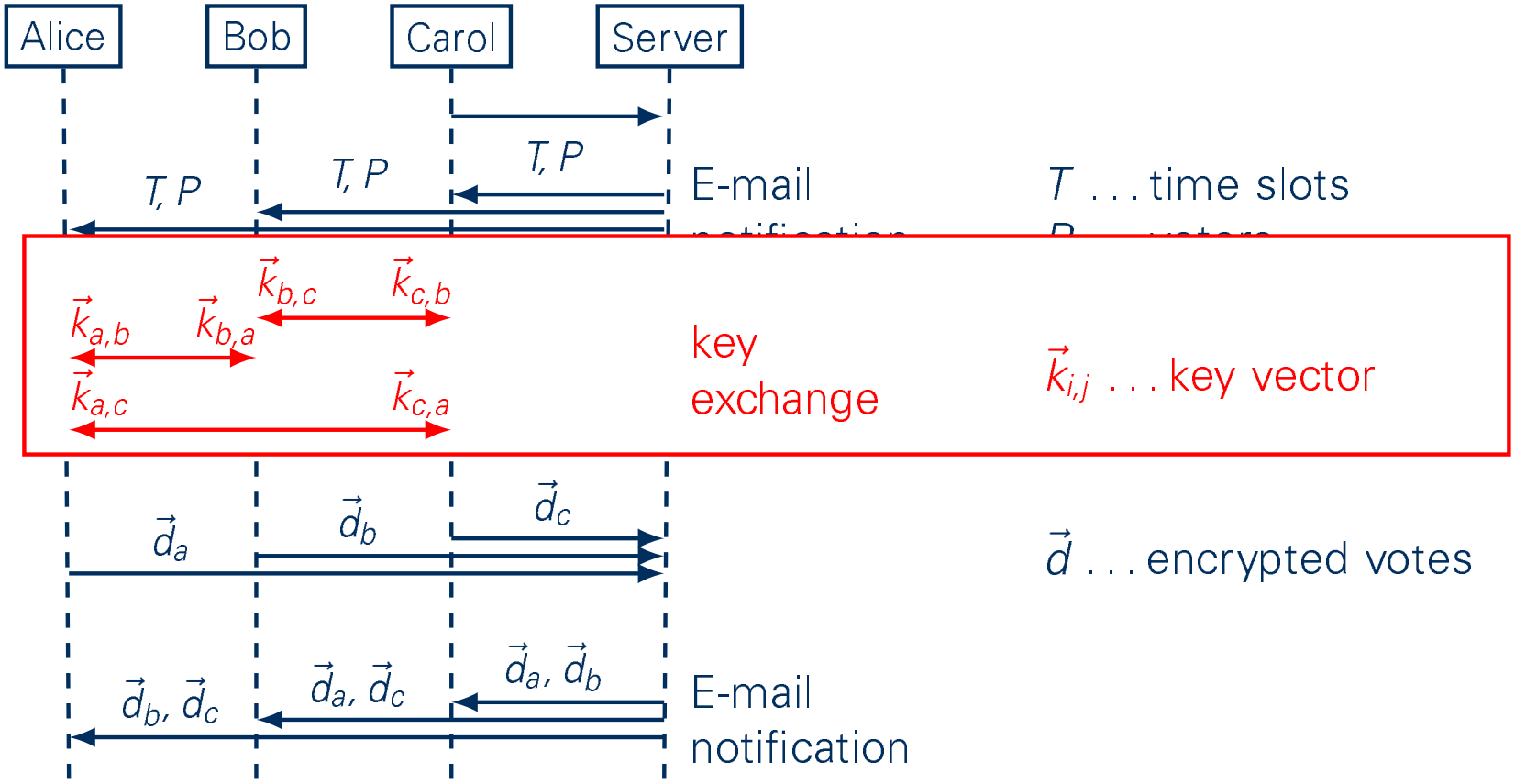


T . . . time slots
P . . . voters

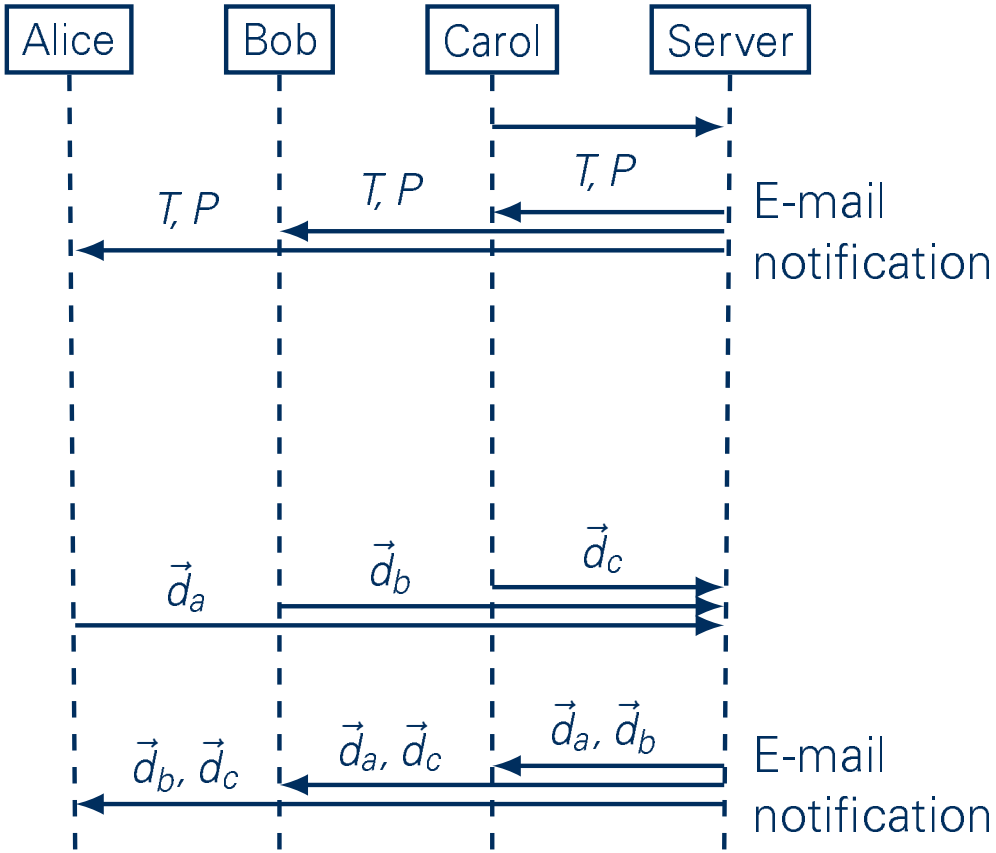
$\vec{k}_{i,j}$ . . . key vector

$\vec{d}$ . . . encrypted votes

Simplifying the Key Exchange



Simplifying the Key Exchange



T . . . time slots
P . . . voters

$\vec{d}$ . . . encrypted votes

Intermezzo – Diffie–Hellman Key Agreement

Discrete Logarithm assumption

$x = g^r \bmod q$

Intermezzo – Diffie–Hellman Key Agreement

Discrete Logarithm assumption

$$x = g^r \bmod q$$

public

Intermezzo – Diffie–Hellman Key Agreement

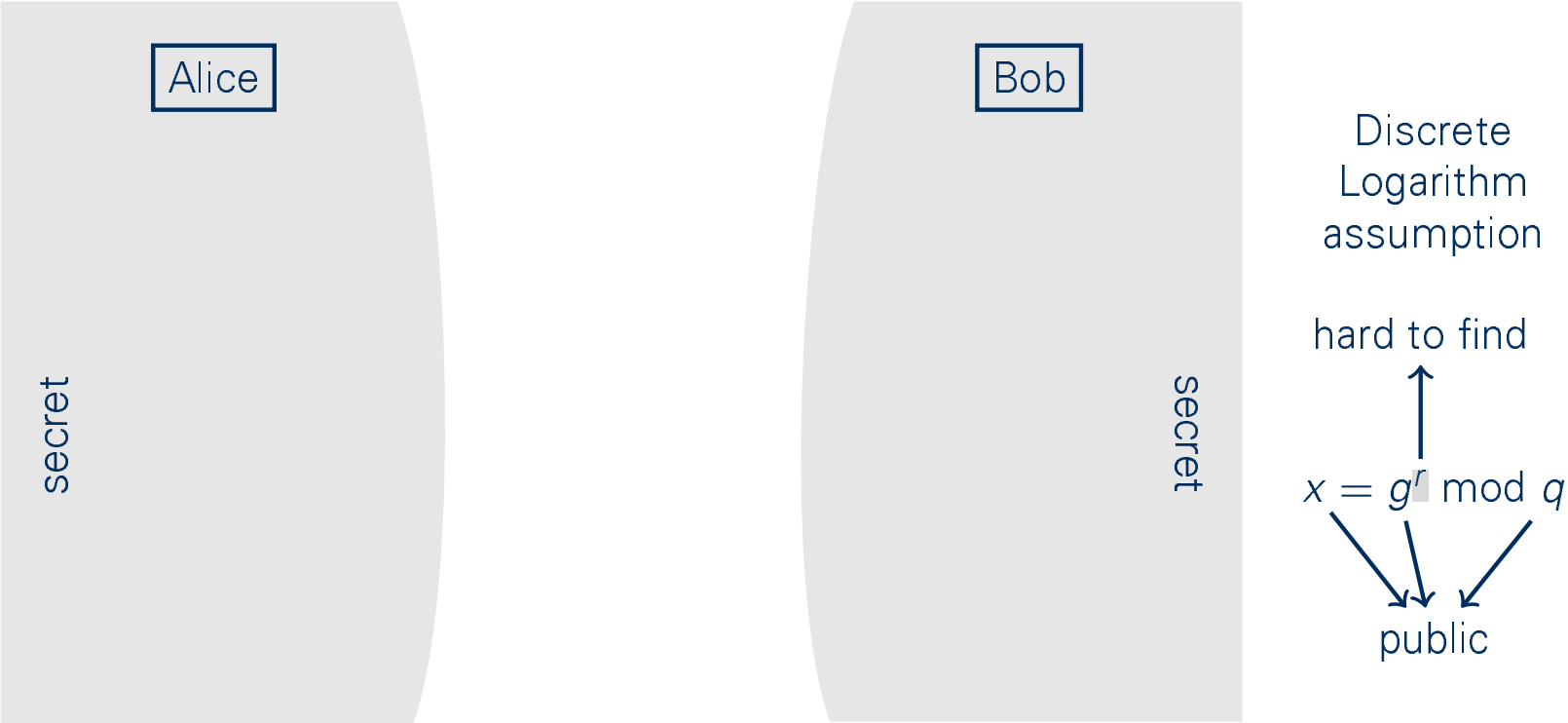
Discrete Logarithm assumption

hard to find

$$x = g^r \bmod q$$

public

Intermezzo – Diffie–Hellman Key Agreement



W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

Intermezzo – Diffie–Hellman Key Agreement

Alice

secret

public
g, q

Bob

secret

Discrete Logarithm assumption

hard to find

$x = g^r \bmod q$

public

W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

Intermezzo – Diffie–Hellman Key Agreement

Alice

chooses r_a

$g^{r_a} \bmod q$
$= x_a$

secret

public
g, q

Bob

chooses r_b

$g^{r_b} \bmod q$
$= x_b$

secret

Discrete Logarithm assumption

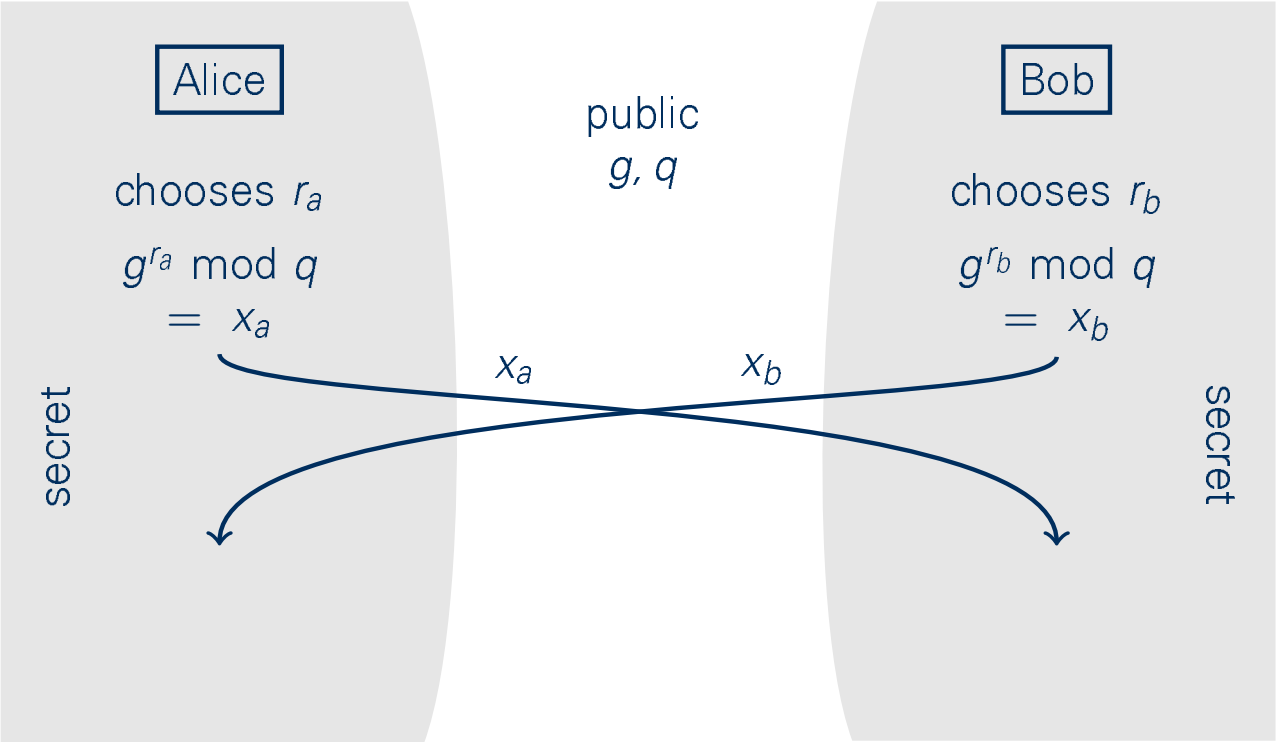
hard to find

$x = g^r \bmod q$

public

W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

Intermezzo – Diffie–Hellman Key Agreement



Discrete Logarithm assumption

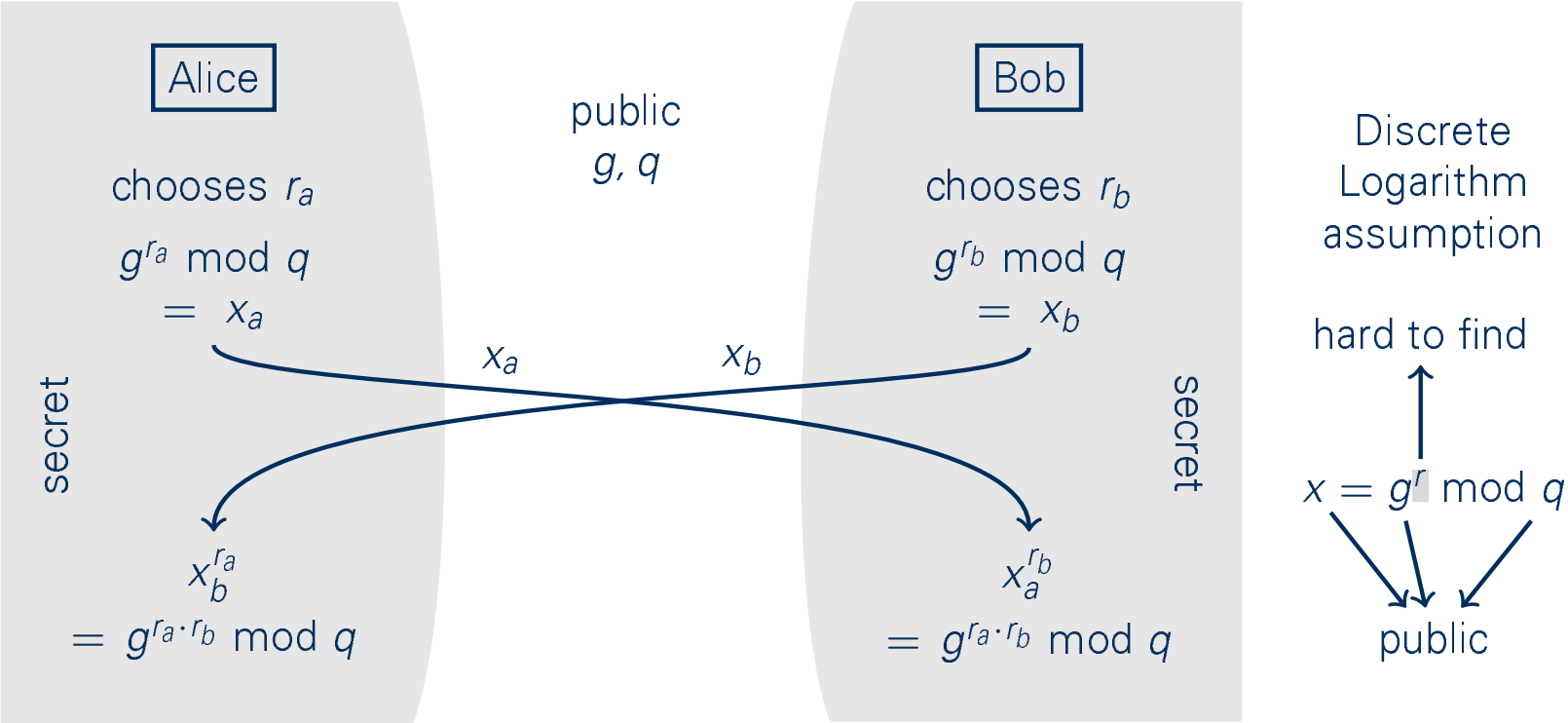
hard to find

$x = g^r \bmod q$

public

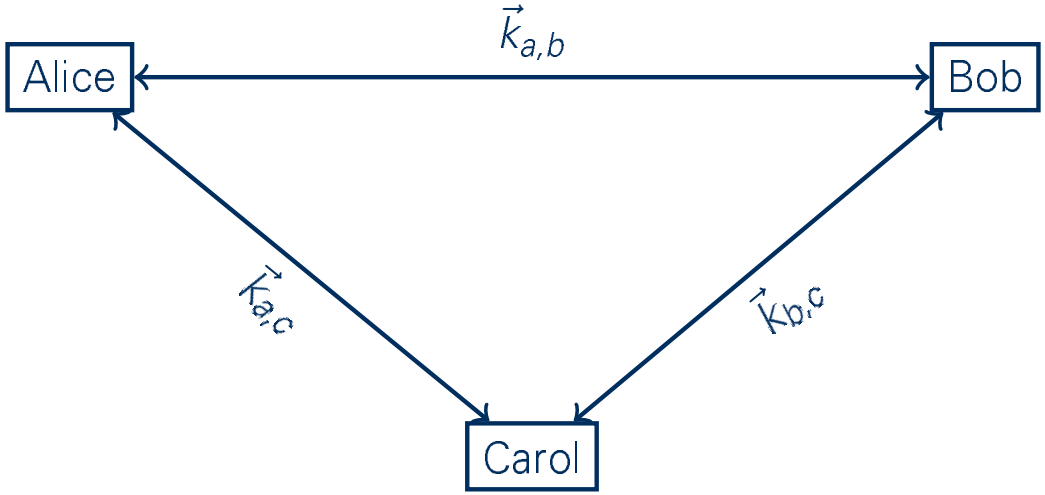
W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

Intermezzo – Diffie–Hellman Key Agreement



W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

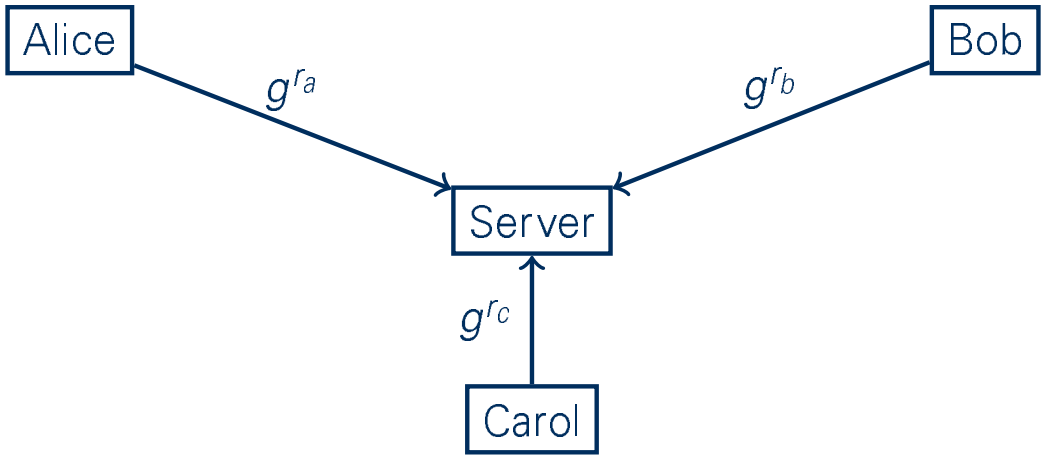
Simplifying the Key Exchange



key exchange

Simplifying the Key Exchange

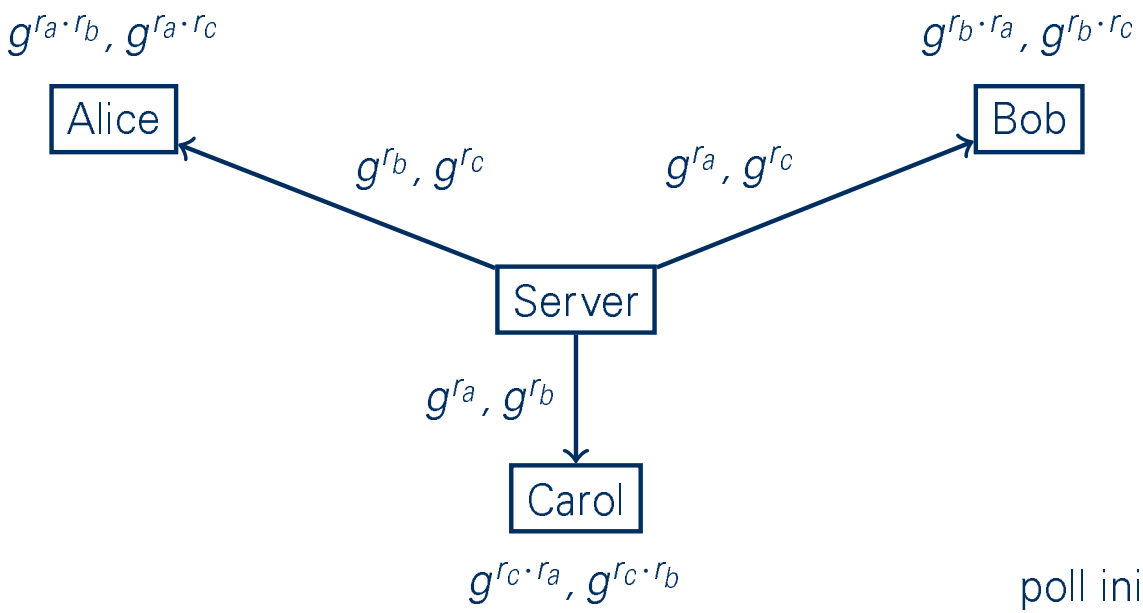
Diffie–Hellman



registration

Simplifying the Key Exchange

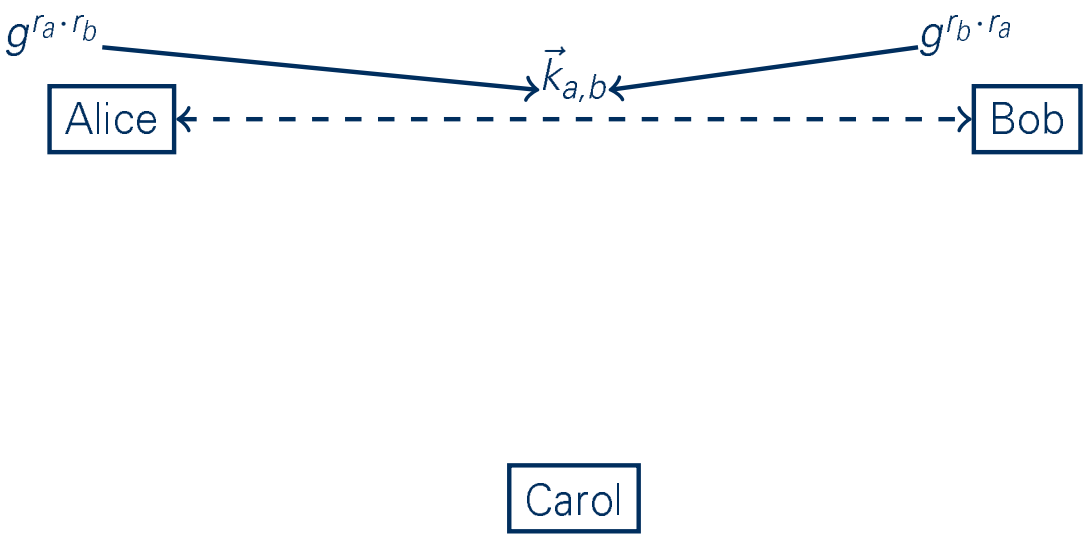
Diffie–Hellman



poll initialization

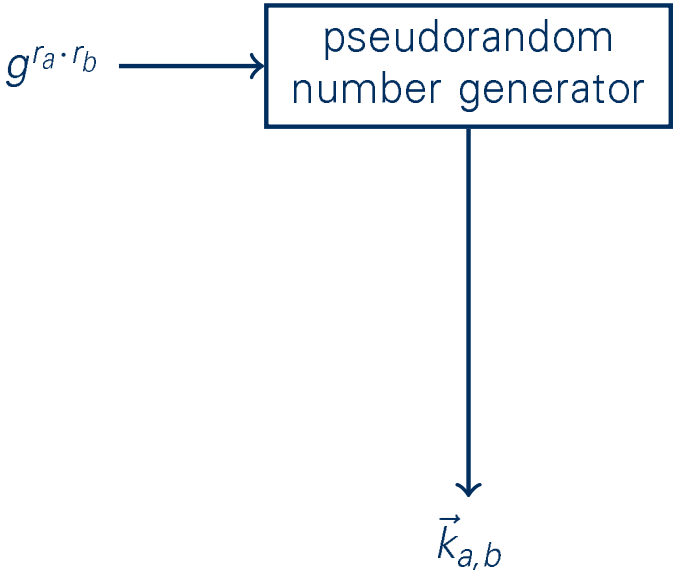
Simplifying the Key Exchange

Diffie–Hellman

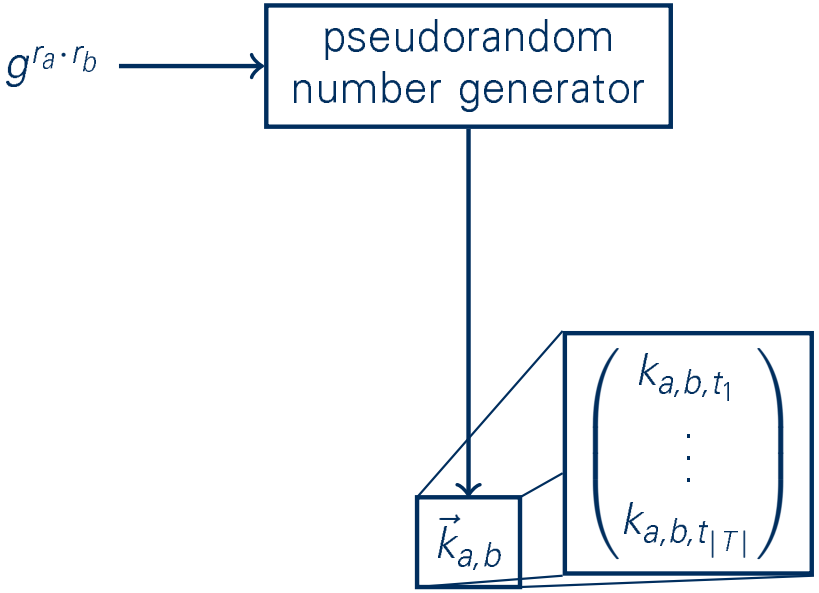


poll initialization

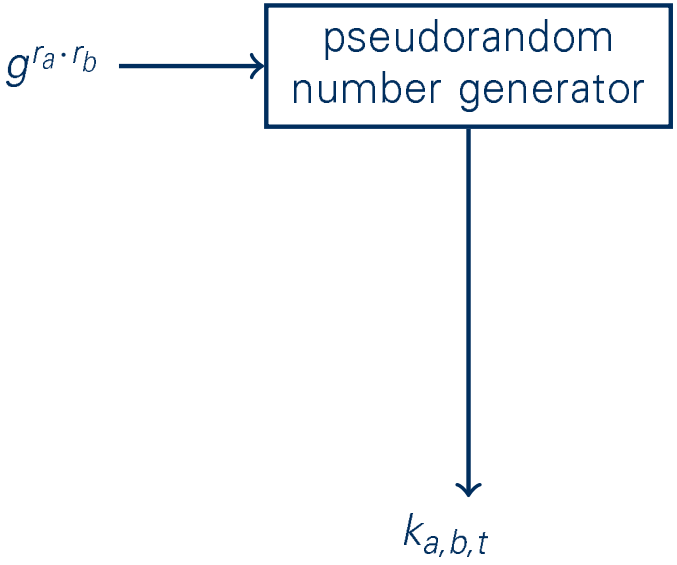
Simplifying the Key Exchange



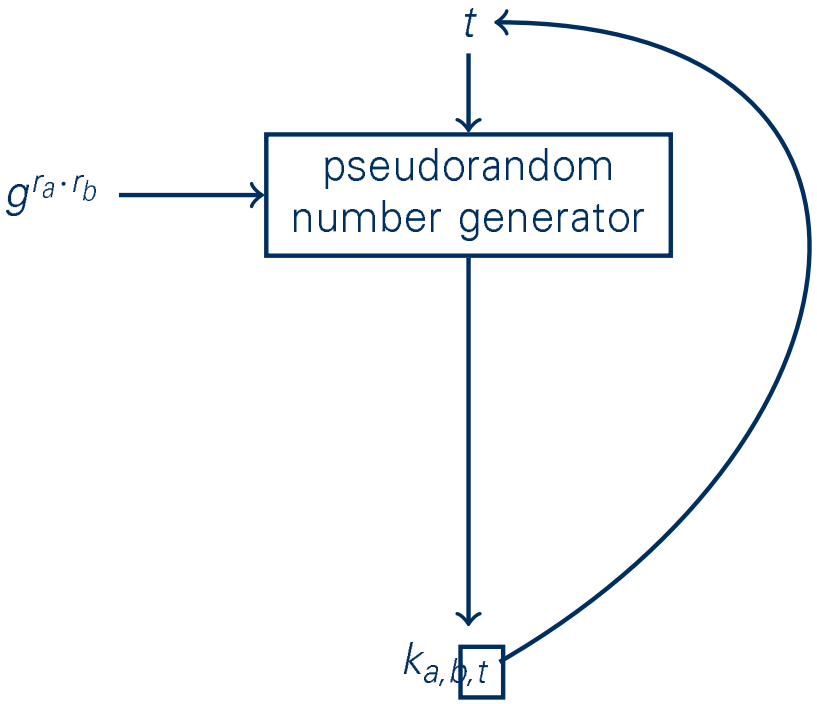
Simplifying the Key Exchange



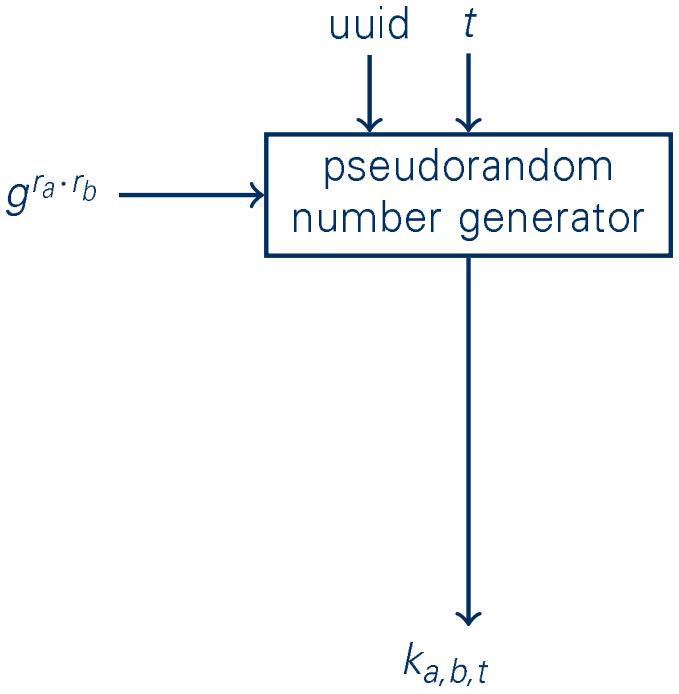
Simplifying the Key Exchange



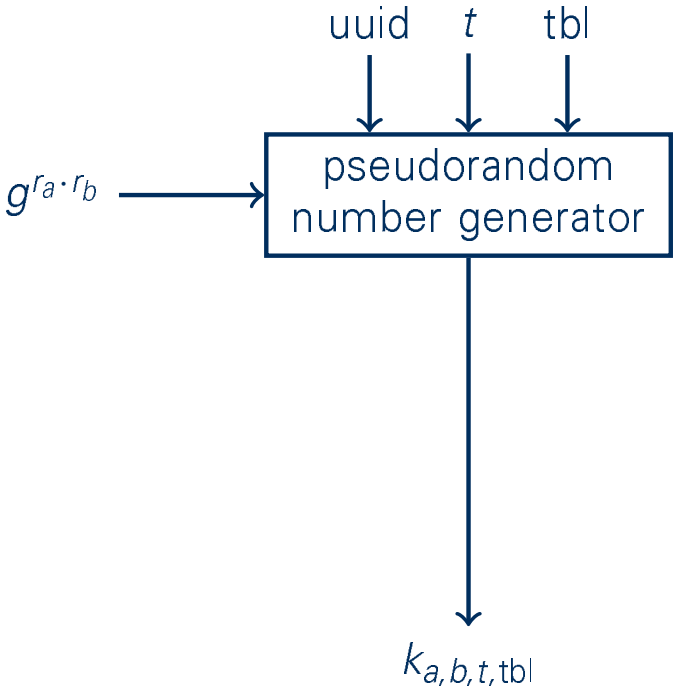
Simplifying the Key Exchange



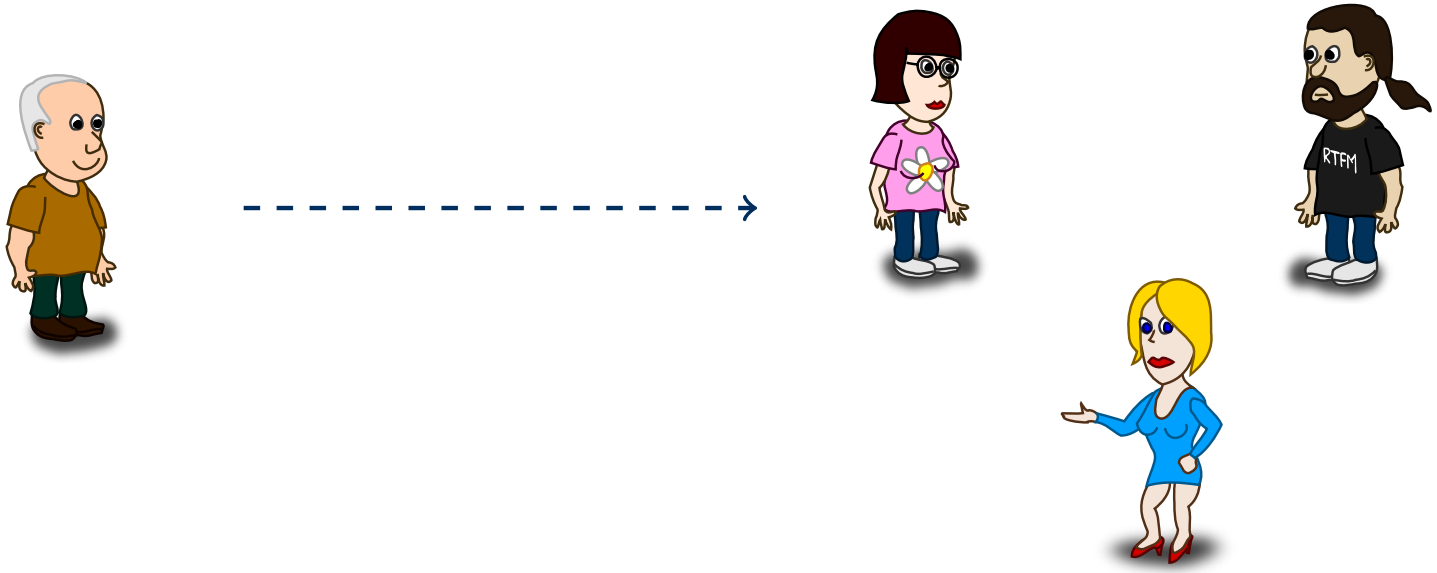
Simplifying the Key Exchange



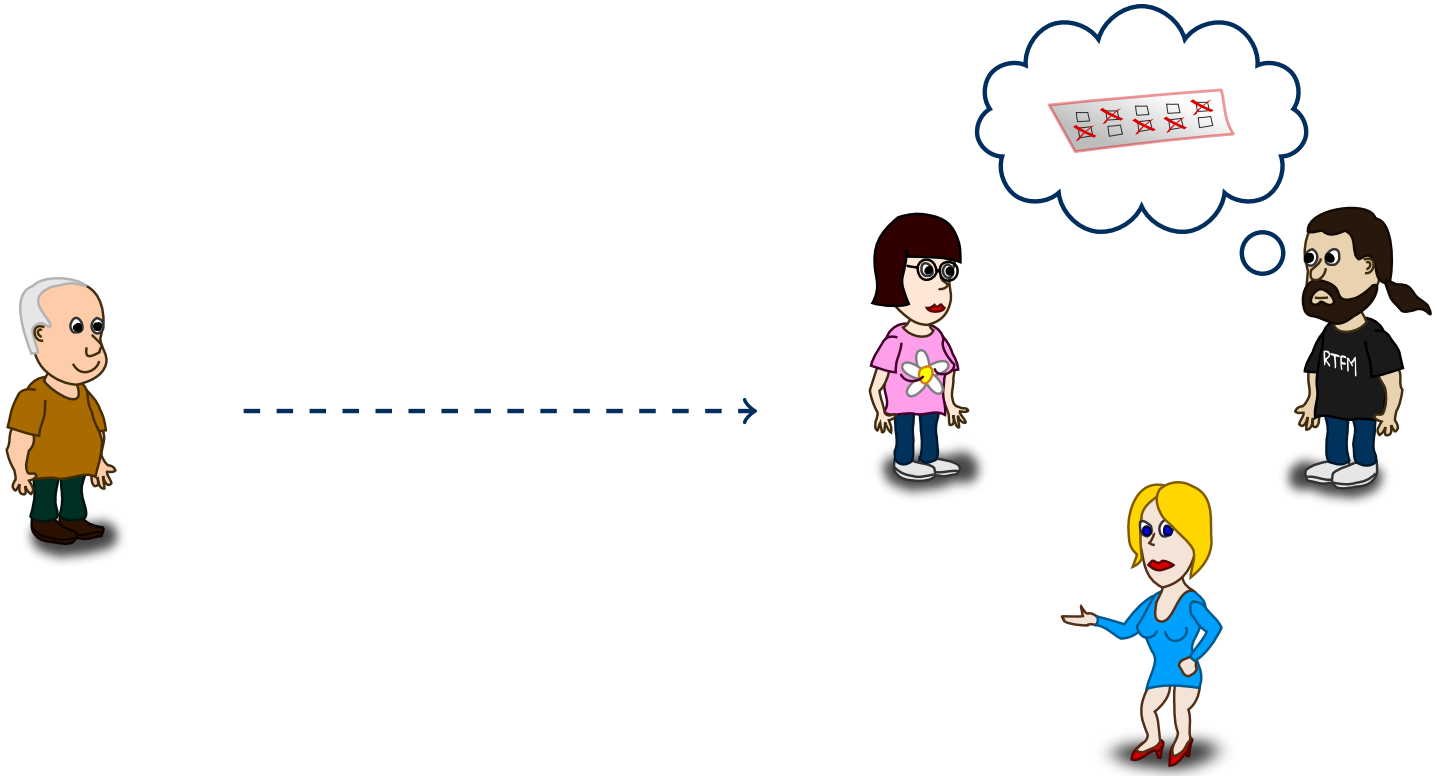
Simplifying the Key Exchange



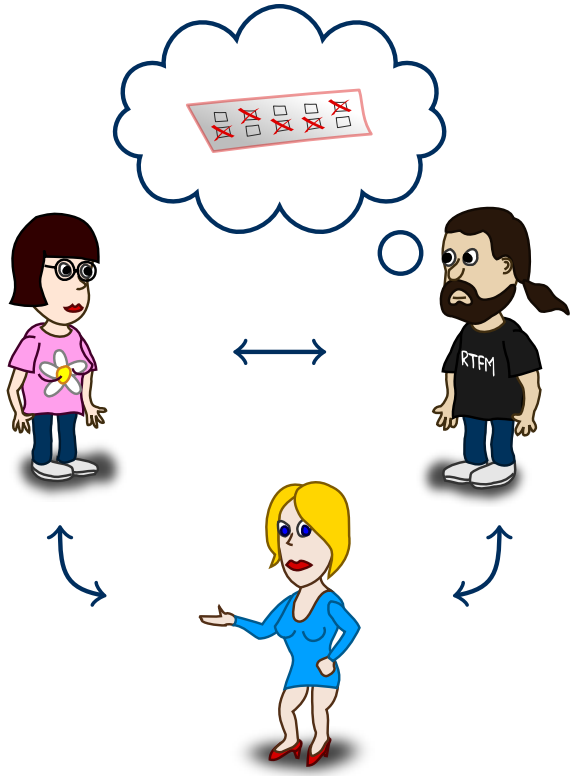
Dynamic Joining



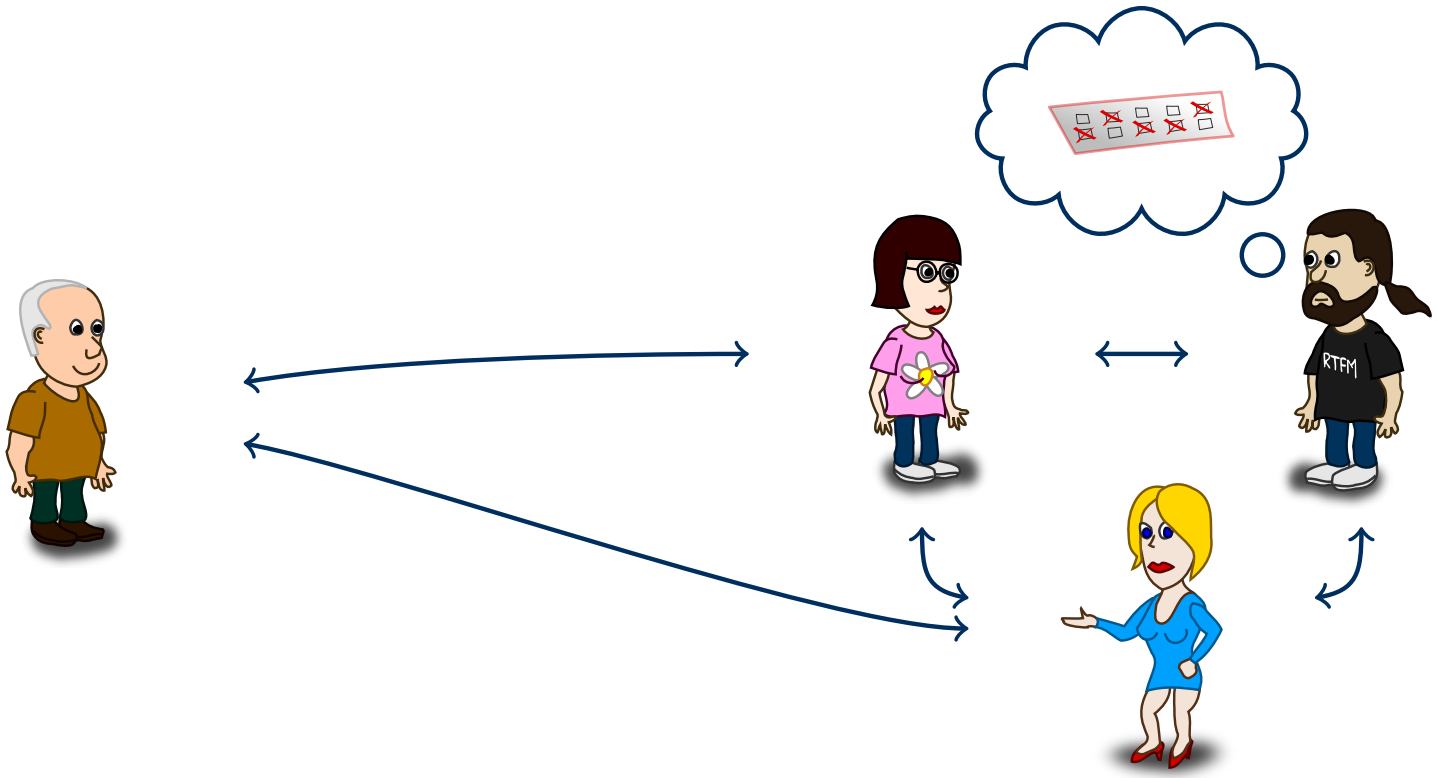
Dynamic Joining



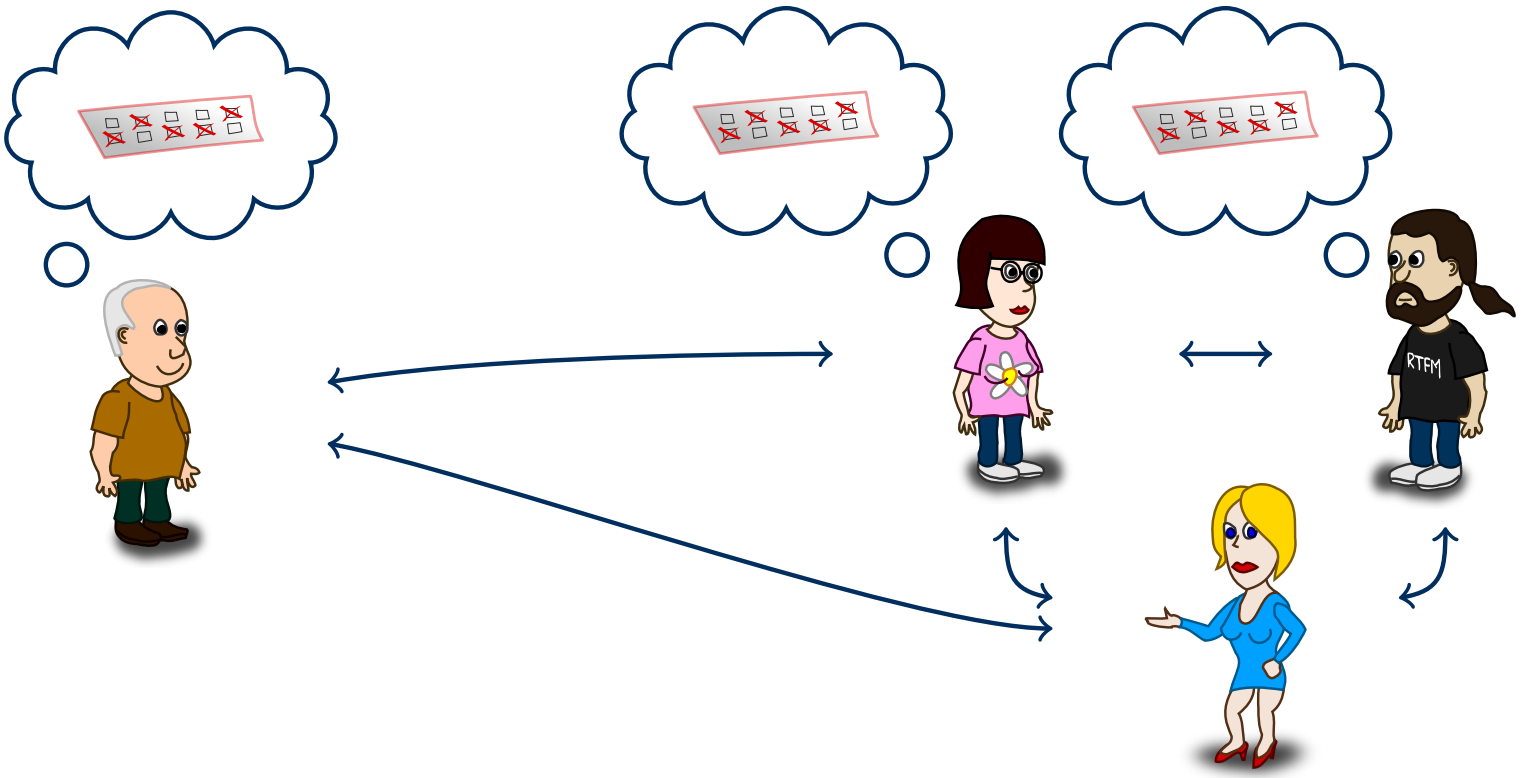
Dynamic Joining



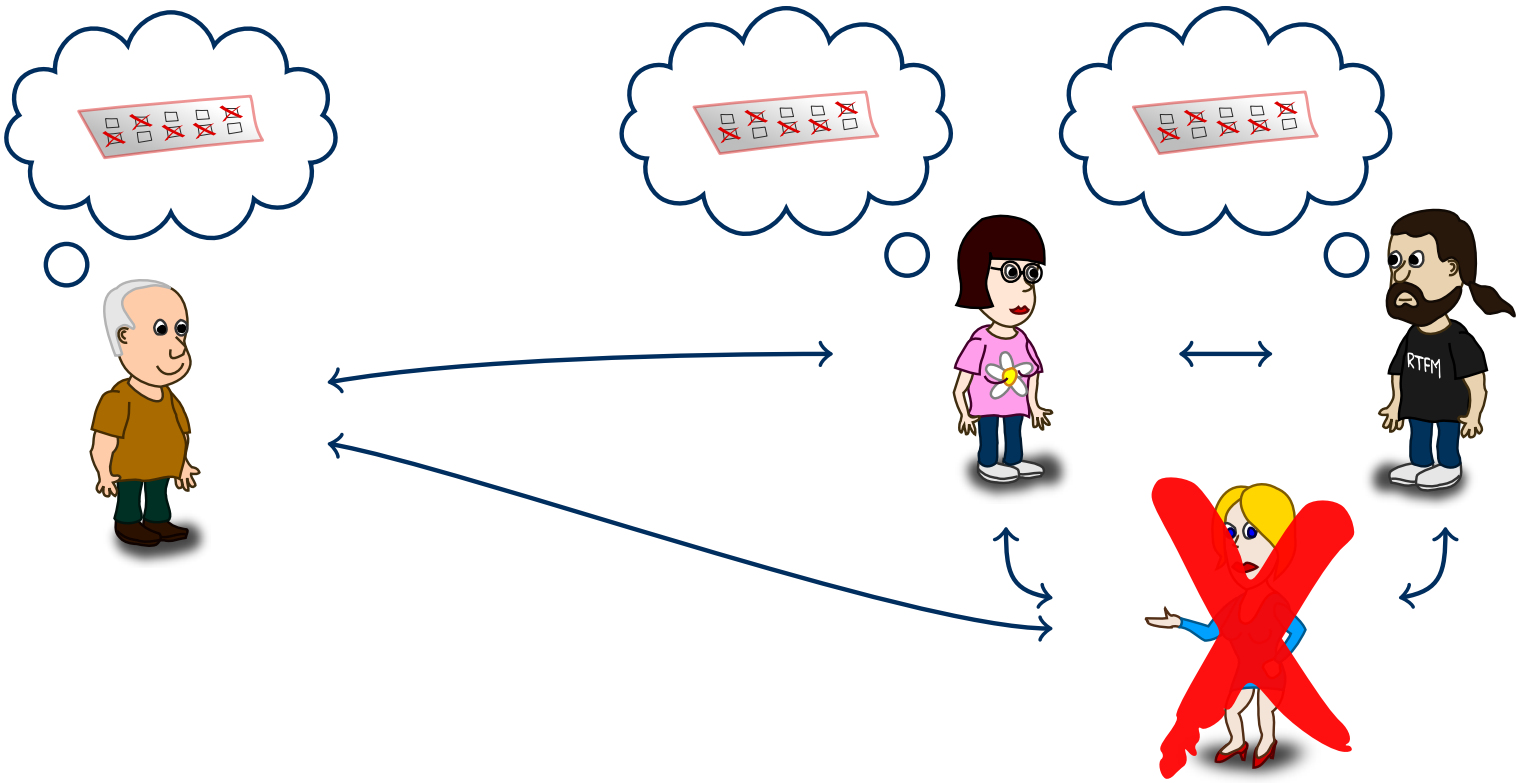
Dynamic Joining



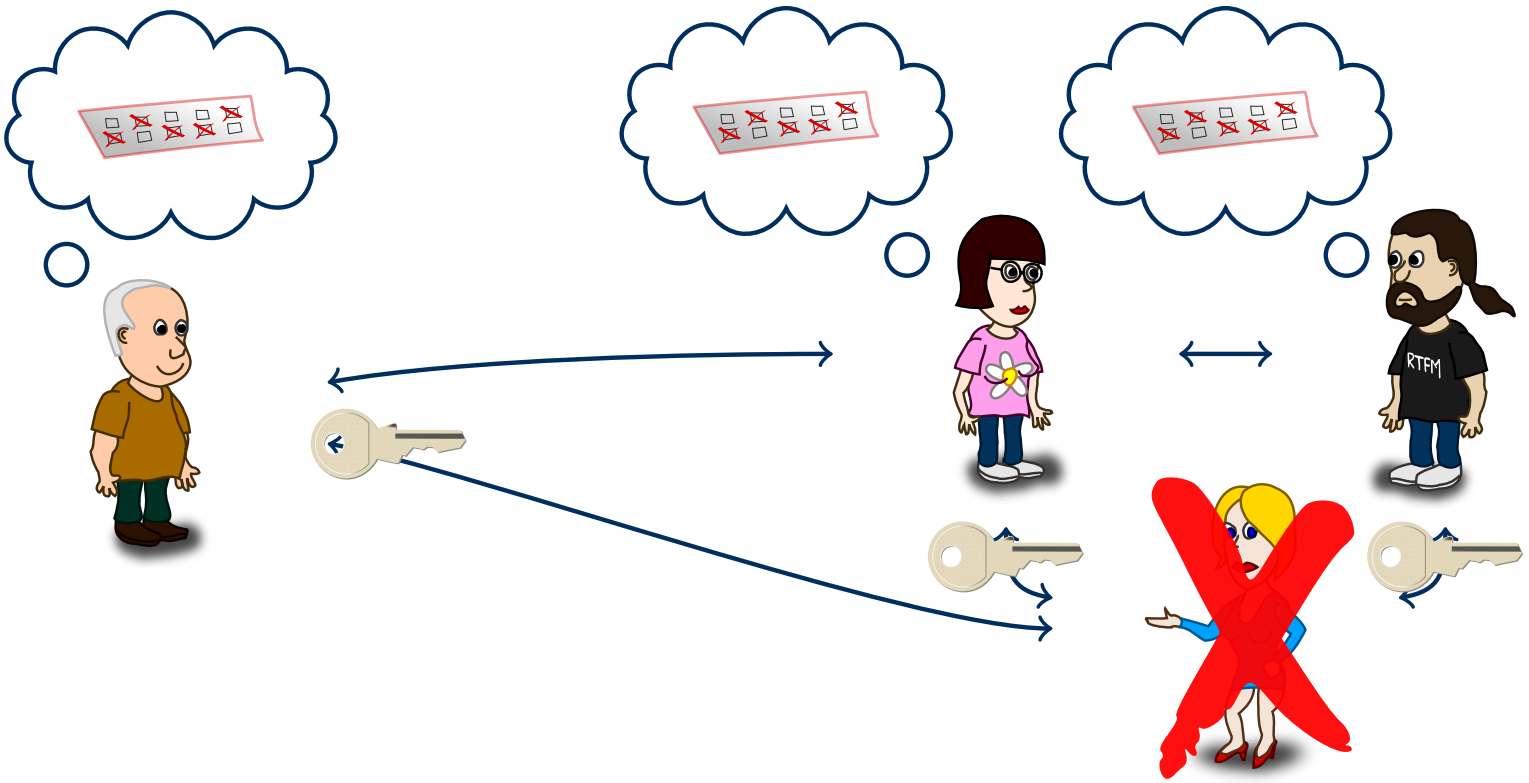
Dynamic Leaving



Dynamic Leaving

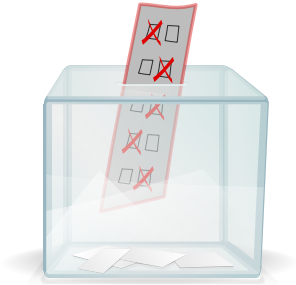


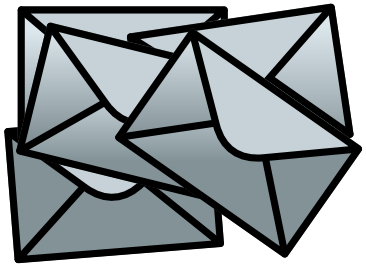
Dynamic Leaving



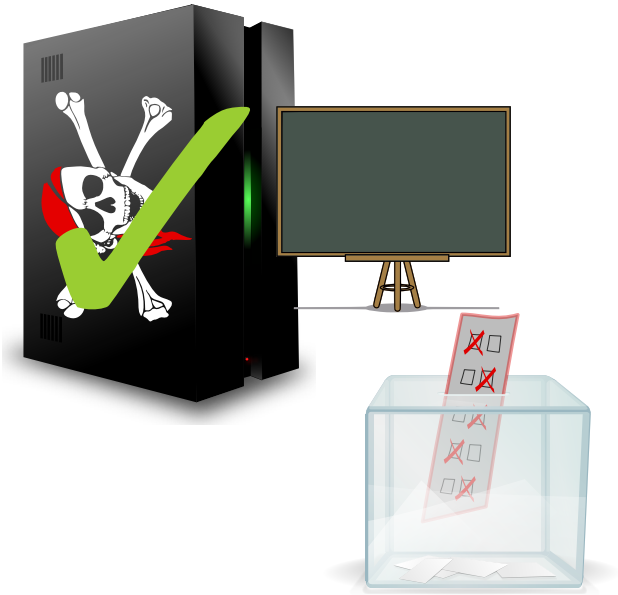
Evaluation

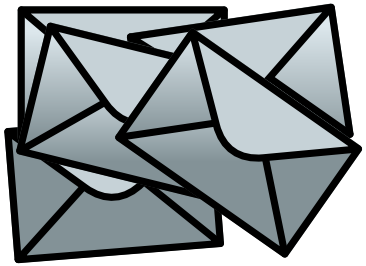
Evaluation



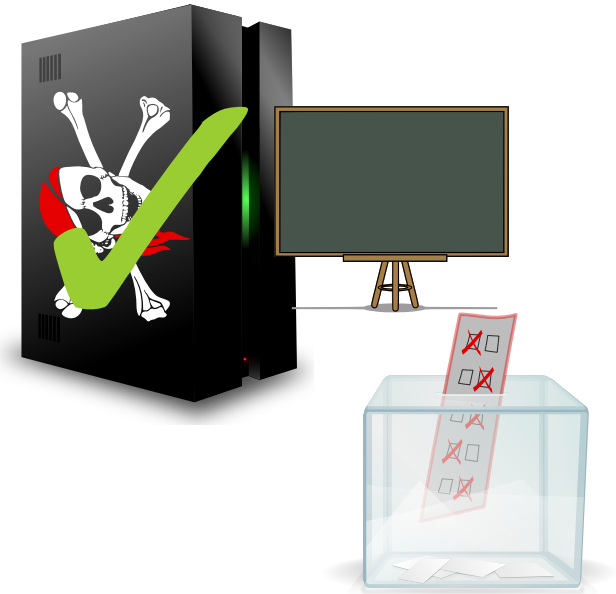


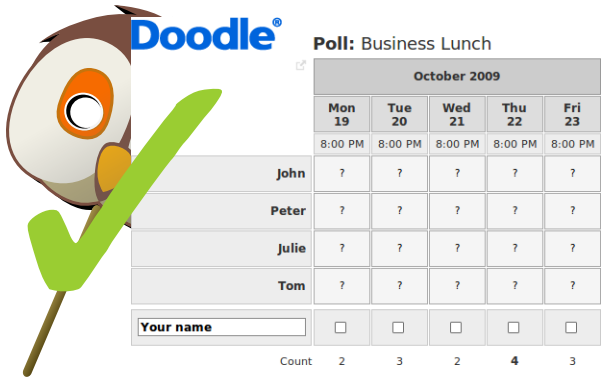
Evaluation

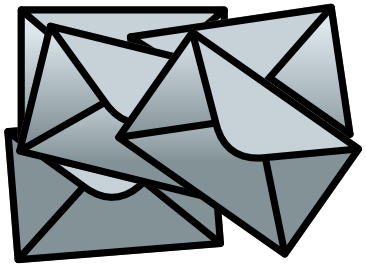




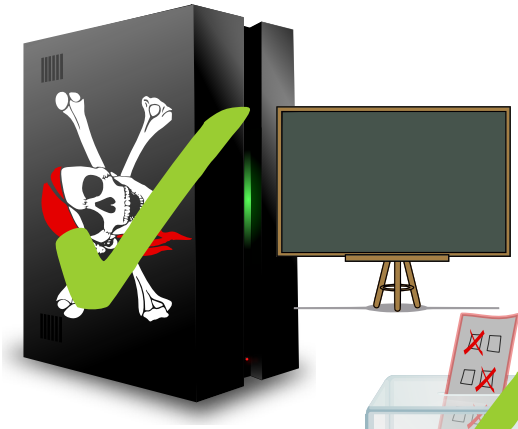
Evaluation

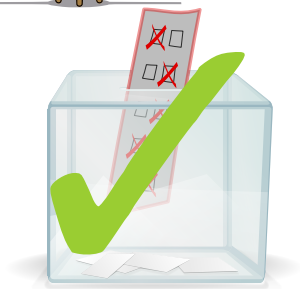


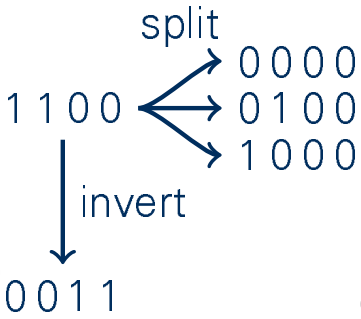

Doodle
Poll: Business Lunch
October 2009
Mon 19
Tue 20
Wed 21
Thu 22
Fri 23
8:00 PM
John
Peter
Julie
Tom
Your name
Count
2
3
2
4
3

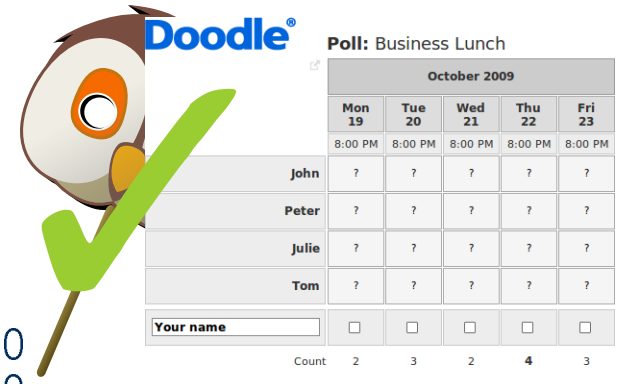


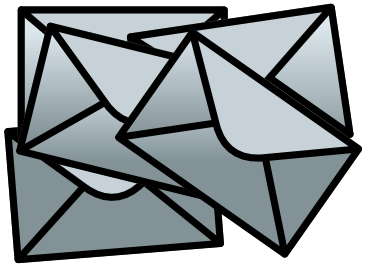
Evaluation



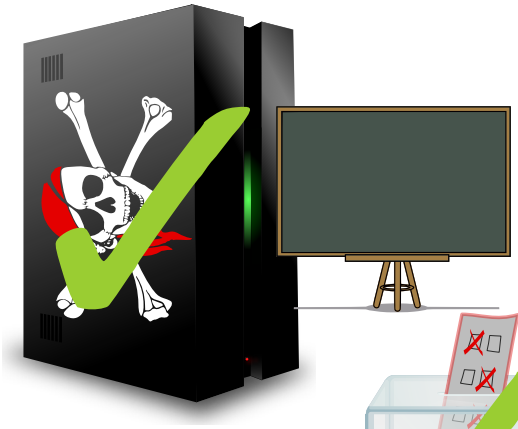


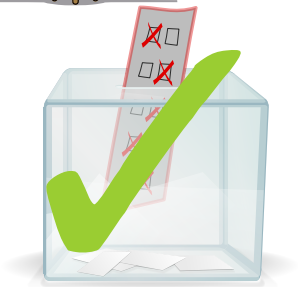

split
1 1 0 0
0 0 0 0
0 1 0 0
1 0 0 0
invert
0 0 1 1

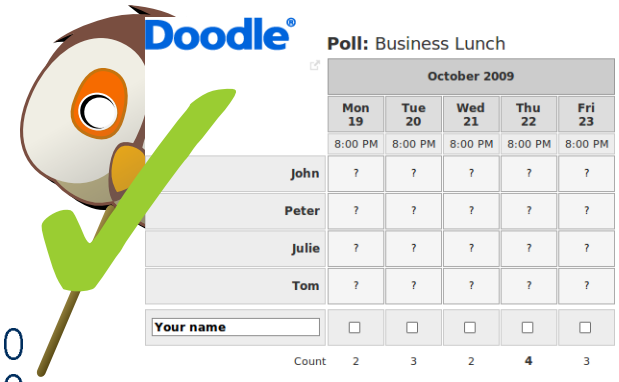

Doodle
Poll: Business Lunch
October 2009
Mon 19
Tue 20
Wed 21
Thu 22
Fri 23
8:00 PM
John
Peter
Julie
Tom
Your name
Count
2
3
2
4
3



Evaluation







split

1 1 0 0 → 0 0 0 0
→ 0 1 0 0
→ 1 0 0 0

invert

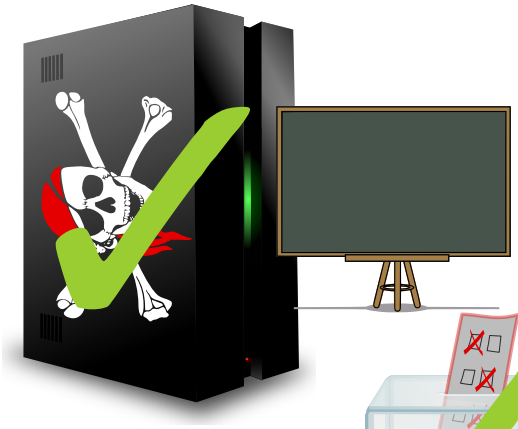
0 0 1 1

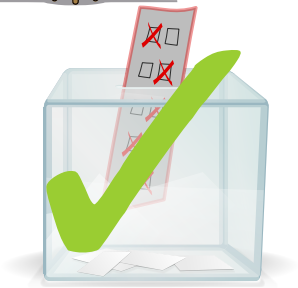
← initialization

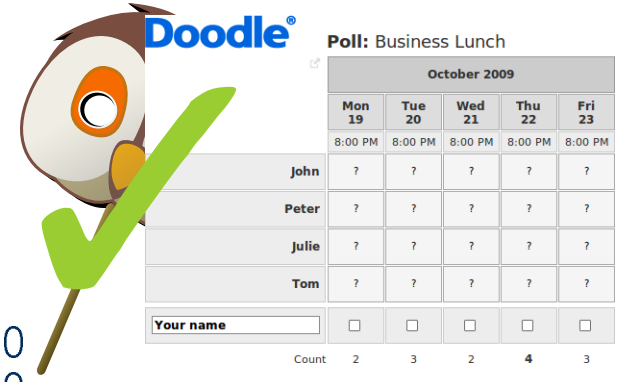
→ vote casting

← result publication

Evaluation







split

1 1 0 0 → 0 0 0 0
→ 0 1 0 0
→ 1 0 0 0

↓ invert

0 0 1 1

← initialization

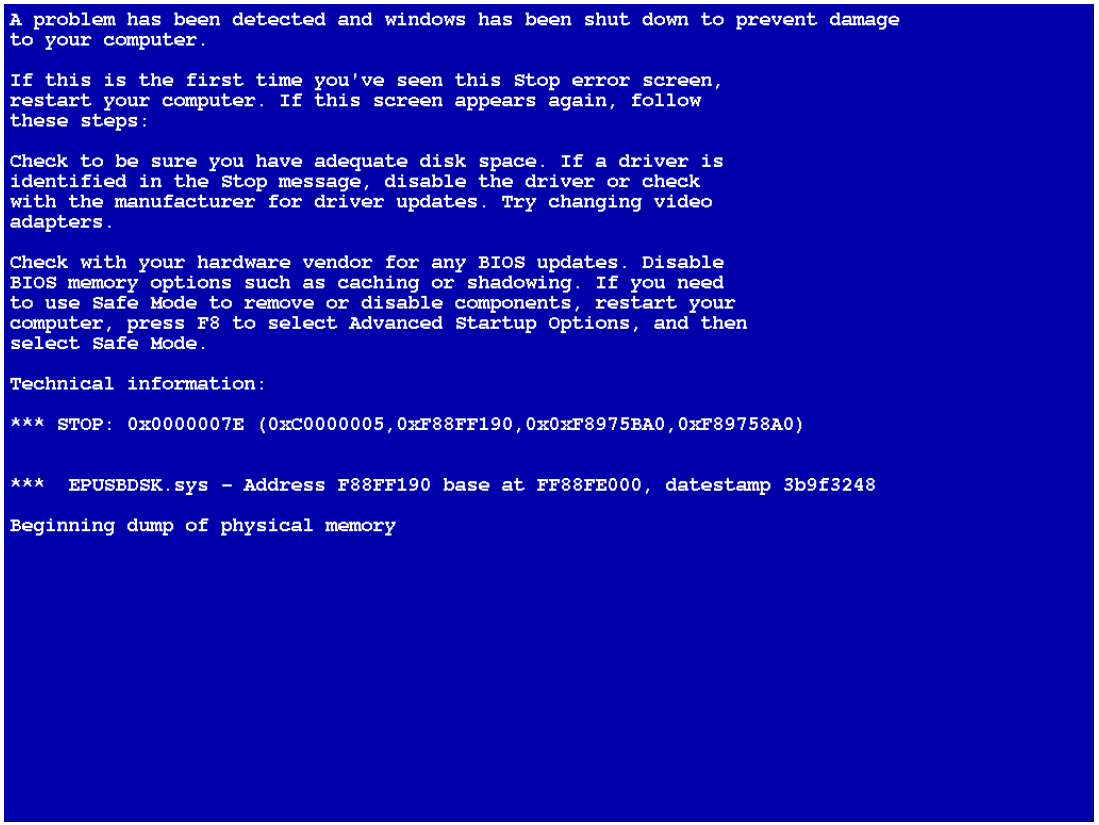
→ vote casting

← result publication

	Date #1	...	Date #240
Yes			✘
No	✘		

scales
($|P|$ — 1 asym. operations per voter)

Demo

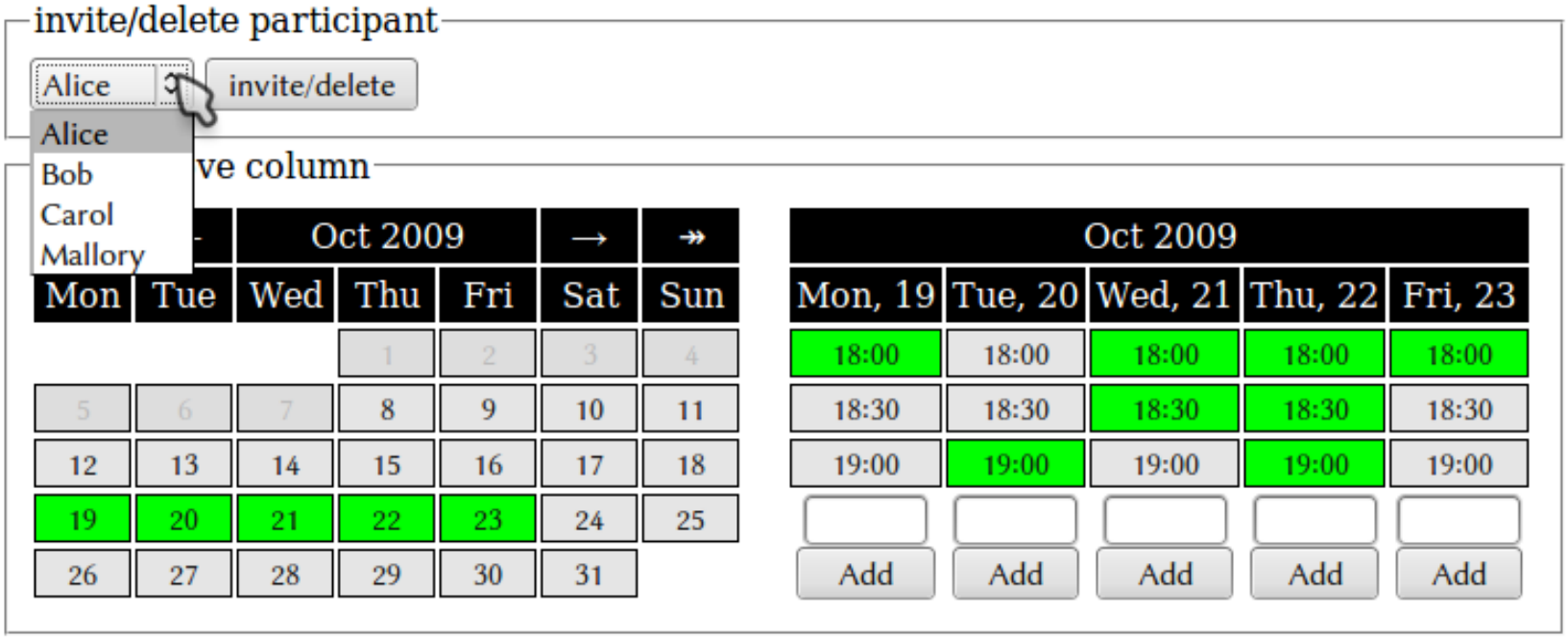


Registration/Login

Name: Bob
Password: ••••••••••••••••••••••
email: Bob@crypto.com
register

Name: Bob
Password: v91aEJ3LUC3eZG0XkCj1CKWZ30hkscpJs=
login

Poll Initialization



Vote Casting

Business Dinner

	Oct 2009								
	Mon, 19	Tue, 20	Wed, 21		Thu, 22			Fri, 23	
Name	18:00	19:00	18:00	18:30	18:00	18:30	19:00	18:00	Last Edit
Alice	☐	☑	☑	☑	☐	☑	☑	☑	submit
Bob	Participant has voted.								08.10, 10:30
Carol	Participant has voted.								08.10, 10:29
Mallory	Participant has not voted yet. kickout								08.10, 10:21

Vote Casting

Business Dinner

	Oct 2009								
	Mon, 19	Tue, 20	Wed, 21		Thu, 22			Fri, 23	
Name	18:00	19:00	18:00	18:30	18:00	18:30	19:00	18:00	Last Edit
Alice	Participant has voted.								08.10, 10:32
Bob	Participant has voted.								08.10, 10:30
Carol	Participant has voted.								08.10, 10:29
Mallory	Participant has not voted yet. kickout								08.10, 10:21

Dynamic Leaving

Business Dinner

	Oct 2009								
	Mon, 19	Tue, 20	Wed, 21		Thu, 22			Fri, 23	
Name	18:00	19:00	18:00	18:30	18:00	18:30	19:00	18:00	Last Edit
Alice	Participant has voted.								08.10, 10:32
Bob	Participant has voted.								08.10, 10:30
Carol	Participant has voted.								08.10, 10:29
Mallory	Bob, Carol want to remove this participant. agree								08.10, 10:21

Result Publication

Business Dinner

	Oct 2009								
	Mon, 19	Tue, 20	Wed, 21		Thu, 22			Fri, 23	
Name	18:00	19:00	18:00	18:30	18:00	18:30	19:00	18:00	Last Edit
Alice	Participant has voted.								08.10, 10:32
Bob	Participant has voted.								08.10, 10:30
Carol	Participant has voted.								08.10, 10:29
Mallory	Participant was removed.								08.10, 10:21
total	1	2	3	3	0	3	3	3	

Conclusion and Outlook

- novel scheme for privacy-enhanced event scheduling
  - ➠ scales in number of time slots
  - ➠ no central trust entity
- partially implemented as Web 2.0 application

- implement missing features
- validate performance
- more features desirable

Thank you for your attention!

http://dudle.inf.tu-dresden.de

Benjamin.Kellermann@tu-dresden.de
D19E 04A8 8895 020A 8DF6
0092 3501 1A32 491A 3D9C

Berlin, December 29, 2009

PrimeLife is a research project funded by the European Commission's 7th Framework Programme

Related

- one specific publication
- mixes
- blind signatures
- homomorphic encryption
- distributed constraint satisfaction/optimization problem

T. Herlea et al., "On Securely Scheduling a Meeting," in *Trusted Information — The New Decade Challenge (Proc. of IFIP SEC)*, M. Dupuy and P. Paradinas, Eds., 2001, pp. 183–198.

Computational Complexity

server

no expensive computation needed

client

1	discrete exponentiation (DH)
$\lvert P\rvert - 1$	discrete exponentiations
1	digital signature
$\lvert T\rvert \cdot (\lvert P\rvert - 1)$	hashes
$\lvert T\rvert \cdot (\lvert P\rvert - 1)$	symmetric decryptions

More Features

- privacy-invasive and privacy-enhanced together
- predefined decision rules
- threshold scheme
- dynamic insertion/deletion of time slots
- updating/revoking votes
- let voters prove that they signaled availability for more than a certain minimum number of time slots

Privacy-Invasive and Privacy-Enhanced

	Oct 2009								
	Mon, 19	Tue, 20	Wed, 21		Thu, 22			Fri, 23	
Name	18:00	19:00	18:00	18:30	18:00	18:30	19:00	18:00	Last Edit
Alice	Participant has voted.								08.10, 10:32
Bob	Participant has voted.								08.10, 10:30
Carol	Participant has voted.								08.10, 10:29
Mallory	Participant was removed.								08.10, 10:21
Dave	✔	✔	✘	✔	✔	✘	✔	✘	10.11, 10:39
Ted	✔	✘	✔	✔	✘	✔	✘	✔	10.11, 10:40
	○ ✔ ◉ ✘ ○ ?	○ ✔ ◉ ✘ ○ ?	○ ✔ ◉ ✘ ○ ?	○ ✔ ◉ ✘ ○ ?	○ ✔ ◉ ✘ ○ ?	○ ✔ ◉ ✘ ○ ?	○ ✔ ◉ ✘ ○ ?	○ ✔ ◉ ✘ ○ ?	add user
total	3	3	4	5	1	4	4	4	

Complex Decision Rules

	Mon, 19	Tue, 20	Wed, 21		Thu, 22			Fri, 23	
Name	18:00	19:00	18:00	18:30	18:00	18:30	19:00	18:00	Last Edit
Alice	Participant has voted.								08.10, 10:32
Bob	Participant has voted.								08.10, 10:30
Carol	Participant has voted.								08.10, 10:29
Mallory	Participant was removed.								08.10, 10:21
Dave	Participant has voted.								08.10, 10:32
Ted	Participant has voted.								08.10, 10:30
Marvin	Participant was removed.								08.10, 10:29
Eve	Participant has voted.								08.10, 10:21
institute	1	3	3	0	3	3	3	3	
leader	1	2	3	3	0	3	3	3	
total	3	4	4	5	4	4	4	4	