TECHNISCHE UNIVERSITÄT DRESDEN

PrimeLife

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

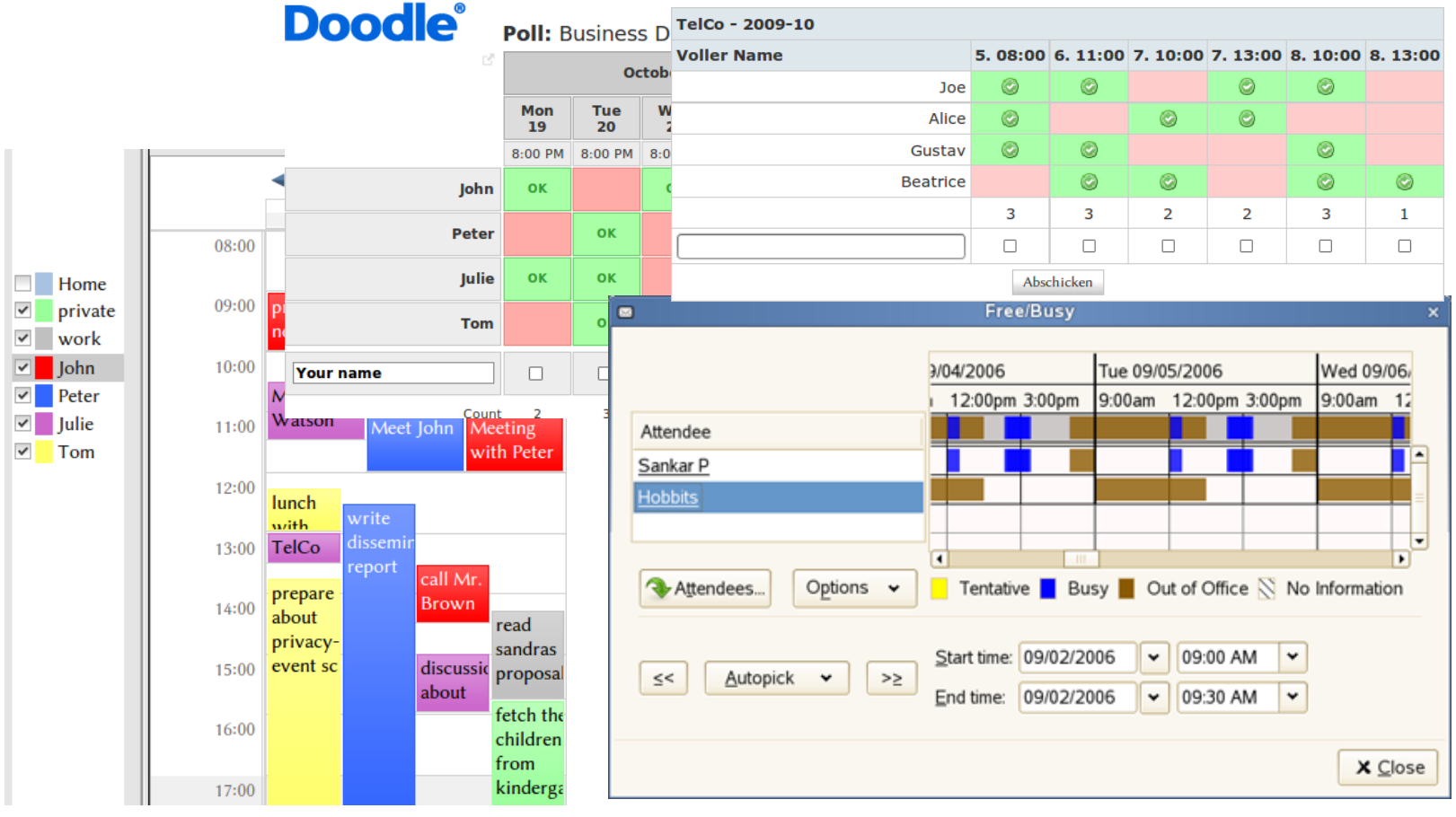
Privacy-Enhanced Event Scheduling

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

Vancouver, August 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

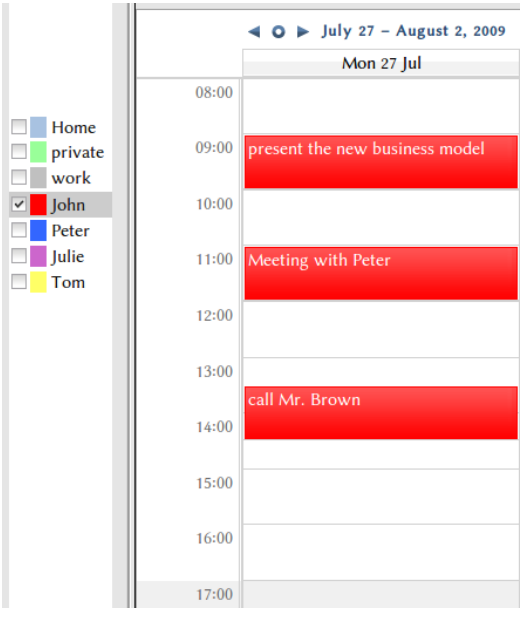
Indirect Inference

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!

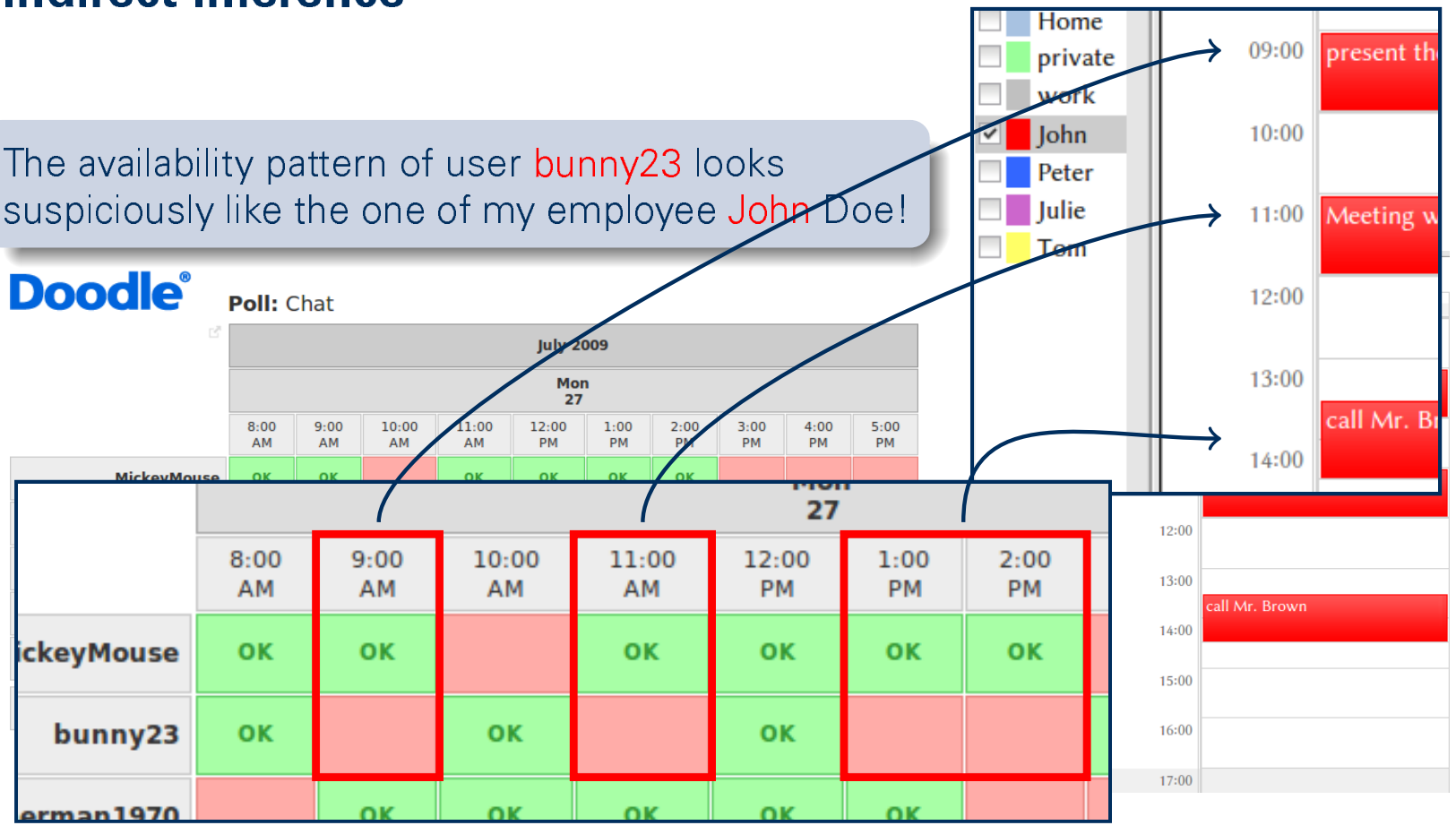


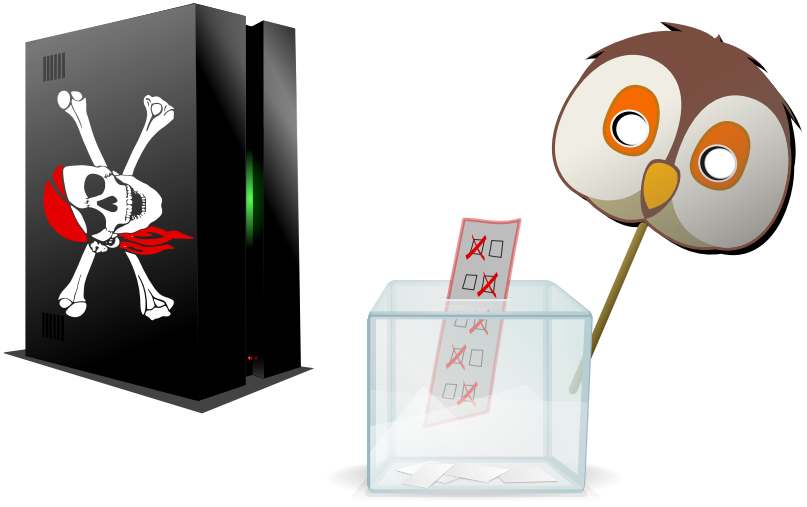
Table of Contents

Requirements

- Untrusted Server

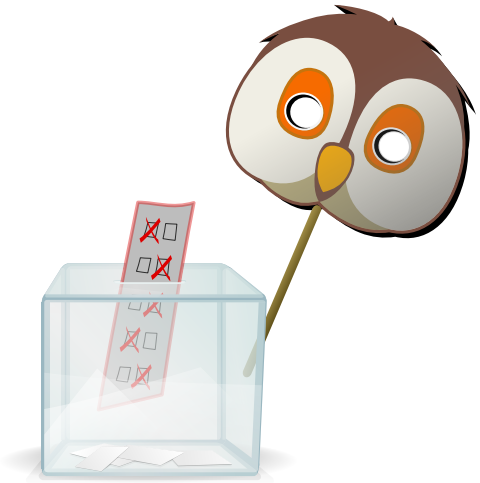
Requirements

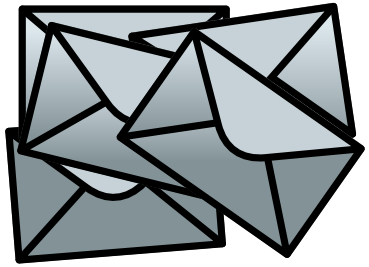
- Untrusted Server
- Privacy
- Verifiability



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

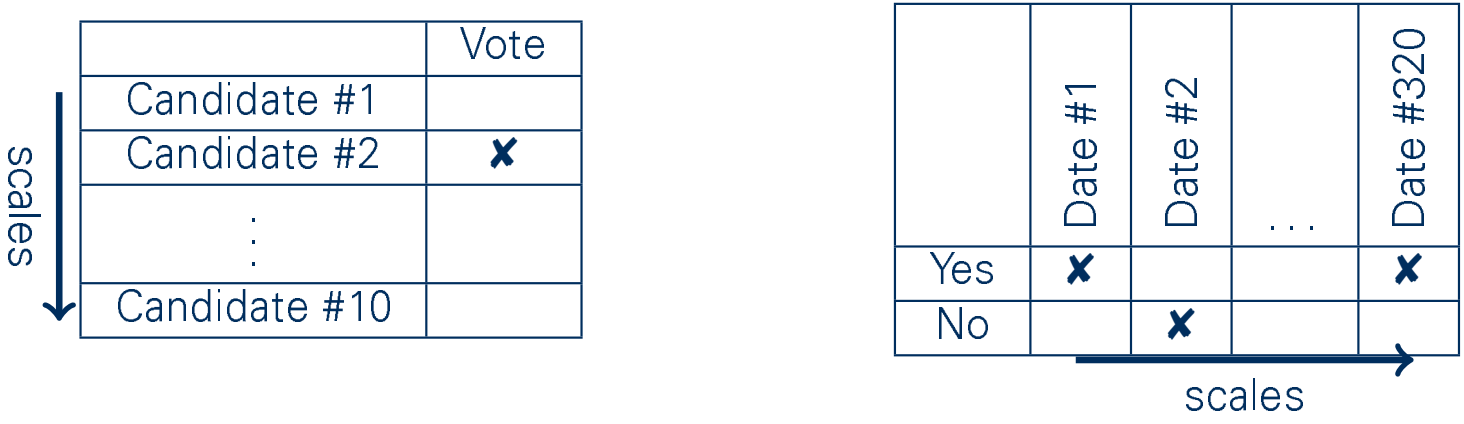
scales

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

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

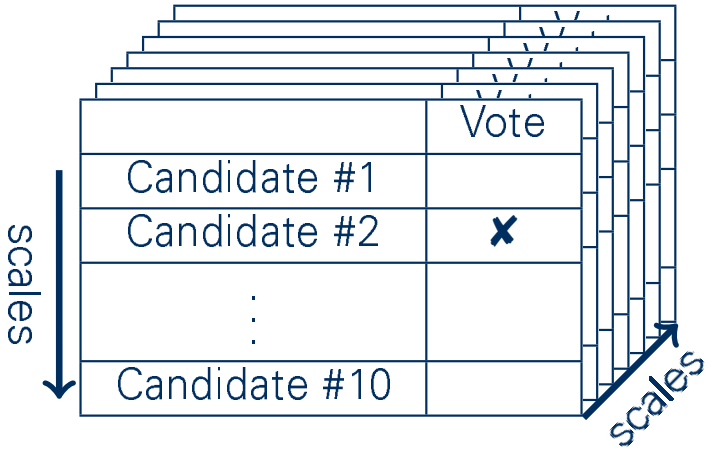
one vote per column

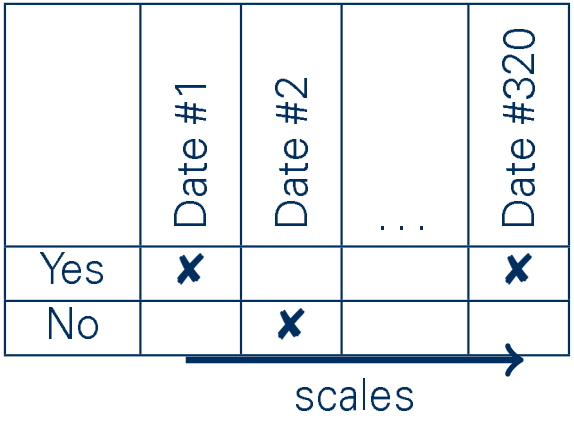
E-Voting vs. Event Scheduling



one vote per column

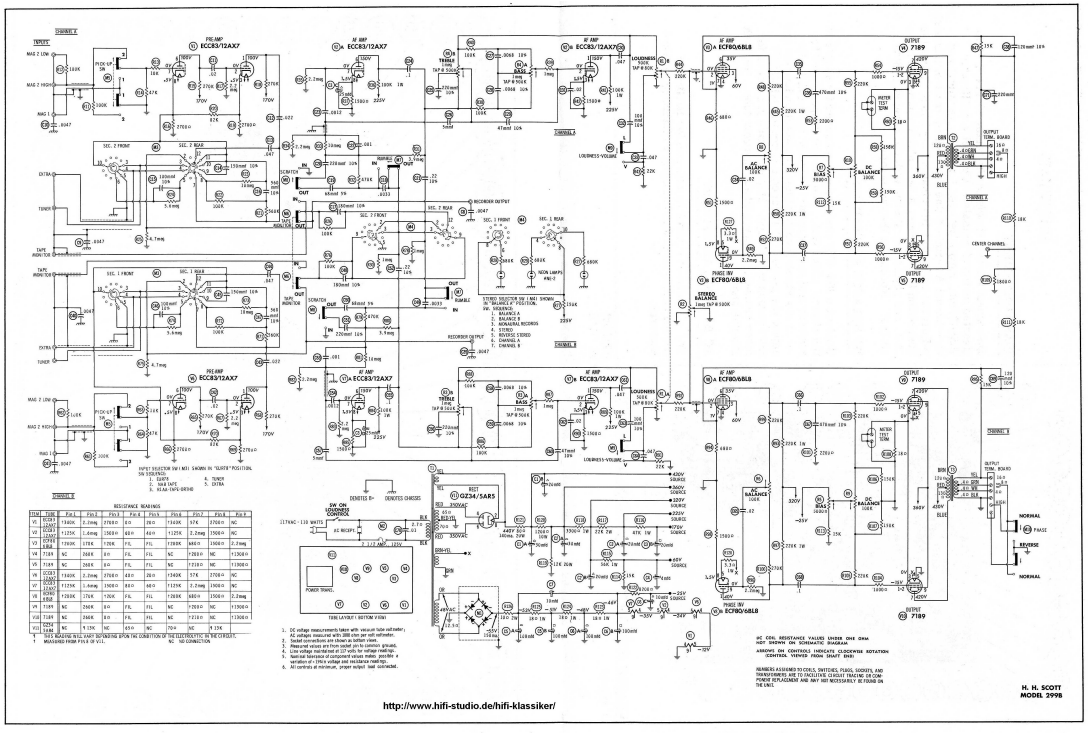
E-Voting vs. Event Scheduling



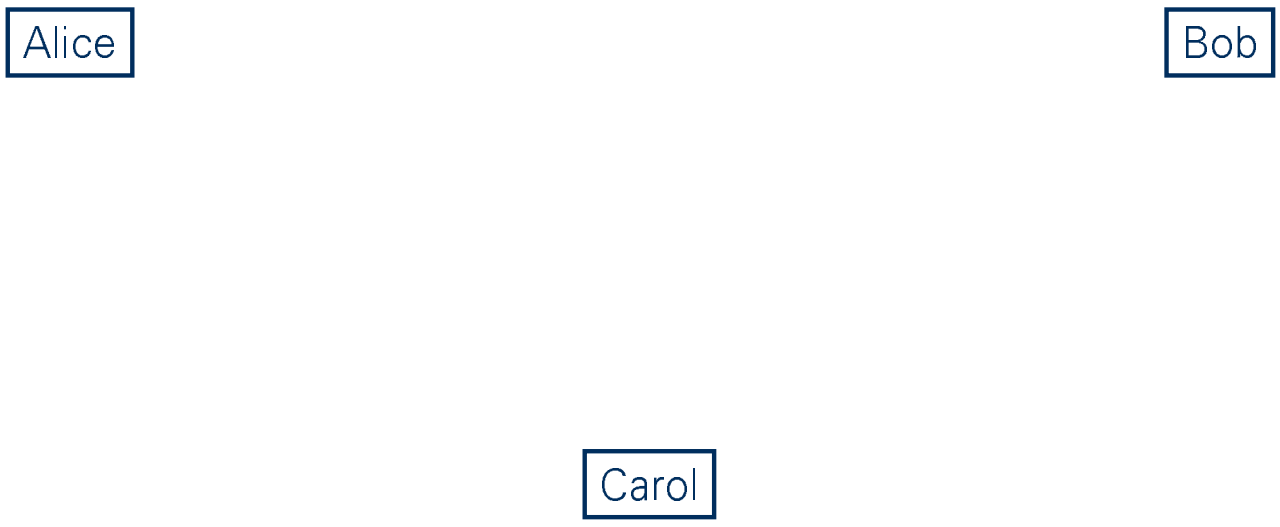


one vote per column

Scheme

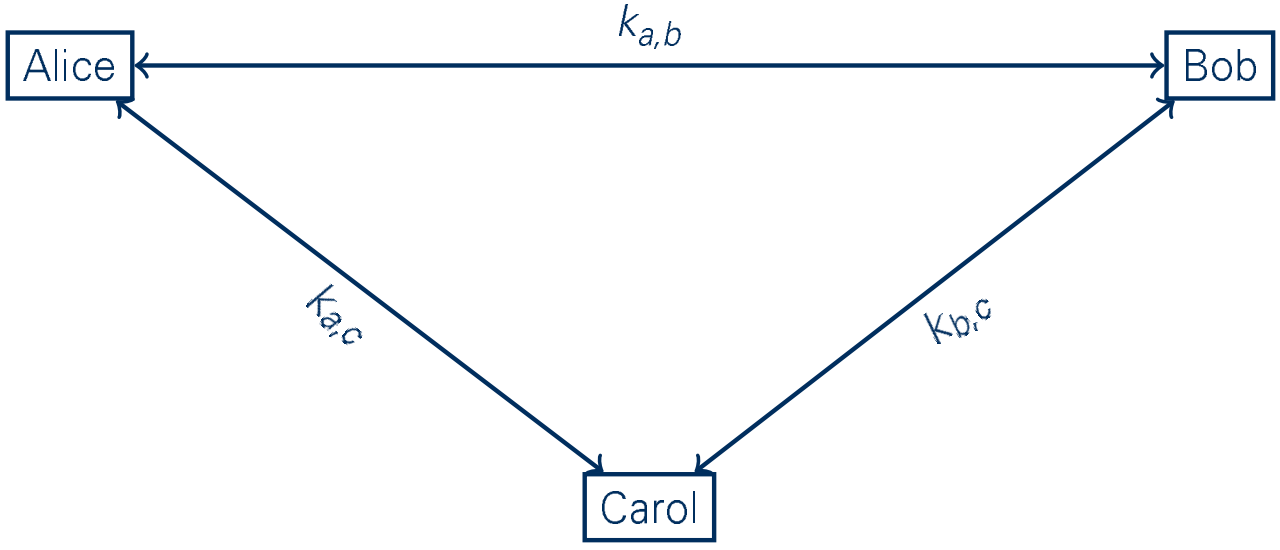


Superposed Sending



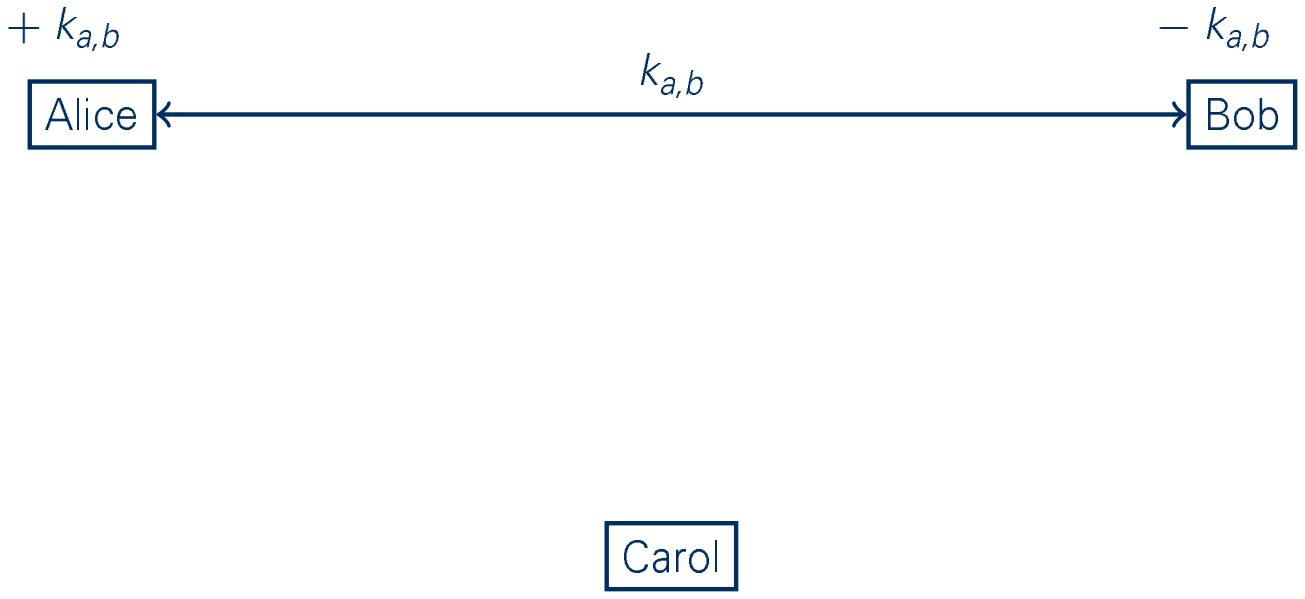
D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

Superposed Sending



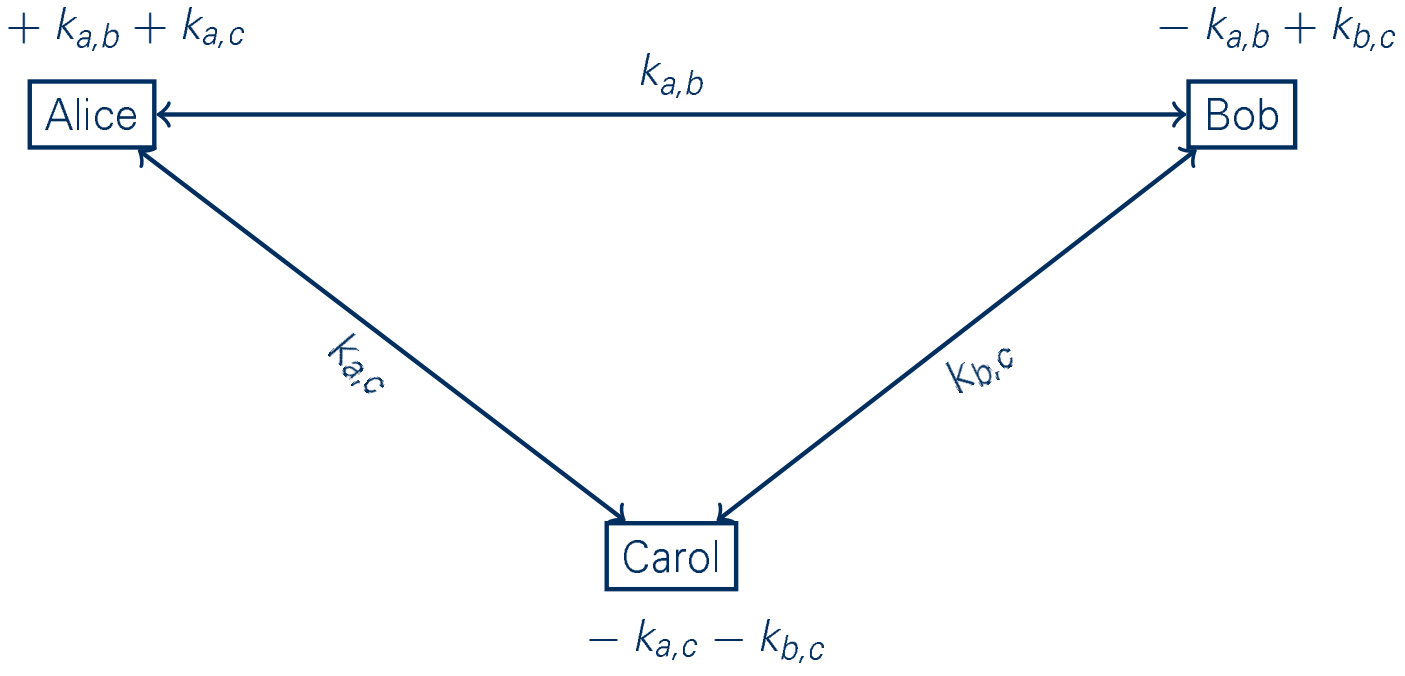
D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

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



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

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

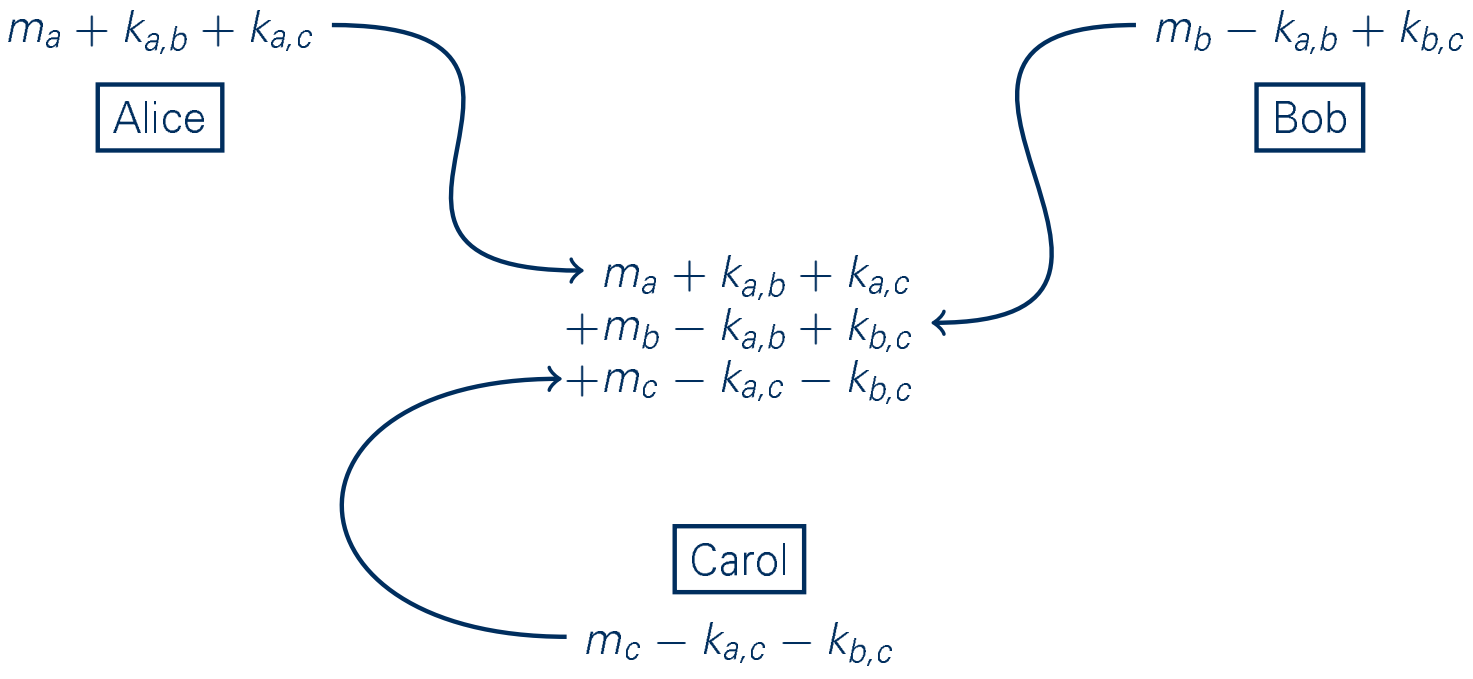
Bob

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

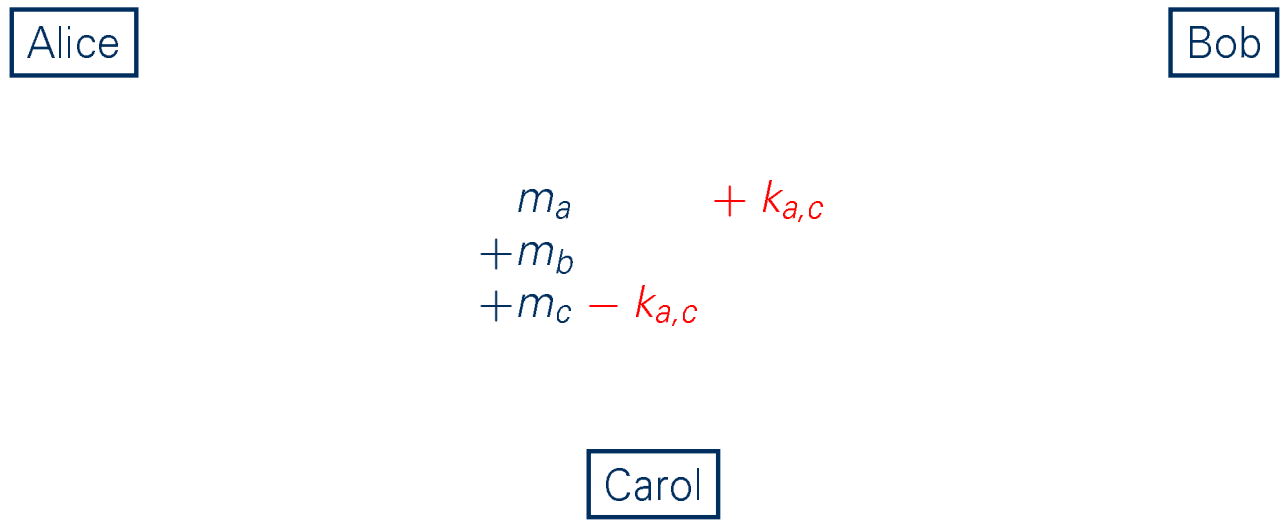
Bob

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

Carol

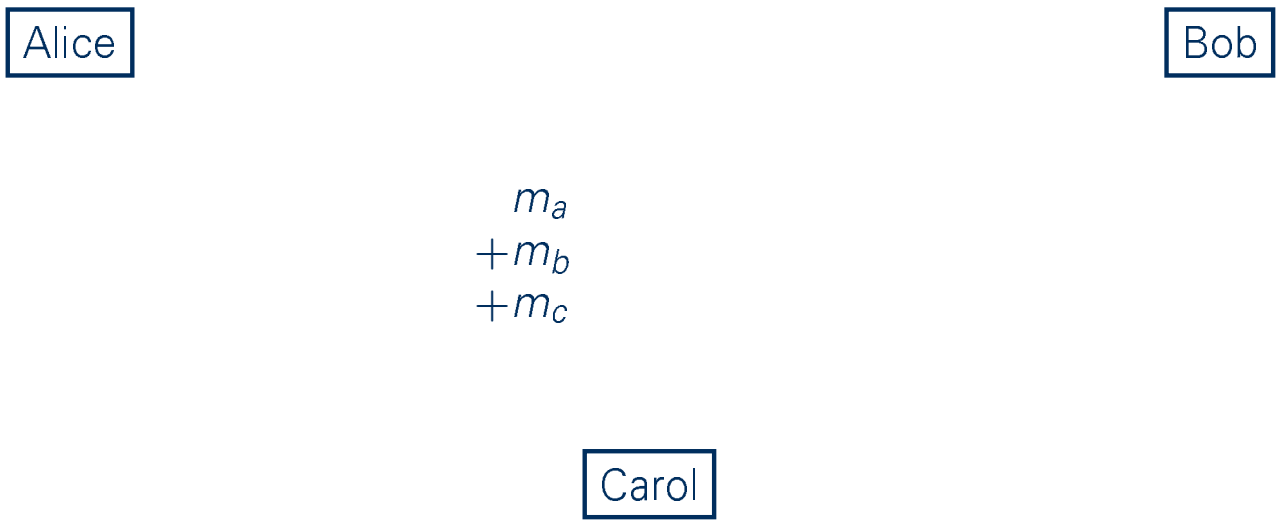
D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

Superposed Sending



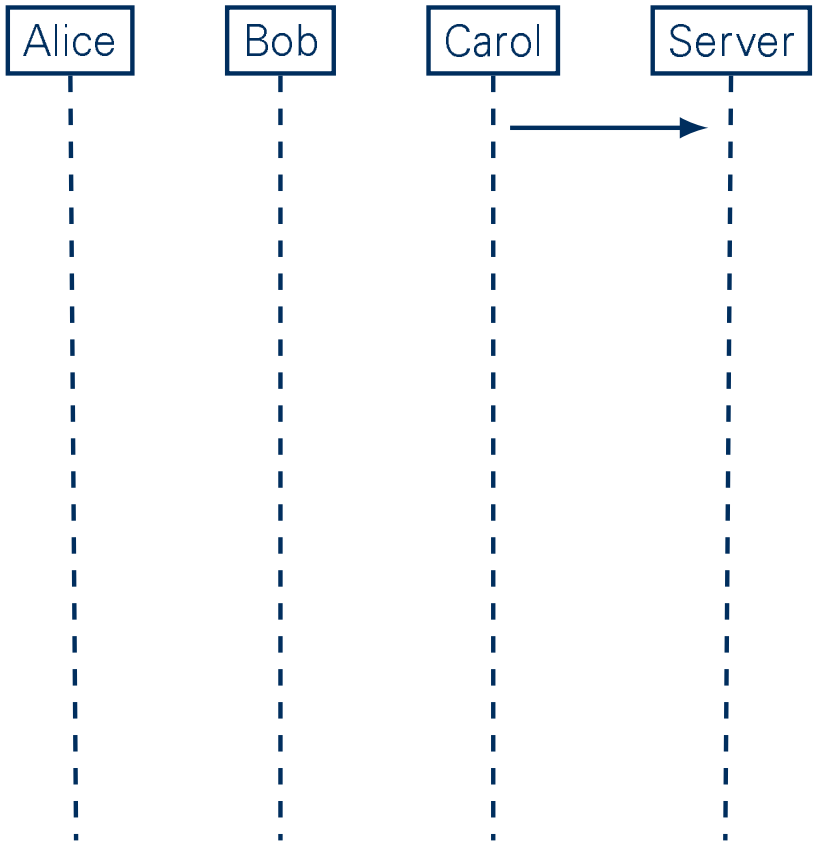
D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

Superposed Sending

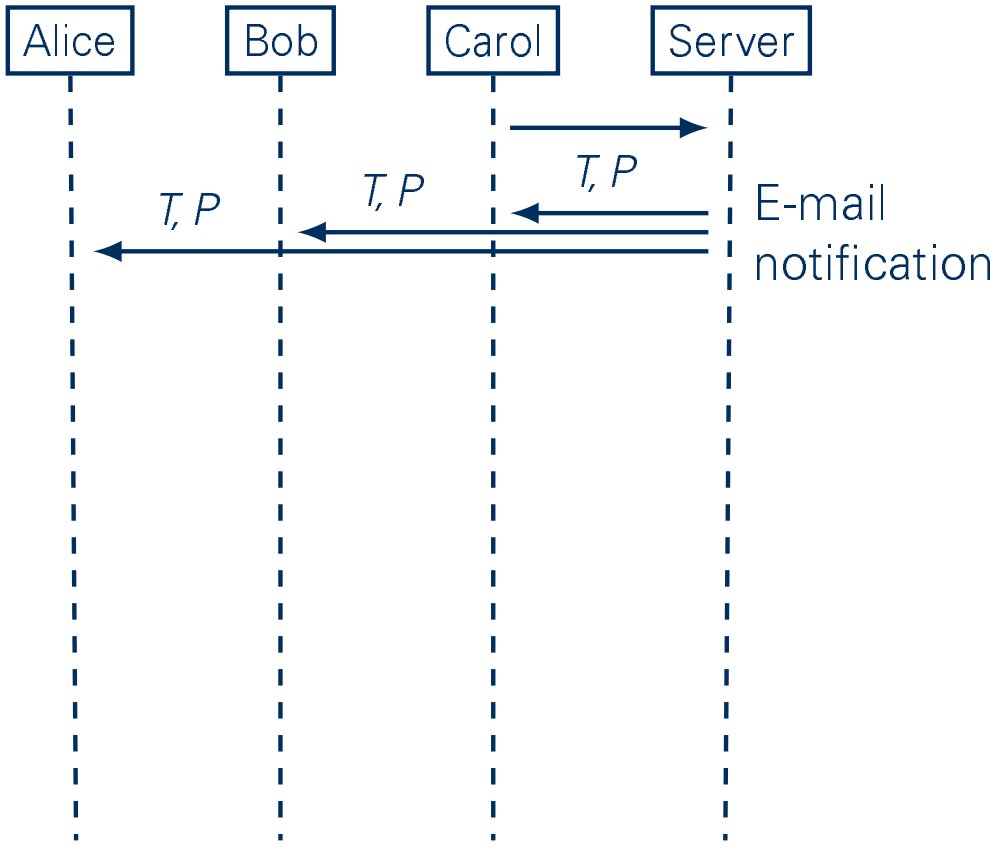


D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

Poll Initialization

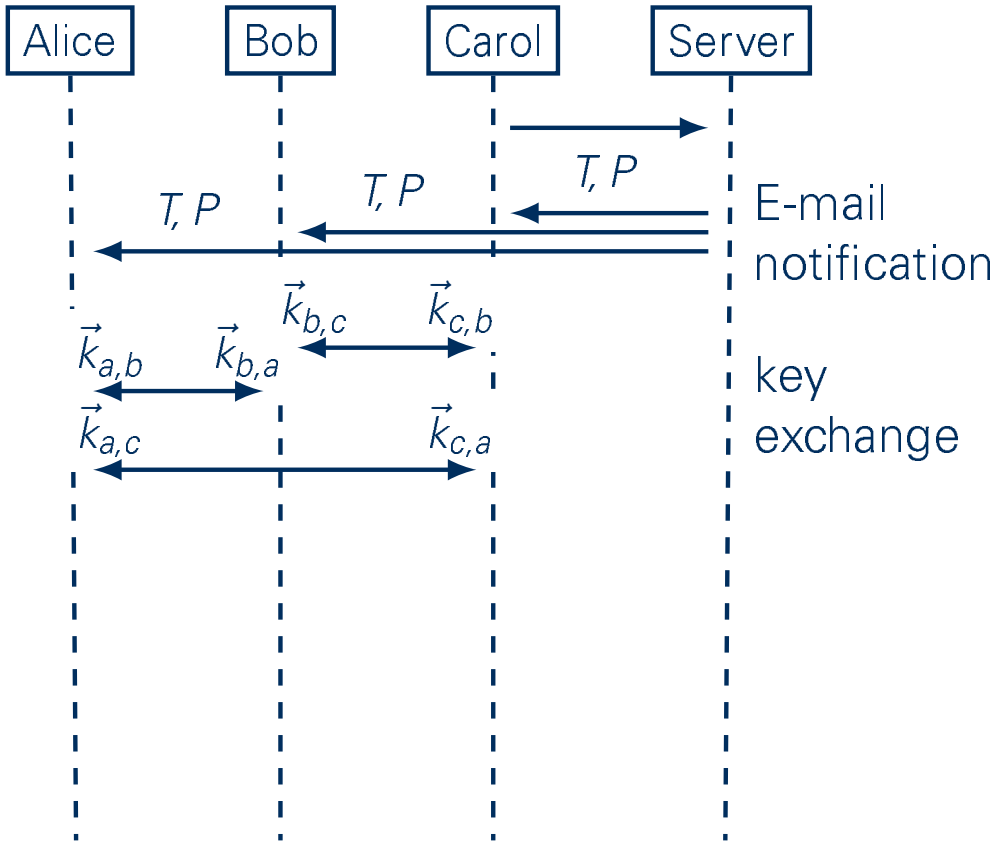


Poll Initialization



T . . . time slots
P . . . voters

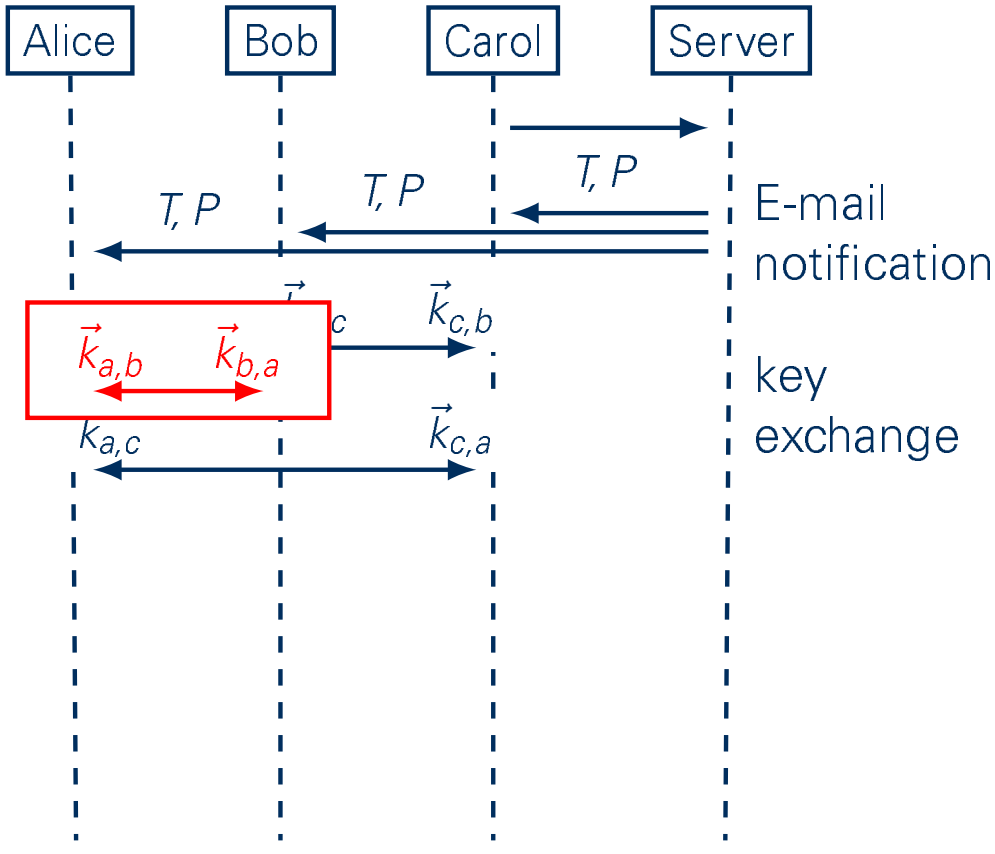
Poll Initialization



T . . . time slots
P . . . voters

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

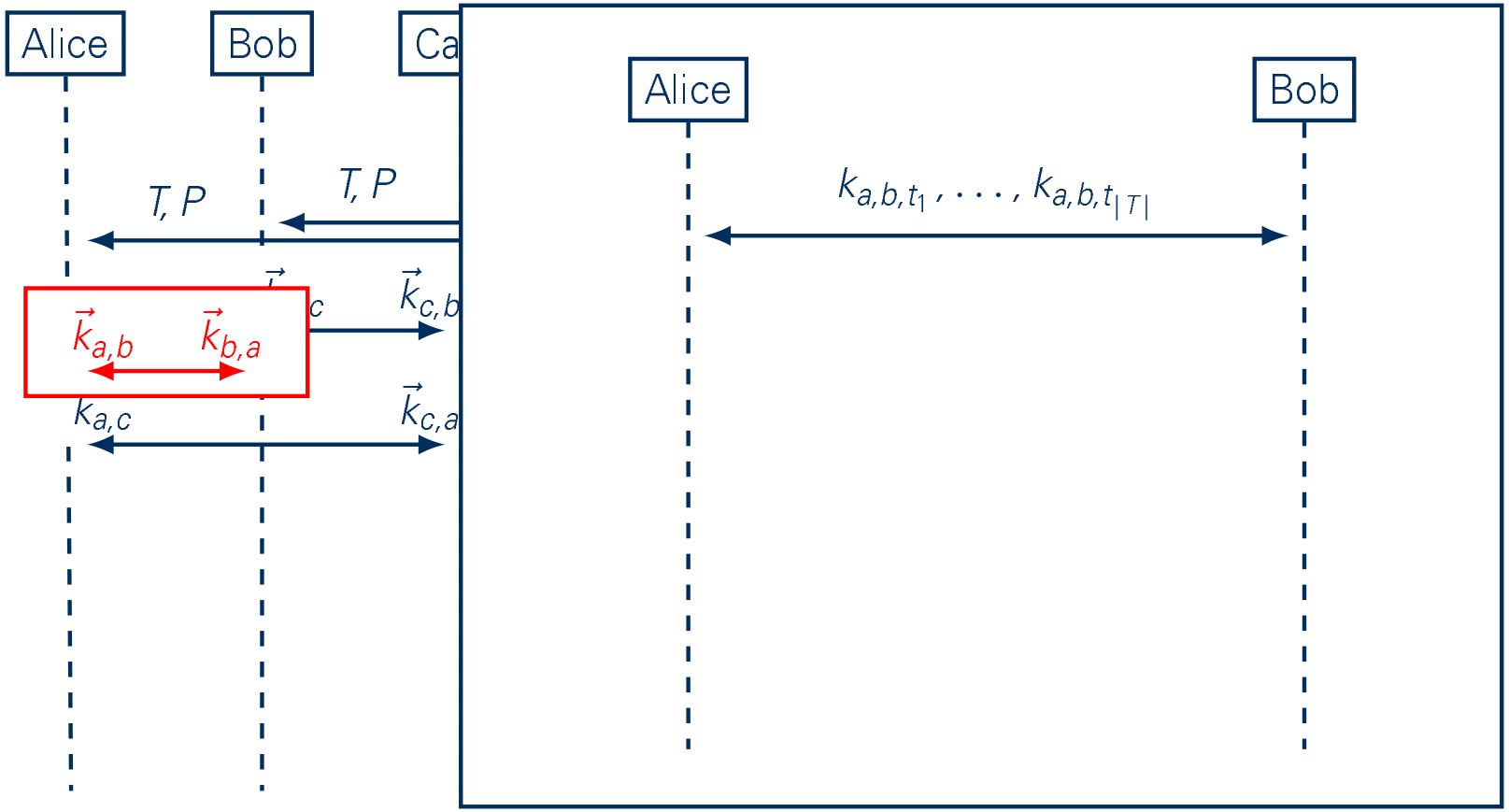
Poll Initialization



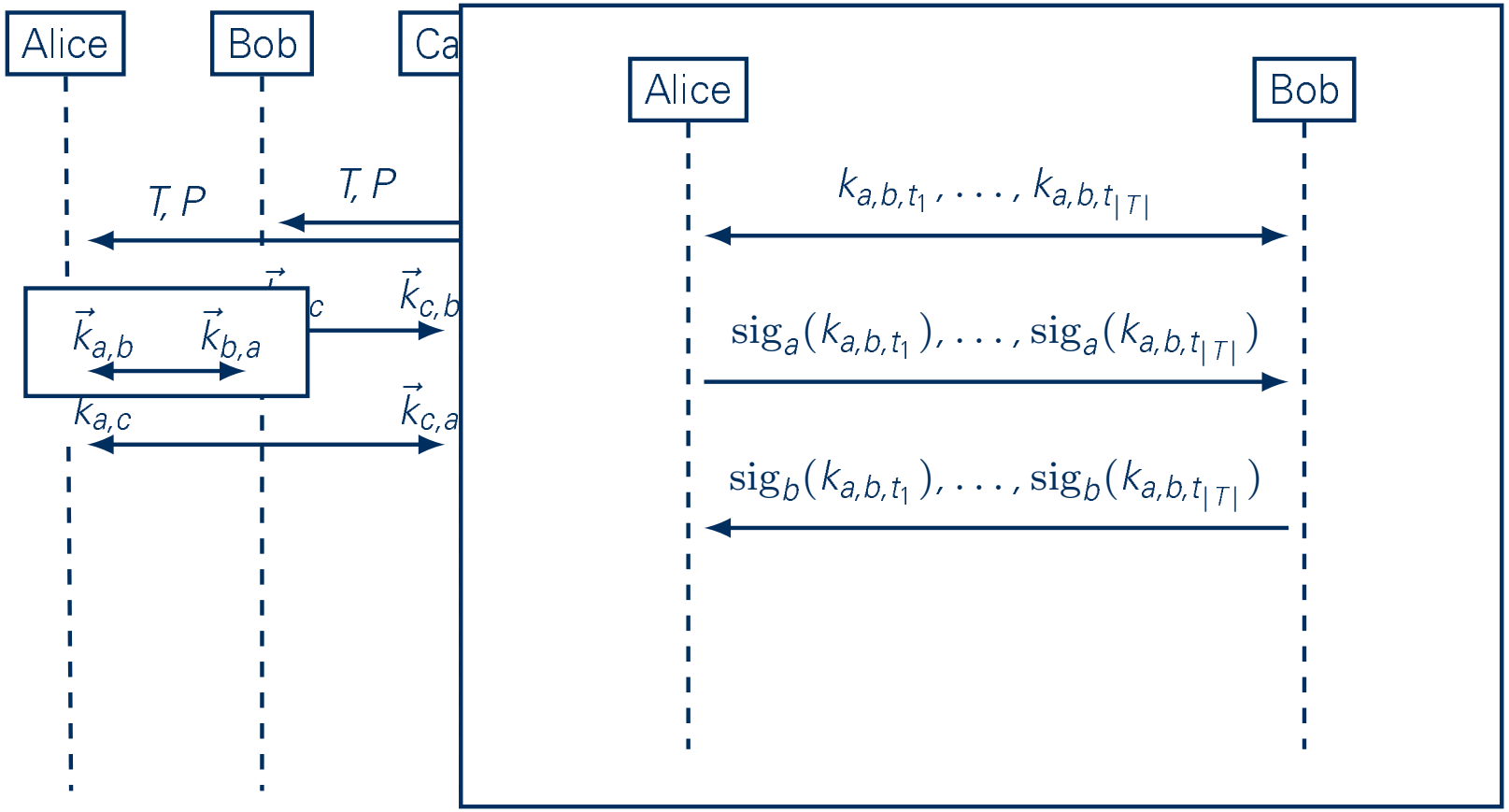
T . . . time slots
P . . . voters

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

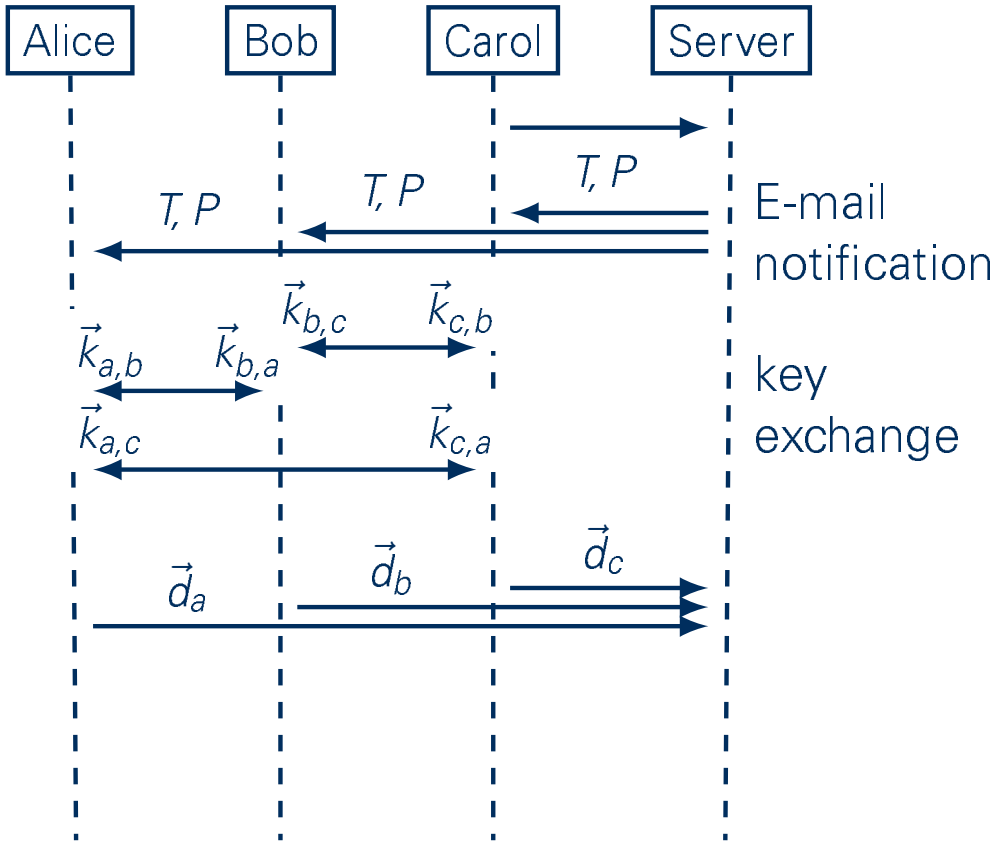
Poll Initialization



Poll Initialization



Casting of Votes

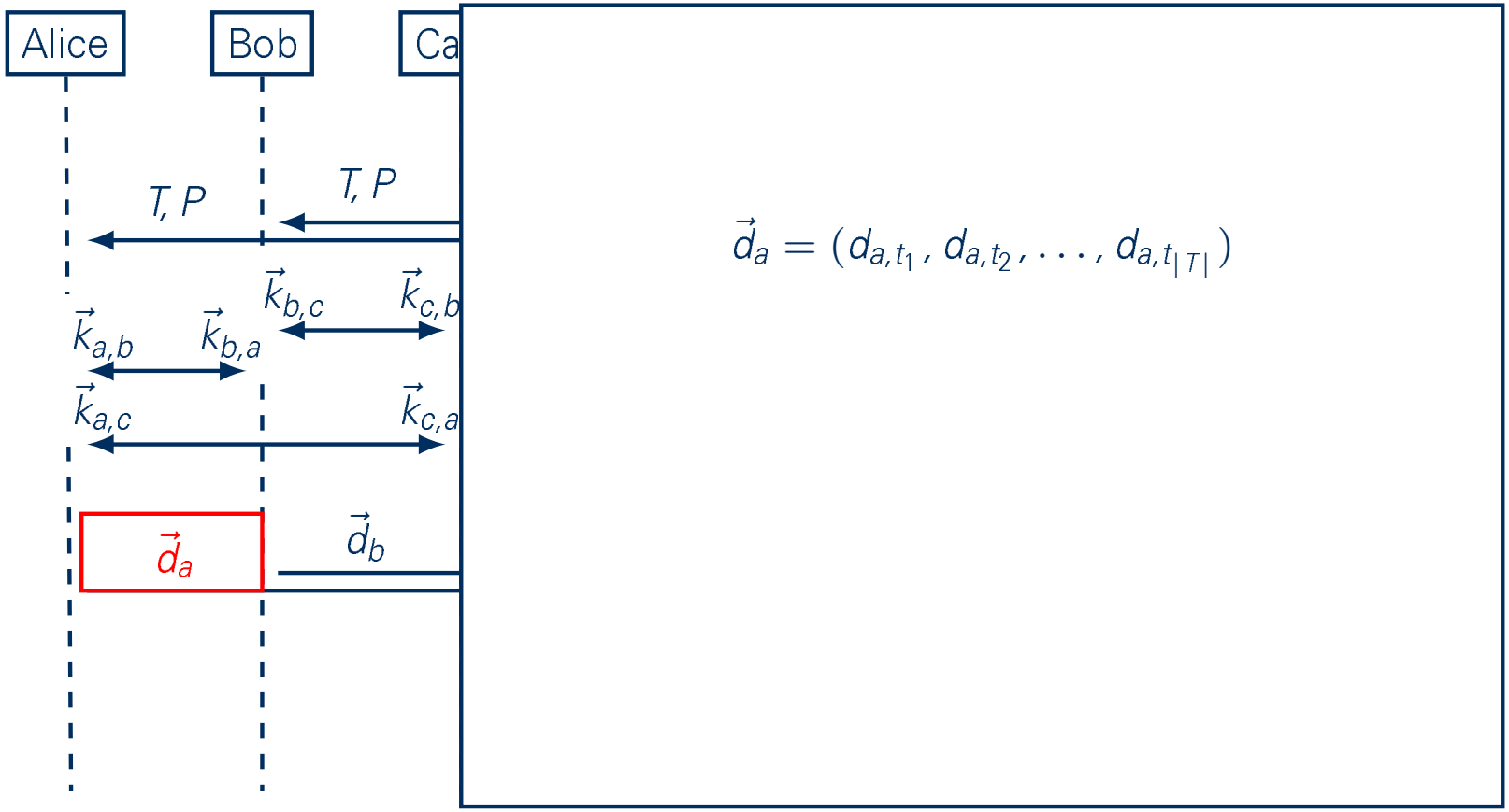


T . . . time slots
P . . . voters

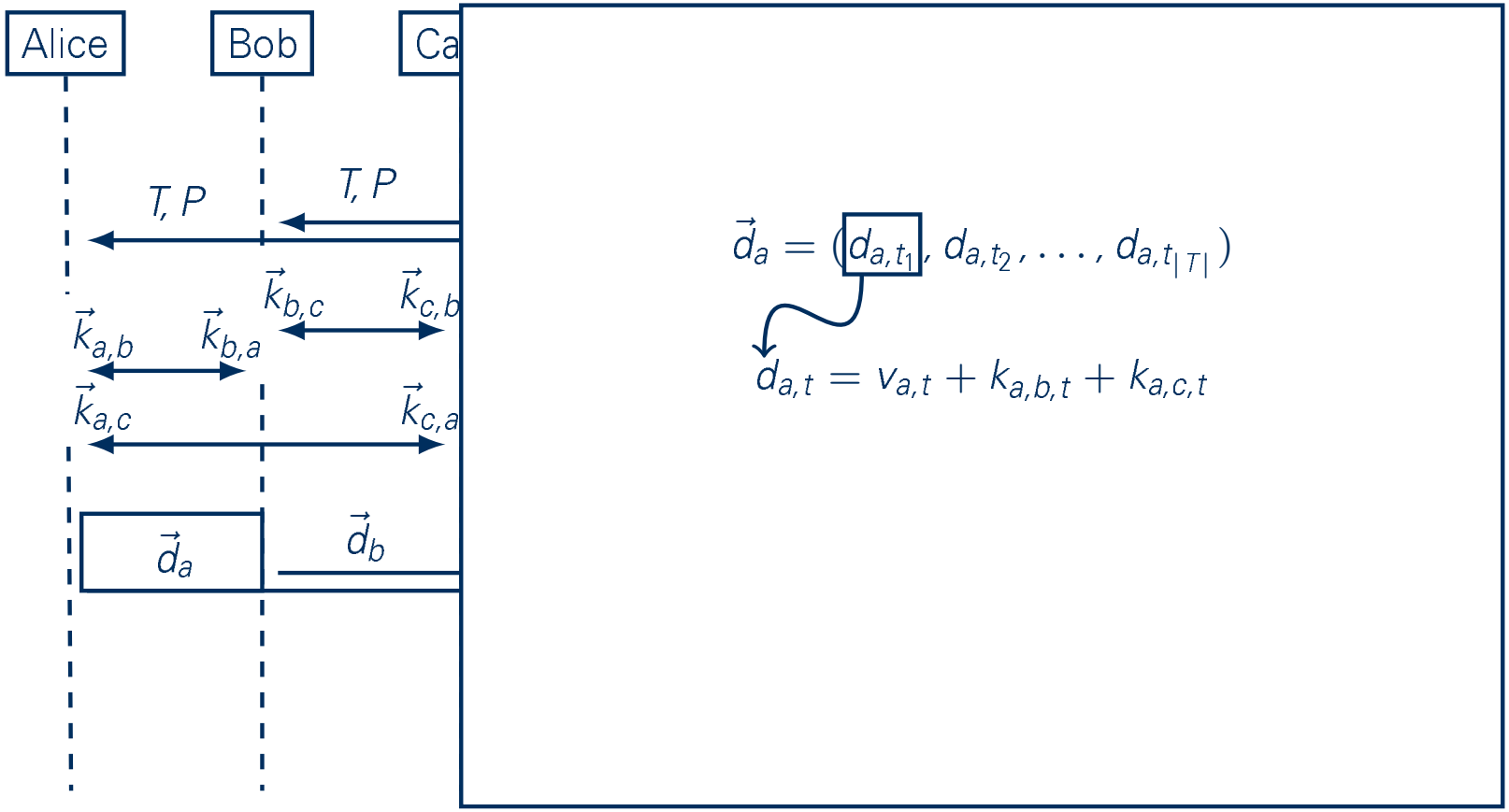
$\vec{k}_{i,j}$ . . . key vector

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

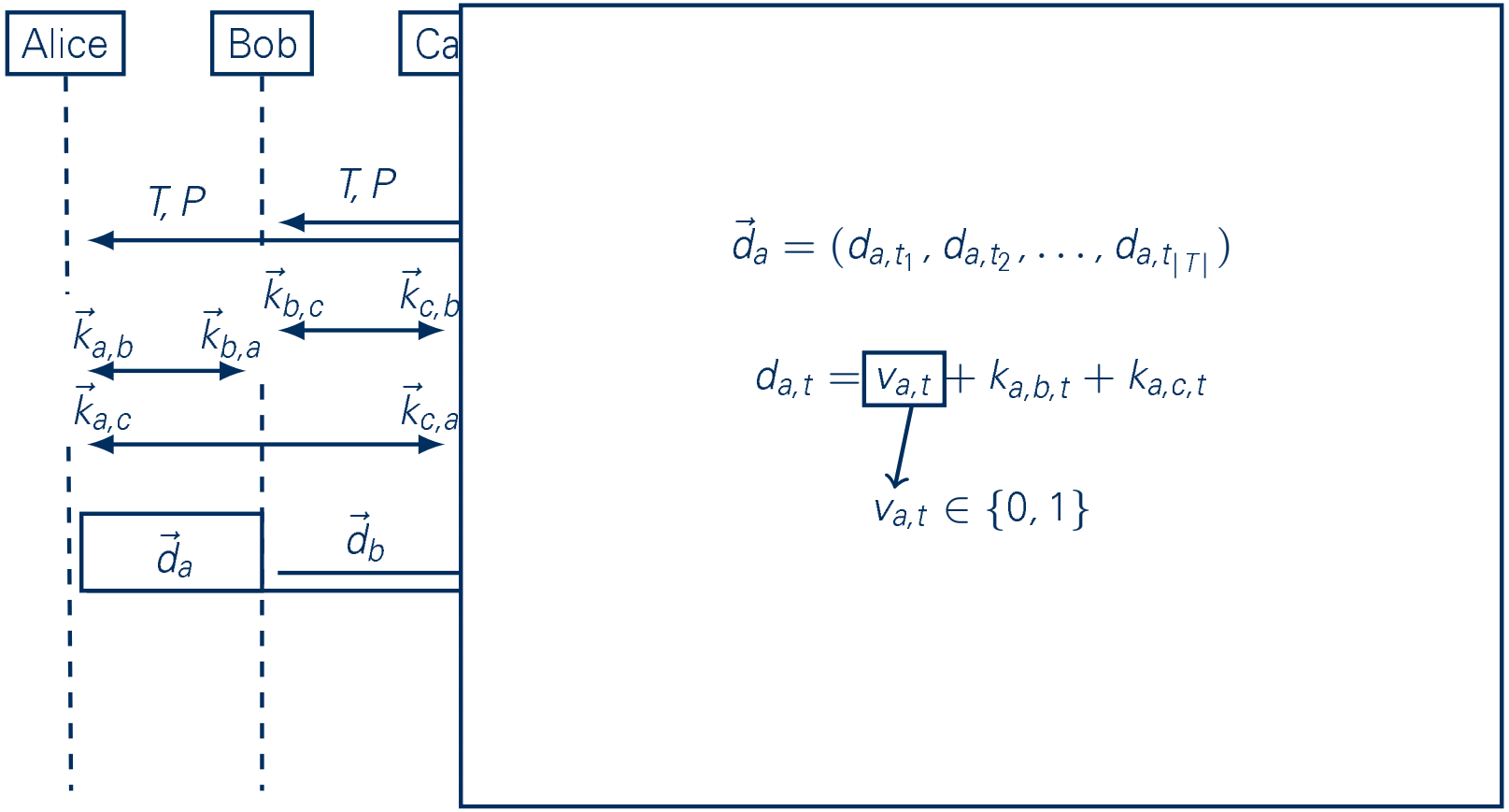
Casting of Votes



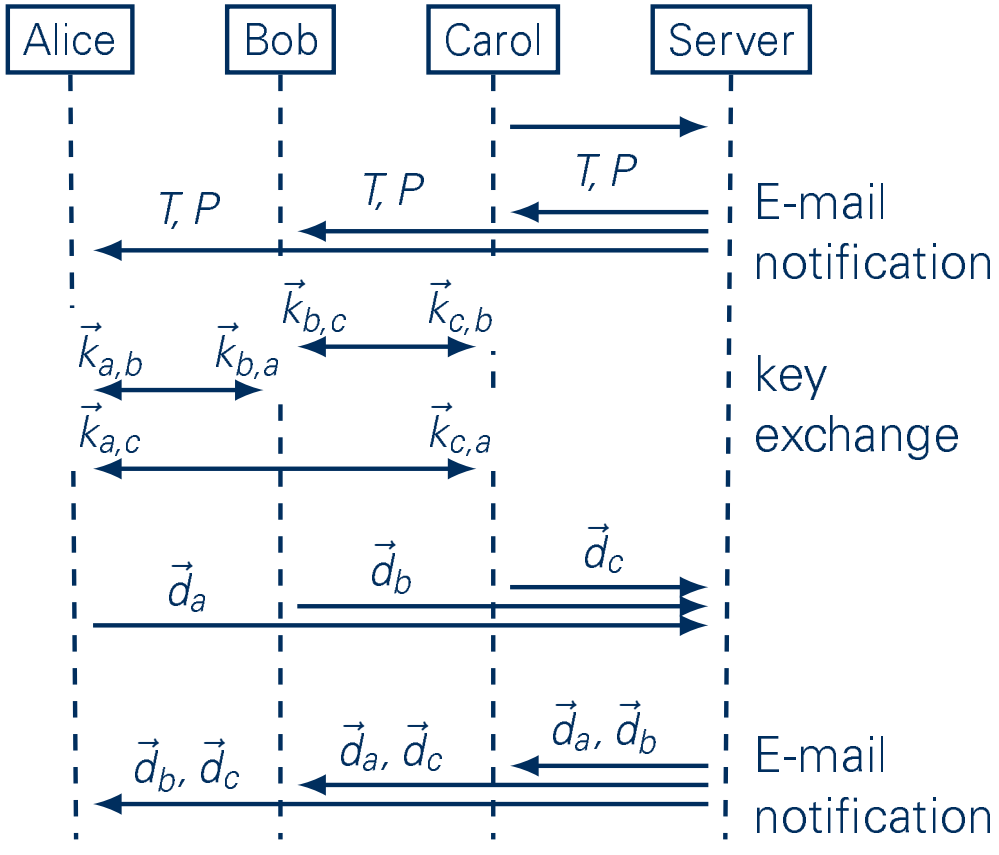
Casting of Votes



Casting of Votes



Result Publication

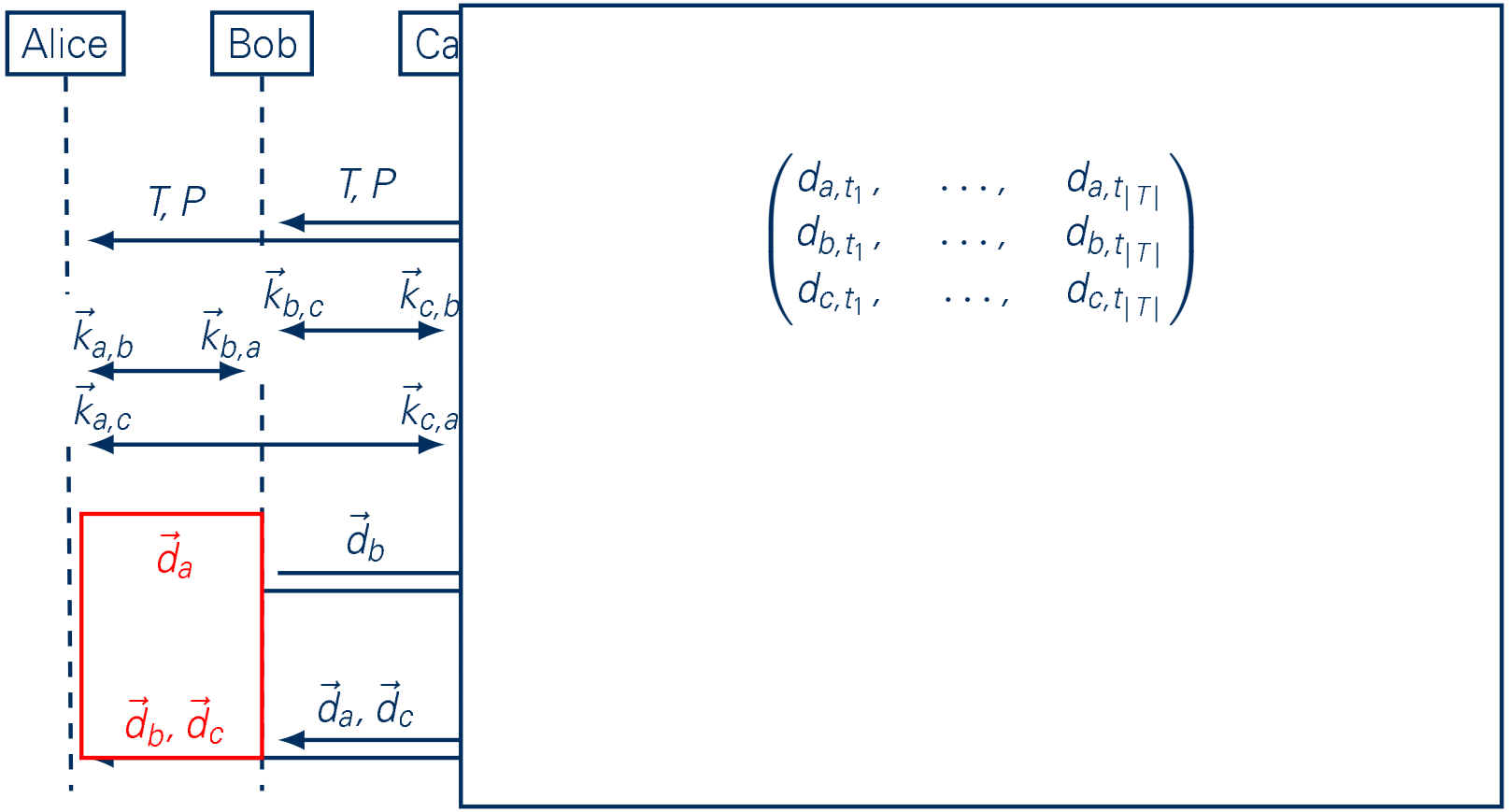


T . . . time slots
P . . . voters

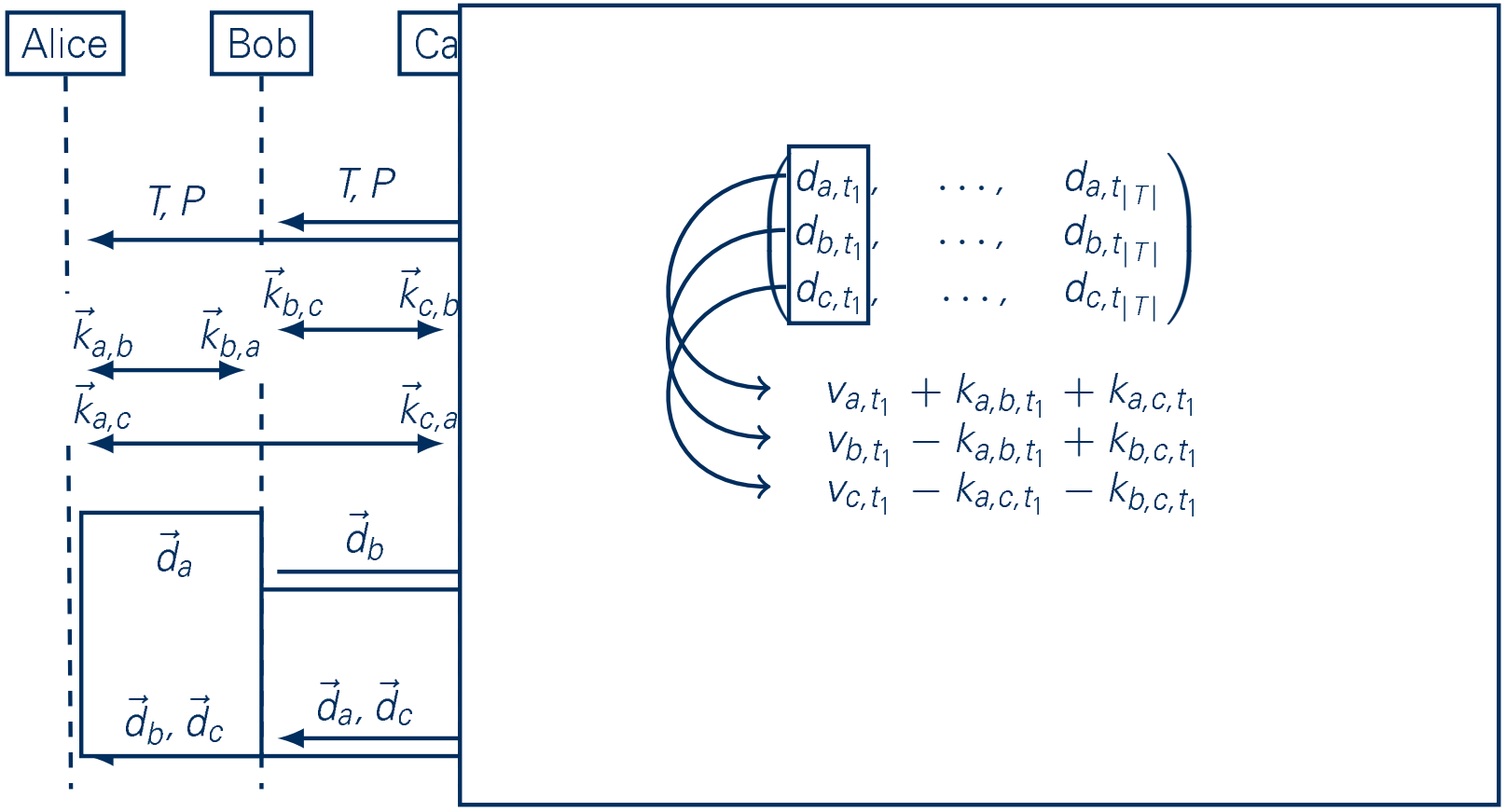
$\vec{k}_{i,j}$ . . . key vector

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

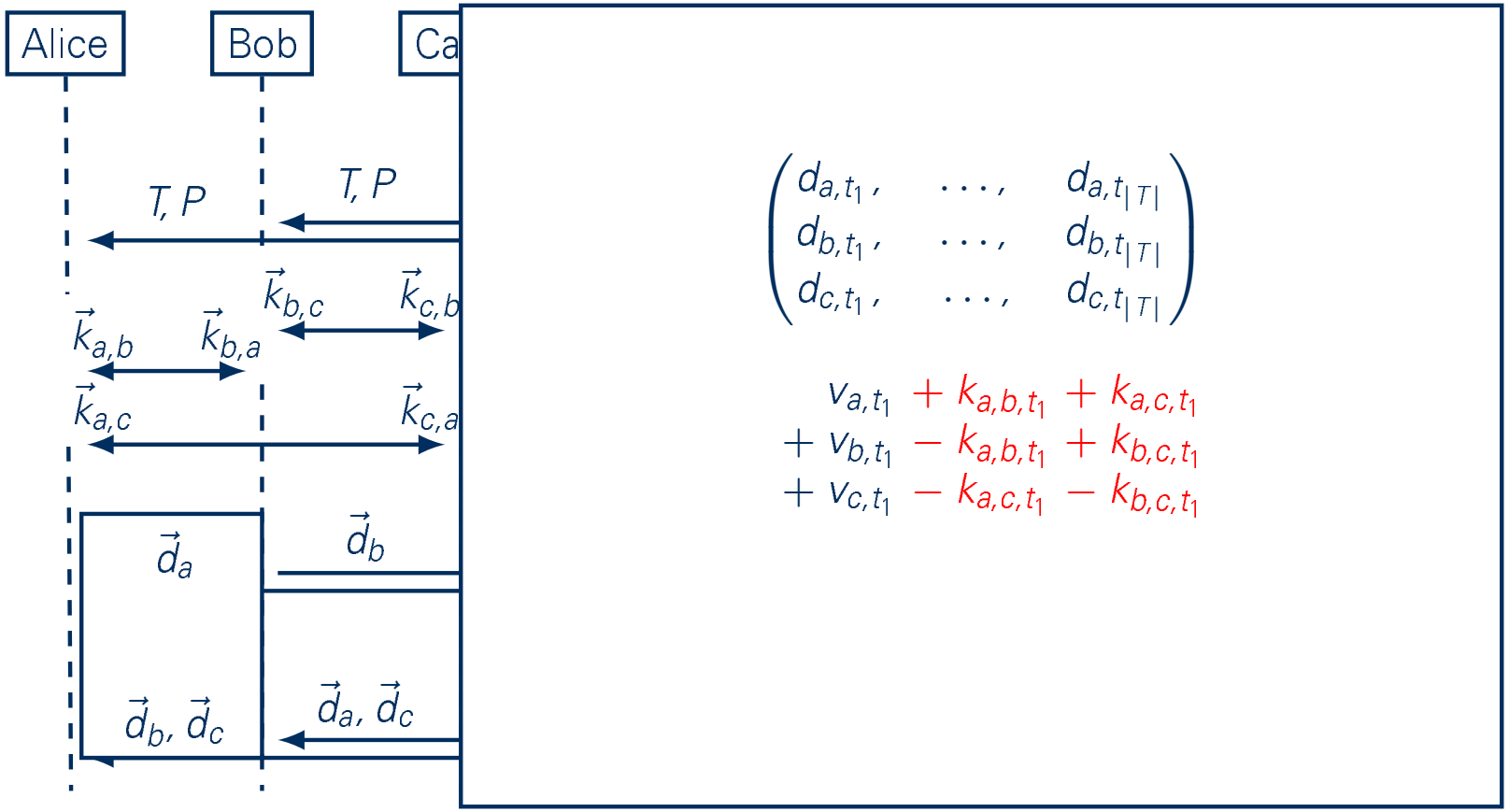
Result Publication



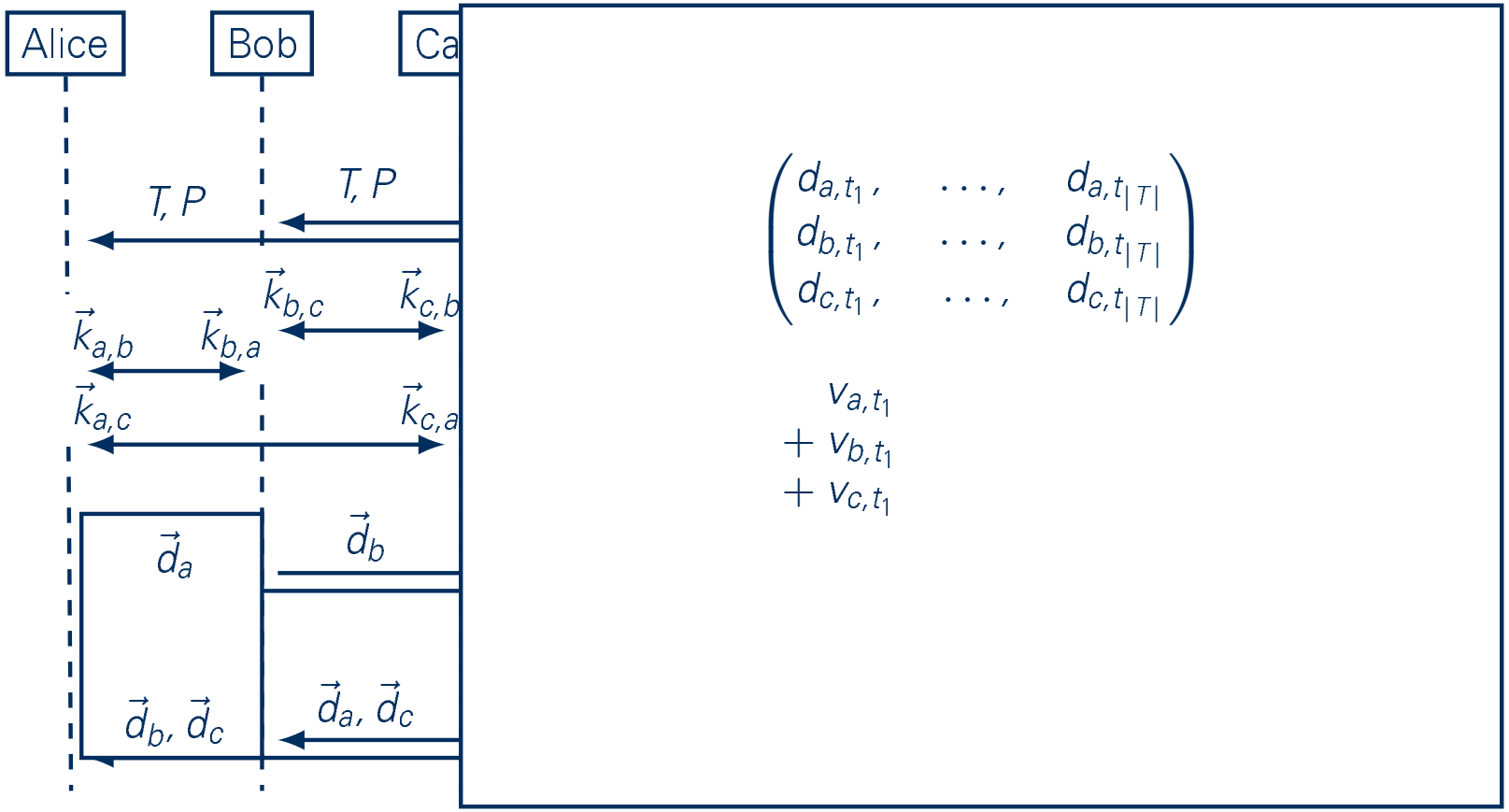
Result Publication



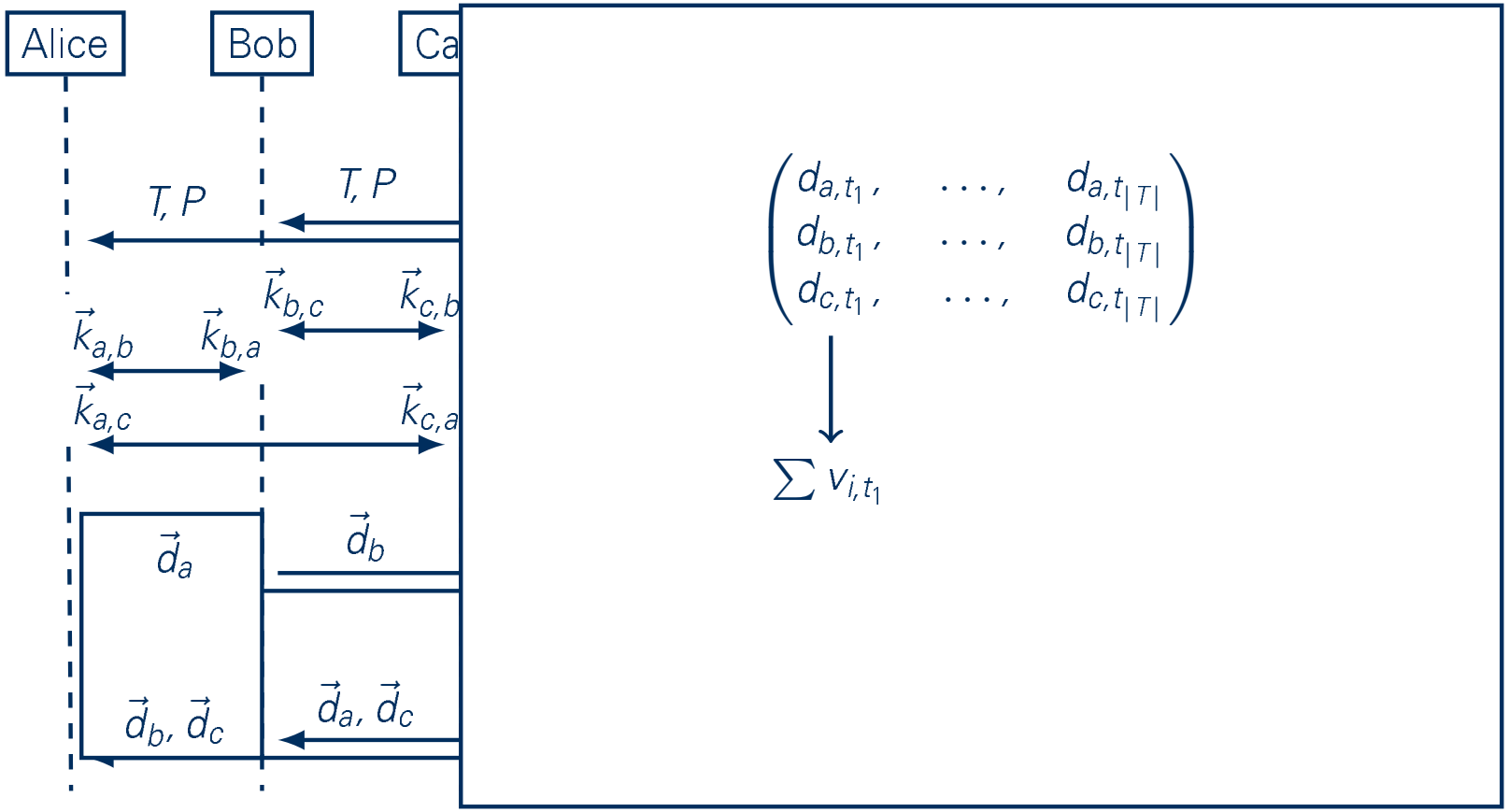
Result Publication



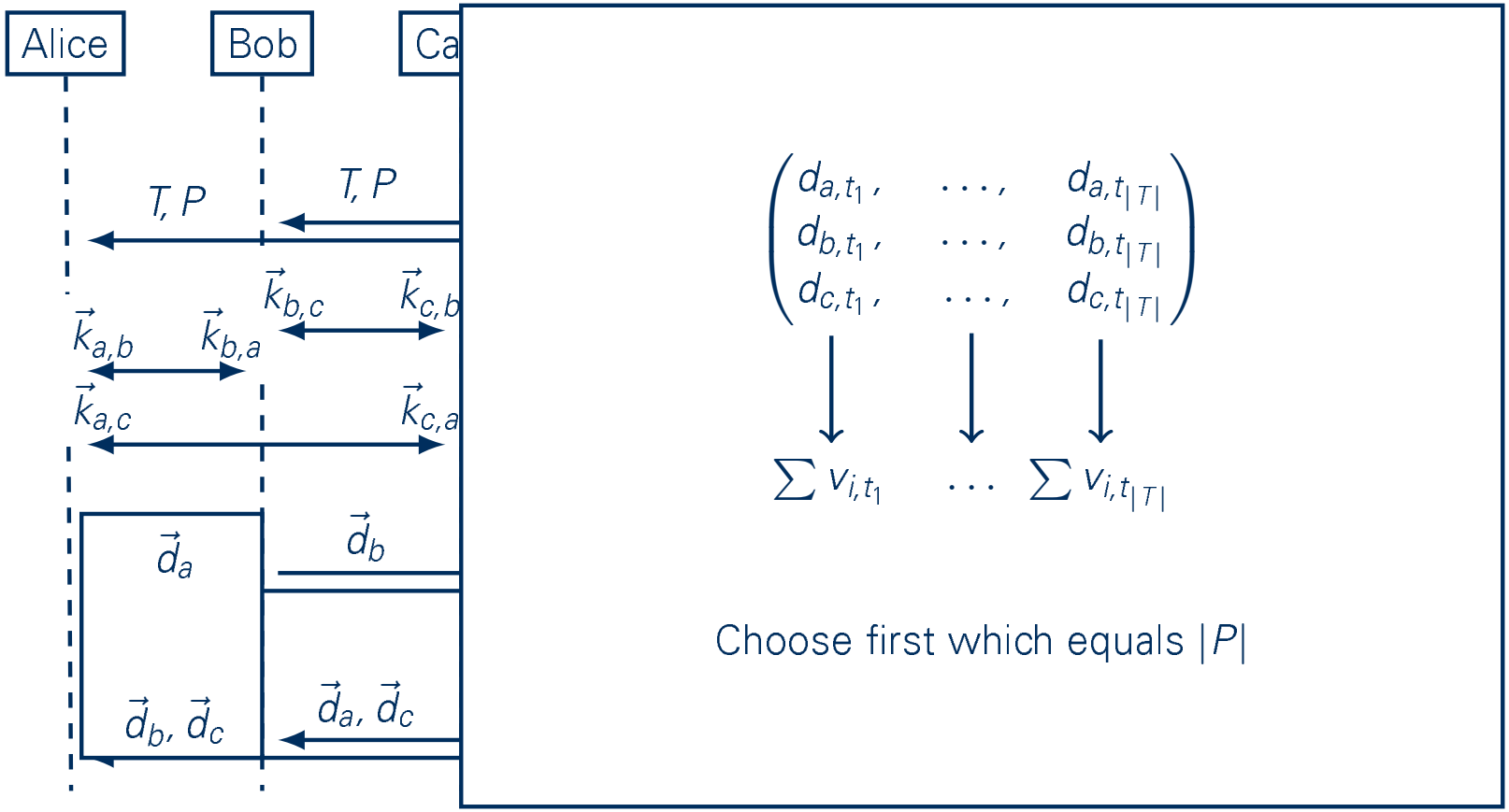
Result Publication



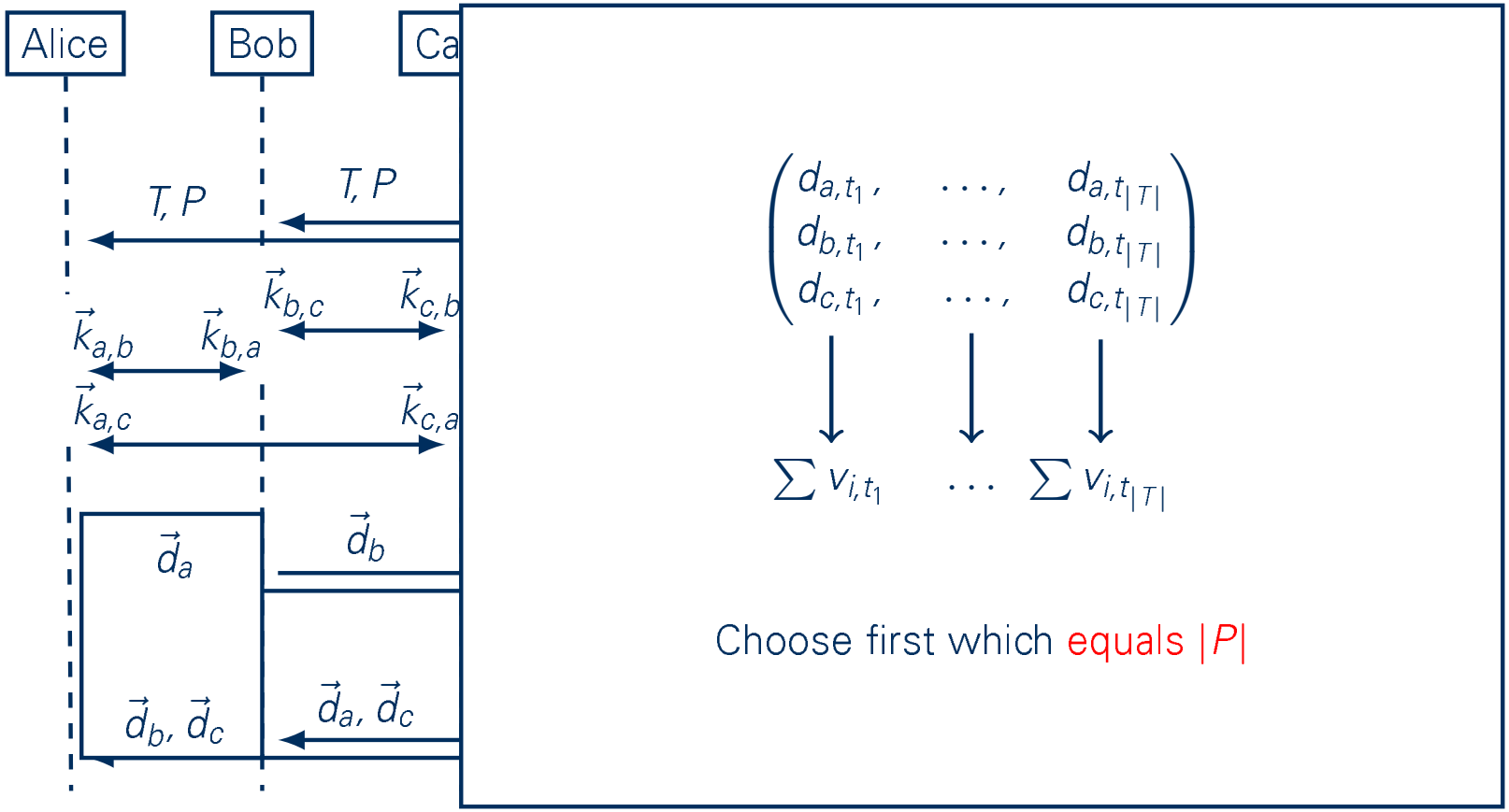
Result Publication



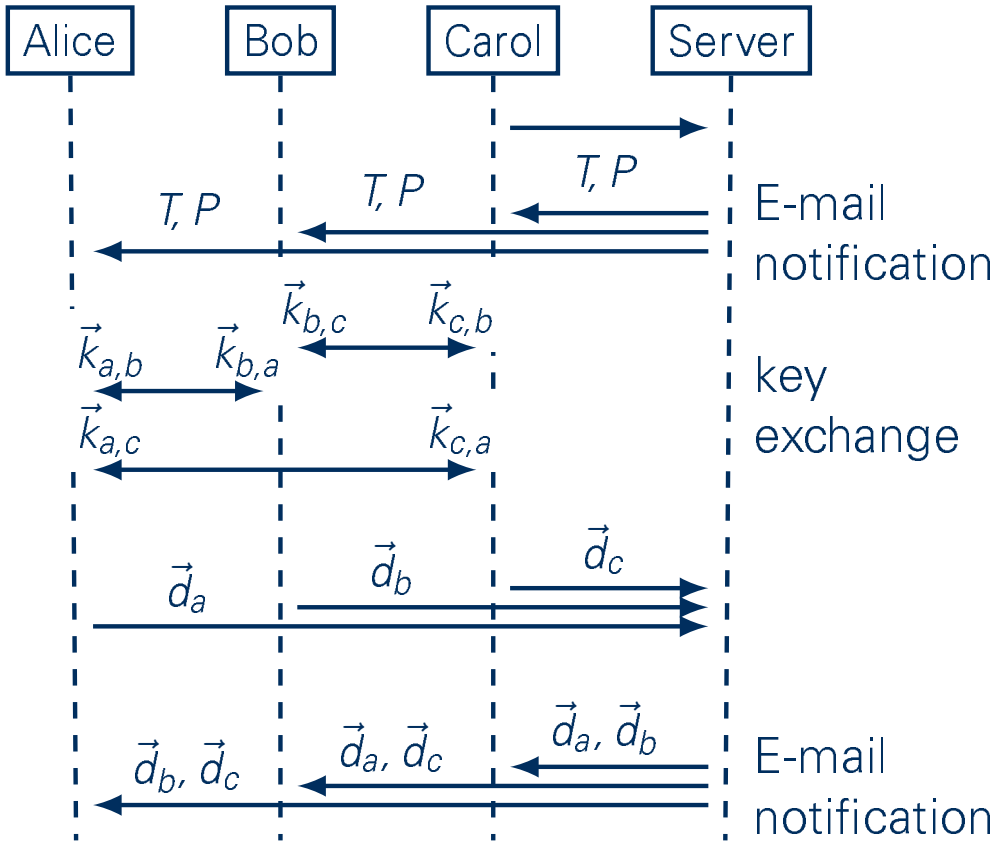
Result Publication



Result Publication



Trying to Cheat

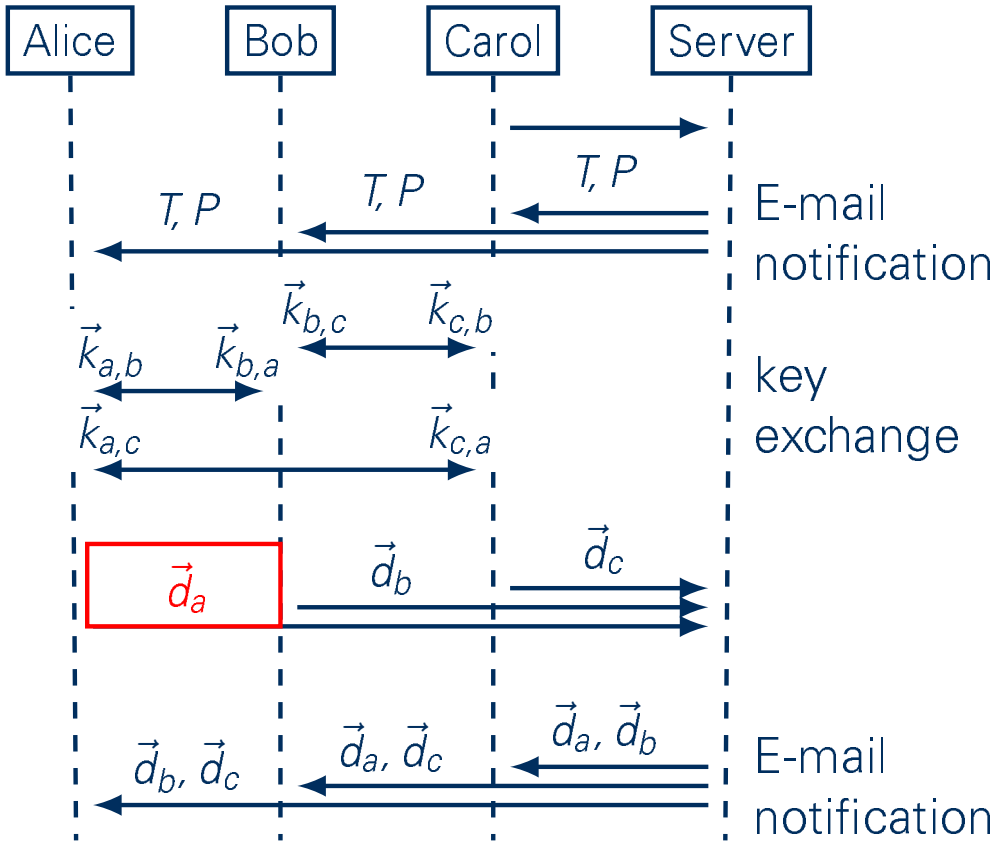


T . . . time slots
P . . . voters

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

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

Trying to Cheat

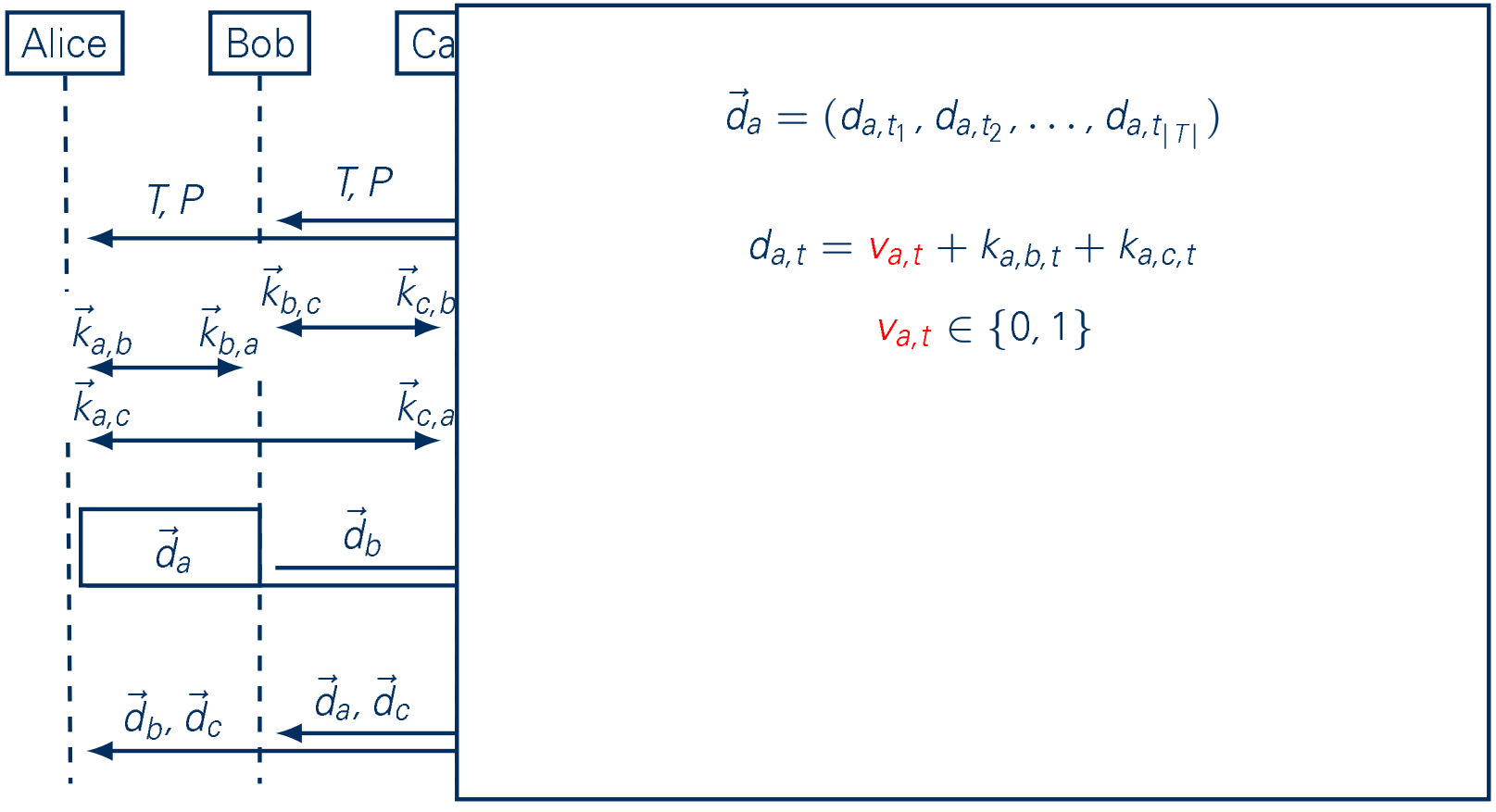


T . . . time slots
P . . . voters

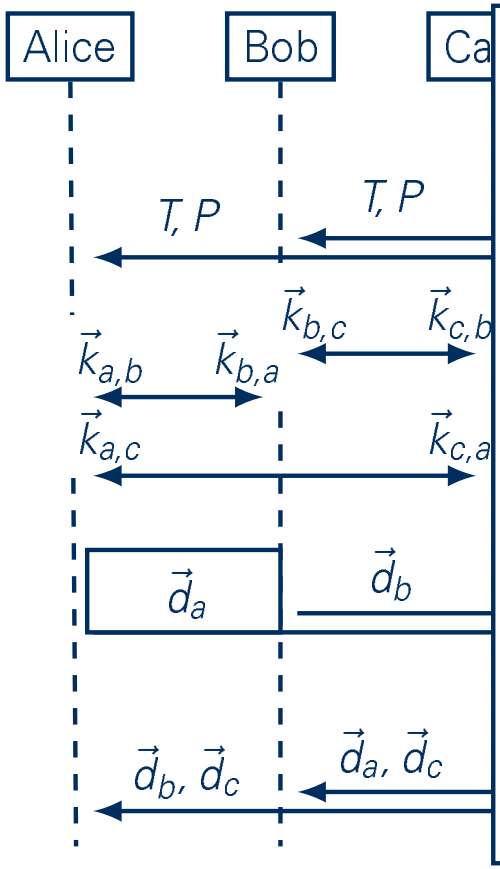
$\vec{k}_{i,j}$ . . . key vector

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

Trying to Cheat



Trying to Cheat



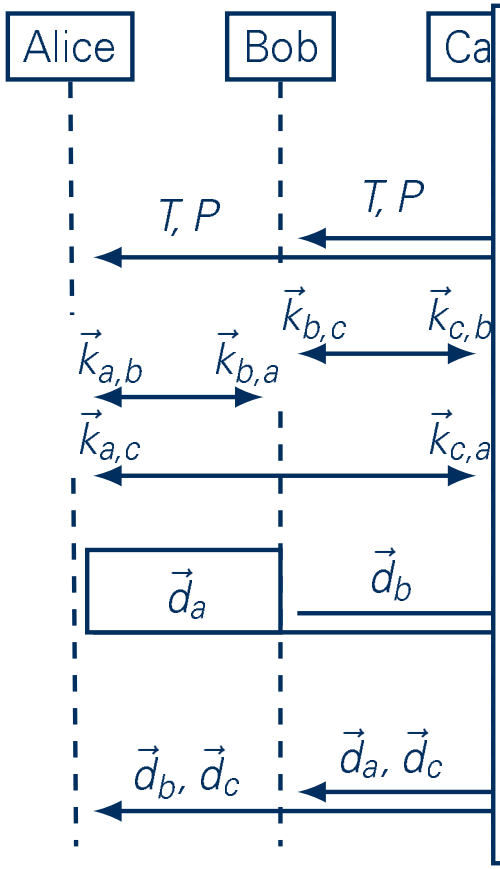
$$\vec{d}_a = (d_{a,t_1}, d_{a,t_2}, \ldots, d_{a,t_{|T|}})$$

$$d_{a,t} = v_{a,t} + k_{a,b,t} + k_{a,c,t}$$

$$v_{a,t} \in \{0, 1\}$$

Alice	0	1	1	1	1	0
Bob	1	0	1	1	0	0
Carol	1	1	1	1	0	1
$\sum$	2	2	3	3	1	1

Trying to Cheat



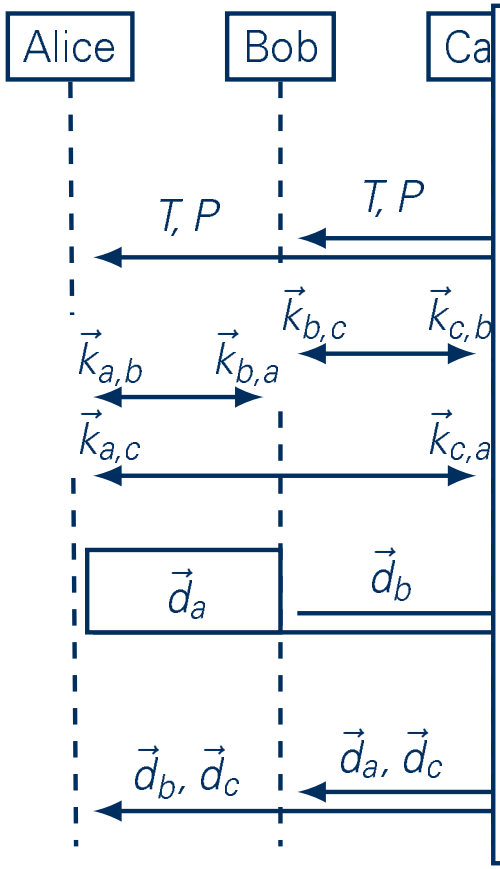
$$\vec{d}_a = (d_{a,t_1}, d_{a,t_2}, \ldots, d_{a,t_{|T|}})$$

$$d_{a,t} = v_{a,t} + k_{a,b,t} + k_{a,c,t}$$

$$v_{a,t} \in \{0, 1\}$$

Alice	0	1	1	1	1	0
Bob	1	0	1	1	0	0
Carol	1	1	1	1	0	1
$\sum$	2	2	3	3	1	1

Trying to Cheat



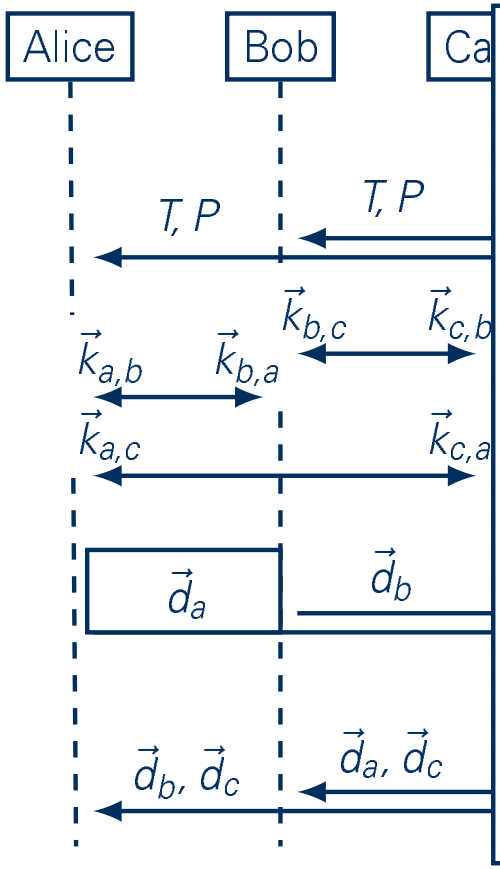
$$\vec{d}_a = (d_{a,t_1}, d_{a,t_2}, \ldots, d_{a,t_{|T|}})$$

$$d_{a,t} = v_{a,t} + k_{a,b,t} + k_{a,c,t}$$

$$v_{a,t} = -1?$$

Alice	−1	1	−1	−1	0	0
Bob	1	0	1	1	0	0
Carol	1	1	1	1	0	1
$\sum$	1	2	1	1	0	1

Trying to Cheat



$$\vec{d}_a = (d_{a,t_1}, d_{a,t_2}, \ldots, d_{a,t_{|T|}})$$

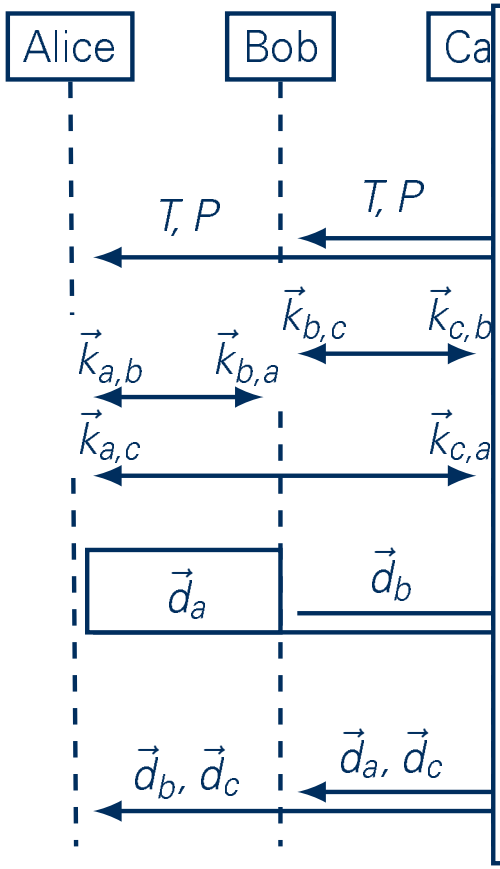
$$d_{a,t} = v_{a,t} + k_{a,b,t} + k_{a,c,t}$$

~~$v_{a,t} = -1$?~~

Alice	−1	1	−1	−1	0	0
Bob	1	0	1	1	0	0
Carol	1	1	1	1	0	1
$\sum$	1	2	1	1	0	1

Choose first which equals $|P|$

Trying to Cheat



$$\vec{d}_a = (d_{a,t_1}, d_{a,t_2}, \ldots, d_{a,t_{|T|}})$$

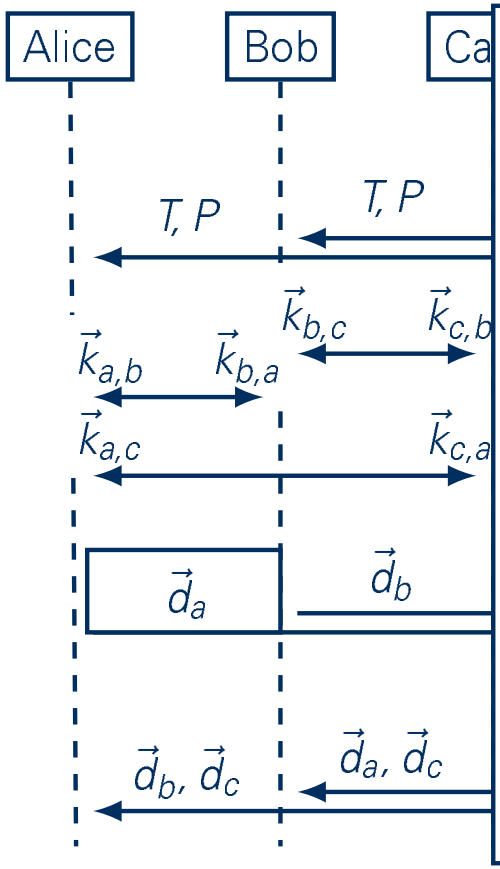
$$d_{a,t} = v_{a,t} + k_{a,b,t} + k_{a,c,t}$$

~~$v_{a,t} == 1$?~~

Alice	0	1	0	0	0	0
Bob	1	0	1	1	0	0
Carol	1	1	1	1	0	1
$\sum$	2	2	2	2	0	1

Choose first which equals $|P|$

Trying to Cheat



$$\vec{d}_a = (d_{a,t_1}, d_{a,t_2}, \ldots, d_{a,t_{|T|}})$$

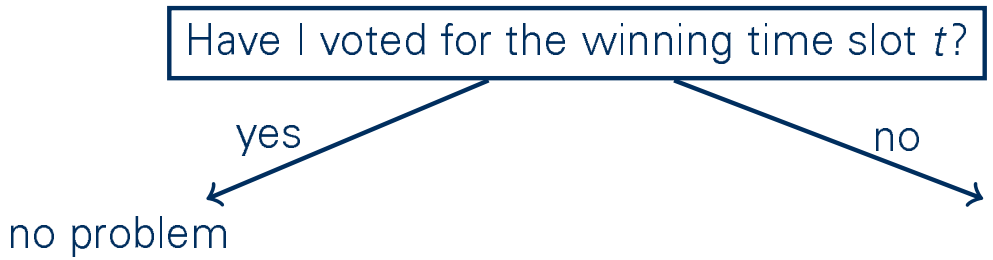
$$d_{a,t} = v_{a,t} + k_{a,b,t} + k_{a,c,t}$$

$$v_{a,t} = 2?$$

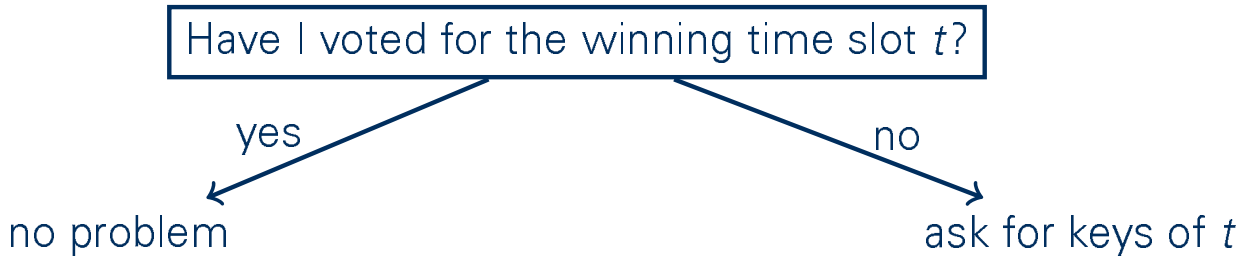
Alice	0	2	1	1	1	0
Bob	1	0	1	1	0	0
Carol	1	1	1	1	0	1
$\sum$	2	3	3	3	1	1

Result Verification

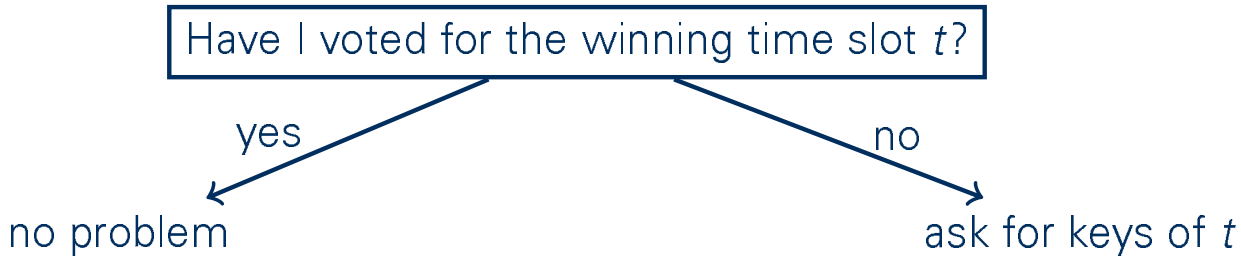
Result Verification



Result Verification



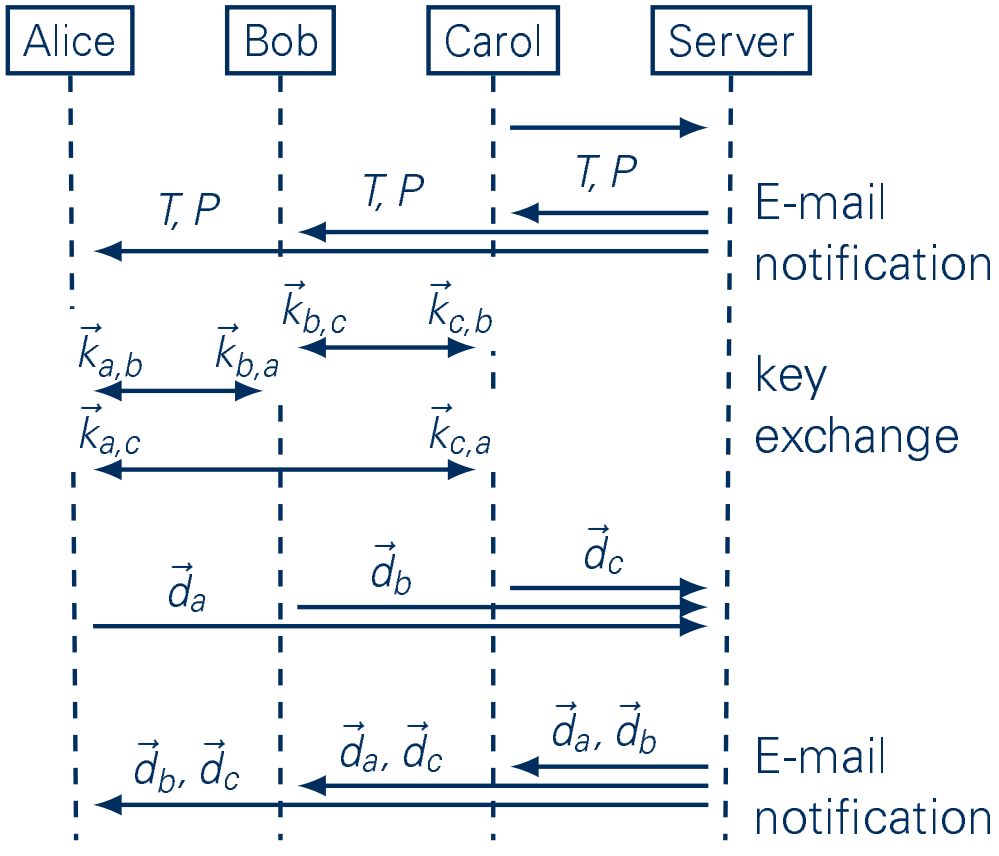
Result Verification



- decrypt everybody's votes ($v_{i,t}$)
- all honest participants voted 1
- key signatures prevent cheating with disclosed keys

Extensions

Simplifying the Key Exchange

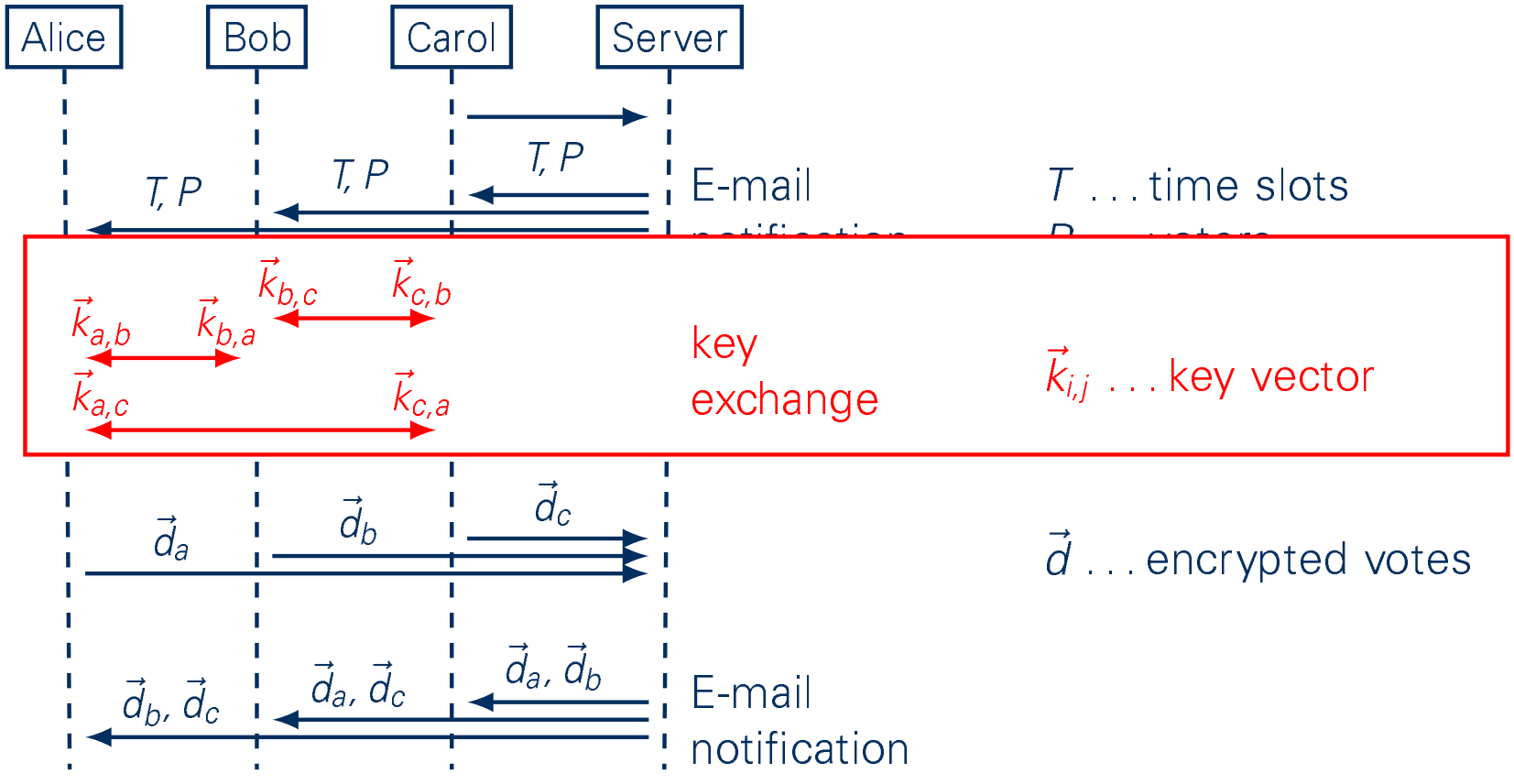


T . . . time slots
P . . . voters

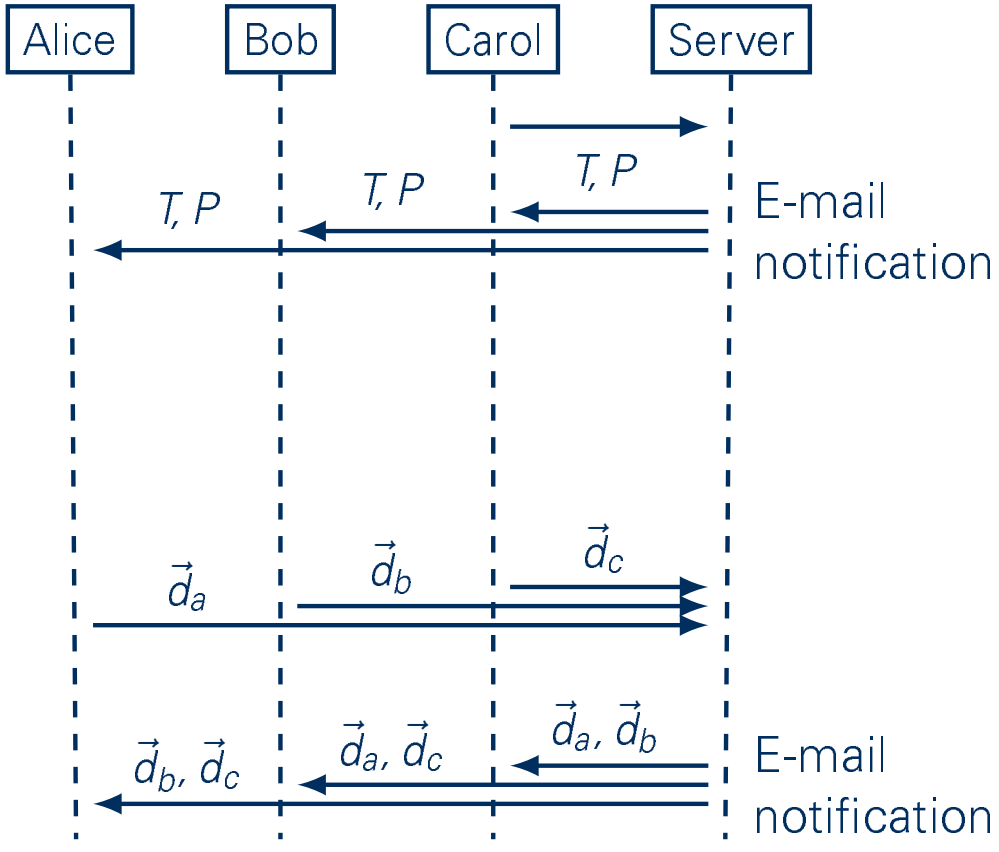
$\vec{k}_{i,j}$ . . . key vector

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

Simplifying the Key Exchange



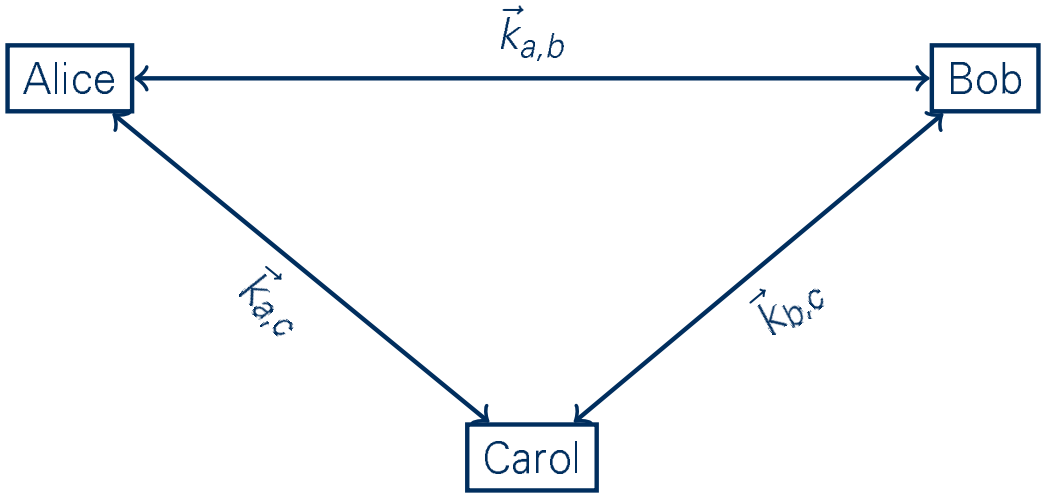
Simplifying the Key Exchange



T . . . time slots
P . . . voters

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

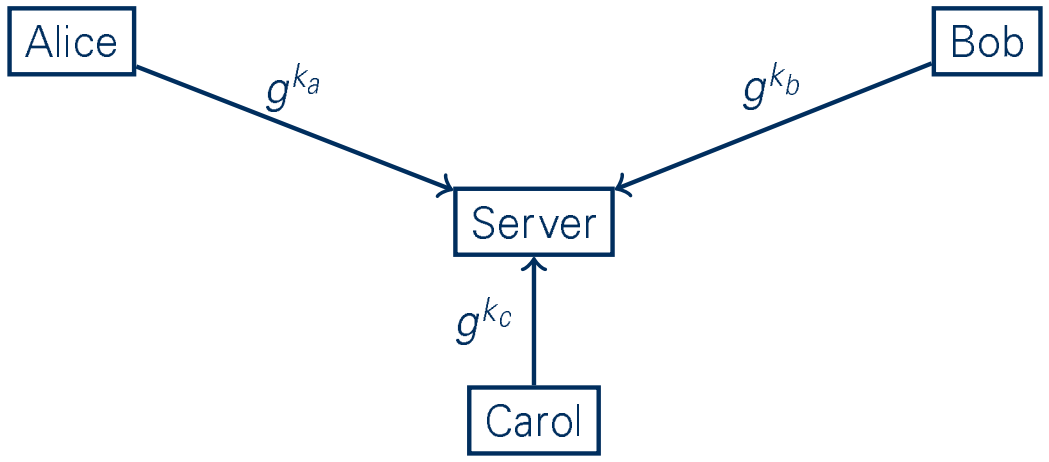
Simplifying the Key Exchange



key exchange

Simplifying the Key Exchange

Diffie–Hellman

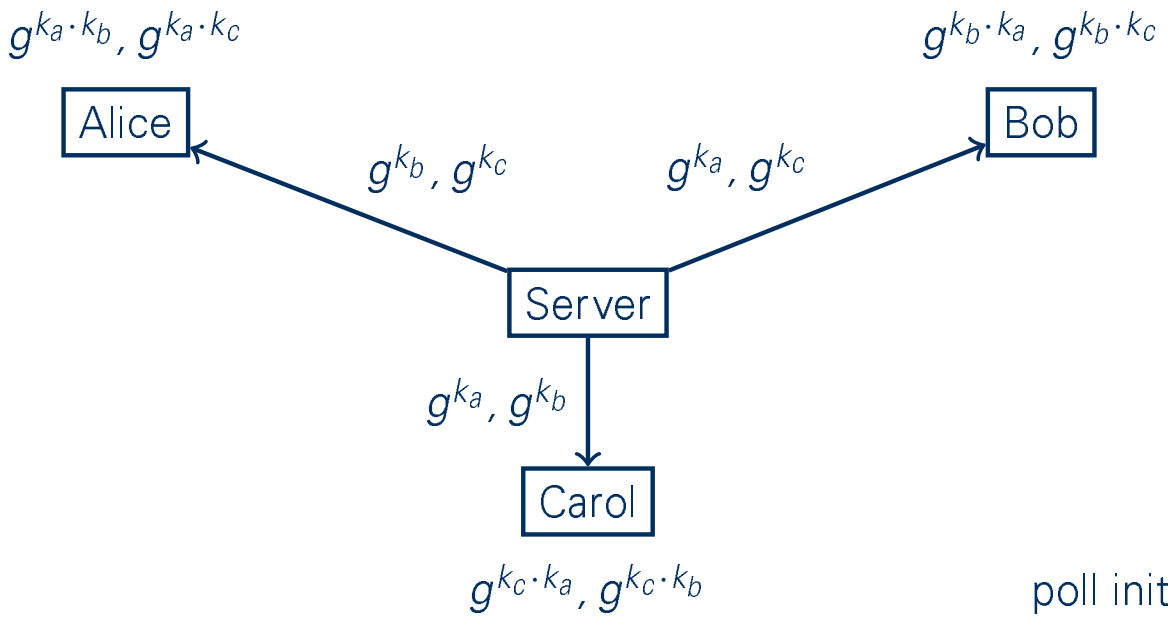


registration

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

Diffie–Hellman

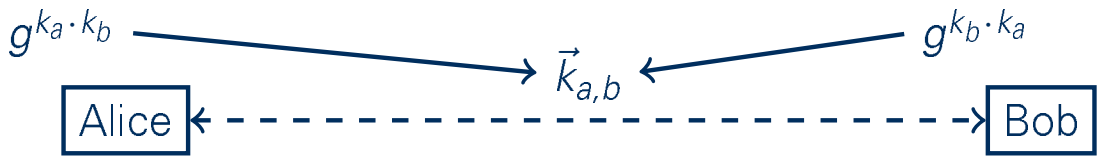


poll initialization

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

Diffie–Hellman



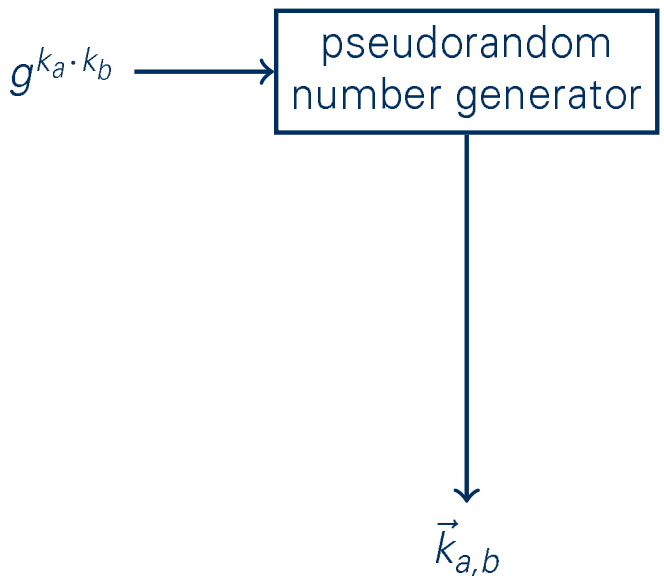
Carol

poll initialization

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

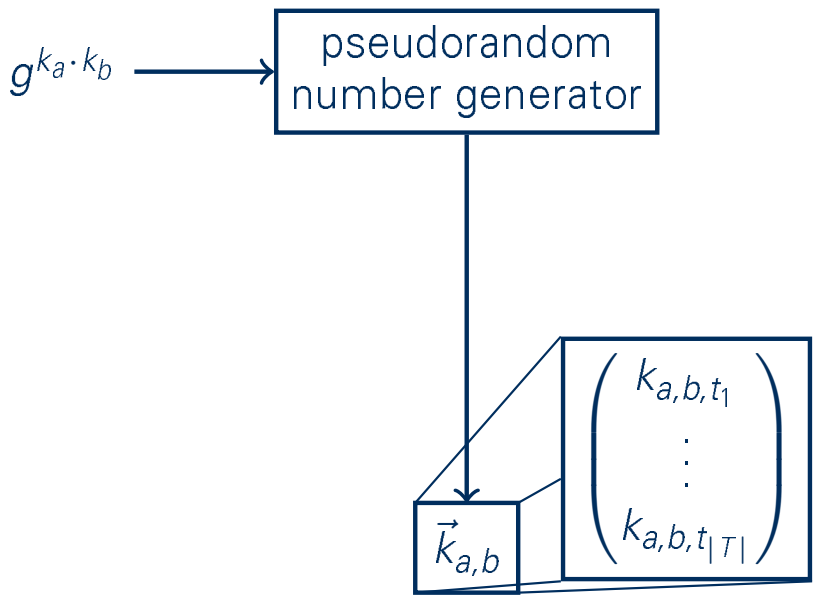
Simplifying the Key Exchange

$$\mathcal{G}(g^{k_a \cdot k_b}) = \vec{k}_{a,b}$$



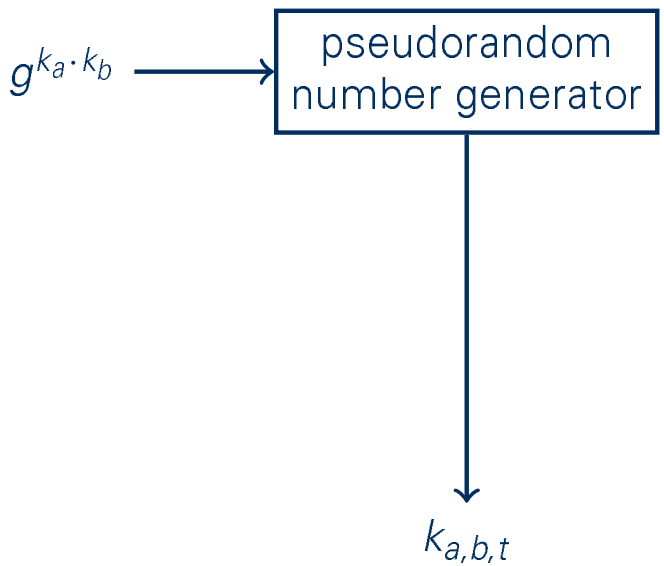
Simplifying the Key Exchange

$$\mathcal{G}(g^{k_a \cdot k_b}) = \vec{k}_{a,b}$$



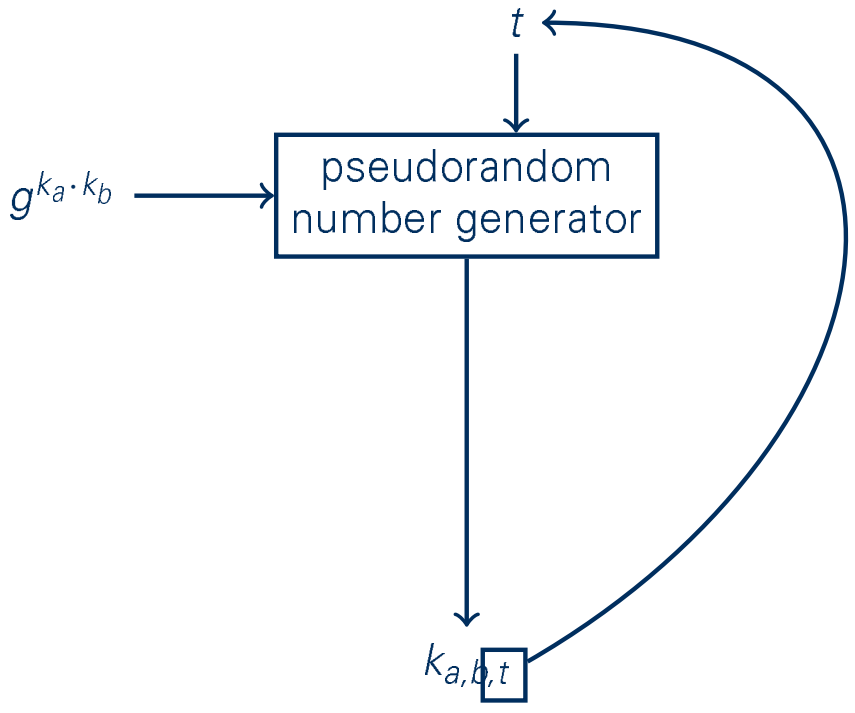
Simplifying the Key Exchange

$$\mathcal{G}(g^{k_a \cdot k_b}) = k_{a,b,t}$$



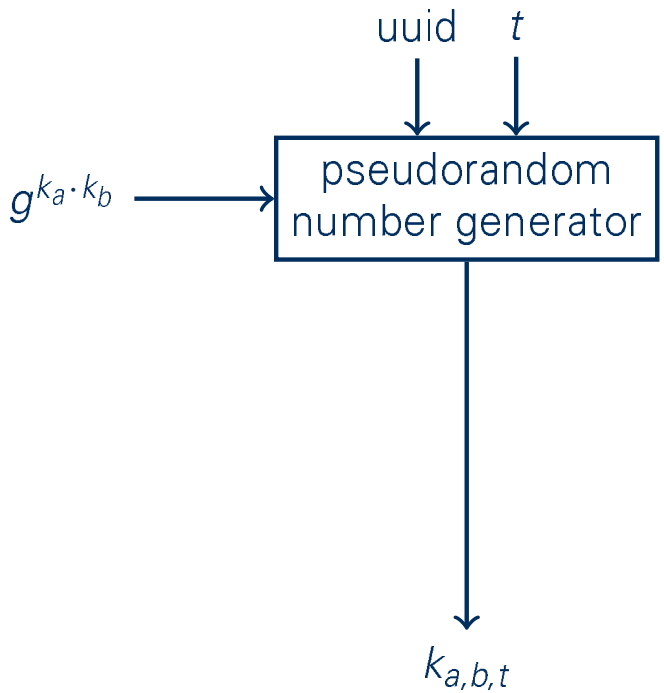
Simplifying the Key Exchange

$$\mathcal{G}(g^{k_a \cdot k_b}, t) = k_{a,b,t}$$



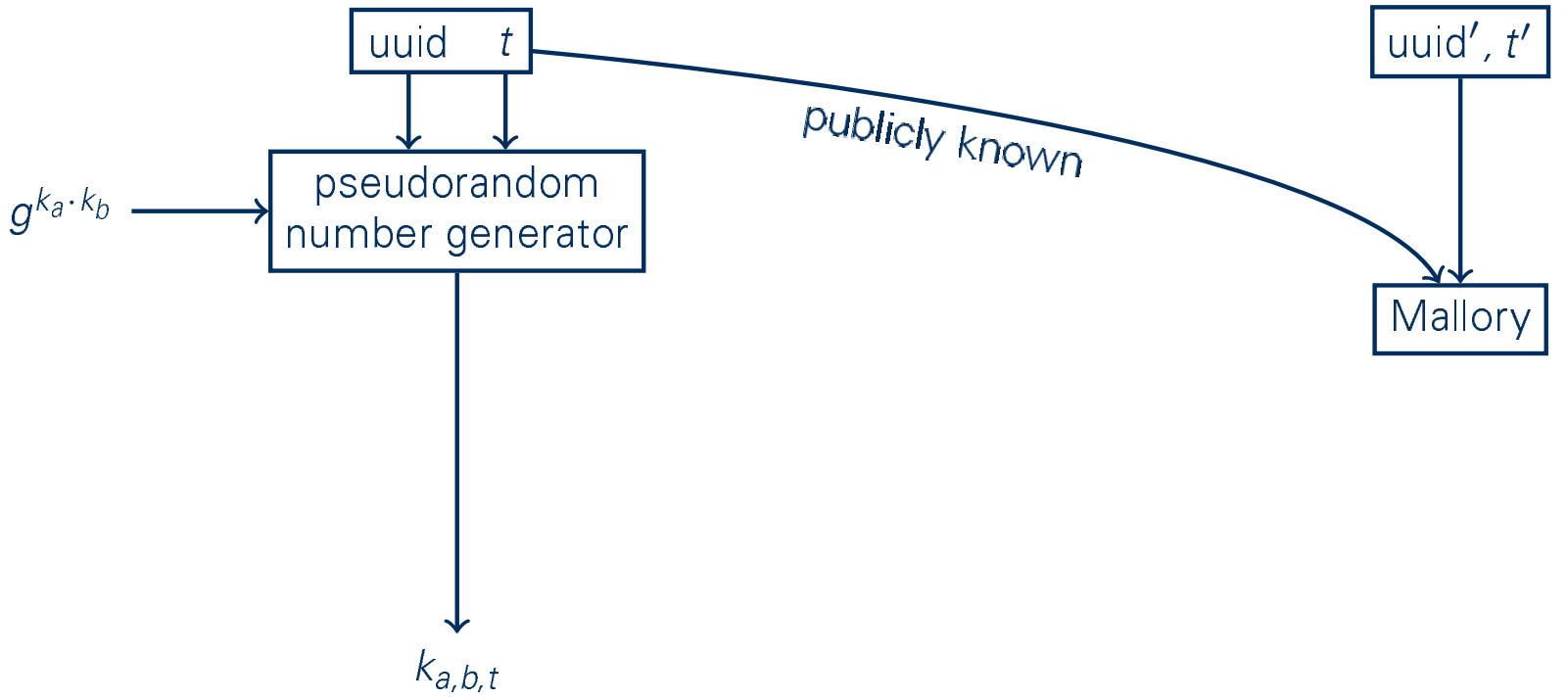
Simplifying the Key Exchange

$$\mathcal{G}(g^{k_a \cdot k_b}, \text{uuid}, t) = k_{a,b,t}$$



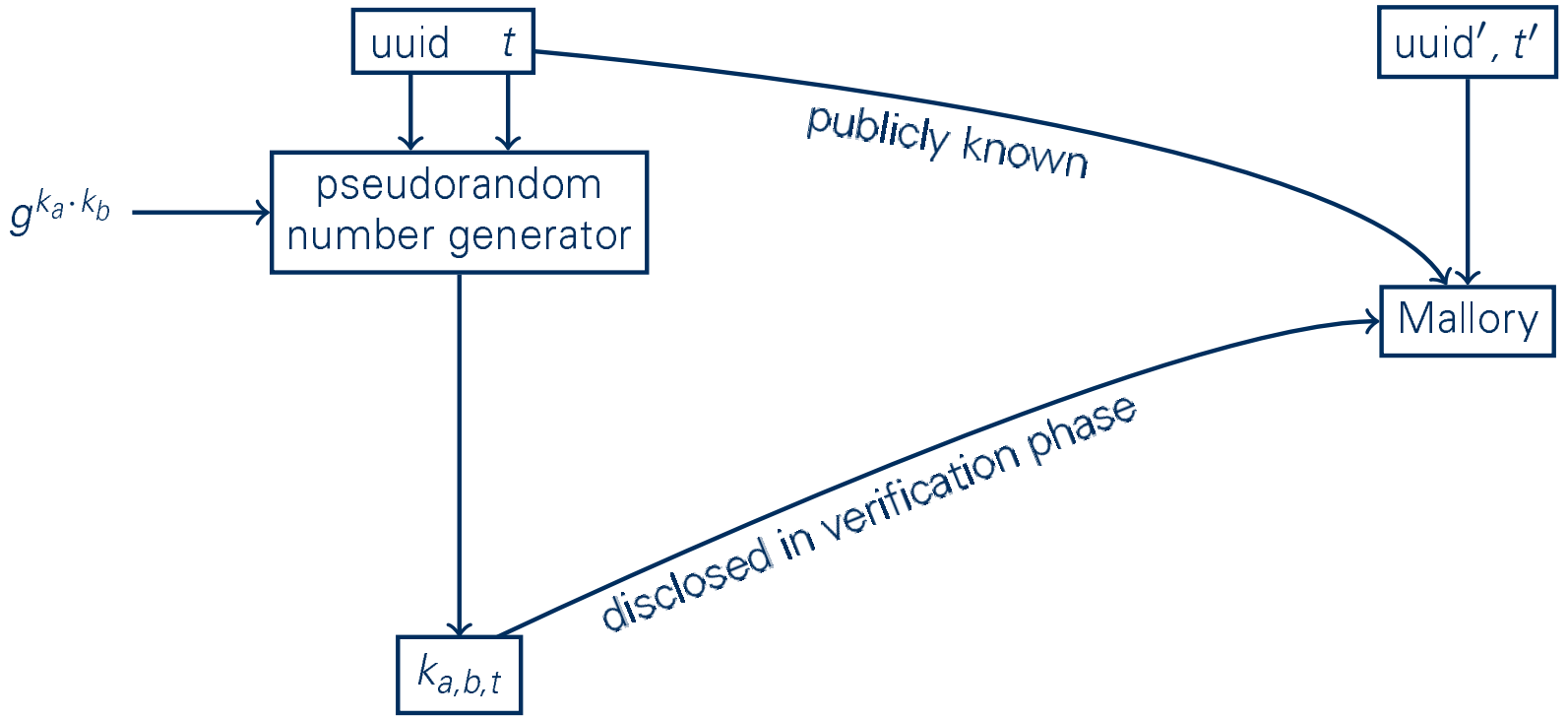
Simplifying the Key Exchange

$$\mathcal{G}(g^{k_a \cdot k_b}, \text{uuid}, t) = k_{a,b,t}$$



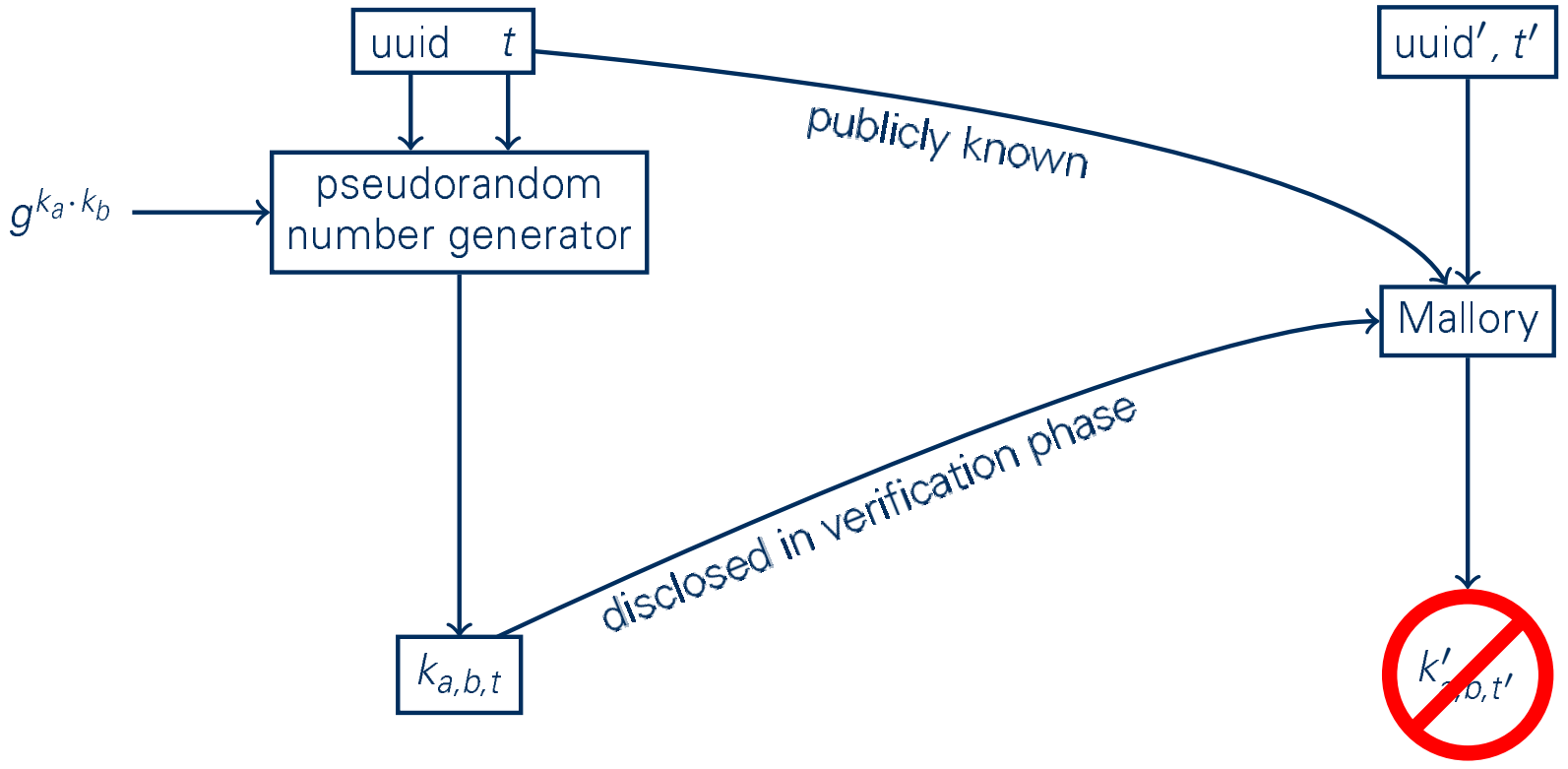
Simplifying the Key Exchange

$$\mathcal{G}(g^{k_a \cdot k_b}, \text{uuid}, t) = k_{a,b,t}$$



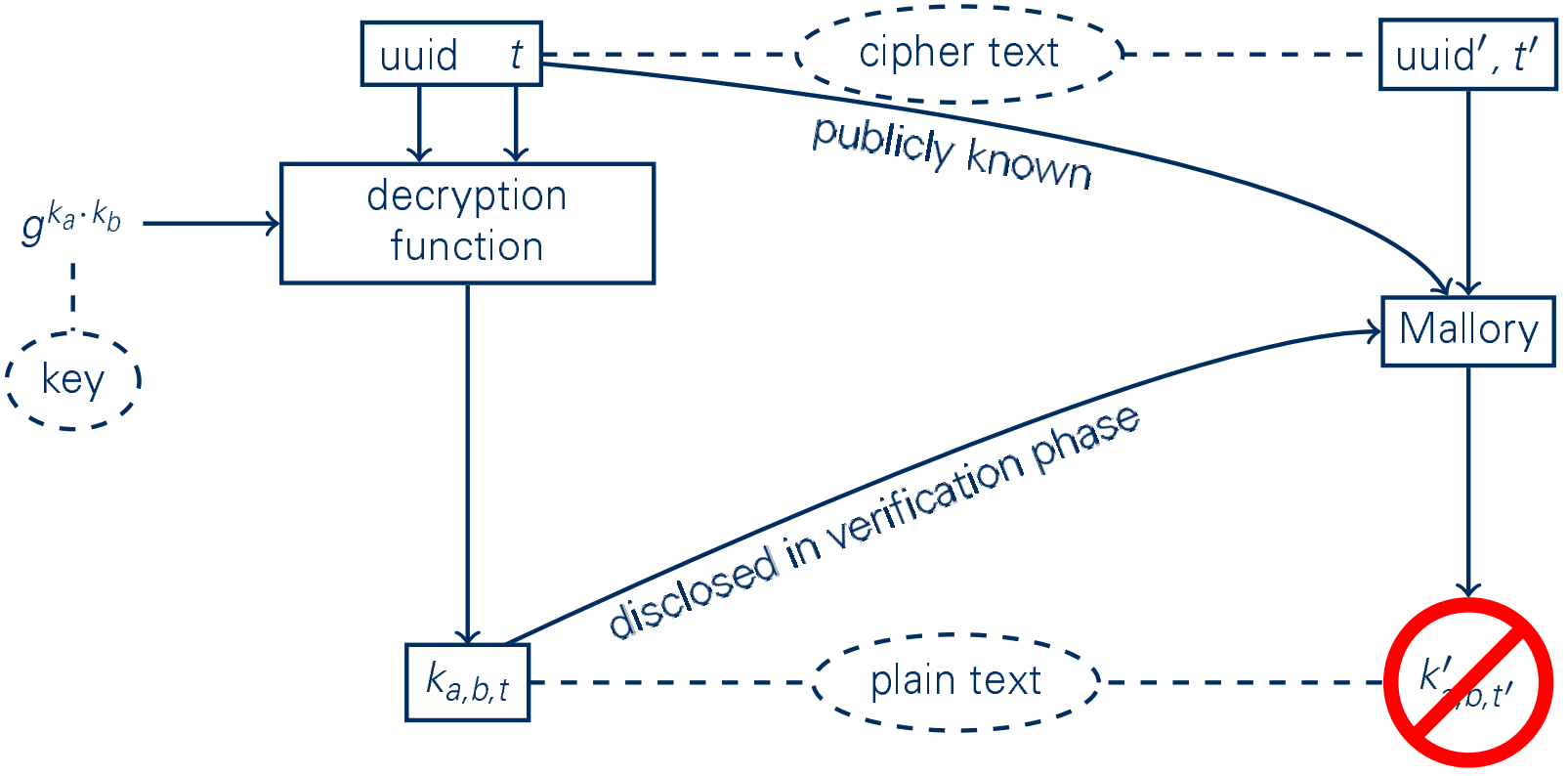
Simplifying the Key Exchange

$$\mathcal{G}(g^{k_a \cdot k_b}, \text{uuid}, t) = k_{a,b,t}$$



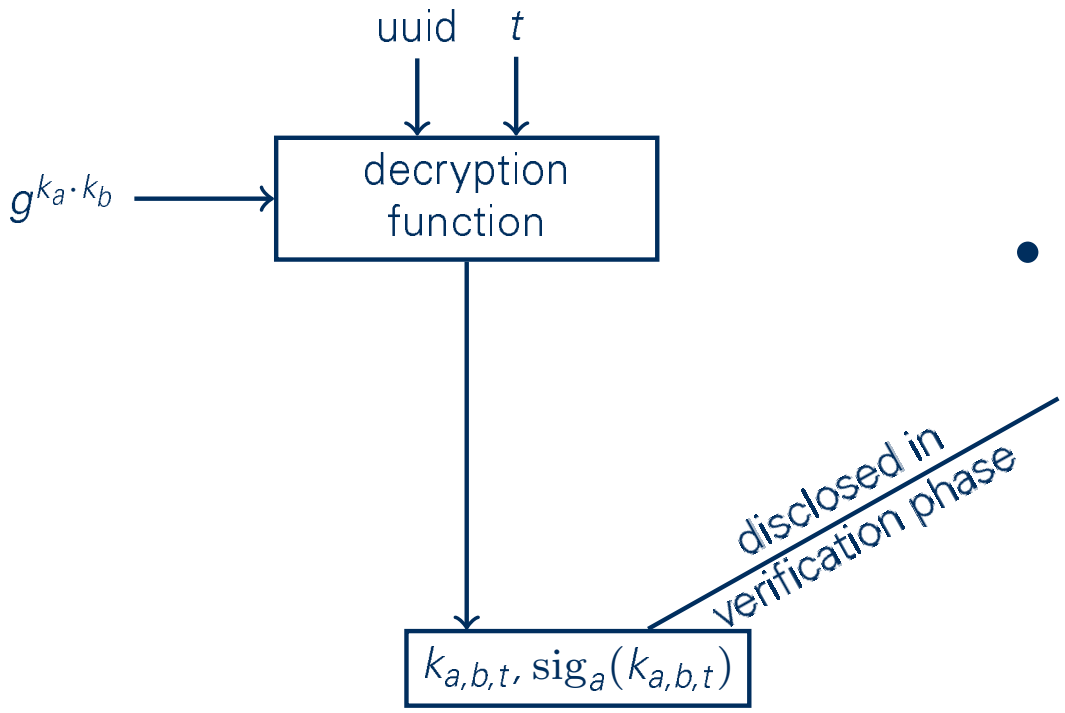
Simplifying the Key Exchange

$$\mathrm{decr}_{g^{k_a \cdot k_b}}(\mathrm{uuid}||t) = k_{a,b,t}$$



Omitting the Key Signatures

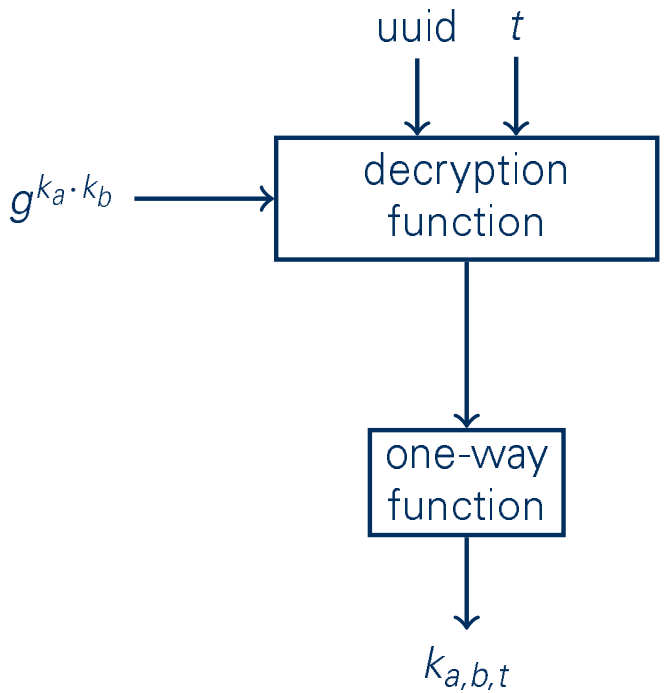
$$\mathrm{decr}_{g^{k_a \cdot k_b}}(\mathrm{uuid}||t) = k_{a,b,t}$$



- key signatures prevent cheating with disclosed keys

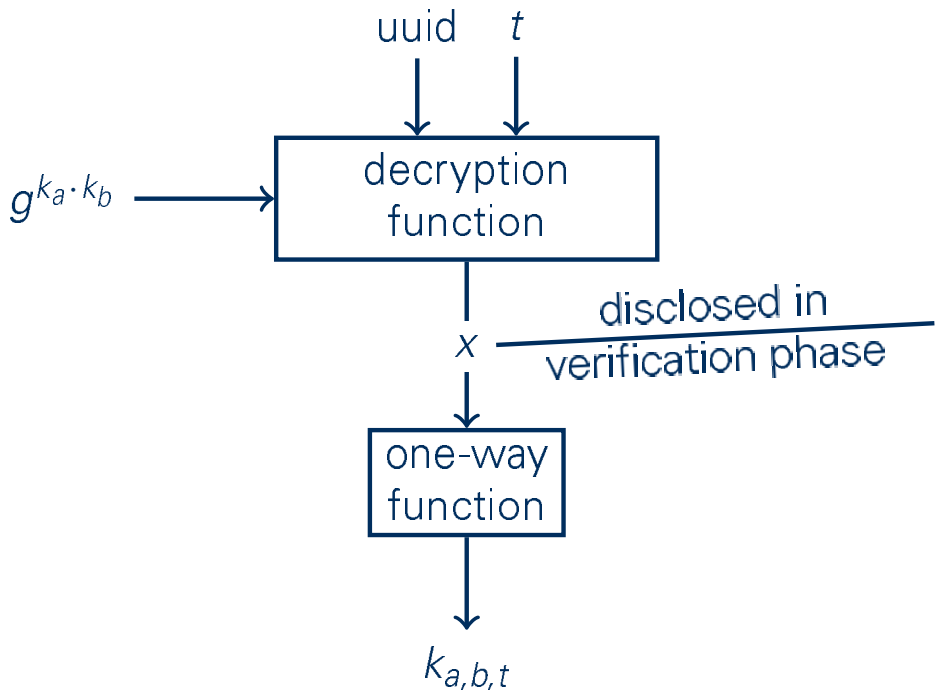
Omitting the Key Signatures

$$\mathrm{decr}_{g^{k_a \cdot k_b}}(\mathrm{uuid}||t) = k_{a,b,t}$$



Omitting the Key Signatures

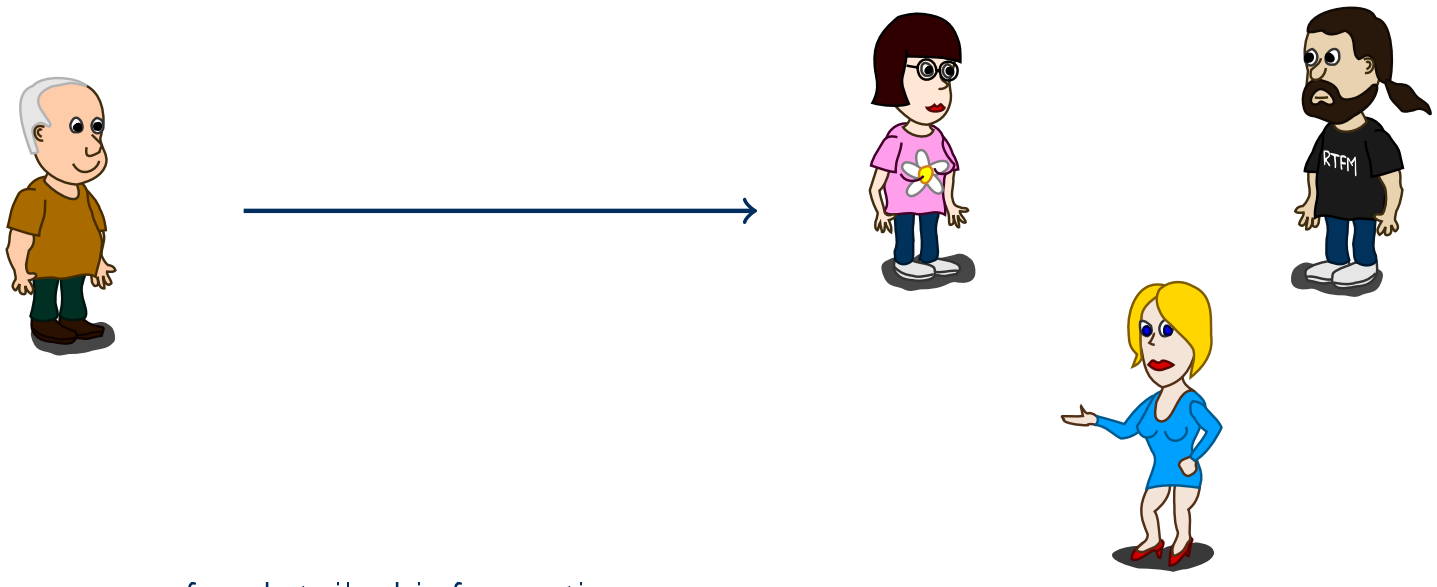
$$\mathrm{h}(\mathrm{decr}_{g^{k_a \cdot k_b}}(\mathrm{uuid}||t)) = k_{a,b,t}$$



- pre-image resistancy prevents cheating with disclosed keys

Additional Extensions

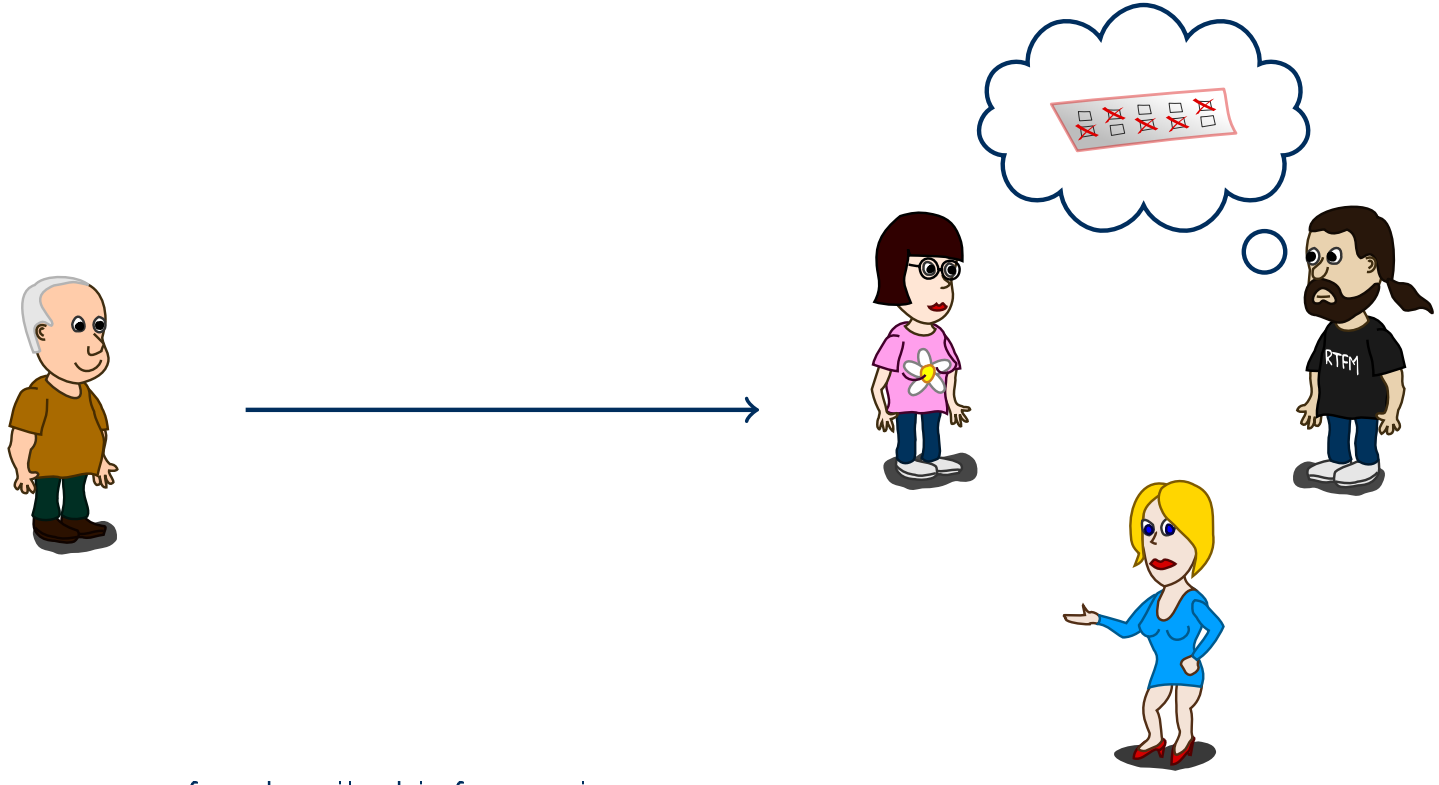
Dynamic Joining



see paper for detailed information

Additional Extensions

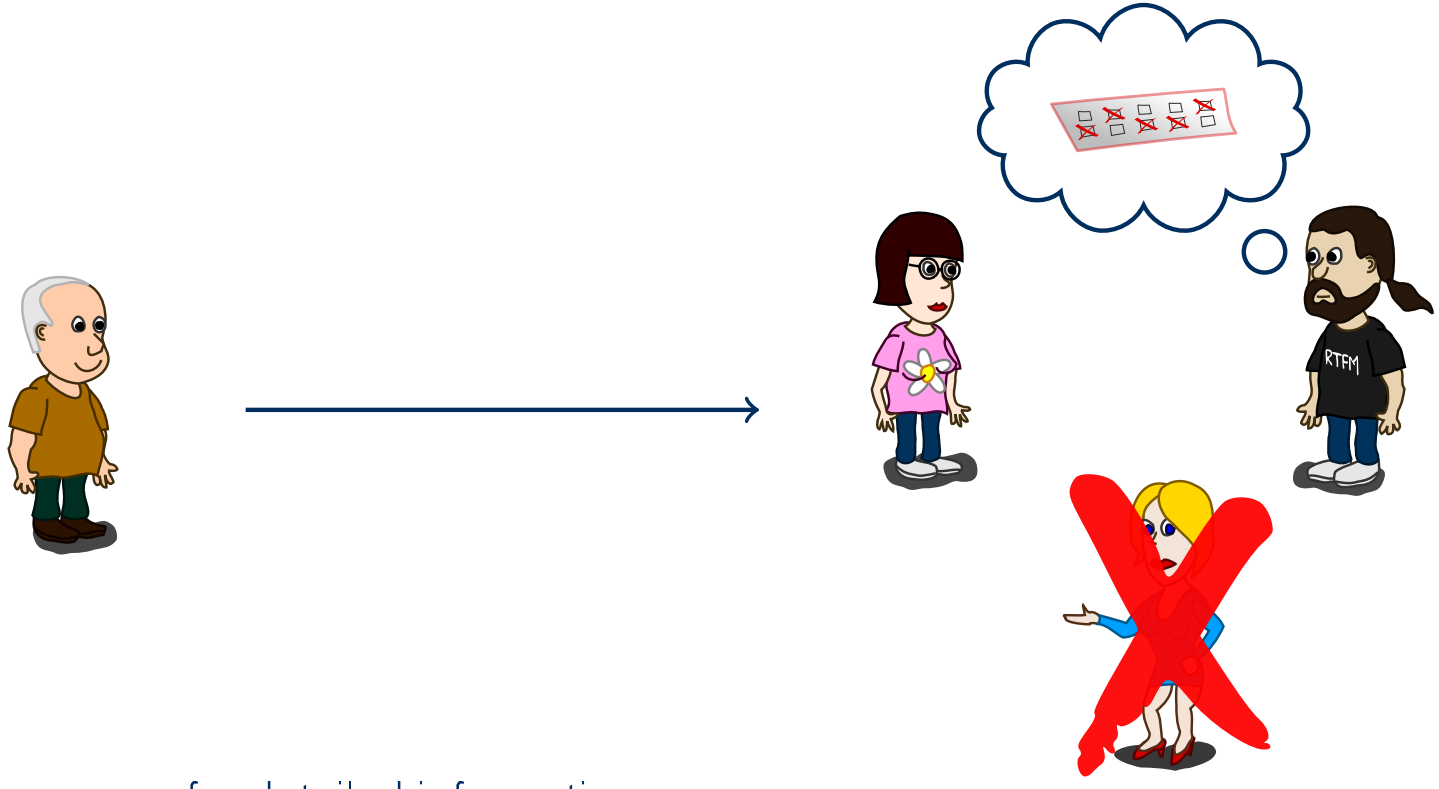
Dynamic Joining



see paper for detailed information

Additional Extensions

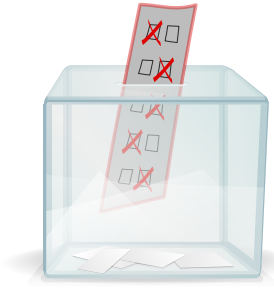
Dynamic Joining/Leaving

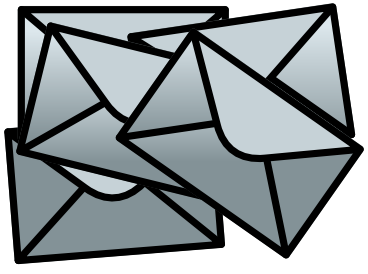


see paper for detailed information

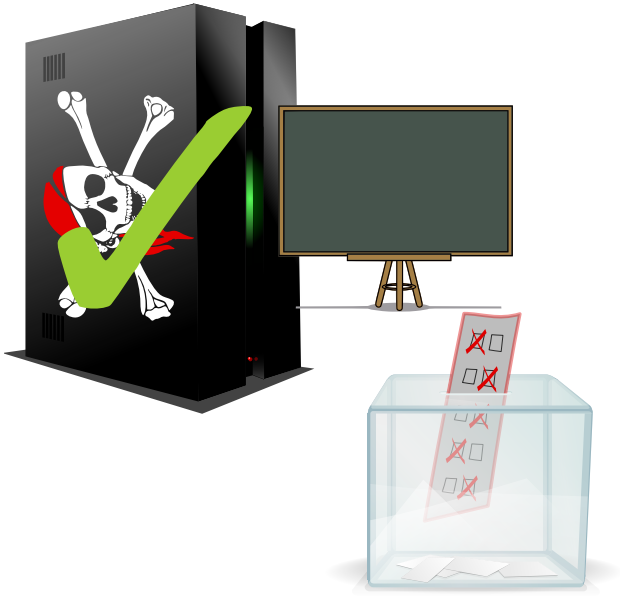
Evaluation

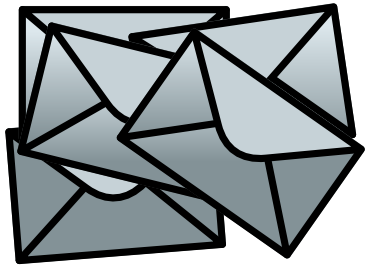
Evaluation



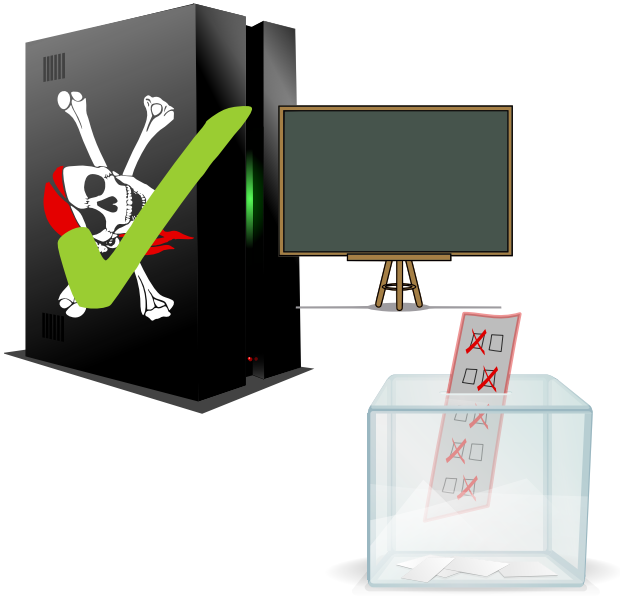


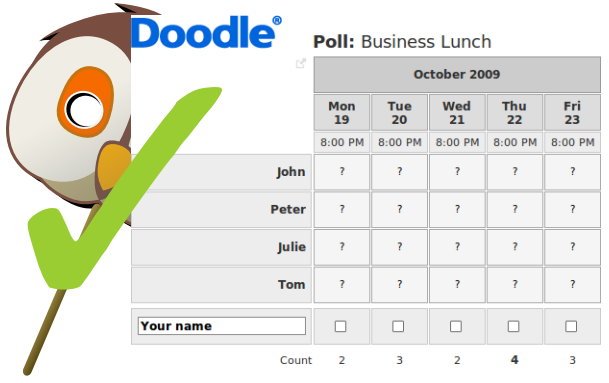
Evaluation

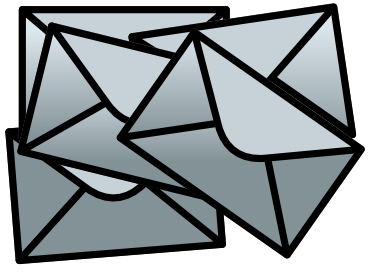




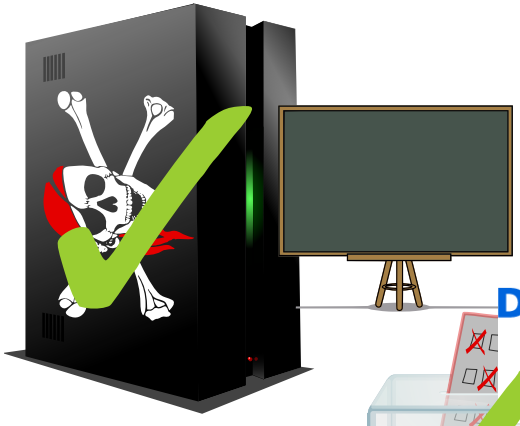
Evaluation




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



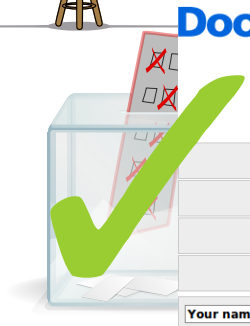
Evaluation



Doodle®

Poll: Business Lunch

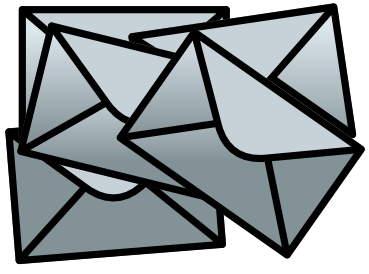
	October 2009				
	Mon 19	Tue 20	Wed 21	Thu 22	Fri 23
	8:00 PM	8:00 PM	8:00 PM	8:00 PM	8:00 PM
John	?	?	?	?	?
Peter	?	?	?	?	?
Julie	?	?	?	?	?
Tom	?	?	?	?	?
Your name	☐	☐	☐	☐	☐
Count	2	3	2	**4**	3



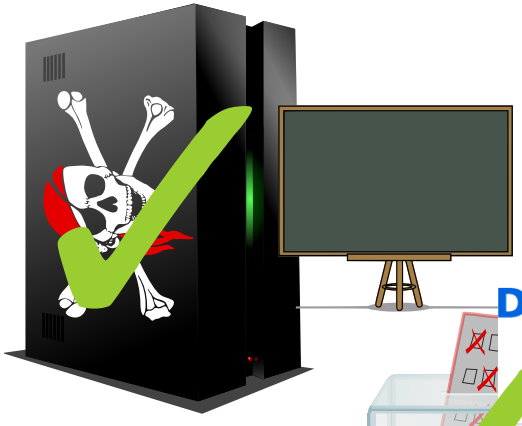
Doodle®

Poll: Business Lunch

	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	?	?	?	2	?
Peter	?	?	?	0	?
Julie	?	?	?	1	?
Tom	?	?	?	1	?
Your name	☐	☐	☐	☐	☐
Count	2	3	2	**4**	3



Evaluation



Doodle®

Poll: Business Lunch

	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	?	?	?	?	?
Peter	?	?	?	?	?
Julie	?	?	?	?	?
Tom	?	?	?	?	?
Your name	☐	☐	☐	☐	☐
Count	2	3	2	**4**	3

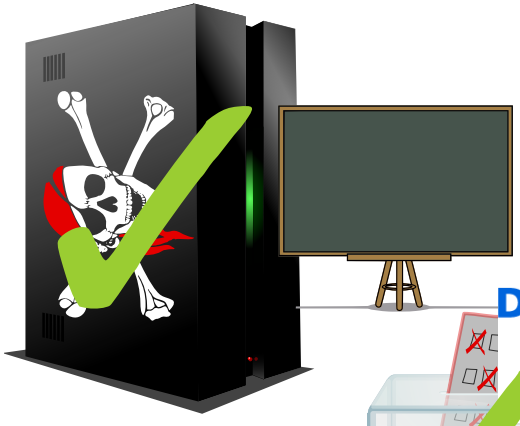
Doodle®

Poll: Business Lunch

	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	?	?	?	2	?
Peter	?	?	?	0	?
Julie	?	?	?	1	?
Tom	?	?	?	1	?
Your name	☐	☐	☐	☐	☐
Count	2	3	2	**4**	3

max. 2 communication steps per voter

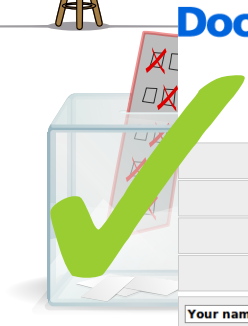
Evaluation



Doodle®

Poll: Business Lunch

	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	?	?	?	?	?
Peter	?	?	?	?	?
Julie	?	?	?	?	?
Tom	?	?	?	?	?
Your name	☐	☐	☐	☐	☐
Count	2	3	2	**4**	3



Doodle®

Poll: Business Lunch

	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	?	?	?	2	?
Peter	?	?	?	0	?
Julie	?	?	?	1	?
Tom	?	?	?	1	?
Your name	☐	☐	☐	☐	☐
Count	2	3	2	**4**	3

max. 2 communication steps per voter

	Date #1	. . .	Date #240
Yes			✘
No	✘		

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

Conclusion and Outlook

- novel scheme for privacy-enhanced event scheduling
  - ➠ scales in number of time slots
  - ➠ no central trust entity
- implement as Web 2.0 application
- validate performance
- more features desirable
  - ➠ other decision rules than unanimous agreement
  - ➠ prevent “legal-but-selfish vote”

TECHNISCHE UNIVERSITÄT DRESDEN

PrimeLife

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

Thank you for your attention!

Discussion

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

Vancouver, August 29, 2009

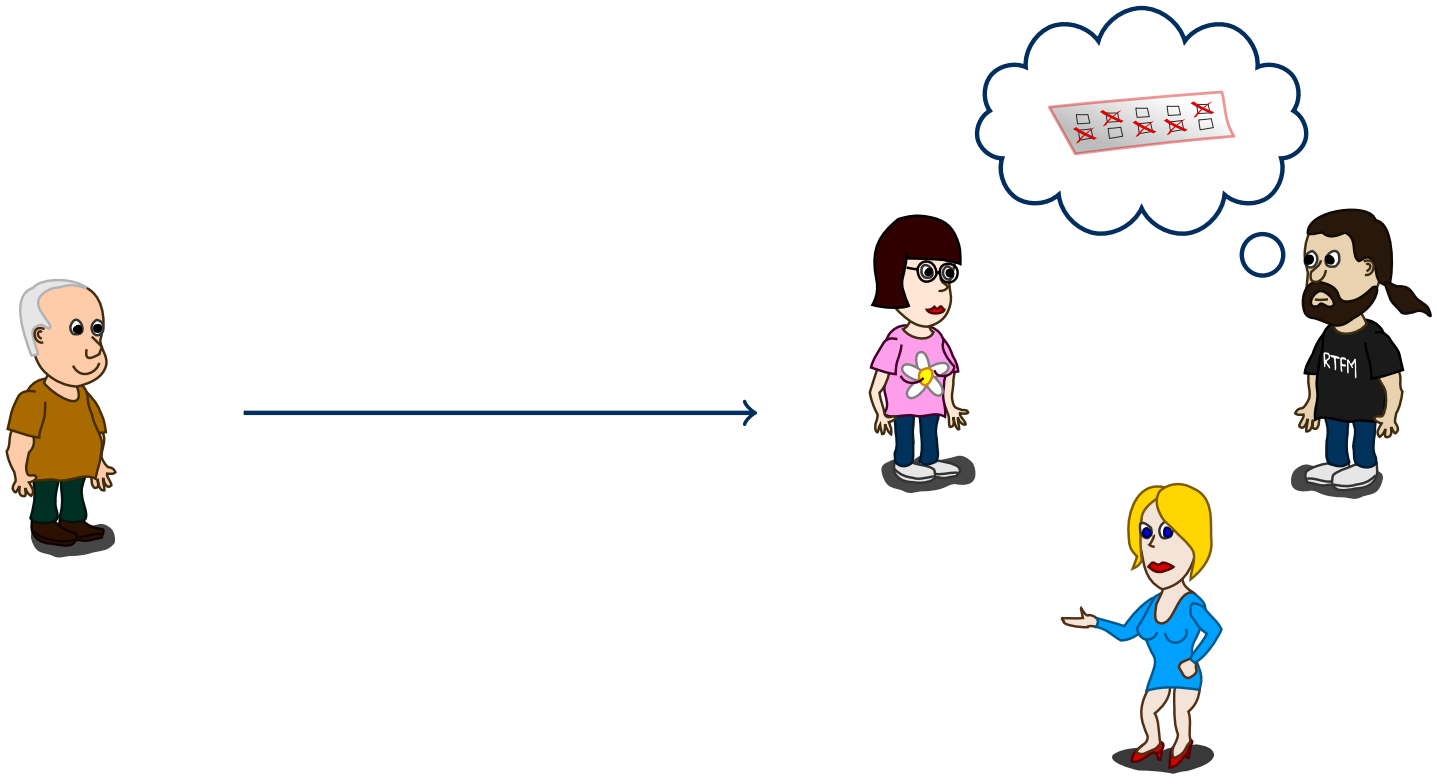
PrimeLife is a research project funded by the European Commission's 7th Framework Programme

Related

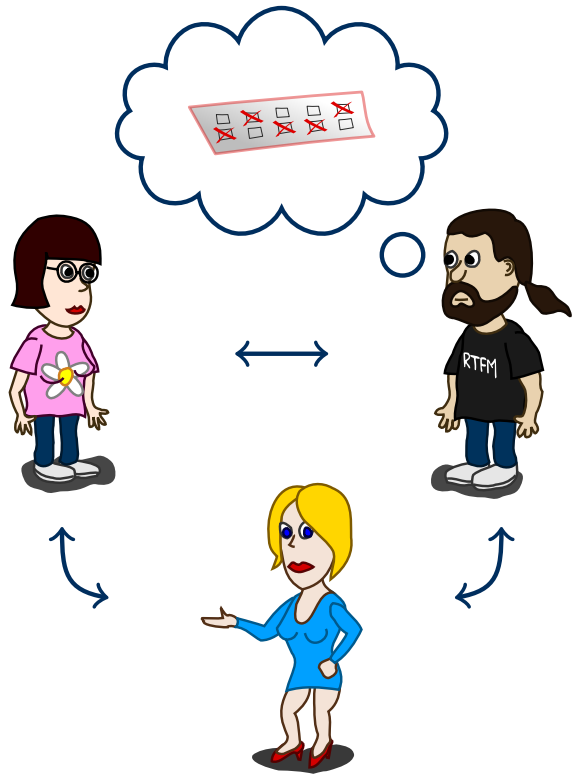
- one specific publication
- mixes
- blind signatures
- homomorphic encryption
- distributed constraint satisfaction/optimization problem

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.

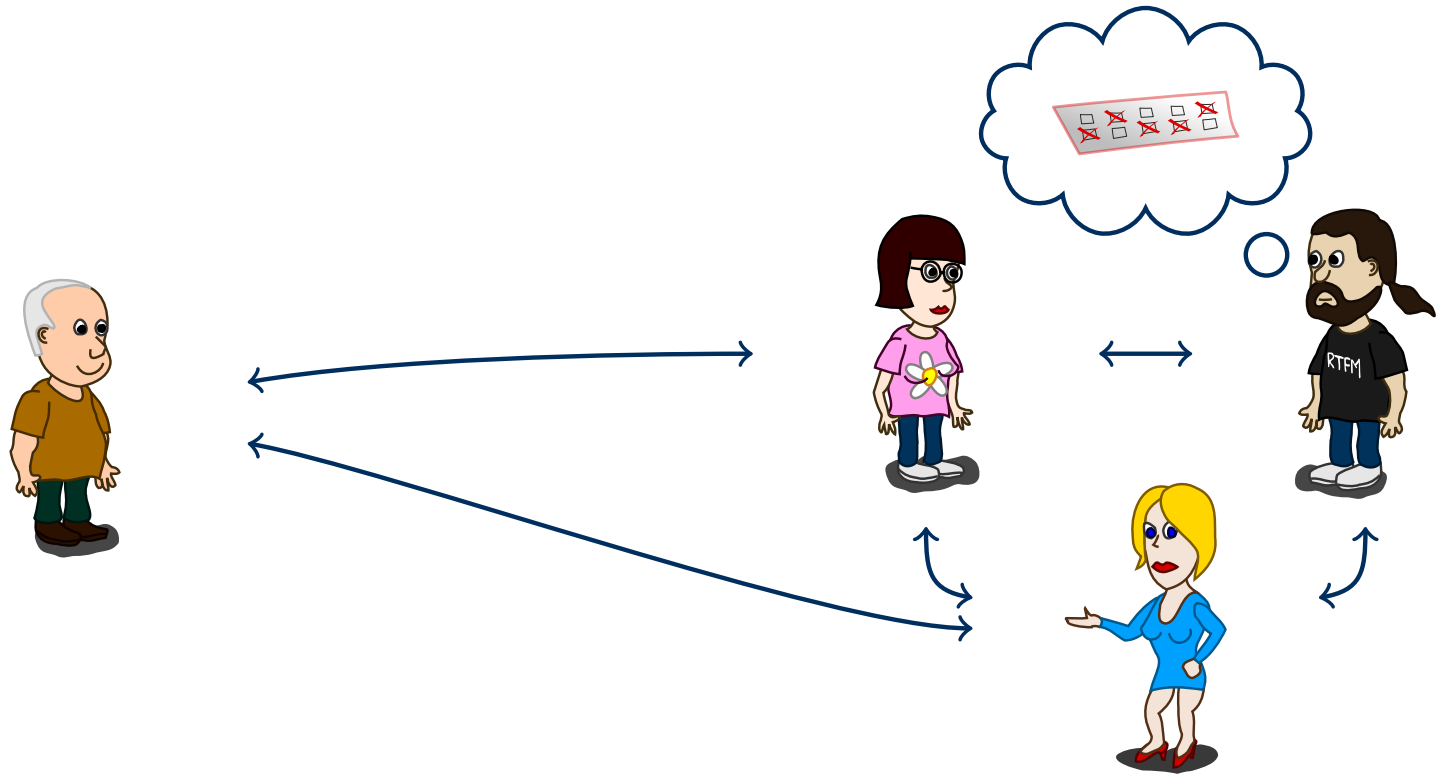
Dynamic Joining



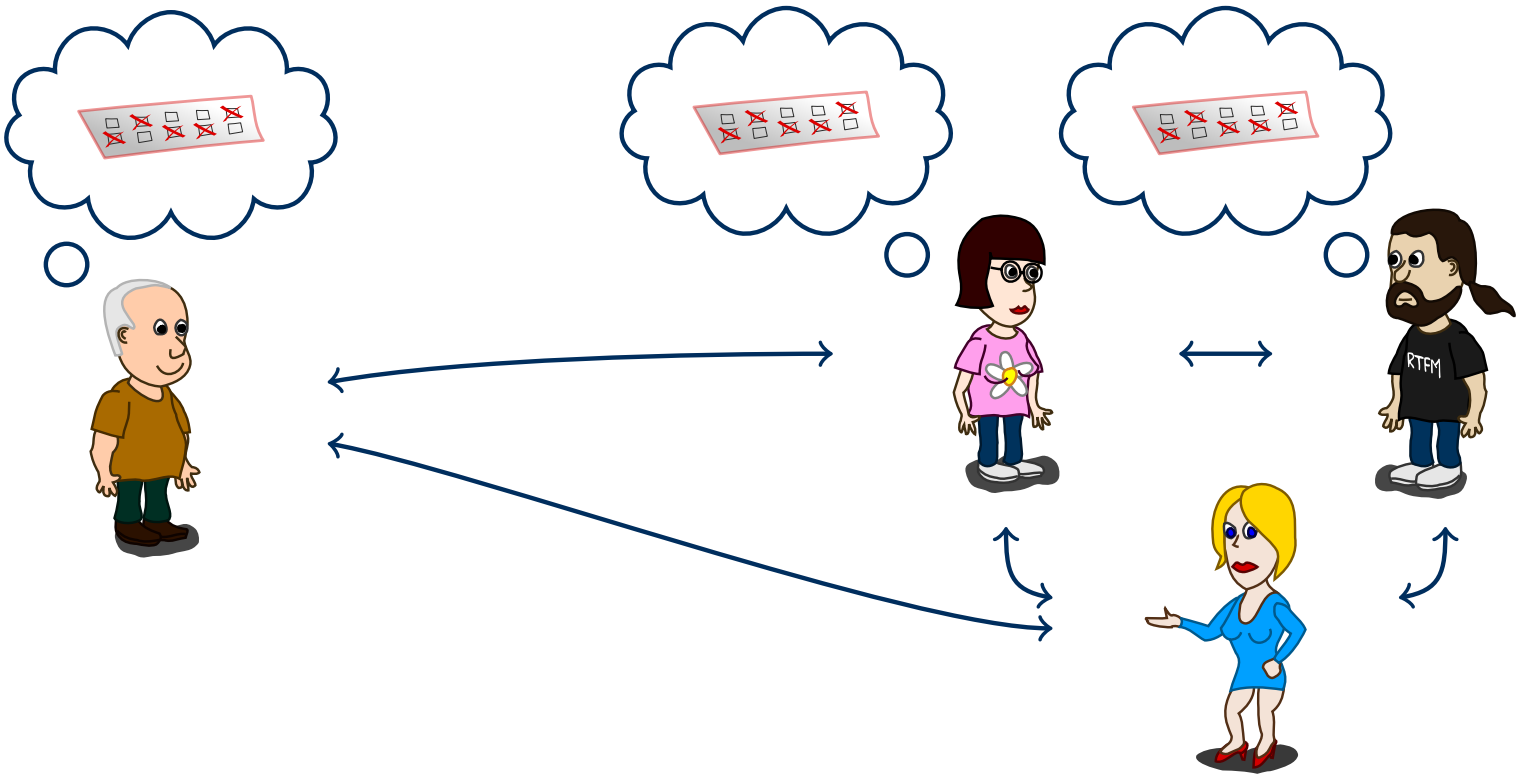
Dynamic Joining



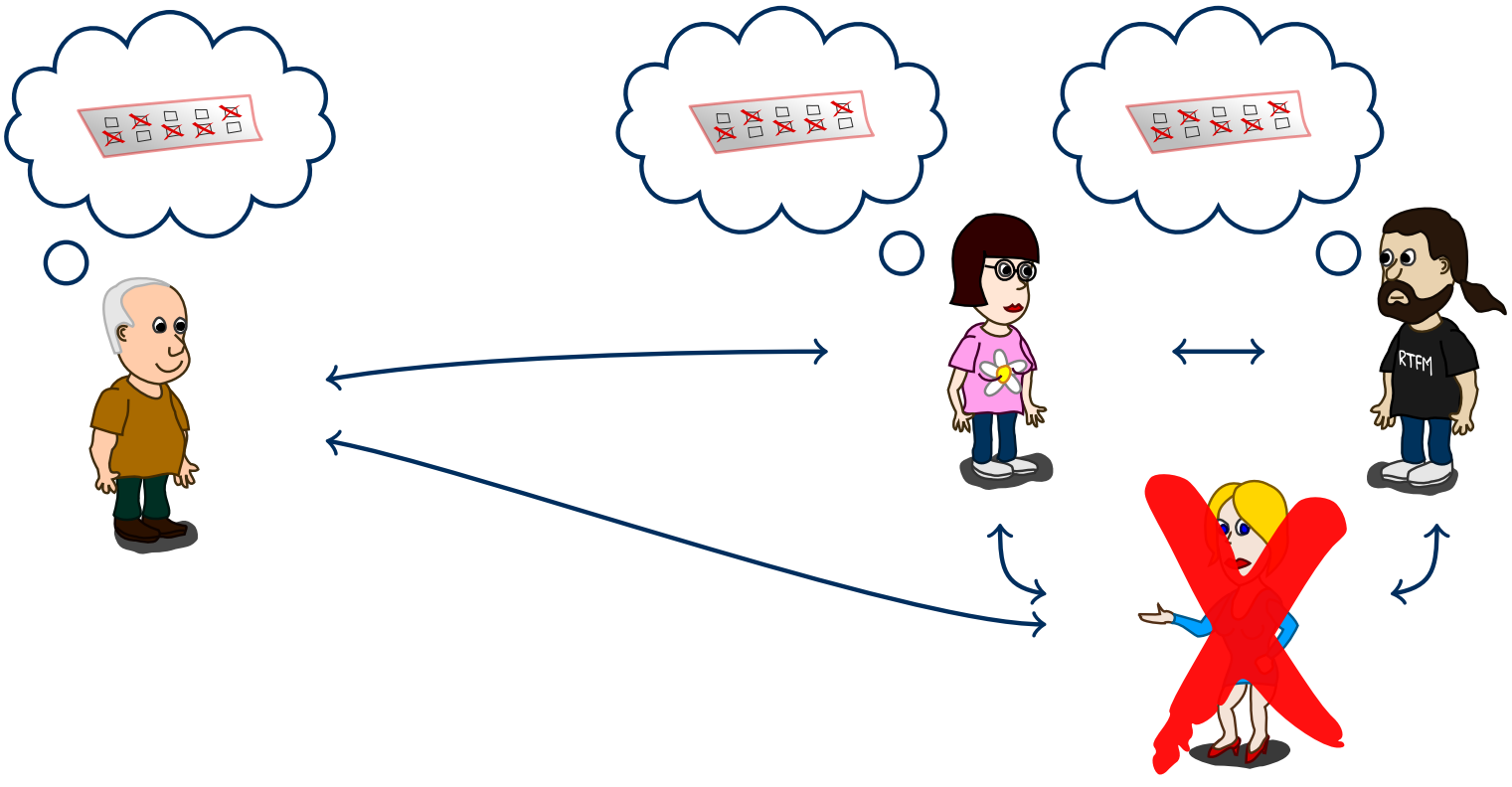
Dynamic Joining



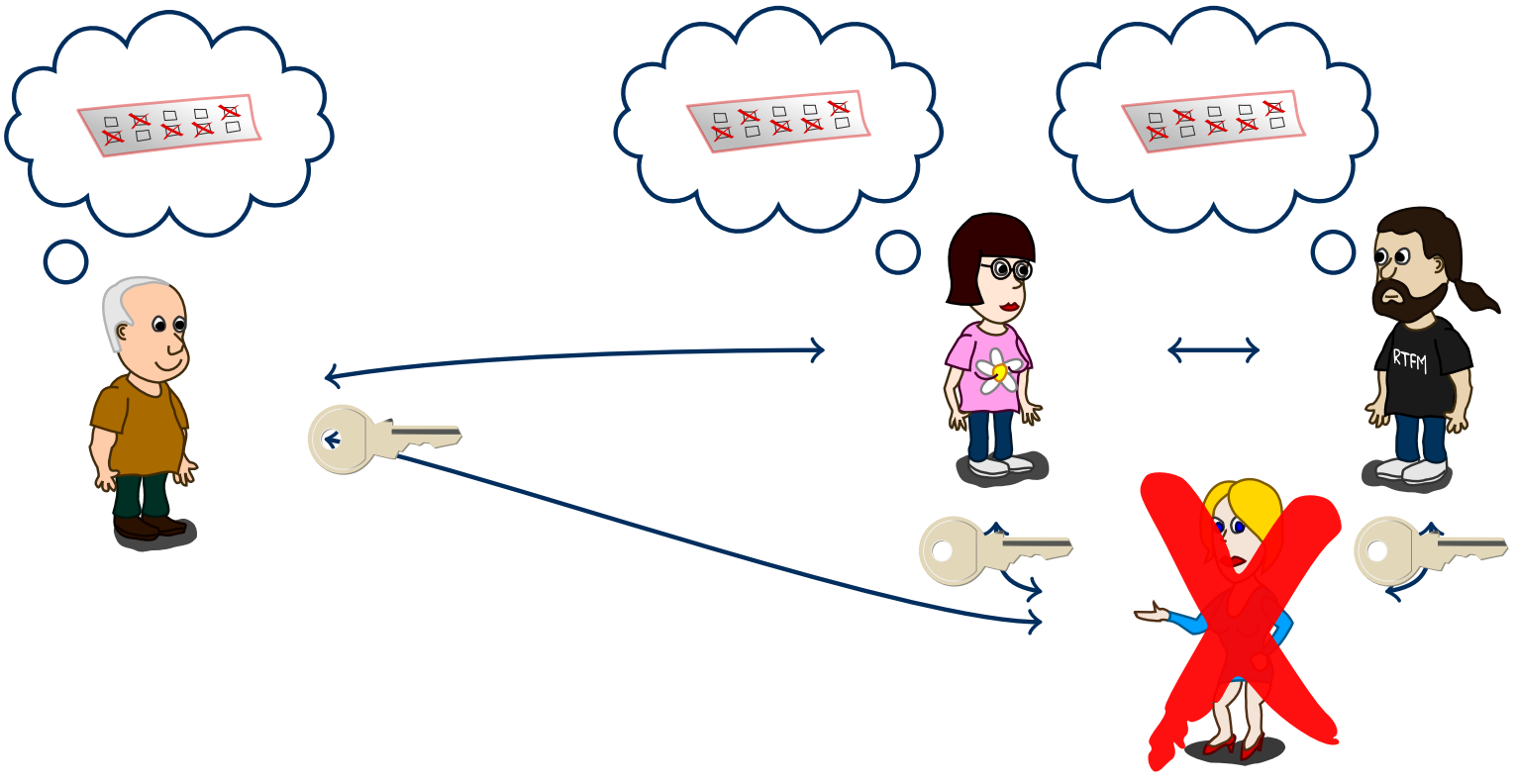
Dynamic Leaving



Dynamic Leaving



Dynamic Leaving



Computational Complexity

server

no expensive computation needed

client

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

More Features

- threshold scheme
- dynamic insertion/deletion of time slots
- updating/revoking votes
- other decision rules than unanimous agreement
- let voters prove that they signaled availability for more than a certain minimum number of time slots