TECHNISCHE UNIVERSITÄT DRESDEN

PrimeLife

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

Privacy-Enhanced Web-Based Event Scheduling with Majority Agreement

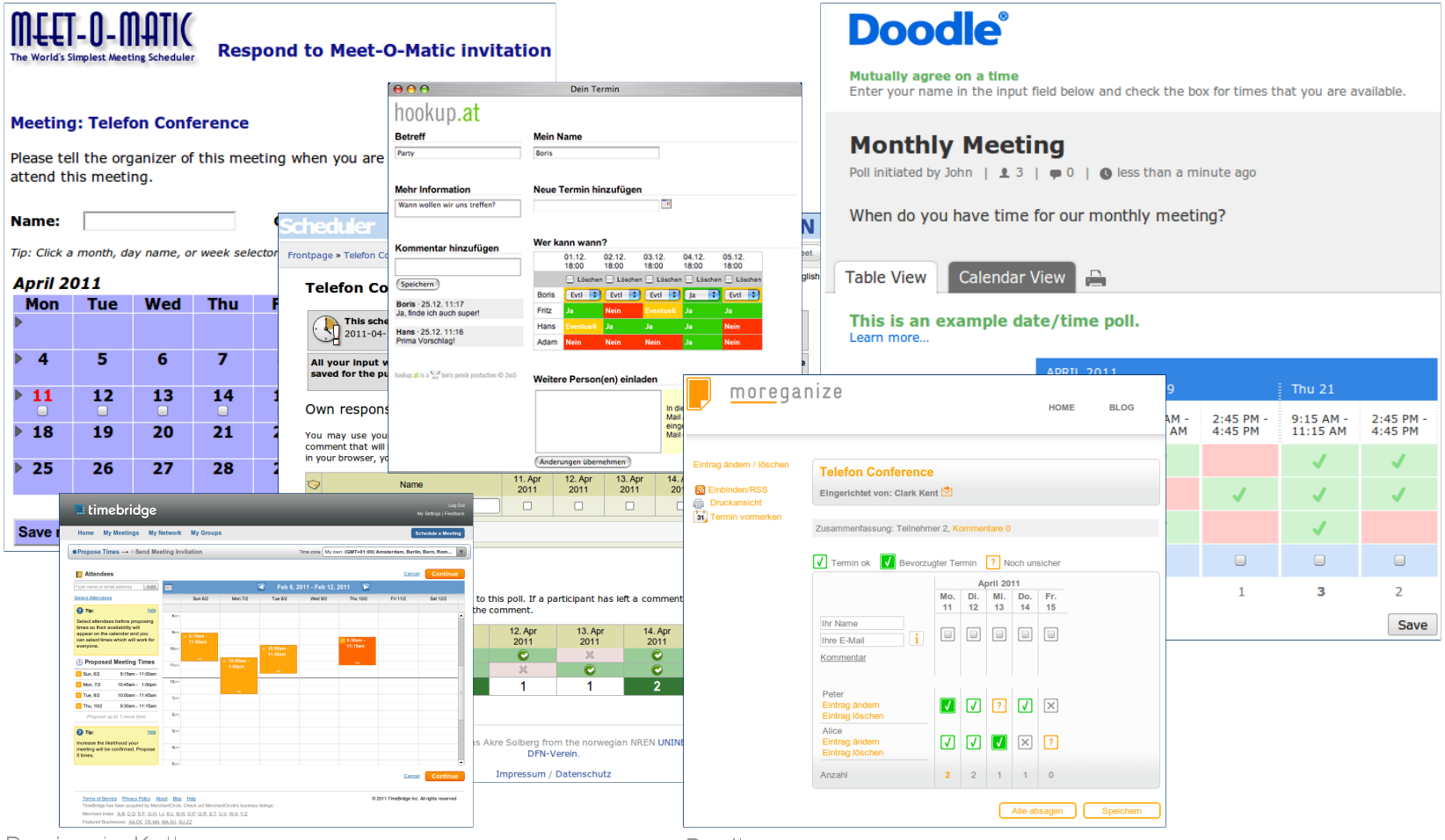
`https://dudle.inf.tu-dresden.de`

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

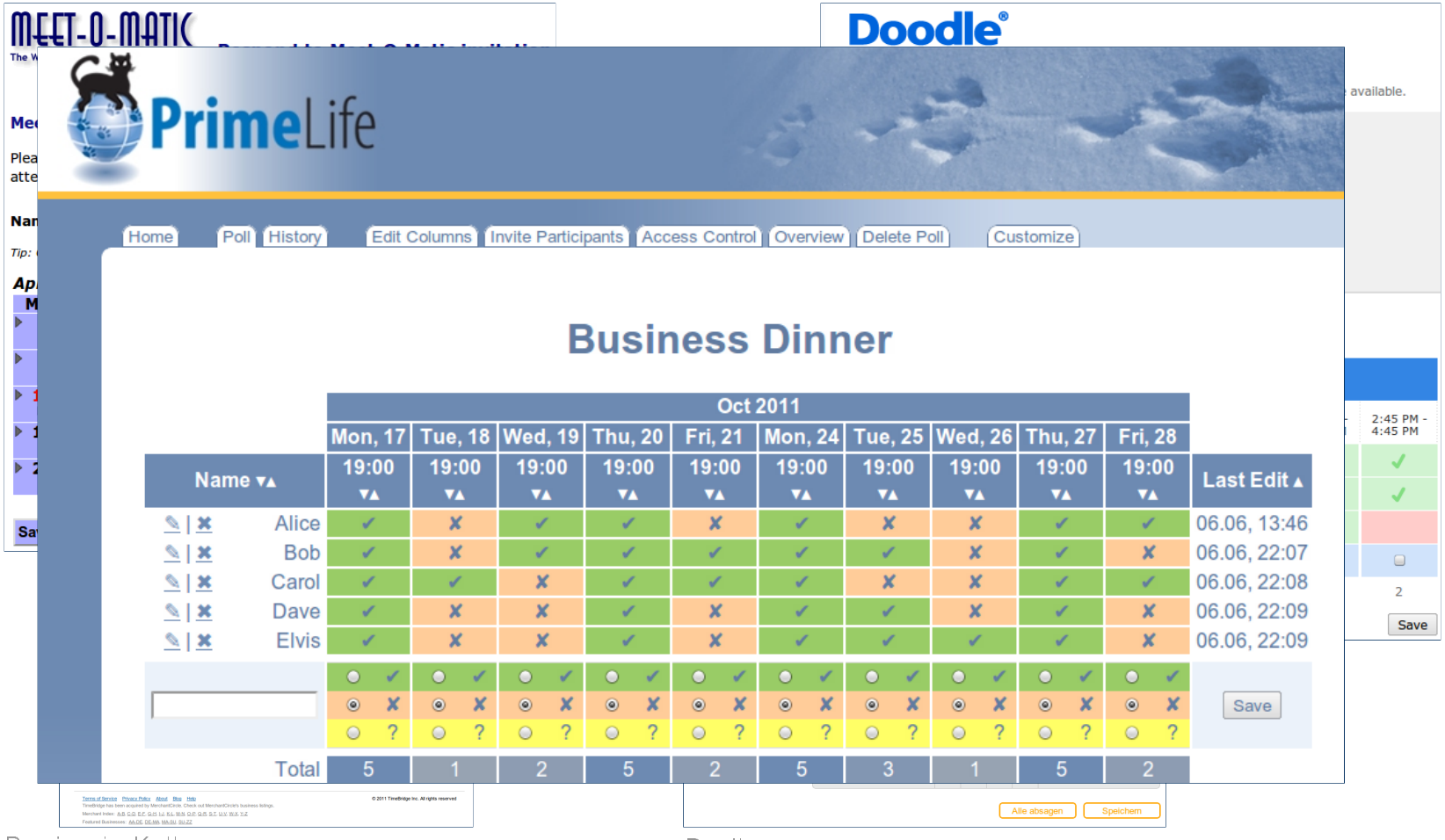
PrimeLife is a research project funded by the European Commission's 7th Framework Programme

Lucerne, June 08, 2011

Web-Based Event Scheduling



Web-Based Event Scheduling



Direct Inference

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

Business Dinner

		Oct 2011										
		Mon, 17	Tue, 18	Wed, 19	Thu, 20	Fri, 21	Mon, 24	Tue, 25	Wed, 26	Thu, 27	Fri, 28	
Name ▾▴		19:00 ▾▴	19:00 ▾▴	19:00 ▾▴	19:00 ▾▴	19:00 ▾▴	19:00 ▾▴	19:00 ▾▴	19:00 ▾▴	19:00 ▾▴	19:00 ▾▴	Last Edit ▴
✎ | ✖	Alice	✓	✗	✓	✓	✗	✓	✗	✗	✓	✓	06.06, 13:46
✎ | ✖	Bob	✓	✗	✓	✓	✓	✓	✓	✗	✓	✗	06.06, 22:07
✎ | ✖	Carol	✓	✓	✗	✓	✓	✓	✗	✗	✓	✓	06.06, 22:08
✎ | ✖	Dave	✓	✗	✗	✓	✗	✓	✓	✗	✓	✗	06.06, 22:09
✎ | ✖	Elvis	✓	✗	✗	✓	✗	✓	✓	✓	✓	✗	06.06, 22:09
		○ ✓ / ◉ ✗ / ○ ?	○ ✓ / ◉ ✗ / ○ ?	○ ✓ / ◉ ✗ / ○ ?	○ ✓ / ◉ ✗ / ○ ?	○ ✓ / ◉ ✗ / ○ ?	○ ✓ / ◉ ✗ / ○ ?	○ ✓ / ◉ ✗ / ○ ?	○ ✓ / ◉ ✗ / ○ ?	○ ✓ / ◉ ✗ / ○ ?	○ ✓ / ◉ ✗ / ○ ?	Save
	Total	5	1	2	5	2	5	3	1	5	2	

Direct Inference

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

Business Dinner

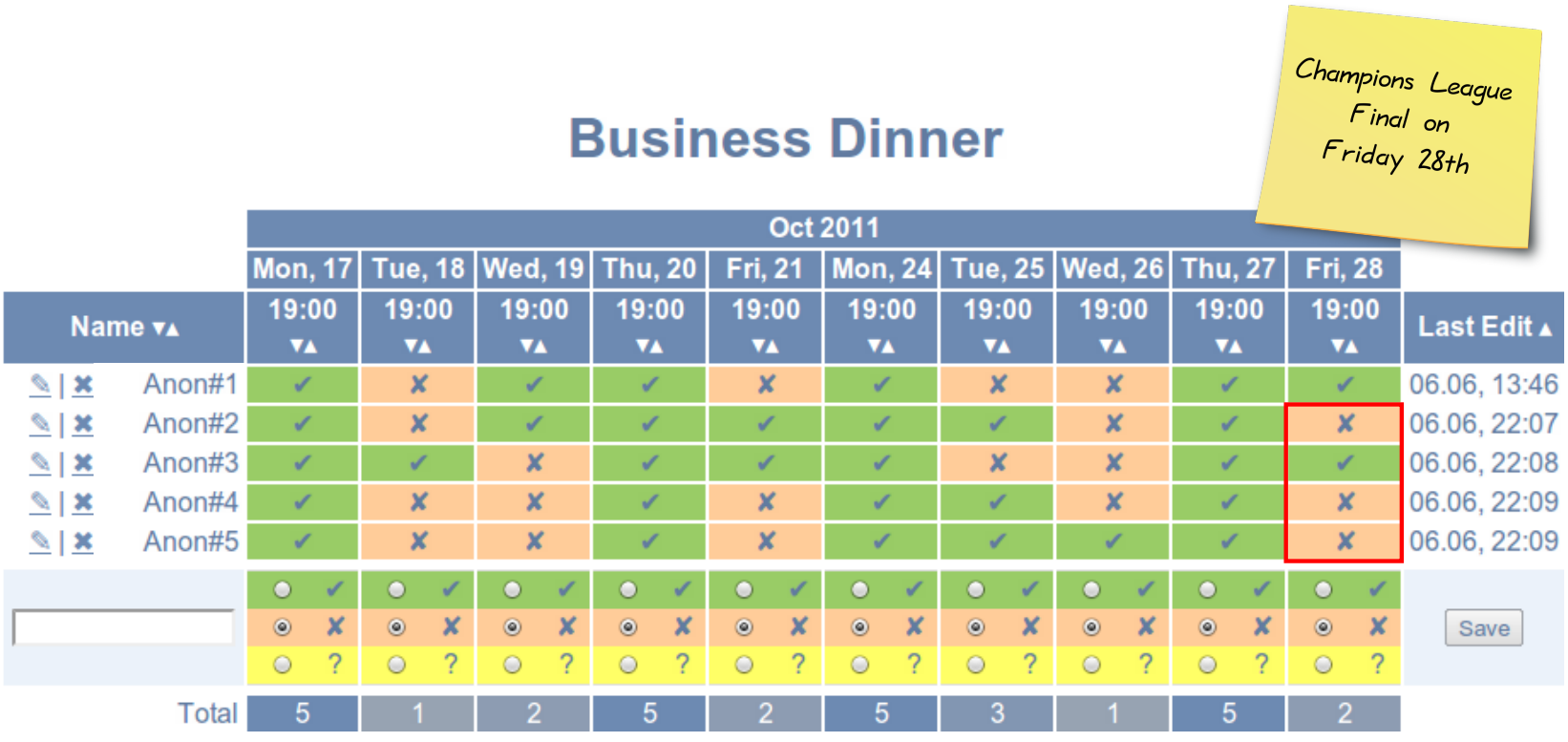
Name	Oct 2011 Mon, 17 19:00	Tue, 18 19:00	Wed, 19 19:00	Thu, 20 19:00	Fri, 21 19:00	Mon, 24 19:00	Tue, 25 19:00	Wed, 26 19:00	Thu, 27 19:00	Fri, 28 19:00	Last Edit
Alice	✓	✗	✓	✓	✗	✓	✗	✗	✓	✓	06.06, 13:46
Bob	✓	✗	✓	✓	✓	✓	✓	✗	✓	✗	06.06, 22:07
Carol	✓	✓	✗	✓	✓	✓	✗	✗	✓	✓	06.06, 22:08
Dave	✓	✗	✗	✓	✗	✓	✓	✗	✓	✗	06.06, 22:09
Elvis	✓	✗	✗	✓	✗	✓	✓	✓	✓	✗	06.06, 22:09
	○ ✓ / ◉ ✗ / ○ ?	○ ✓ / ◉ ✗ / ○ ?	○ ✓ / ◉ ✗ / ○ ?	○ ✓ / ◉ ✗ / ○ ?	○ ✓ / ◉ ✗ / ○ ?	○ ✓ / ◉ ✗ / ○ ?	○ ✓ / ◉ ✗ / ○ ?	○ ✓ / ◉ ✗ / ○ ?	○ ✓ / ◉ ✗ / ○ ?	○ ✓ / ◉ ✗ / ○ ?	Save
Total	5	1	2	5	2	5	3	1	5	2	

Indirect Inference

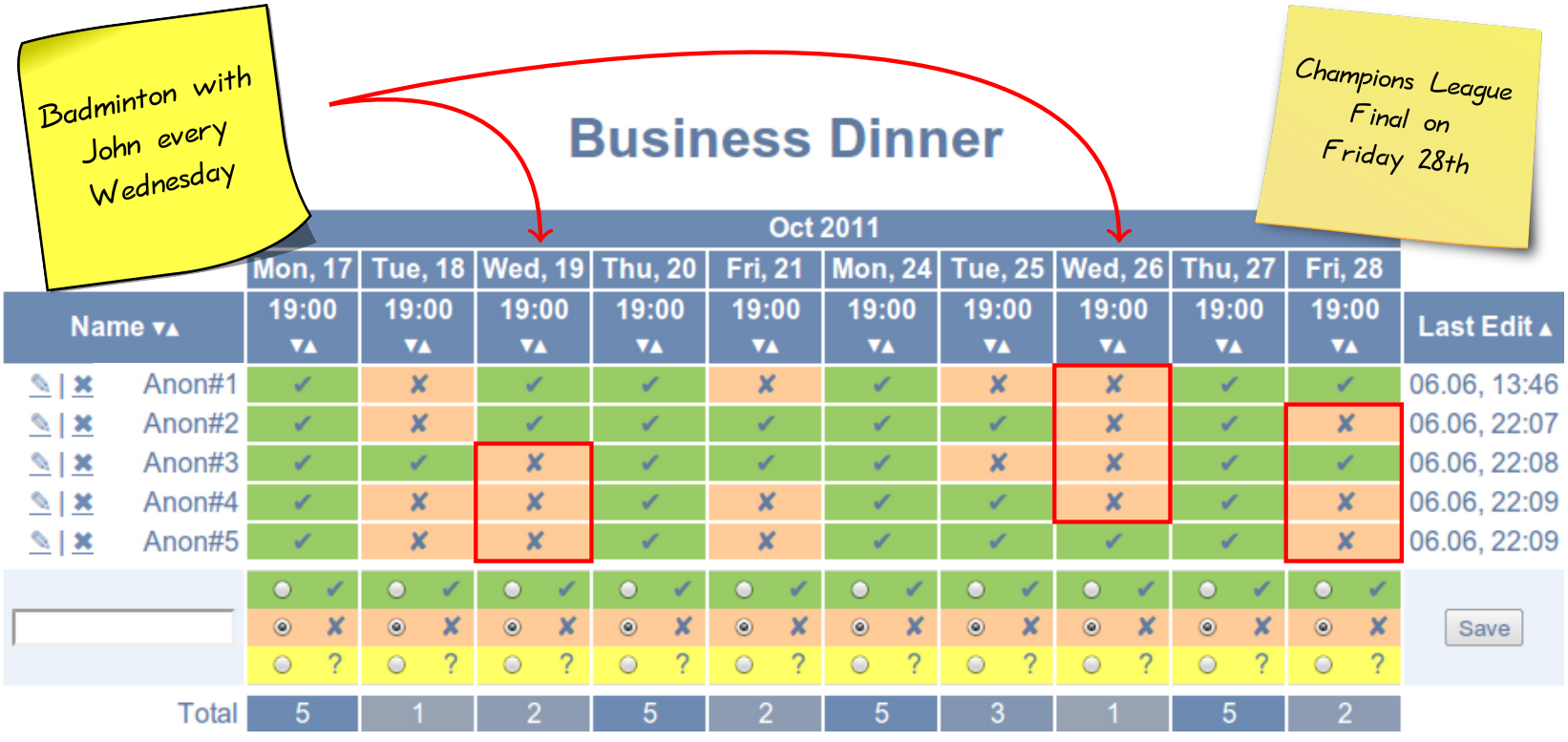
Business Dinner

	Oct 2011										
	Mon, 17	Tue, 18	Wed, 19	Thu, 20	Fri, 21	Mon, 24	Tue, 25	Wed, 26	Thu, 27	Fri, 28	
Name ▾▴	19:00 ▾▴	19:00 ▾▴	19:00 ▾▴	19:00 ▾▴	19:00 ▾▴	19:00 ▾▴	19:00 ▾▴	19:00 ▾▴	19:00 ▾▴	19:00 ▾▴	Last Edit ▴
✎ | ✖ Anon#1	✓	✘	✓	✓	✘	✓	✘	✘	✓	✓	06.06, 13:46
✎ | ✖ Anon#2	✓	✘	✓	✓	✓	✓	✓	✘	✓	✘	06.06, 22:07
✎ | ✖ Anon#3	✓	✓	✘	✓	✓	✓	✘	✘	✓	✓	06.06, 22:08
✎ | ✖ Anon#4	✓	✘	✘	✓	✘	✓	✓	✘	✓	✘	06.06, 22:09
✎ | ✖ Anon#5	✓	✘	✘	✓	✘	✓	✓	✓	✓	✘	06.06, 22:09
	○ ✓ / ◉ ✘ / ○ ?	○ ✓ / ◉ ✘ / ○ ?	○ ✓ / ◉ ✘ / ○ ?	○ ✓ / ◉ ✘ / ○ ?	○ ✓ / ◉ ✘ / ○ ?	○ ✓ / ◉ ✘ / ○ ?	○ ✓ / ◉ ✘ / ○ ?	○ ✓ / ◉ ✘ / ○ ?	○ ✓ / ◉ ✘ / ○ ?	○ ✓ / ◉ ✘ / ○ ?	Save
Total	5	1	2	5	2	5	3	1	5	2	

Indirect Inference



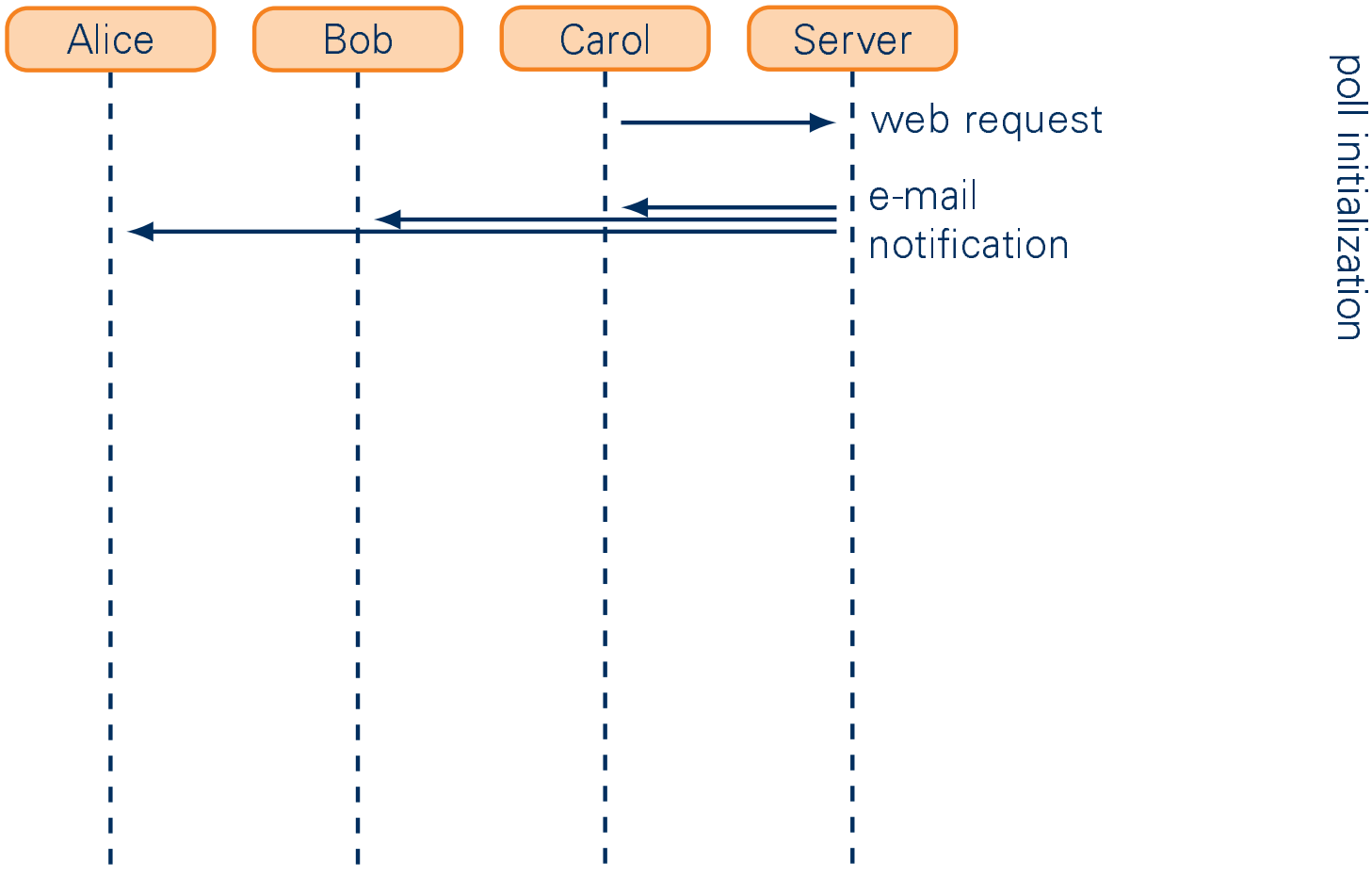
Indirect Inference



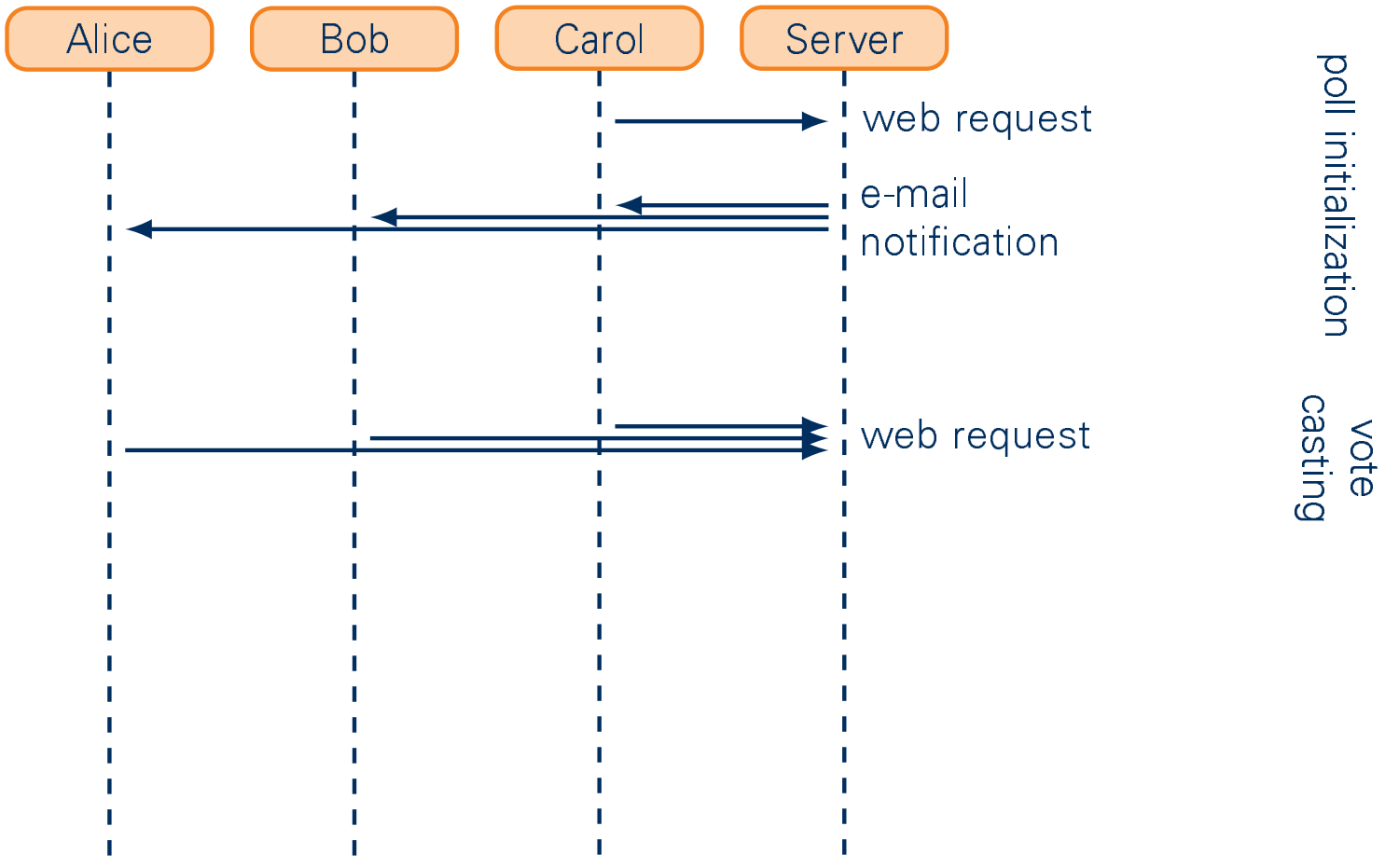
Indirect Inference

Table of Contents

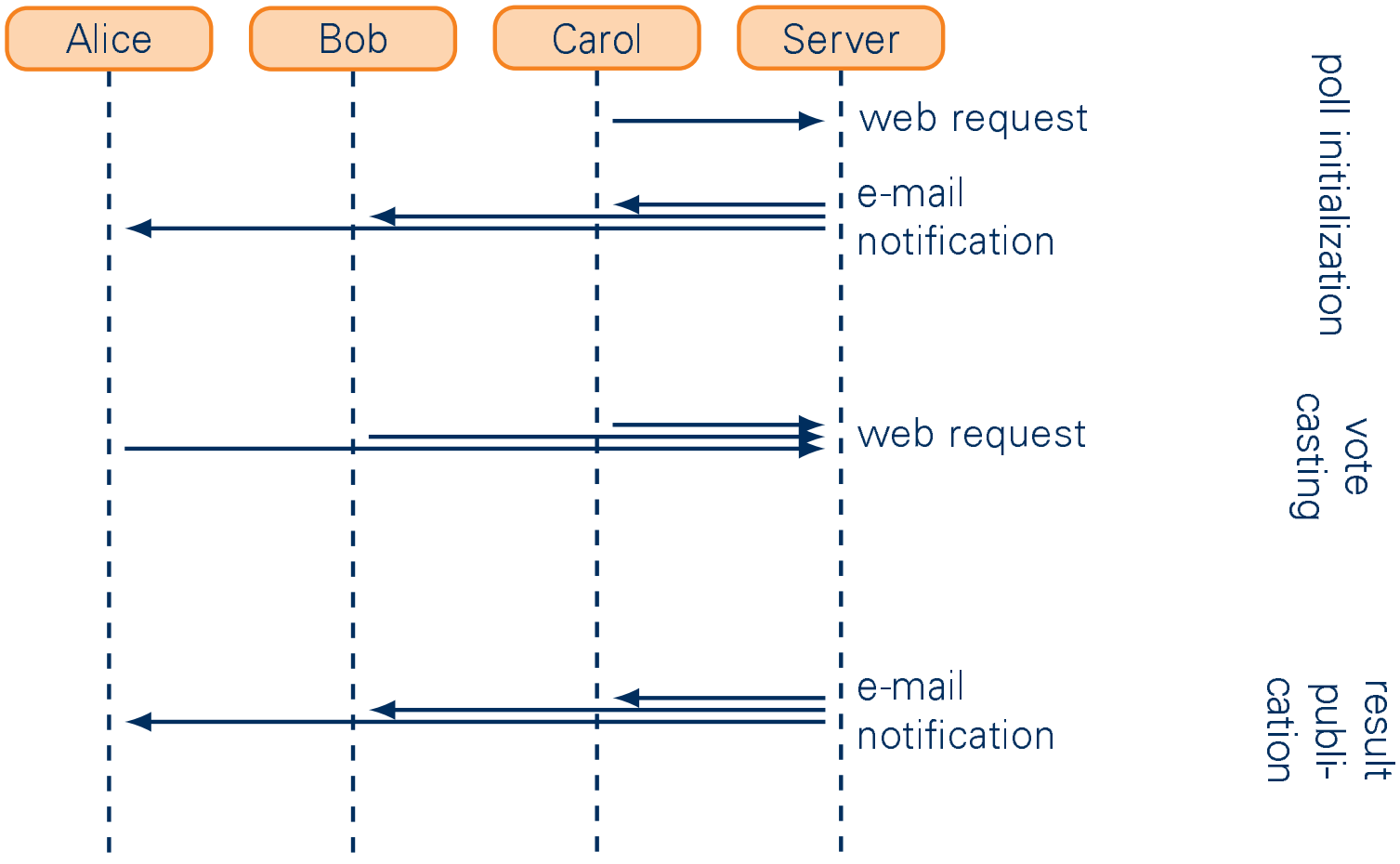
Phases


Alice
Bob
Carol
Server
web request
e-mail notification
poll initialization

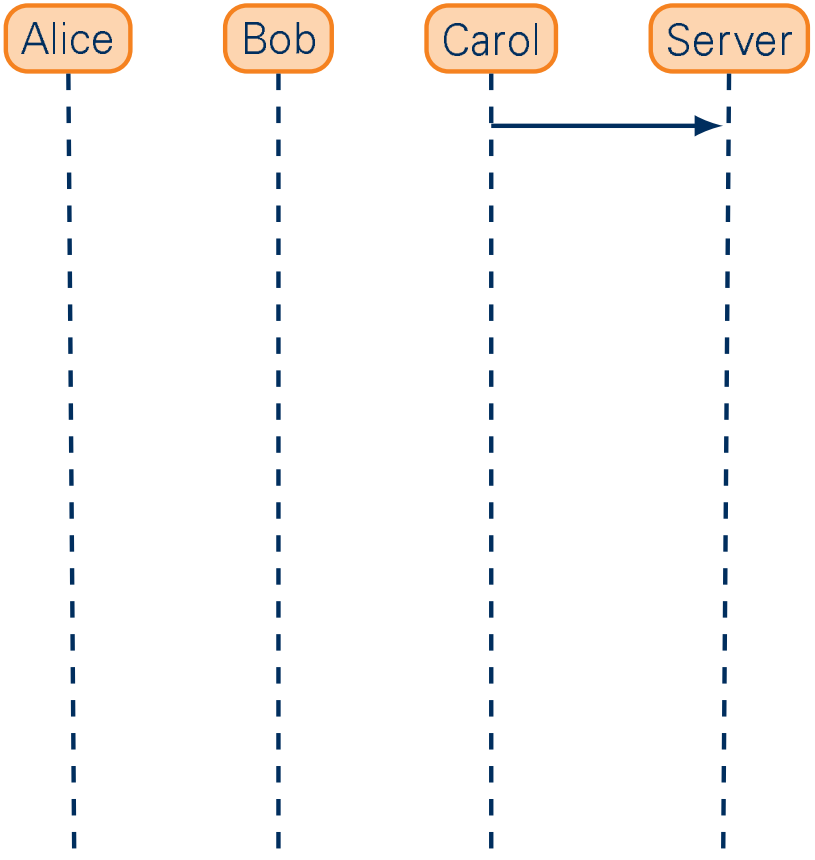
Phases


Alice
Bob
Carol
Server
web request
e-mail notification
web request
poll initialization
vote casting

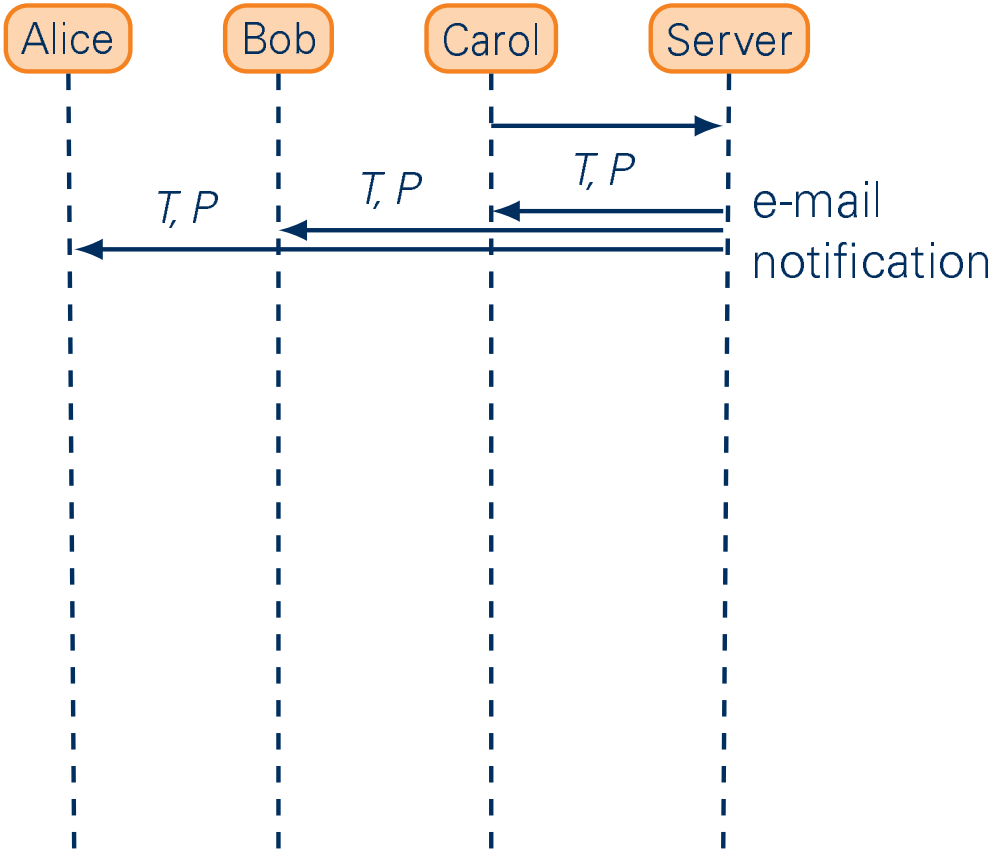
Phases


Alice
Bob
Carol
Server
web request
e-mail notification
web request
e-mail notification
poll initialization
vote casting
result publi-cation

Poll Initialization

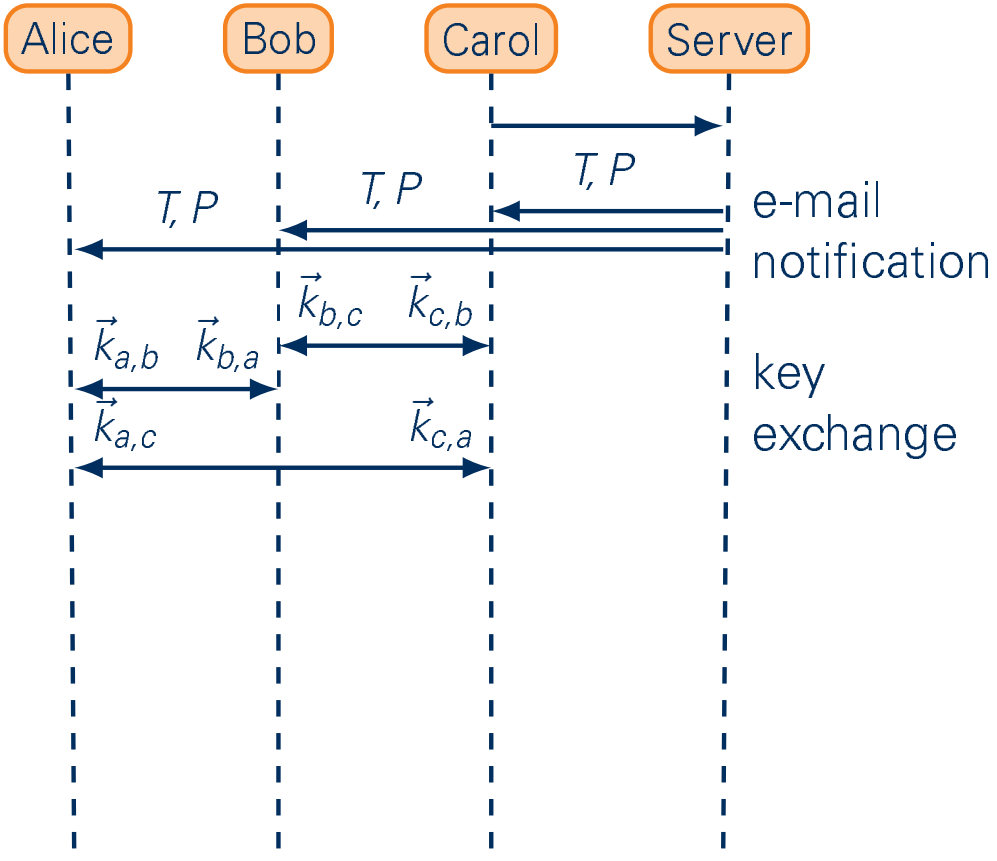


Poll Initialization



T . . . time slots
P . . . participants

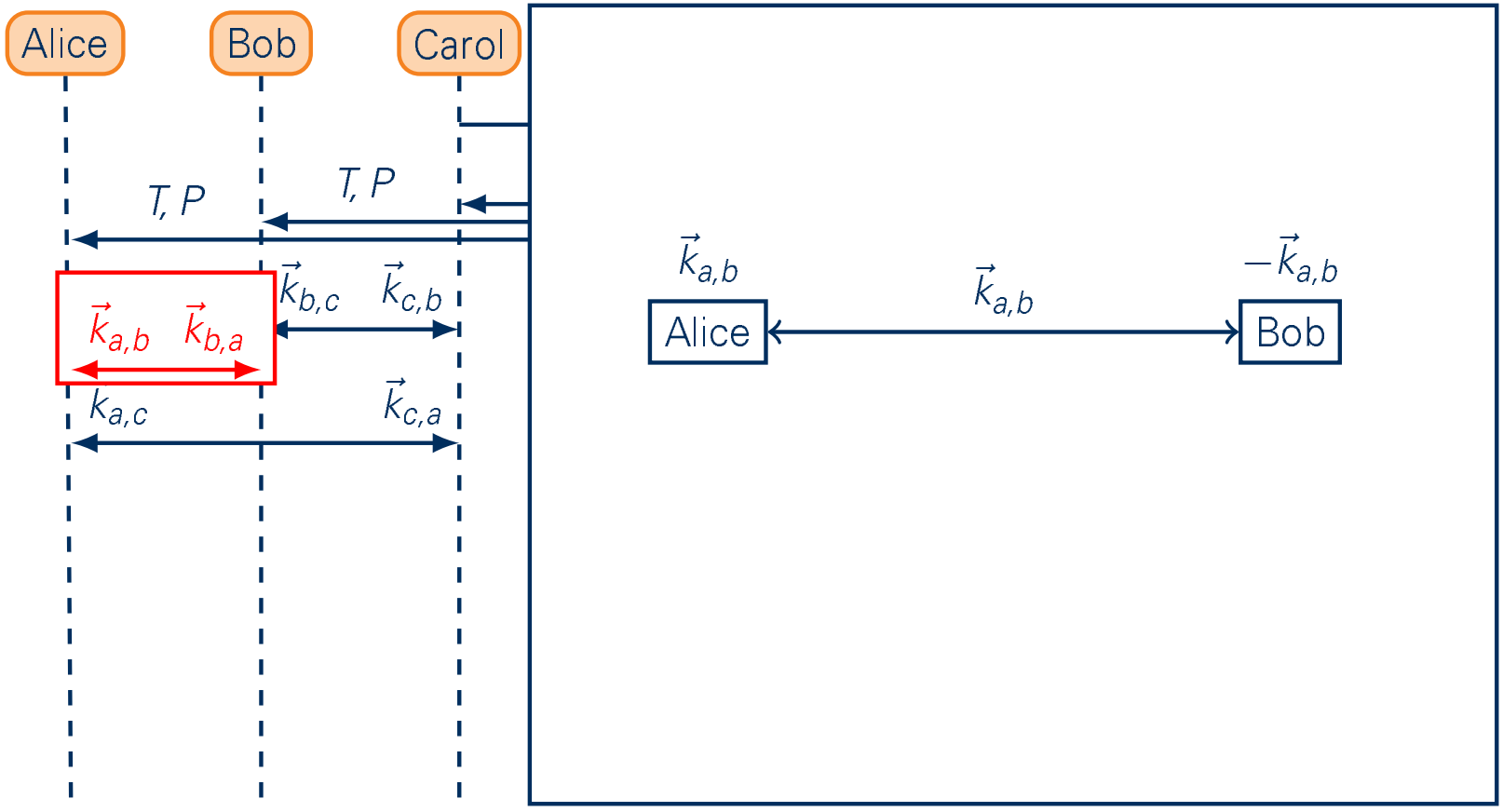
Poll Initialization



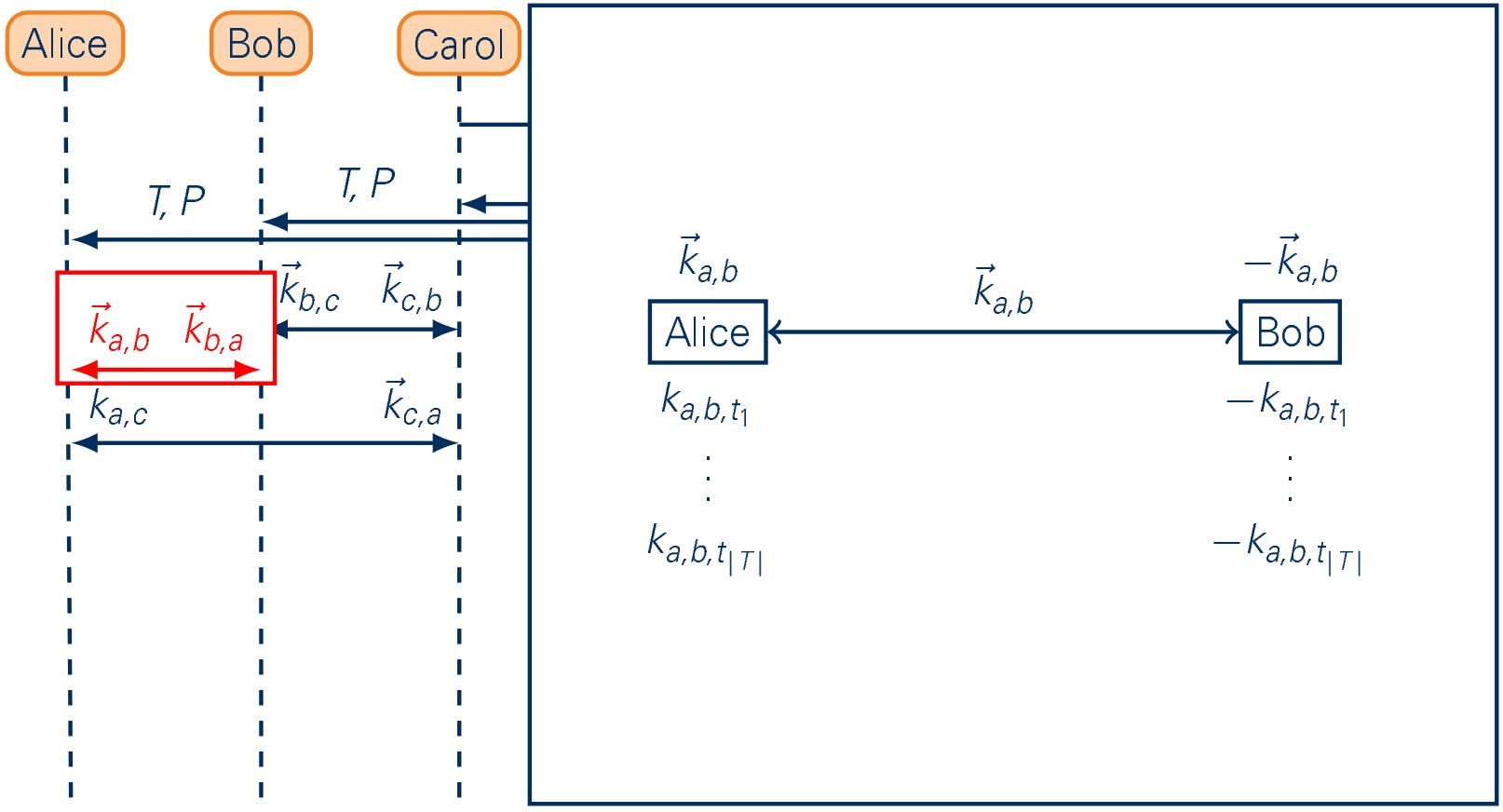
T . . . time slots
P . . . participants

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

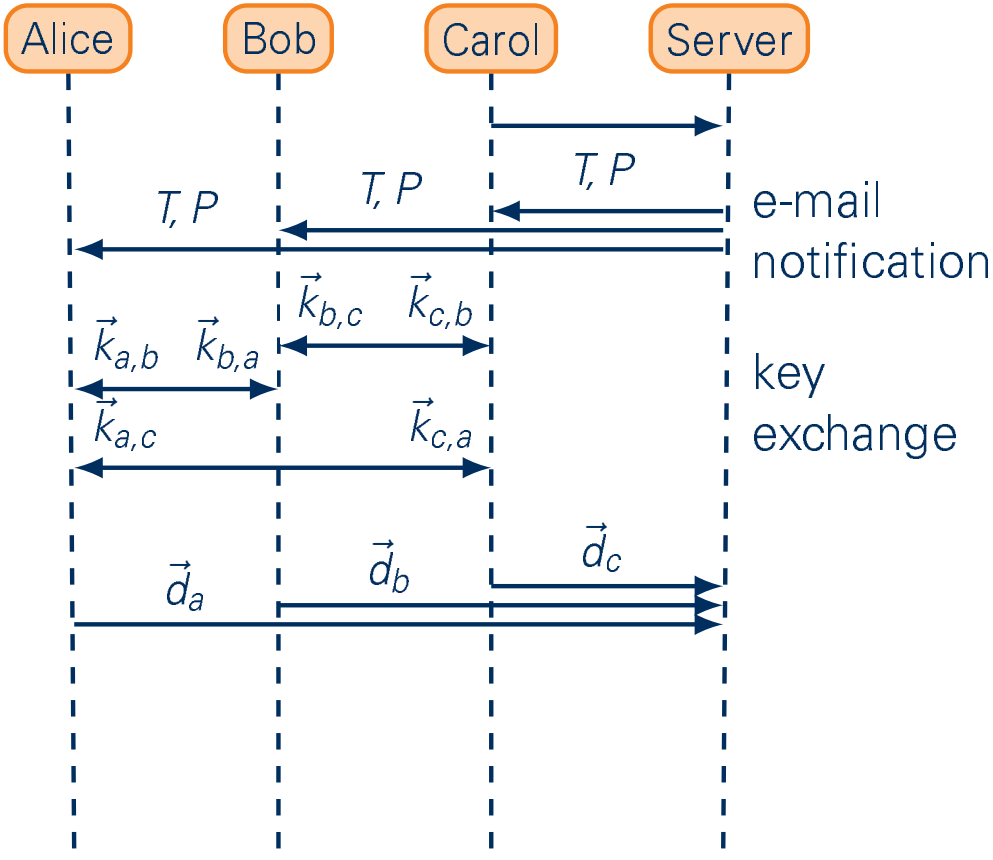
Poll Initialization



Poll Initialization



Casting of Votes

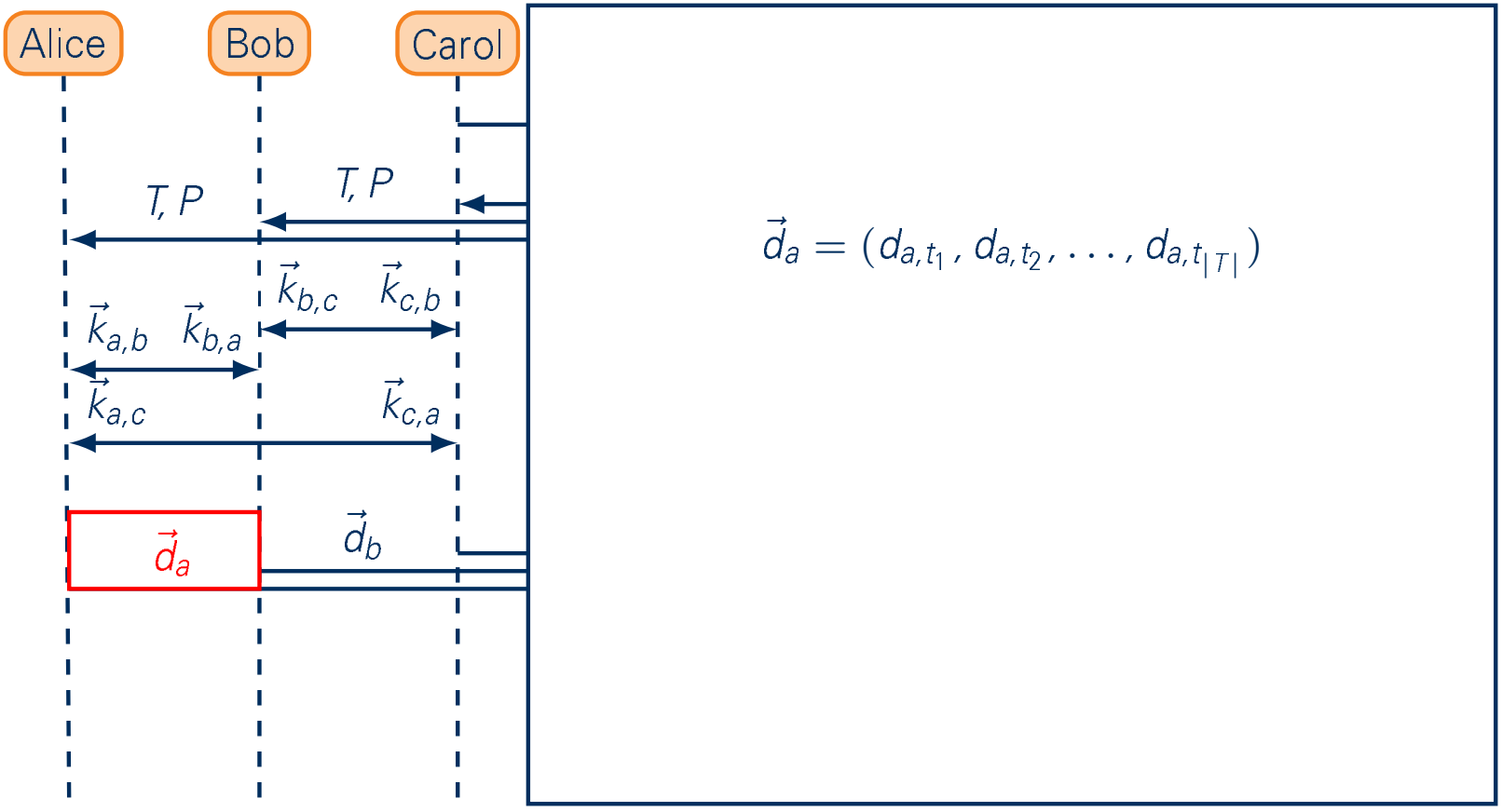


T . . . time slots
P . . . participants

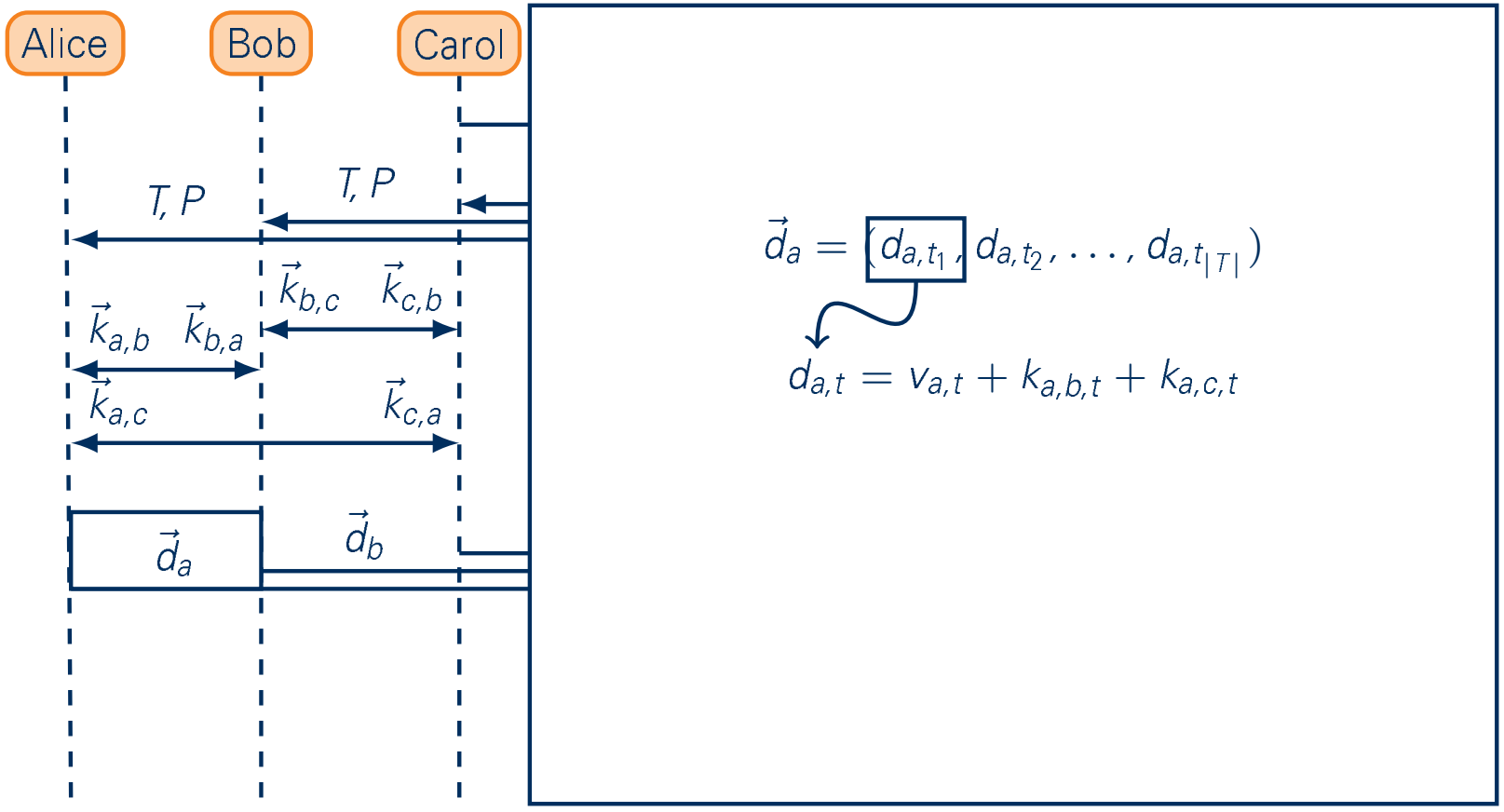
$\vec{k}_{i,j}$ . . . key vector

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

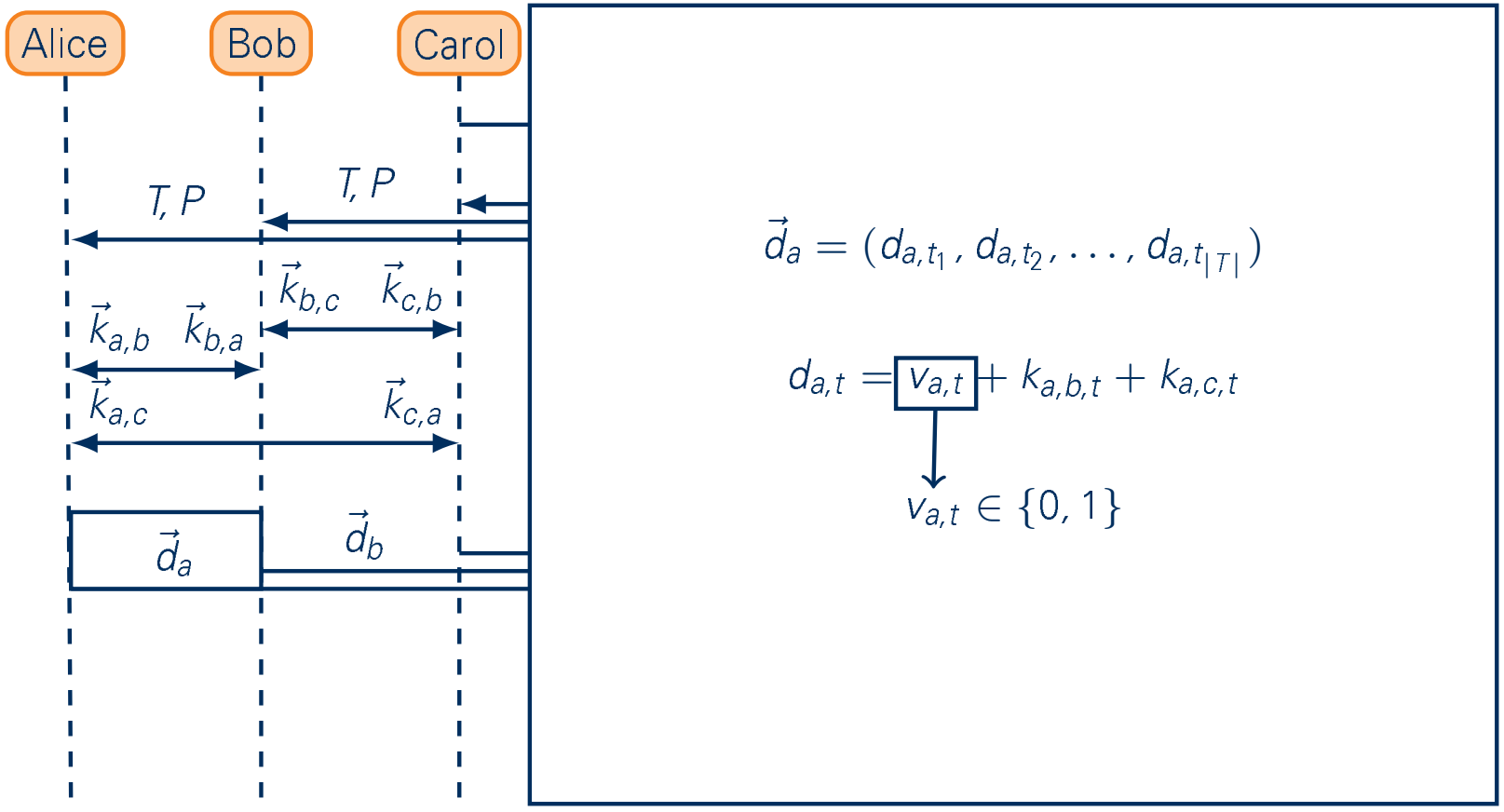
Casting of Votes



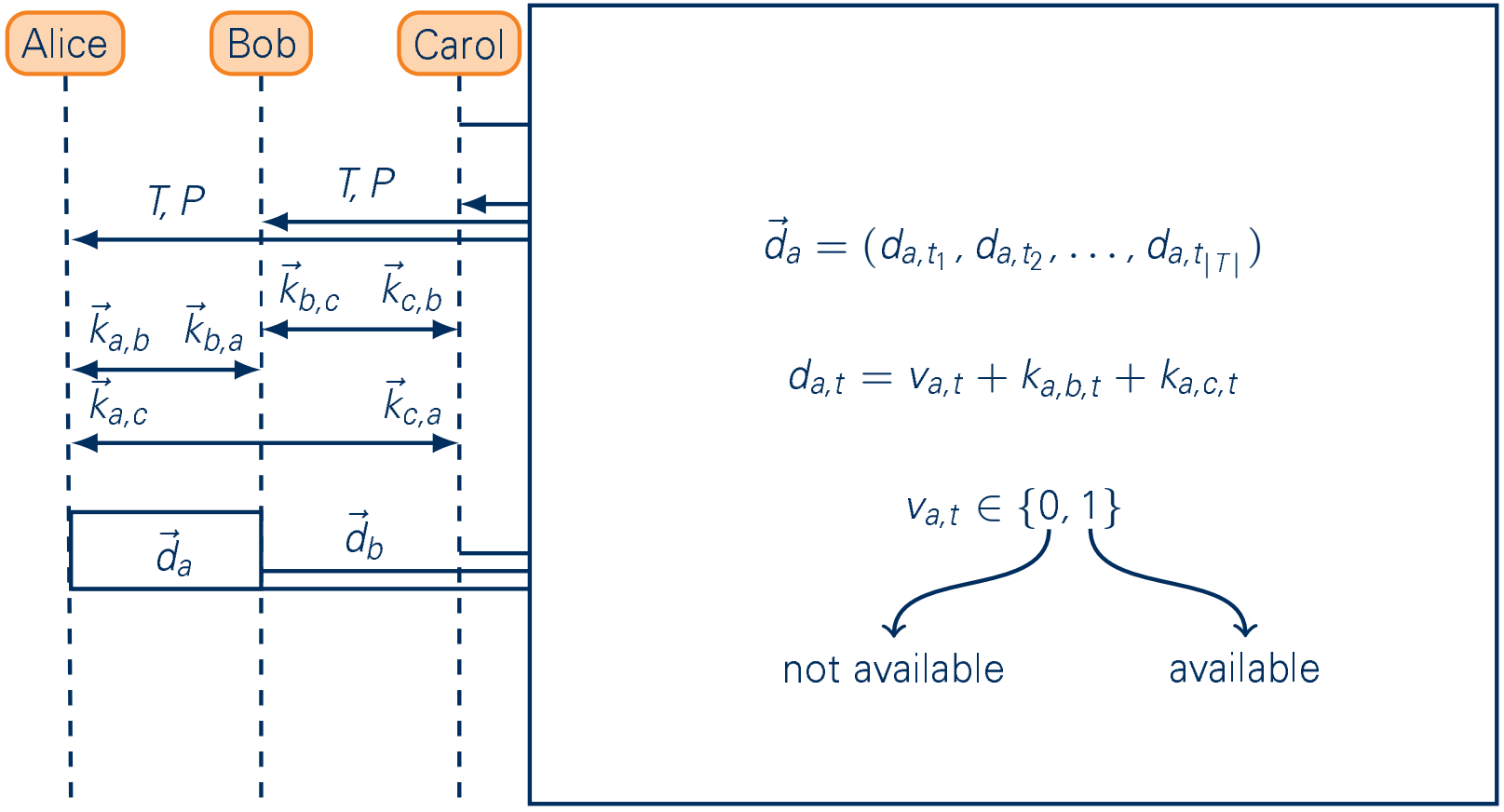
Casting of Votes



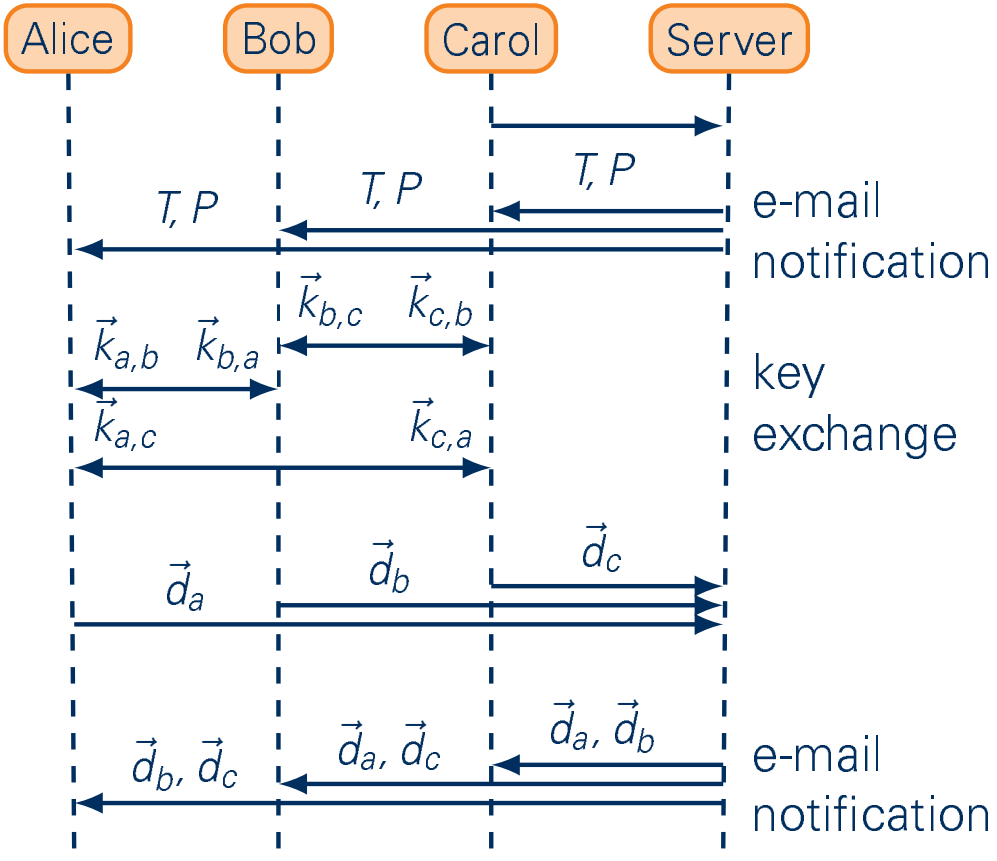
Casting of Votes



Casting of Votes



Result Publication

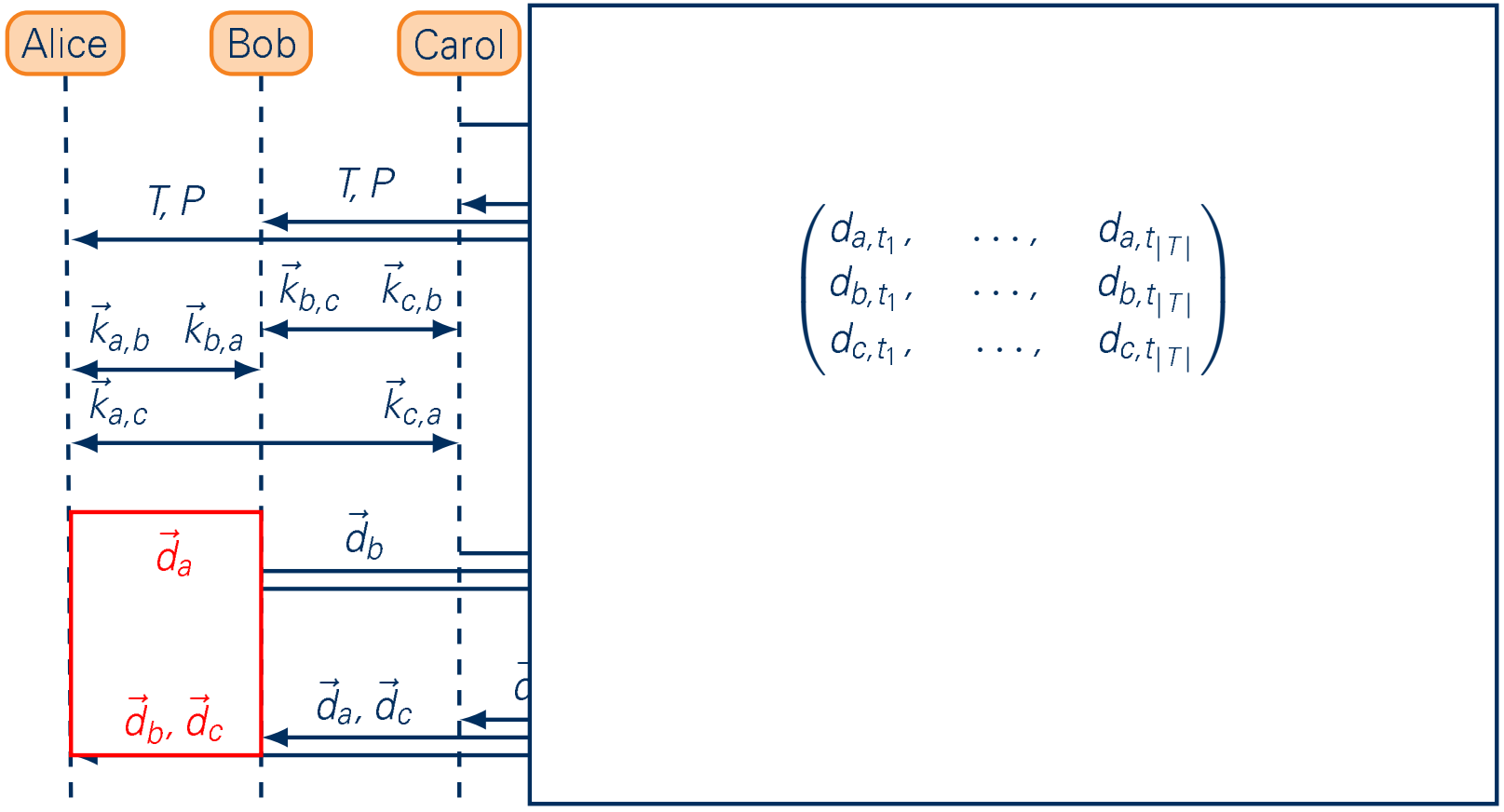


T . . . time slots
P . . . participants

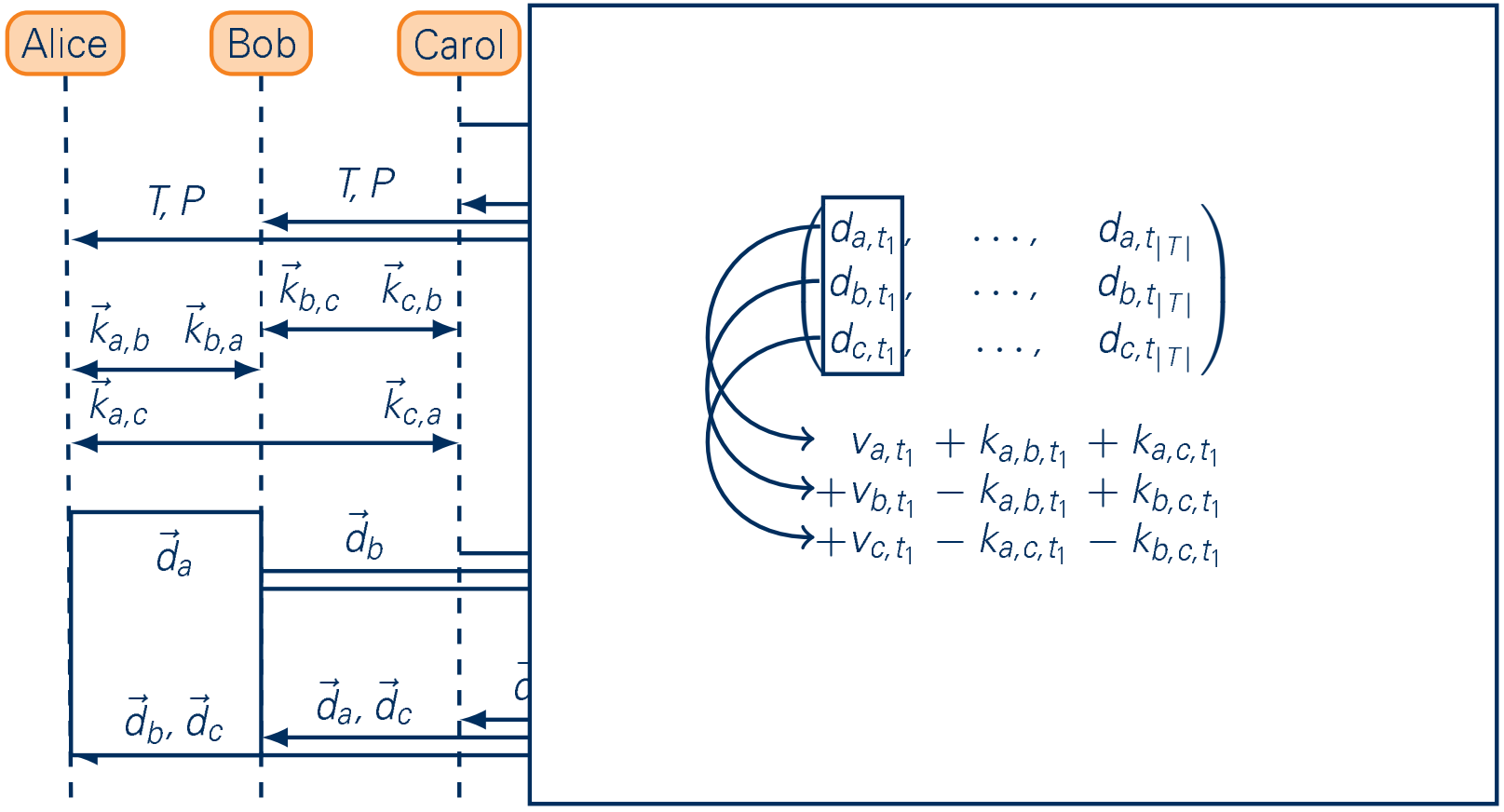
$\vec{k}_{i,j}$ . . . key vector

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

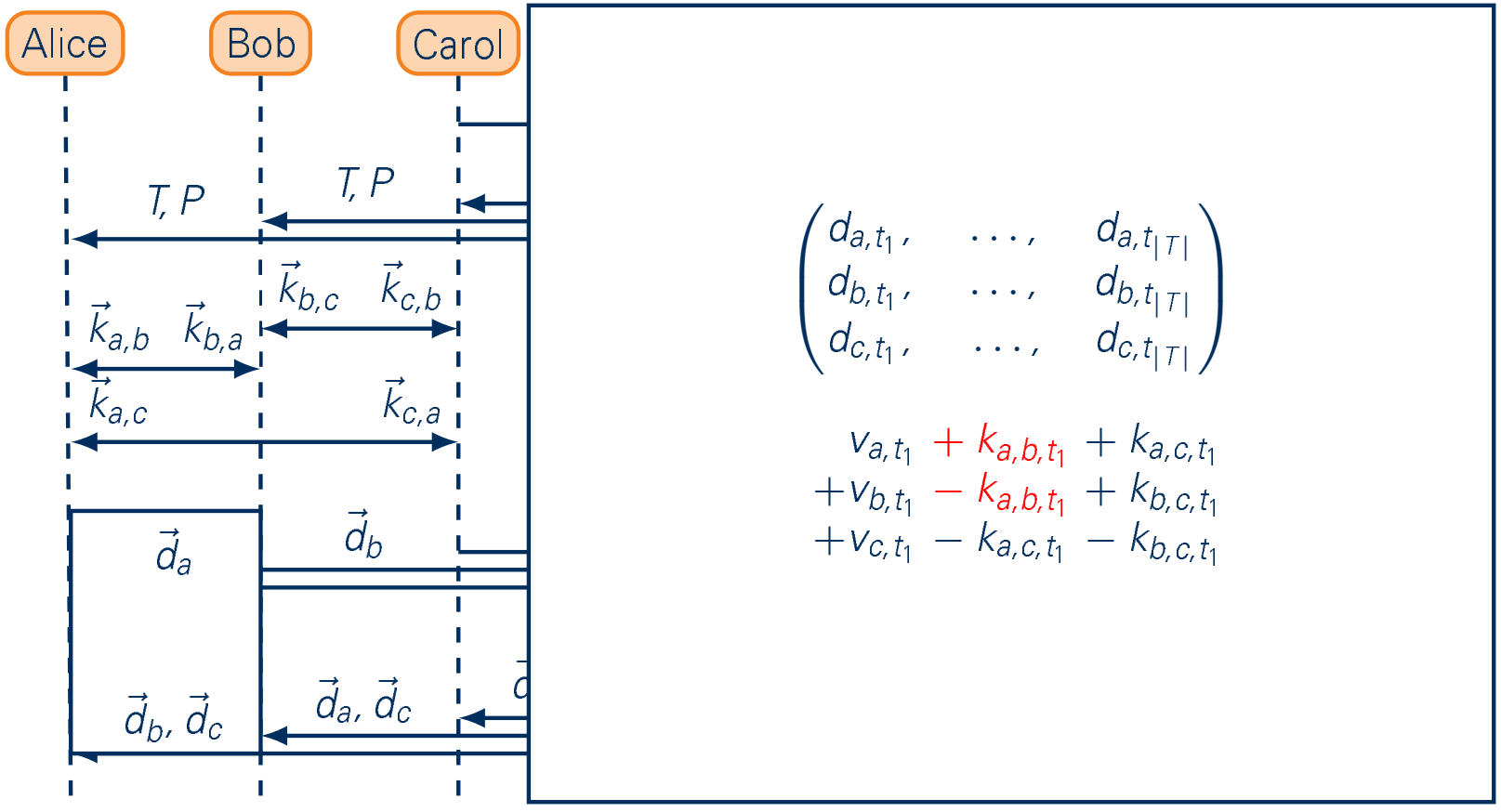
Result Publication



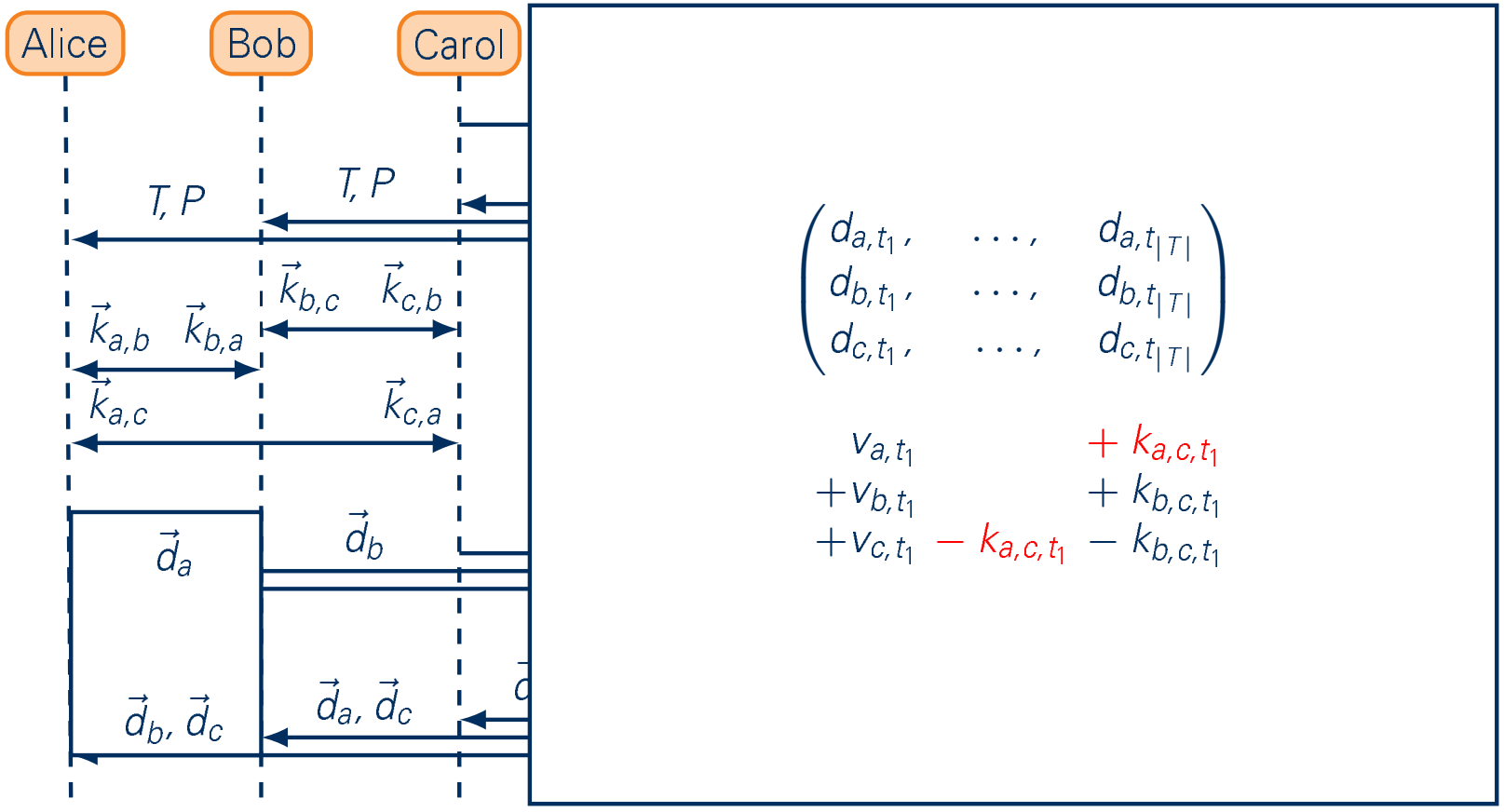
Result Publication



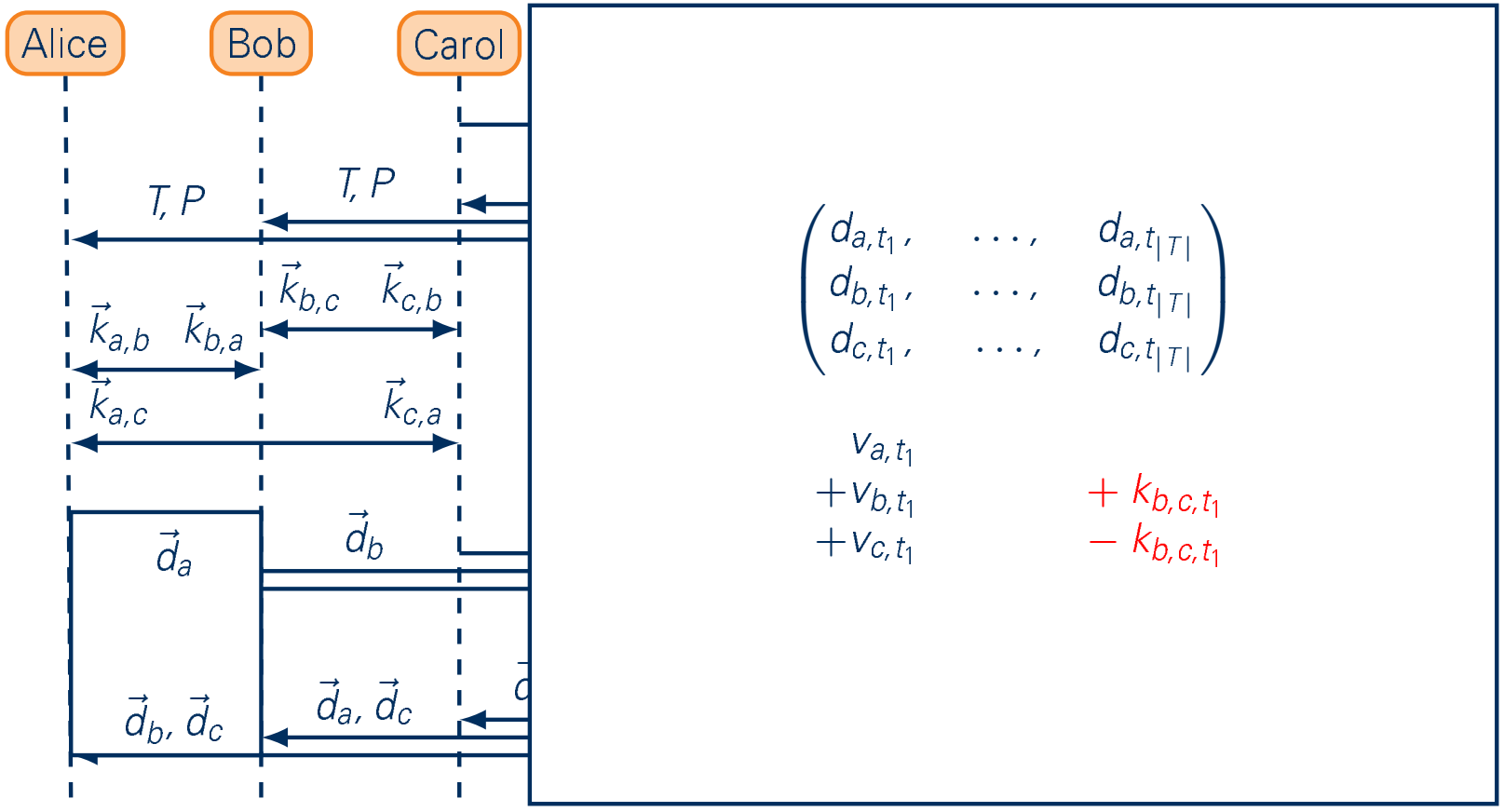
Result Publication



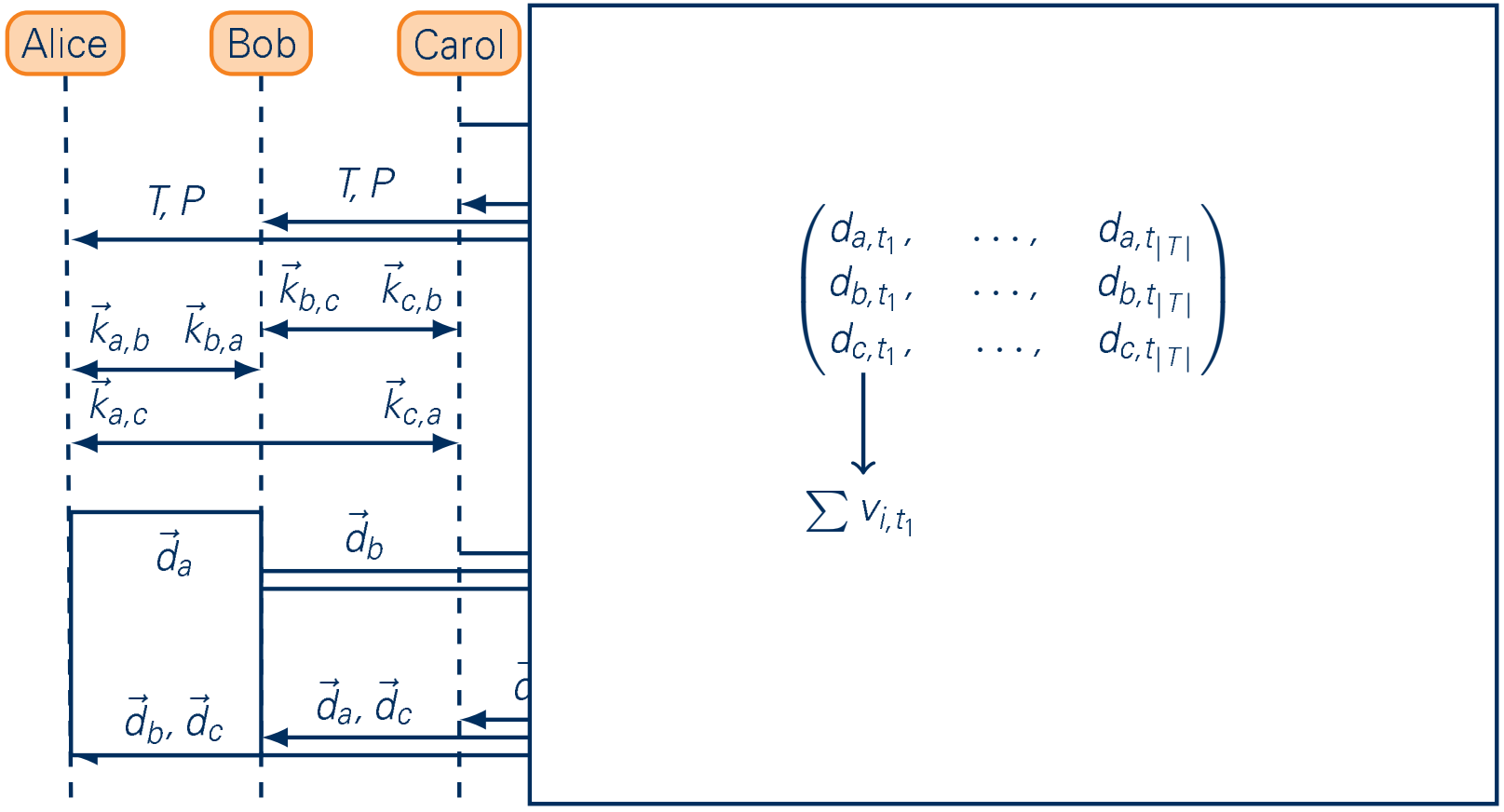
Result Publication



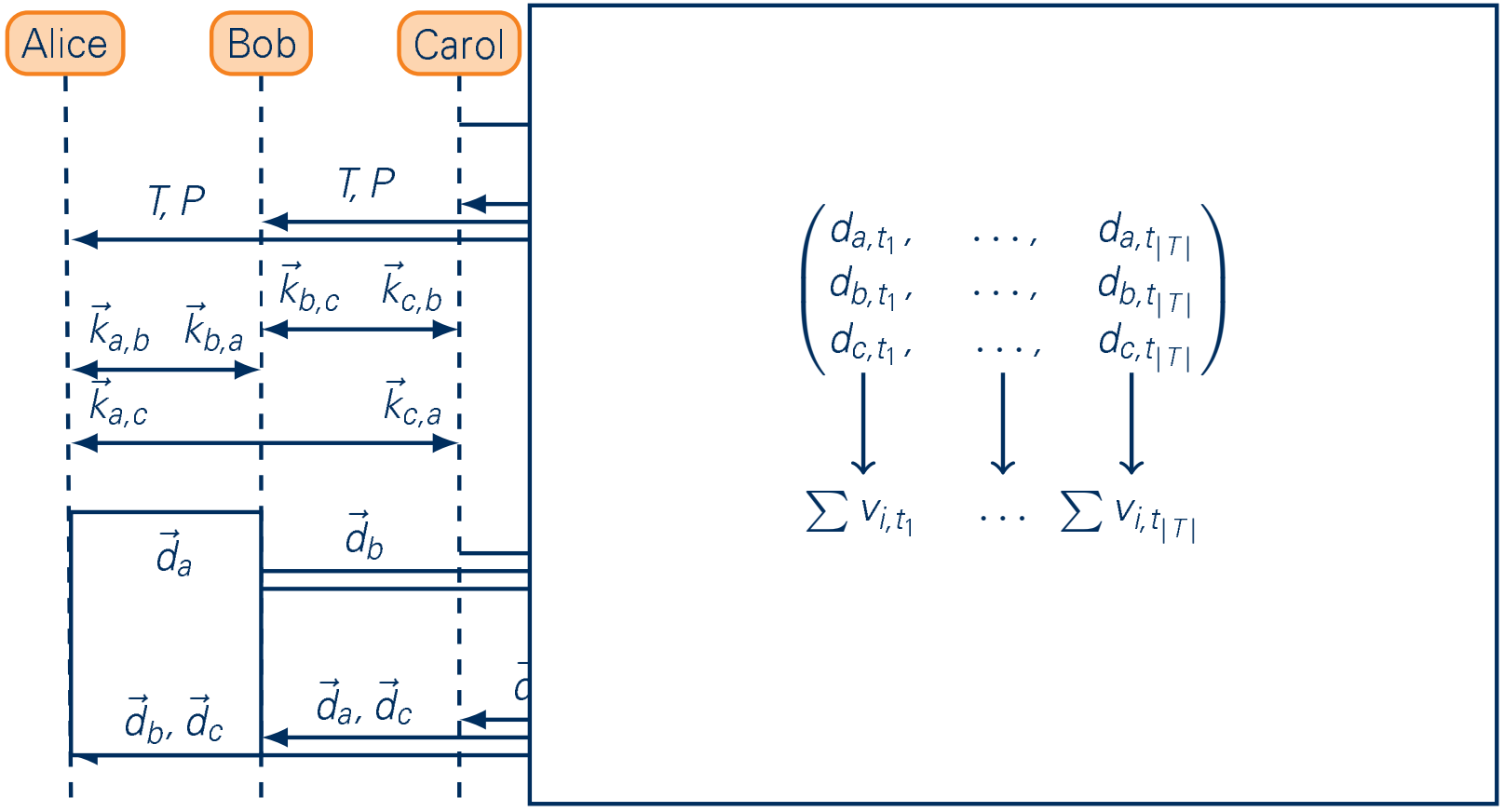
Result Publication



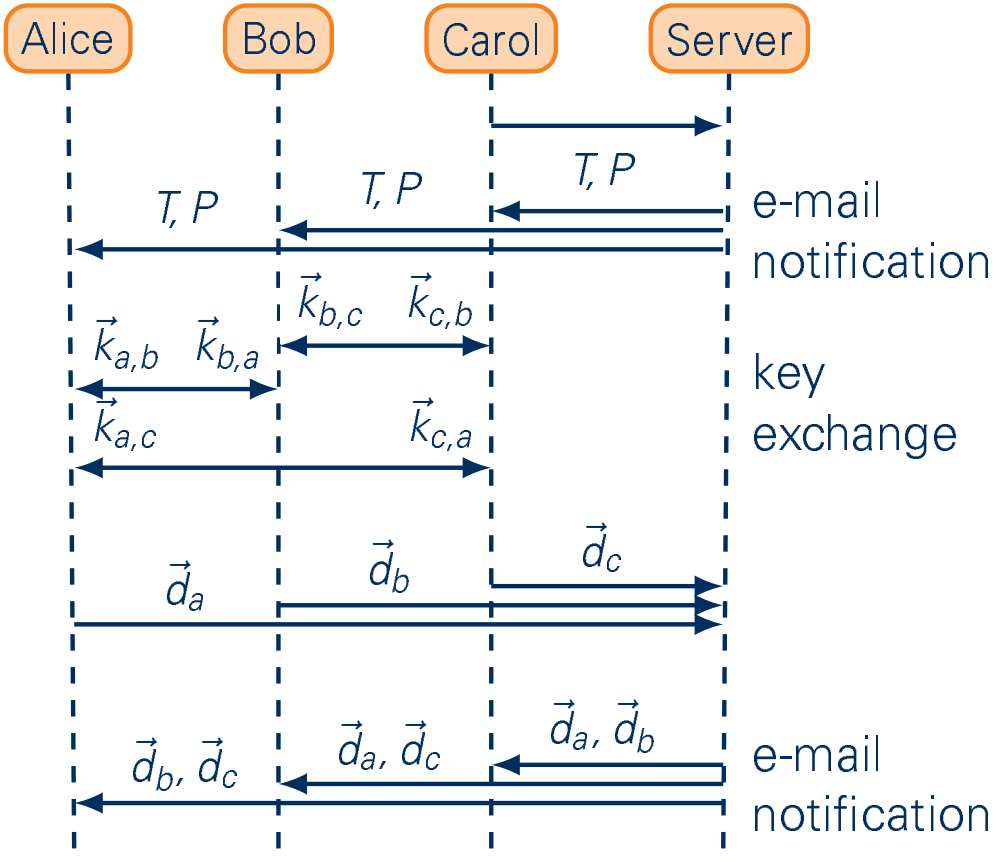
Result Publication



Result Publication



Detect Attackers

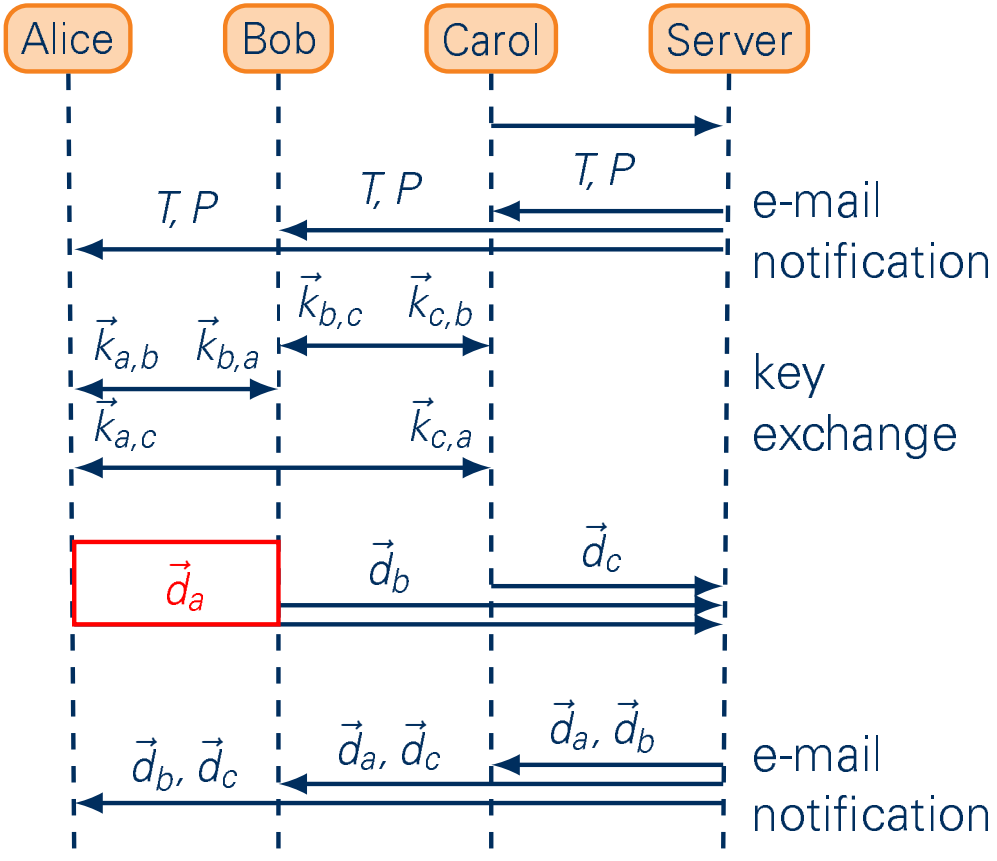


T . . . time slots
P . . . participants

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

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

Detect Attackers

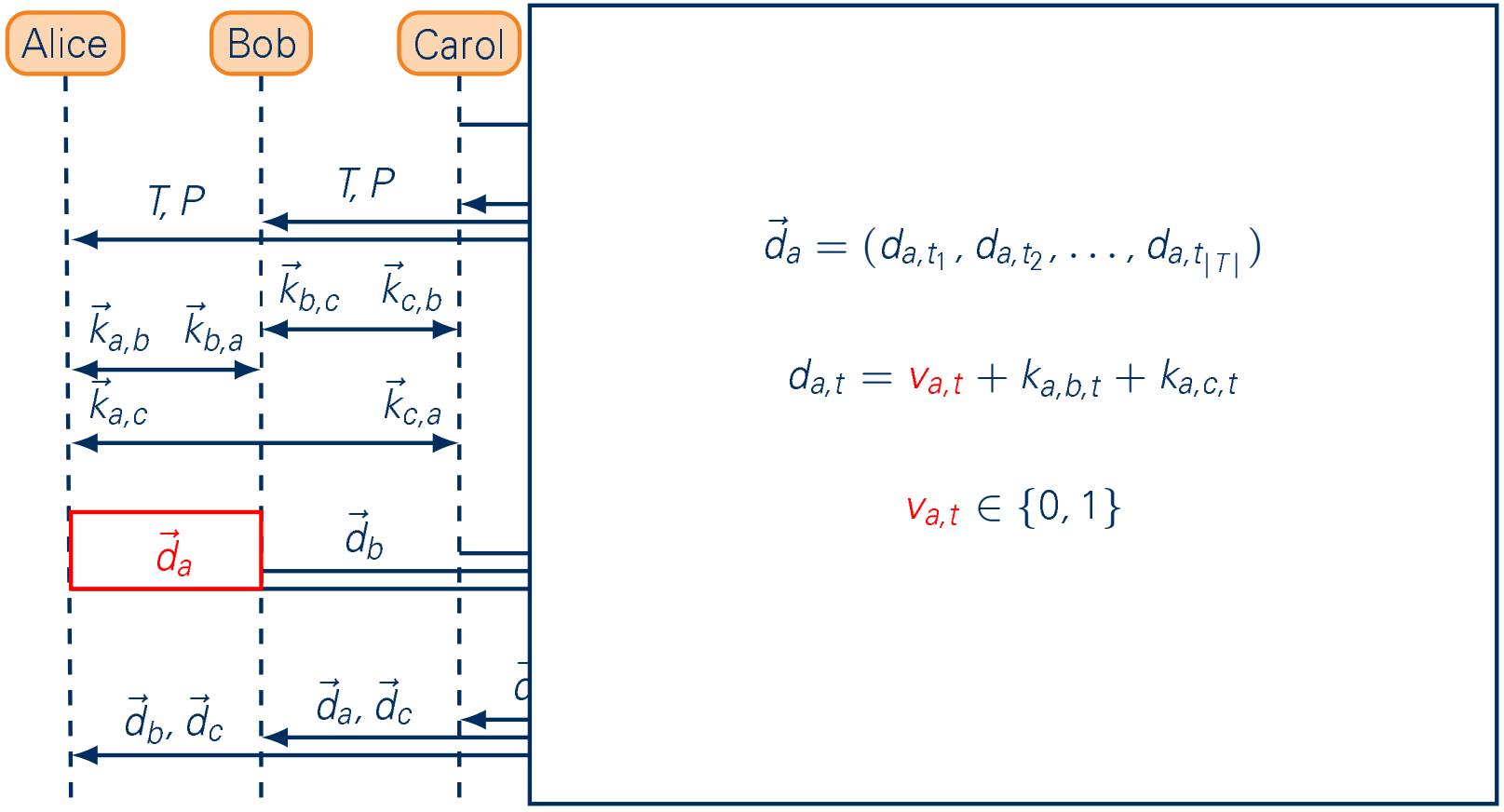


T . . . time slots
P . . . participants

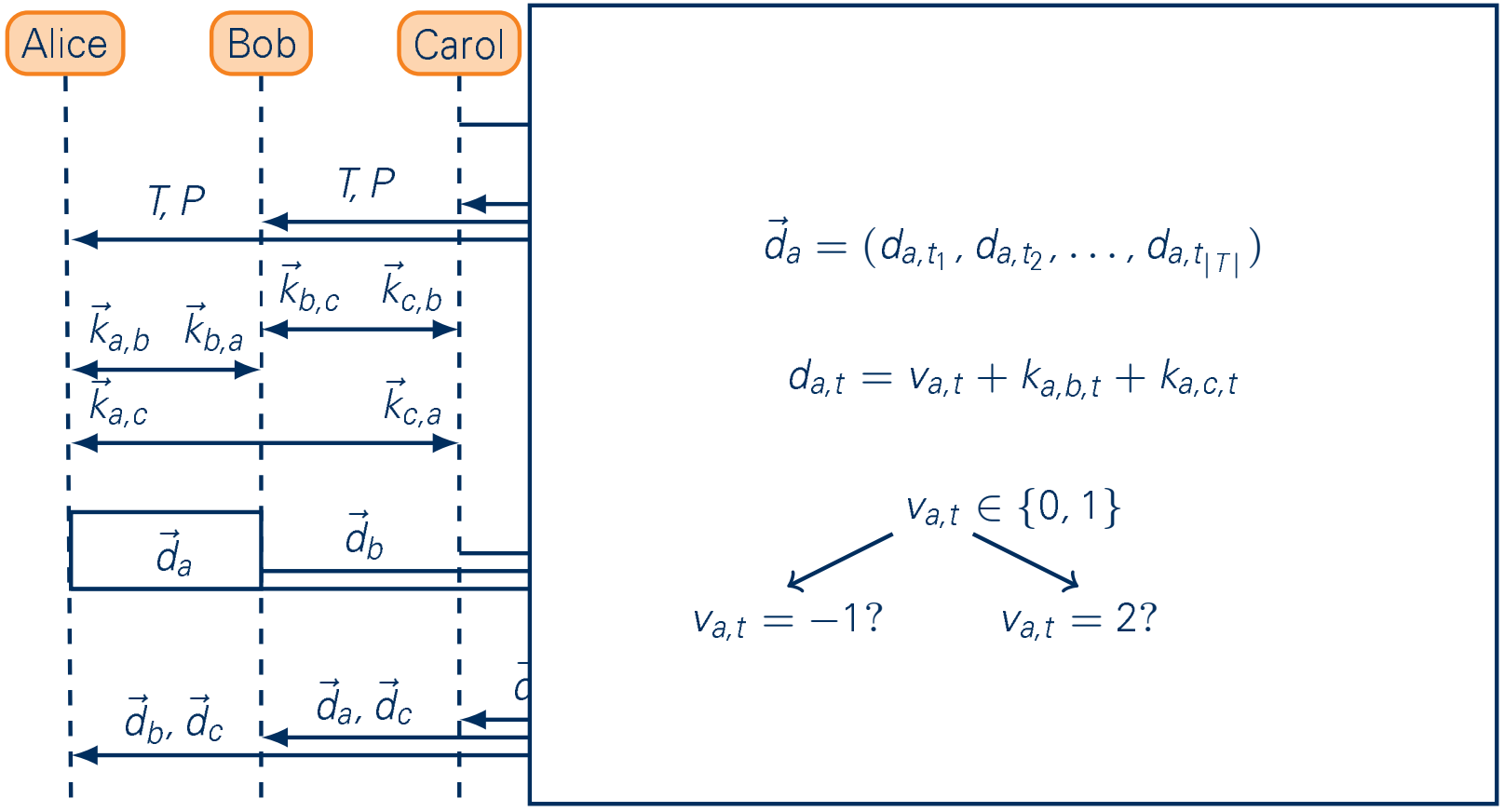
$\vec{k}_{i,j}$ . . . key vector

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

Detect Attackers



Detect Attackers

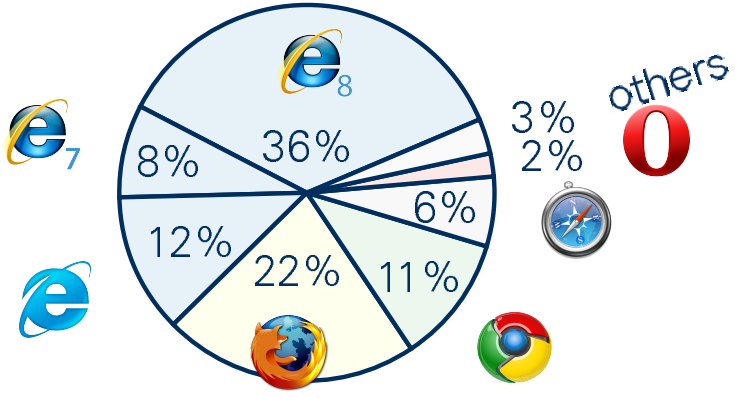


Benchmarks

	 8.0	 7.0	 6.0	 3.6.13	 9.0.597	 5.0.3	 11.01
modPow() – JS-Wu	**4.89 s**	**5.39 s**	**5.49 s**	1.74 s	**0.18 s**	1.49 s	0.52 s
modPow() – JS-Baird	8.46 s	13.43 s	13.56 s	**0.76 s**	0.25 s	**0.25 s**	**0.30 s**
modPow() – Java	0.03 s	0.04 s	0.03 s	0.04 s	0.04 s	0.03 s	0.03 s
1000 × AES256	1.02 s	2.51 s	2.52 s	0.35 s	0.04 s	0.08 s	0.07 s

Benchmarks

	8.0	7.0	6.0	3.6.13	9.0.597	5.0.3	11.01
modPow() – JS-Wu	**4.89 s**	**5.39 s**	**5.49 s**	1.74 s	**0.18 s**	1.49 s	0.52 s
modPow() – JS-Baird	8.46 s	13.43 s	13.56 s	**0.76 s**	0.25 s	**0.25 s**	**0.30 s**
modPow() – Java	0.03 s	0.04 s	0.03 s	0.04 s	0.04 s	0.03 s	0.03 s
1000 × AES256	1.02 s	2.51 s	2.52 s	0.35 s	0.04 s	0.08 s	0.07 s



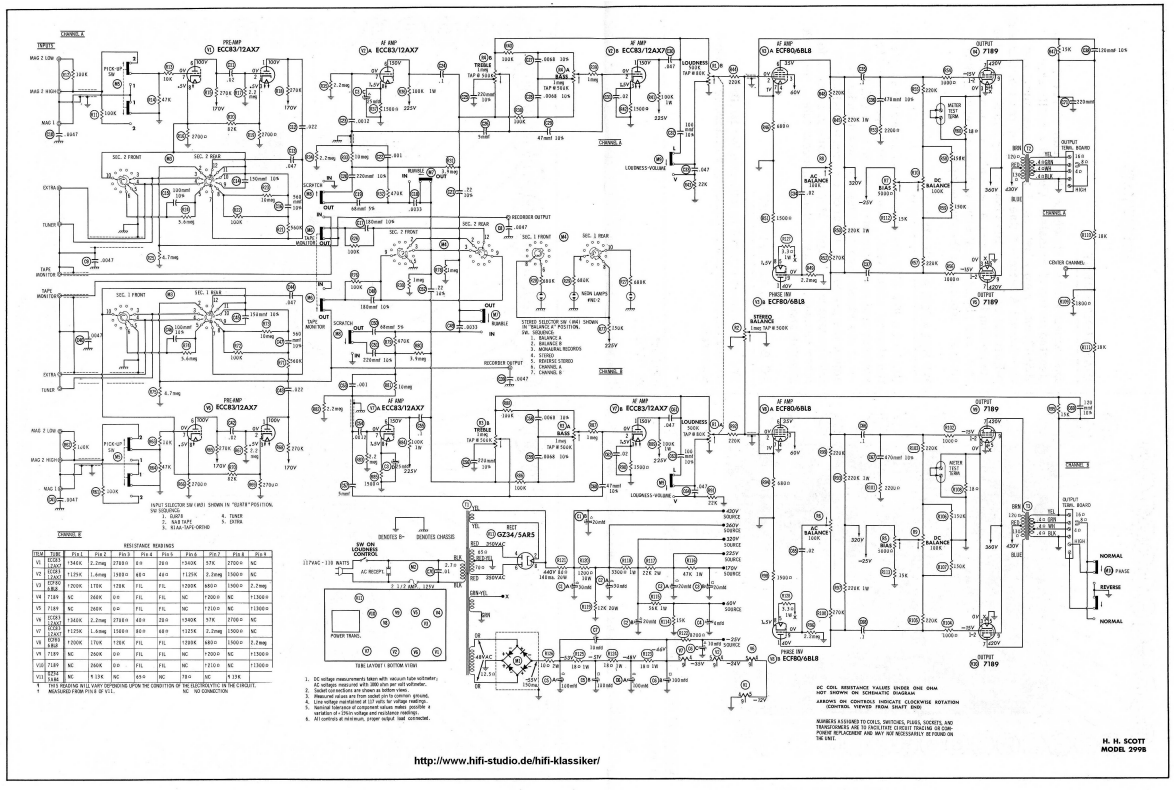
web browser market share (February 2011)

New Scheme

Terminology

The Story so Far. . .

New Scheme



Detect (−1)-Attacks

	t_1	t_2	t_3	t_4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	0	0	1	0
$\sum$	1	2	2	0

Detect (−1)-Attacks

	t_1	t_2	t_3	t_4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	0	0	1	0
$\sum$	1	2	2	0

Detect (−1)-Attacks

	t_1	t_2	t_3	t_4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	0	0	1	0
$\sum$	1	2	2	0

Detect (−1)-Attacks

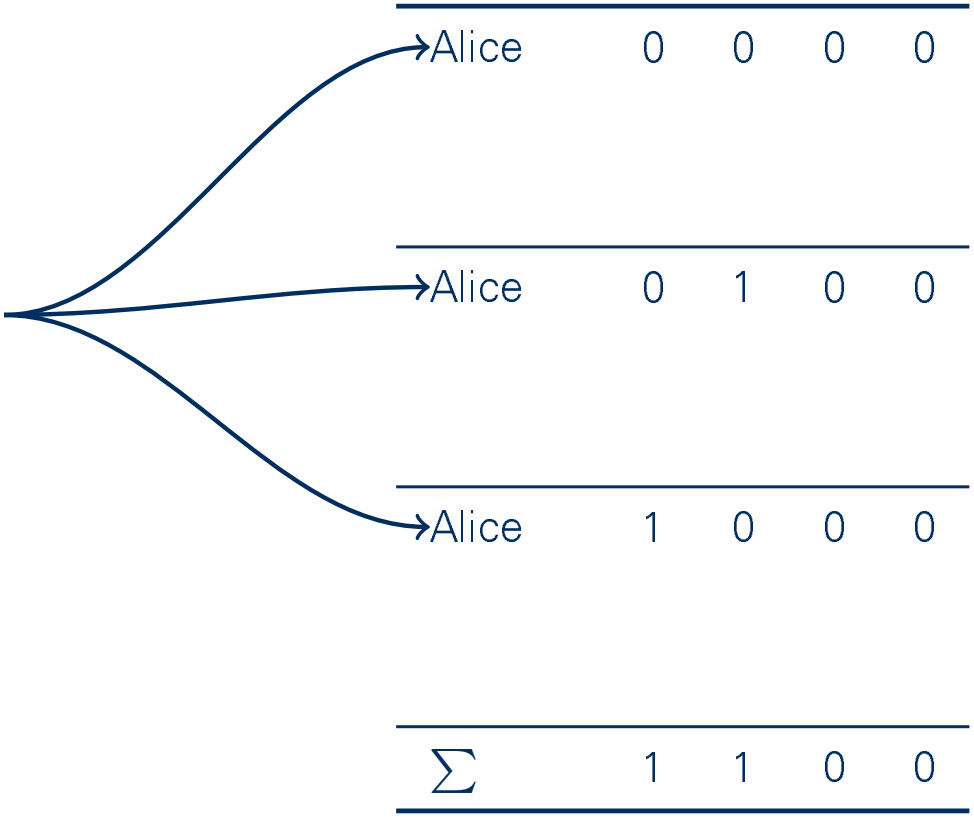
	t_1	t_2	t_3	t_4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	−1	−1	1	−1
$\sum$	0	1	2	−1

Detect (−1)-Attacks

	t_1	t_2	t_3	t_4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	0	−1	1	0
$\sum$	1	1	2	0

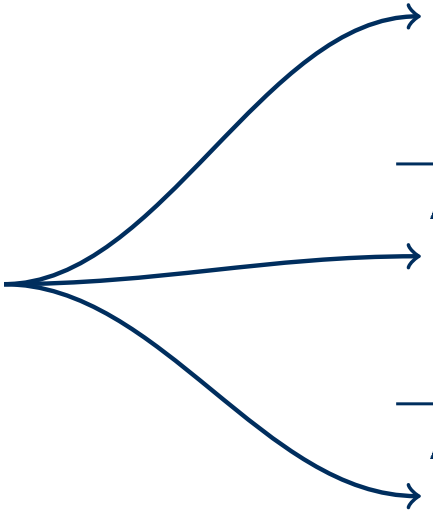
Detect (−1)-Attacks

	t_1	t_2	t_3	t_4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	0	−1	1	0
$\sum$	1	1	2	0



Detect (−1)-Attacks

	t_1	t_2	t_3	t_4
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

Detect (−1)-Attacks

	t_1	t_2	t_3	t_4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	0	−1	1	0
$\sum$	1	1	2	0

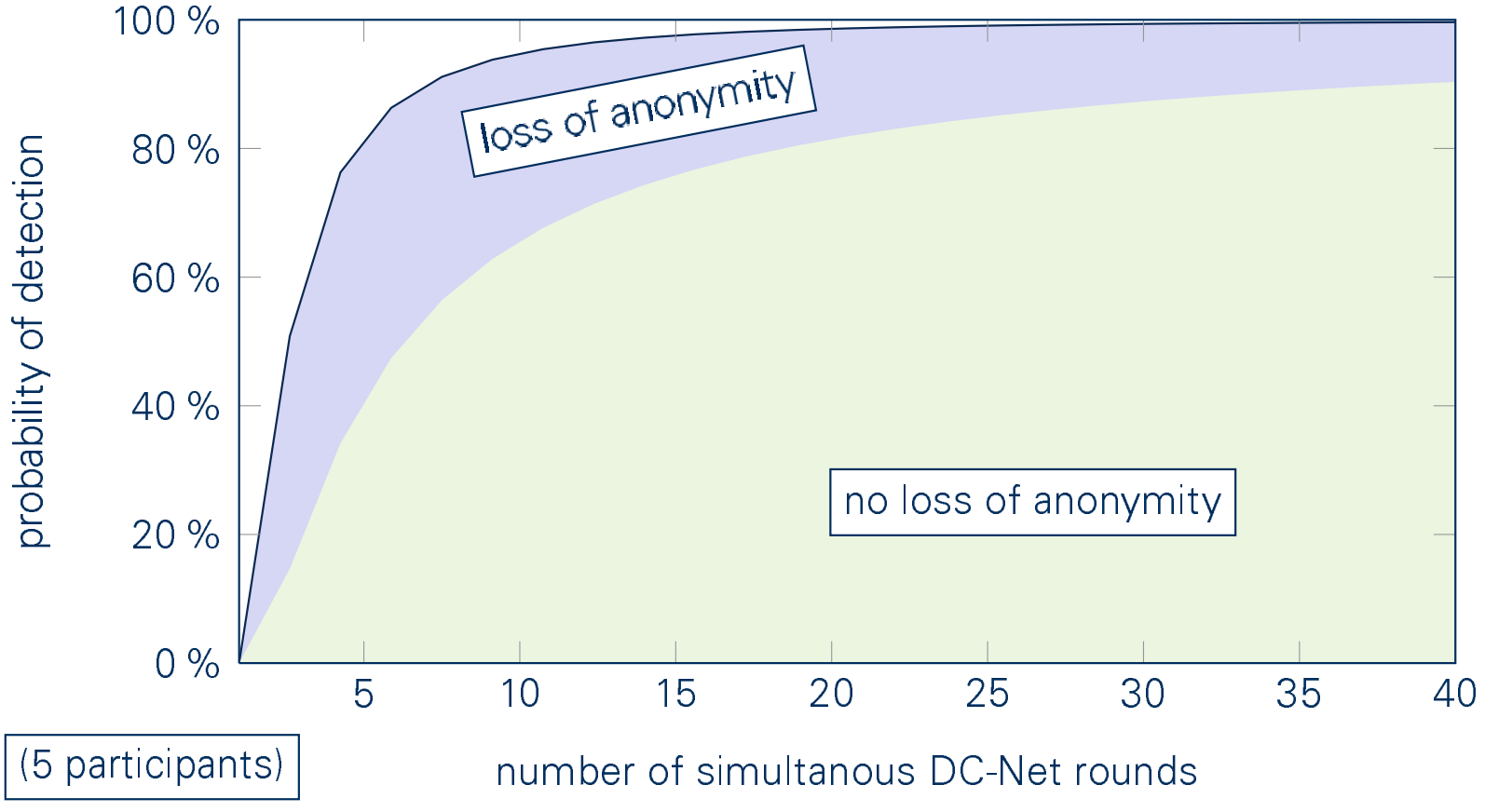
Alice	0	0	0	0
Bob	0	1	0	0
$\sum$		≥ 0?		
Alice	0	1	0	0
Bob	0	0	0	0
$\sum$		≥ 0?		
Alice	1	0	0	0
Bob	0	0	1	0
$\sum$		≥ 0?		
$\sum$	1	2	1	0

Detect (−1)-Attacks

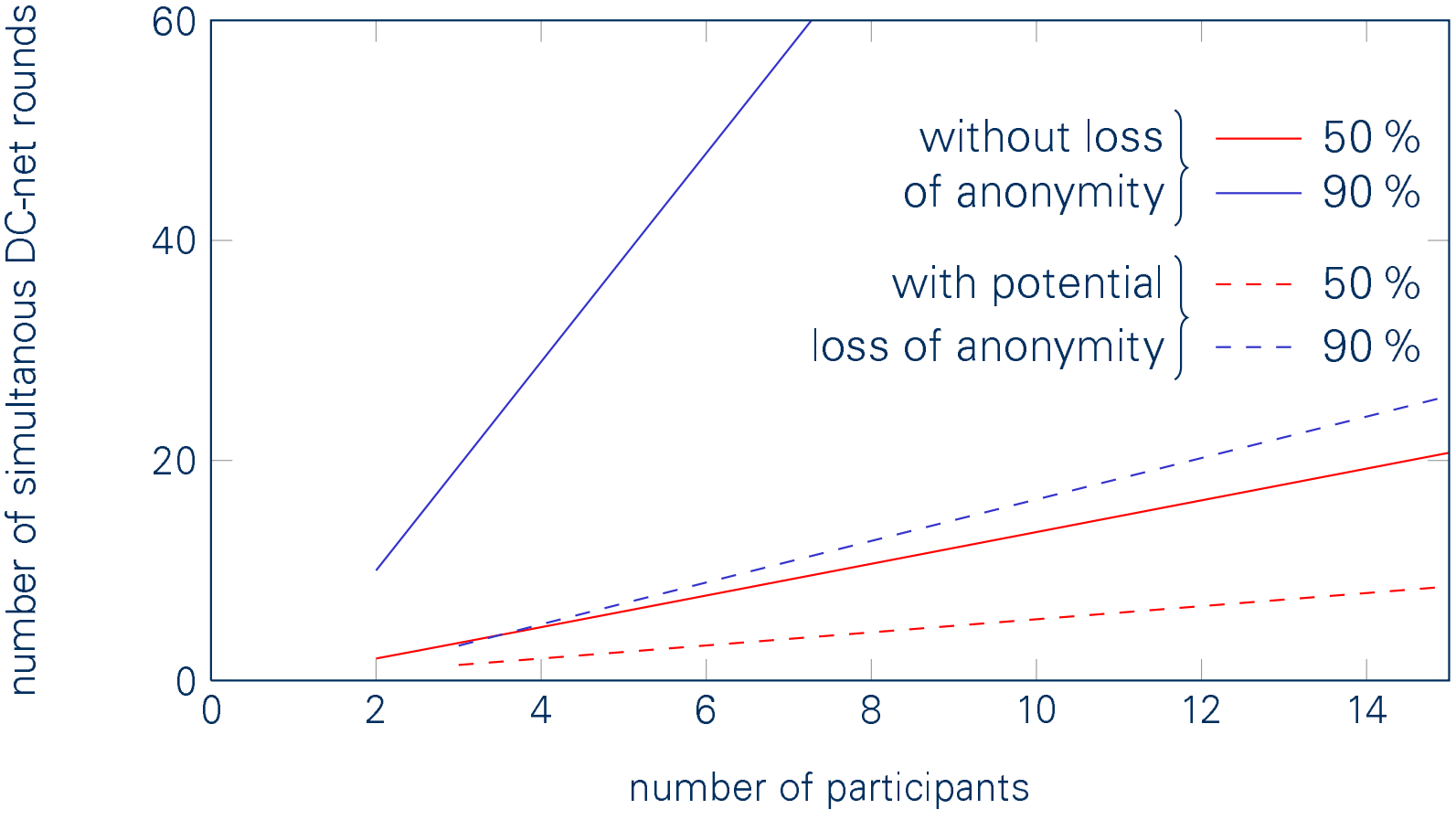
	t_1	t_2	t_3	t_4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	0	−1	1	0
$\sum$	1	1	2	0

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

Probability of Detection



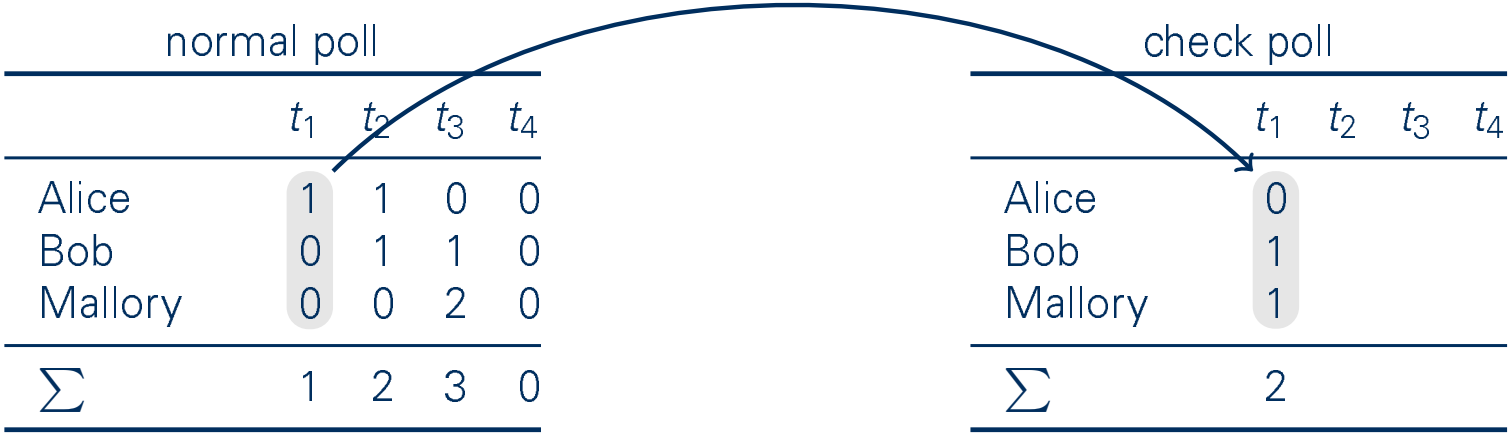
Security Parameter



Detect (+2)-Attacks

	t_1	t_2	t_3	t_4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	0	0	2	0
$\sum$	1	2	3	0

Detect (+2)-Attacks



	t_1	t_2	t_3	t_4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	0	0	2	0
$\sum$	1	2	3	0

	t_1	t_2	t_3	t_4
Alice	0			
Bob	1			
Mallory	1			
$\sum$	2			

Detect (+2)-Attacks

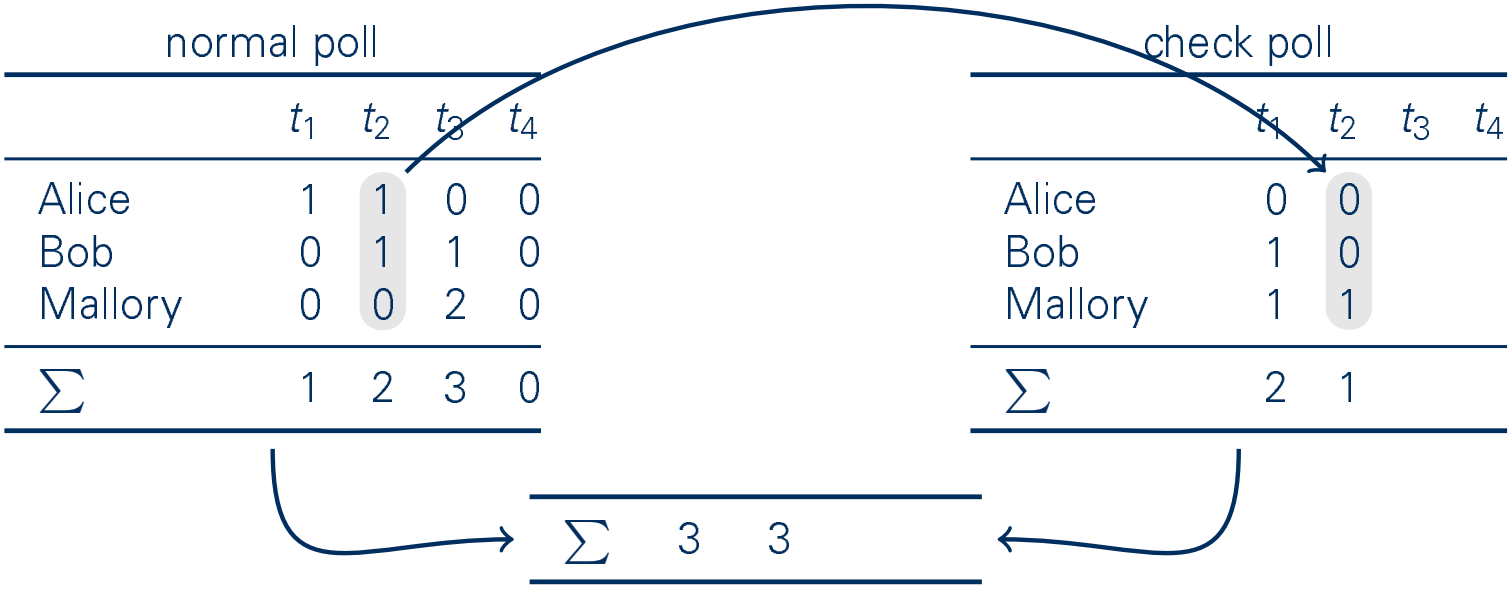
normal poll

	t_1	t_2	t_3	t_4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	0	0	2	0
$\sum$	1	2	3	0

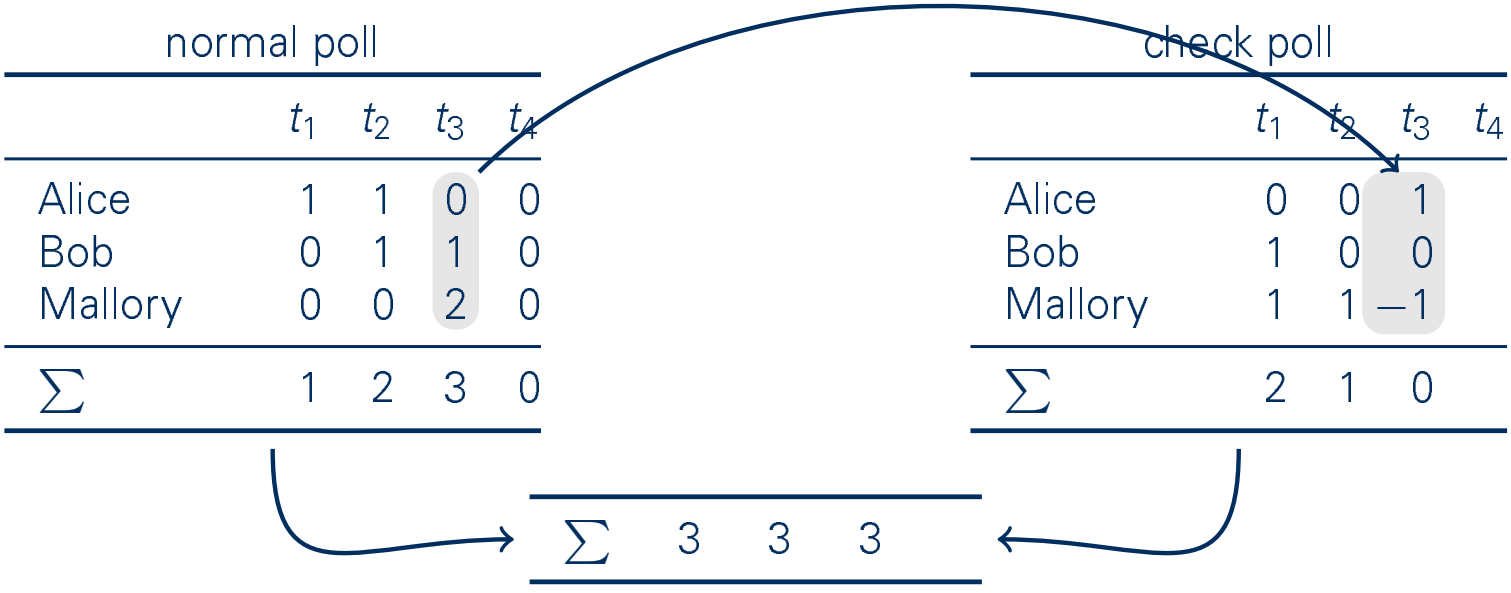
check poll

	t_1	t_2	t_3	t_4
Alice	0			
Bob	1			
Mallory	1			
$\sum$	2			

Detect (+2)-Attacks



Detect (+2)-Attacks



Avoid Attacks on Availability

- attack occured?
  - ➥ identify attacker (reveal keys)
    - ➥ loss of reputation due to small groups

Avoid Attacks on Availability

- attack occured?
  - ➥ identify attacker (reveal keys)
    - ➥ loss of reputation due to small groups
- cheating with keys?
  - ➥ commit to key in vote casting phase

Efficiency

computational complexity

	discrete exp.	symmetric decr.	hash values
original scheme	$\lvert P\rvert - 1$	$\lvert T\rvert \cdot (\lvert P\rvert - 1)$	$\lvert T\rvert \cdot (\lvert P\rvert - 1)$
new scheme	$\lvert P\rvert - 1$	$2 \cdot l \cdot \lvert T\rvert \cdot (\lvert P\rvert - 1)$	$2 \cdot l \cdot \lvert T\rvert \cdot (\lvert P\rvert - 1)$

Efficiency

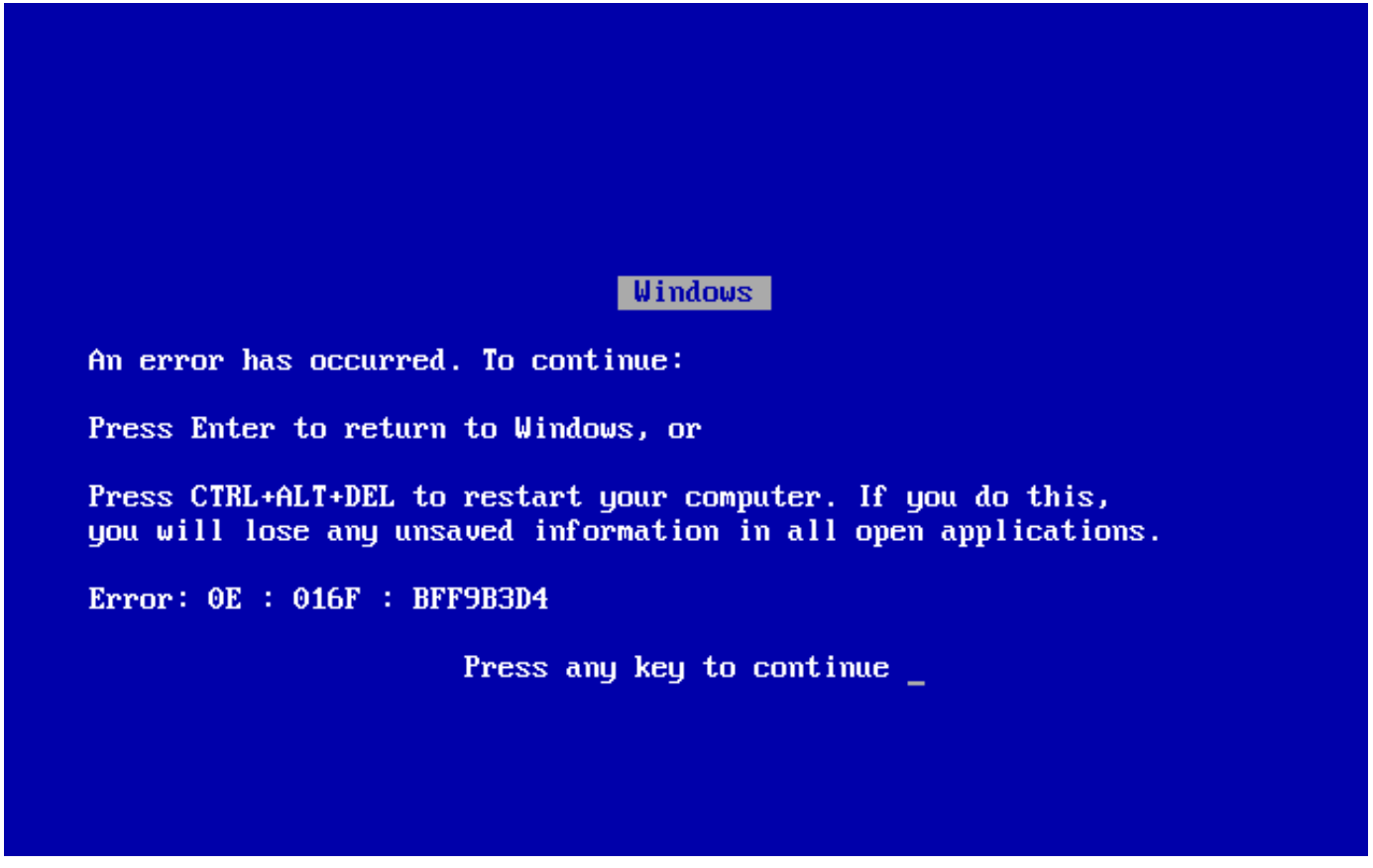
computational complexity

	discrete exp.	symmetric decr.	hash values
original scheme	$\|P\| - 1$	$\|T\| \cdot (\|P\| - 1)$	$\|T\| \cdot (\|P\| - 1)$
new scheme	$\|P\| - 1$	$2 \cdot l \cdot \|T\| \cdot (\|P\| - 1)$	$2 \cdot l \cdot \|T\| \cdot (\|P\| - 1)$

measurements

$\|P\|=5$, $\|T\|=20$, $l=20$	8.0.6001	3.6.12	5.0.3	10.63	8.0.552	Firefox 4.0b2
AES-128+SHA-256	18.4 s	7.7 s	2.9 s	1.4 s	2.8 s	31.7 s
DH (1024 bit)	15.0 s	11.7 s	8.2 s	2.0 s	2.5 s	40.5 s
total	37.6 s	22.5 s	13.5 s	4.3 s	6.3 s	84.2 s

Demo


Windows
An error has occurred. To continue:
Press Enter to return to Windows, or
Press CTRL+ALT+DEL to restart your computer. If you do this,
you will lose any unsaved information in all open applications.
Error: 0E : 016F : BFF9B3D4
Press any key to continue _

Conclusion and Outlook

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

- ☐ Trusted JavaScript
- ☐ Formal proof of correctness
- ☐ More usability tests
  - ➠ Problem of understanding "keys"
- ☐ meet.me@Doodle, appointment-slot@google, tungle.me

TECHNISCHE UNIVERSITÄT DRESDEN

PrimeLife

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

Discussion

`https://dudle.inf.tu-dresden.de`

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

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

Lucerne, June 08, 2011

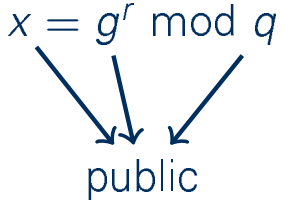
Diffie–Hellman Key Agreement

Discrete Logarithm assumption

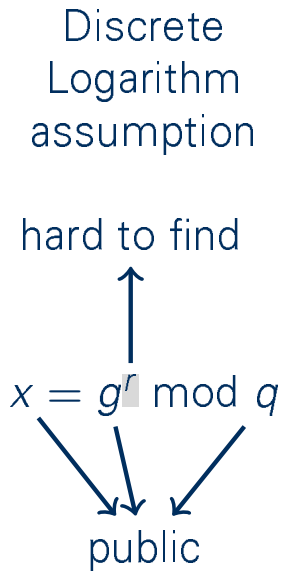
$x = g^r \bmod q$

Diffie–Hellman Key Agreement

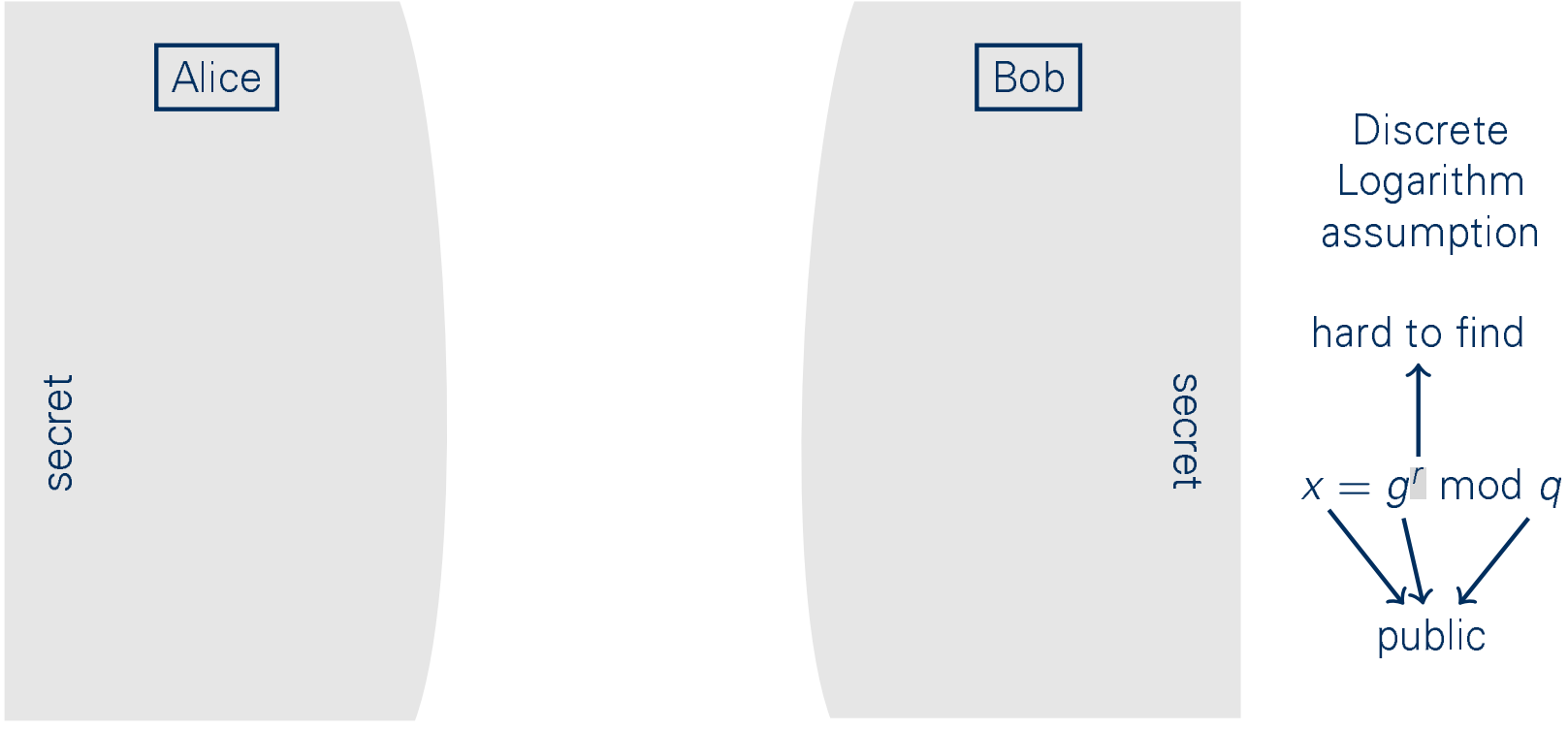
Discrete Logarithm assumption



Diffie–Hellman Key Agreement

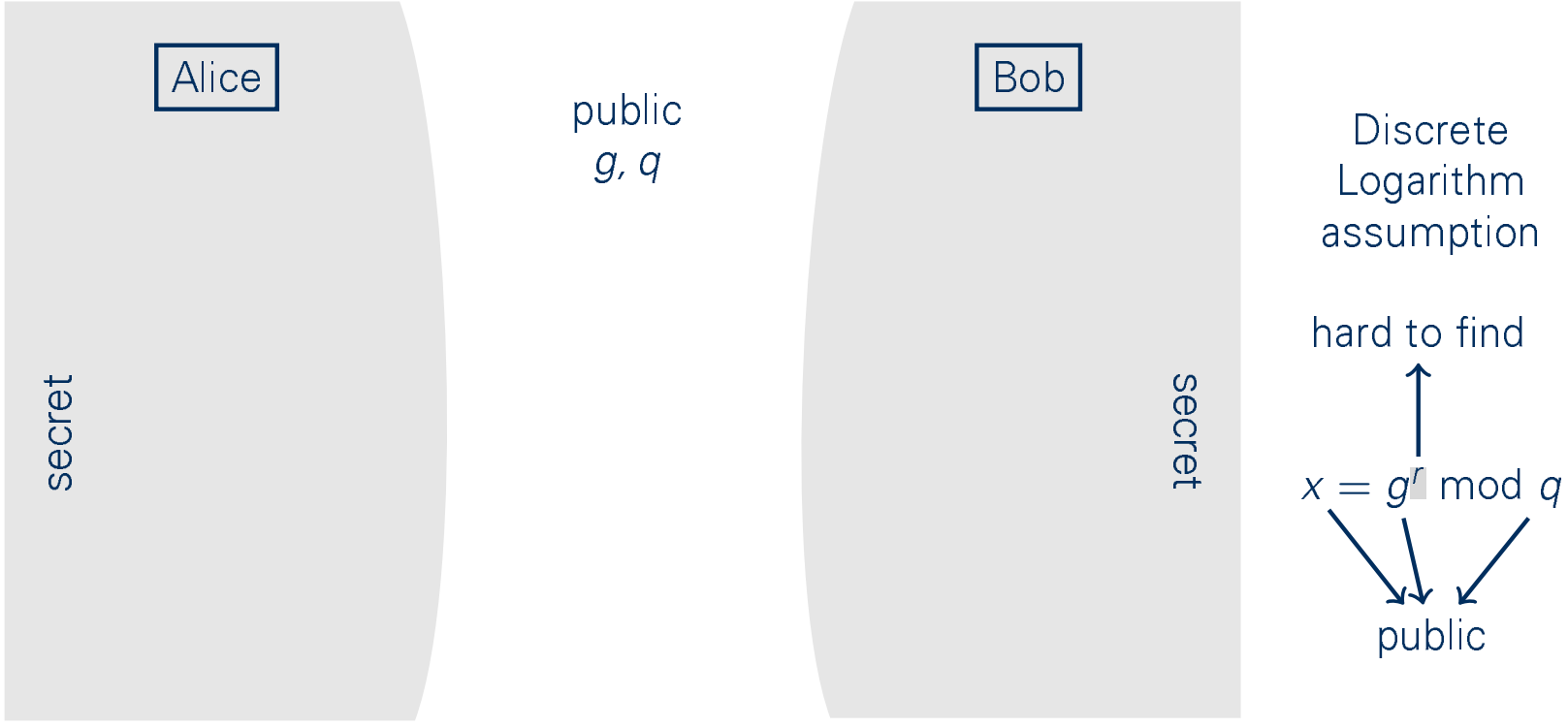


Diffie–Hellman Key Agreement



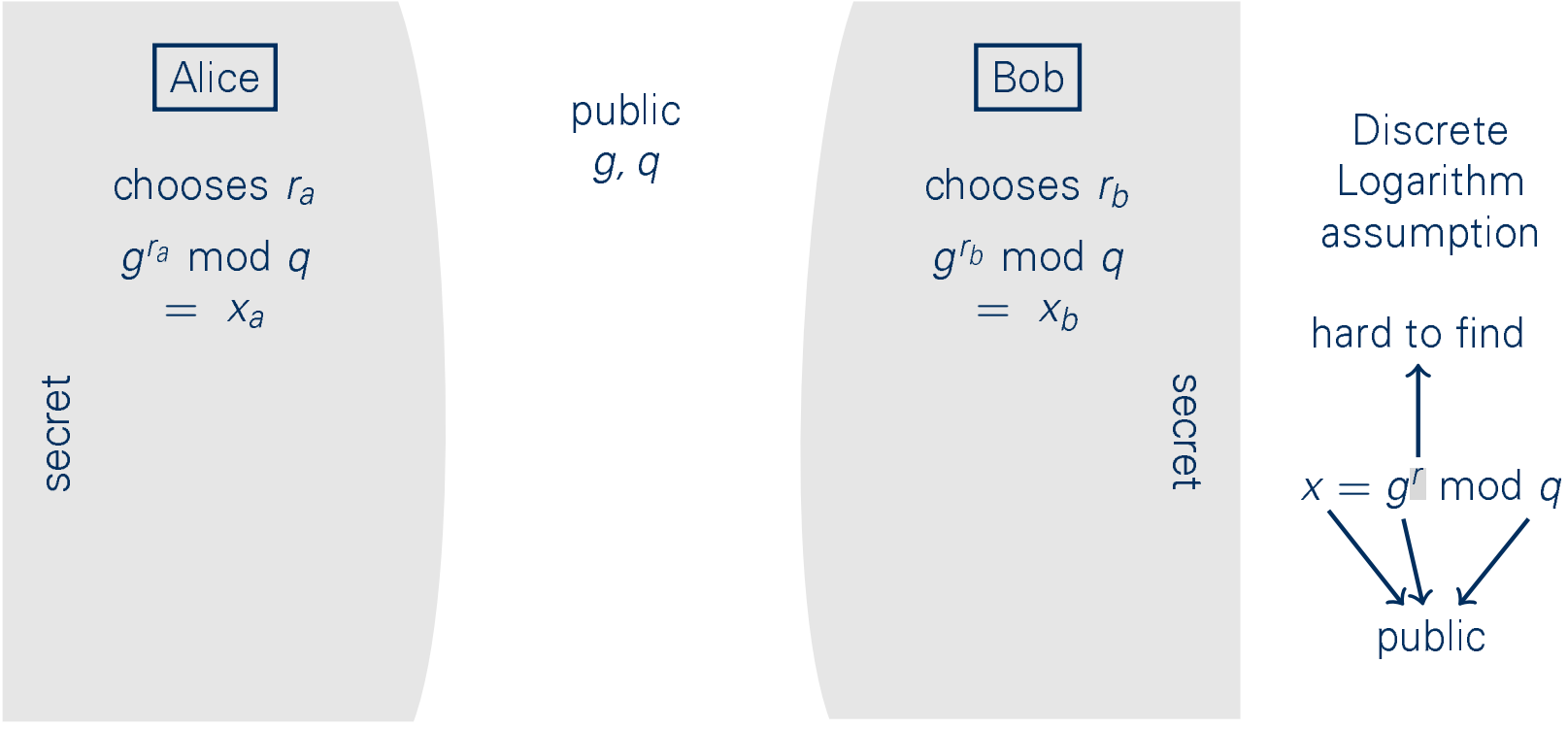
W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

Diffie–Hellman Key Agreement



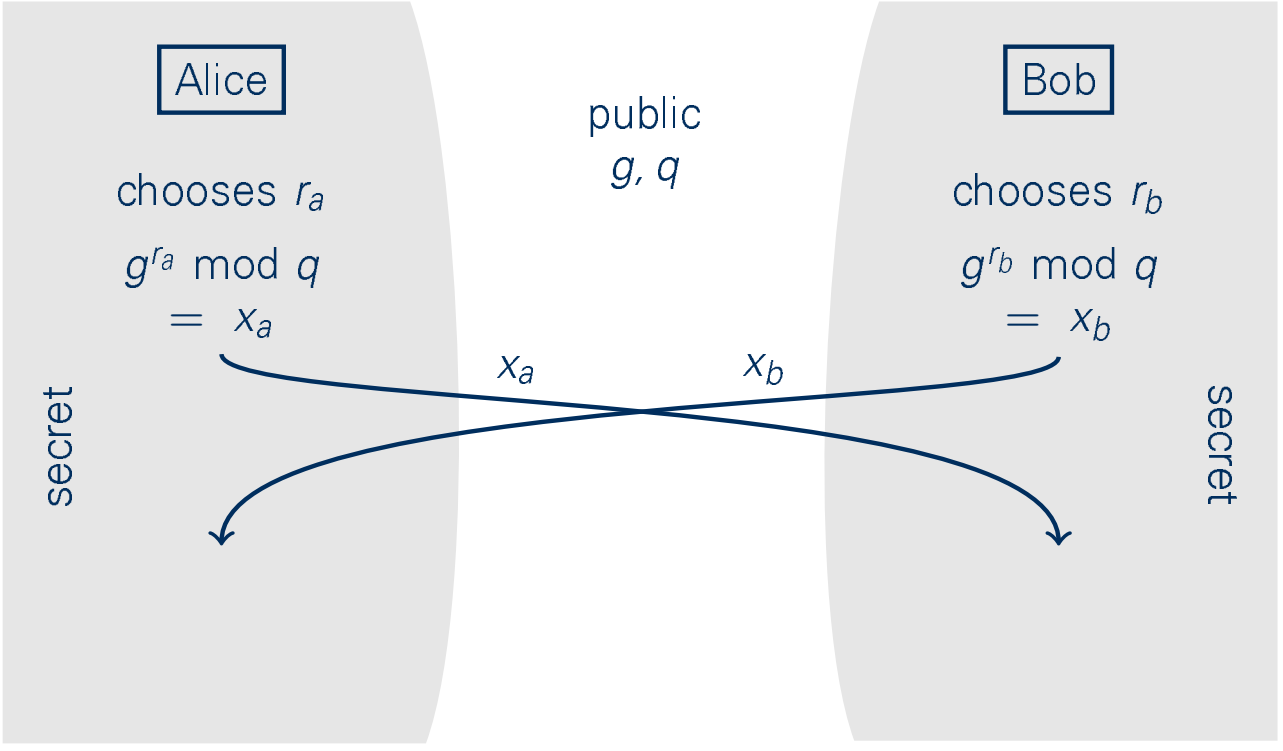
W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

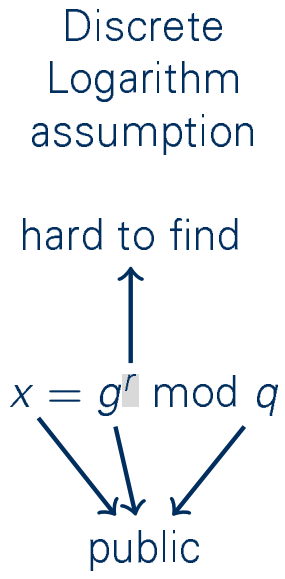
Diffie–Hellman Key Agreement



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

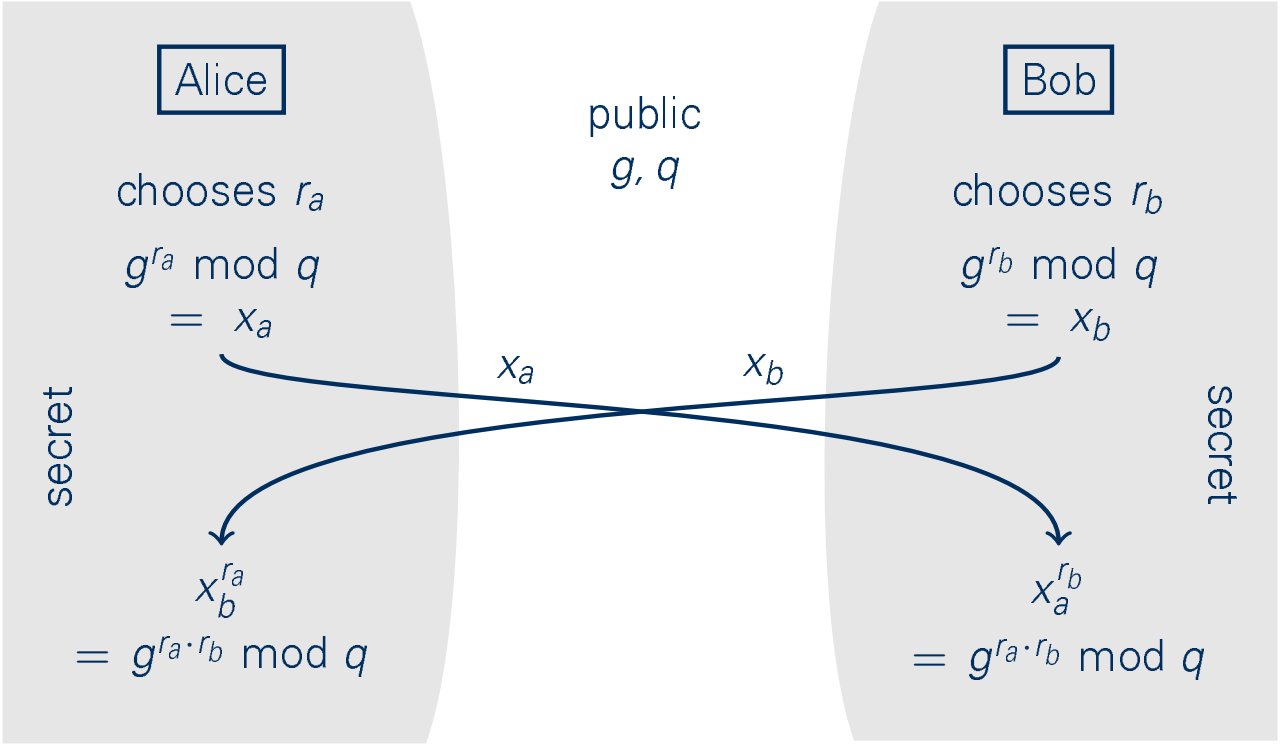
Diffie–Hellman Key Agreement



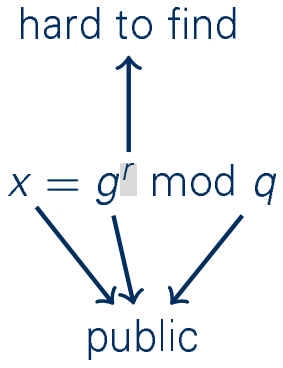


W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

Diffie–Hellman Key Agreement

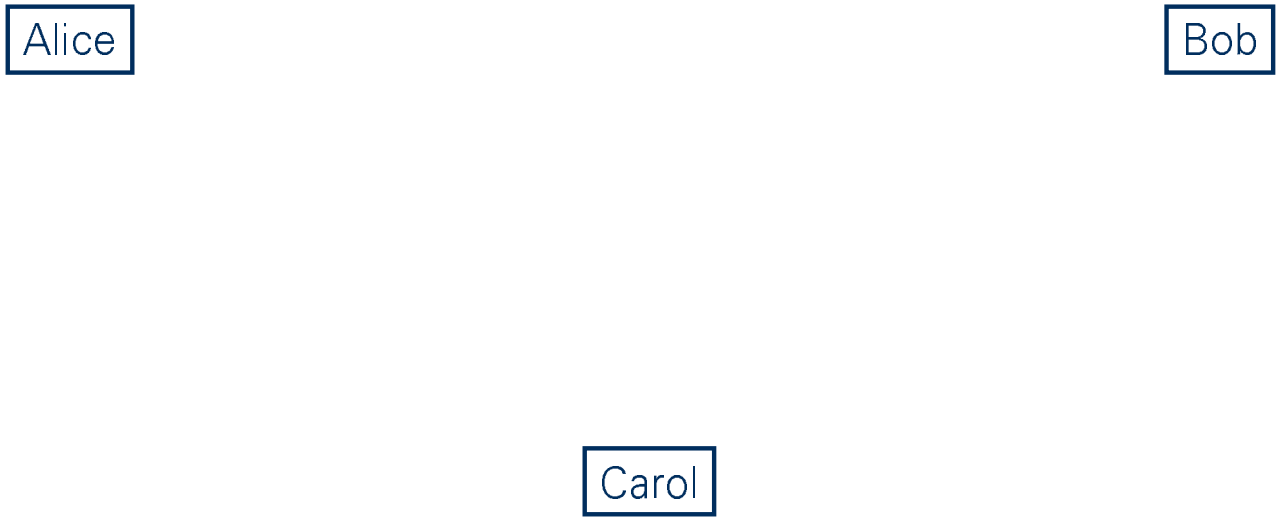


Discrete Logarithm assumption



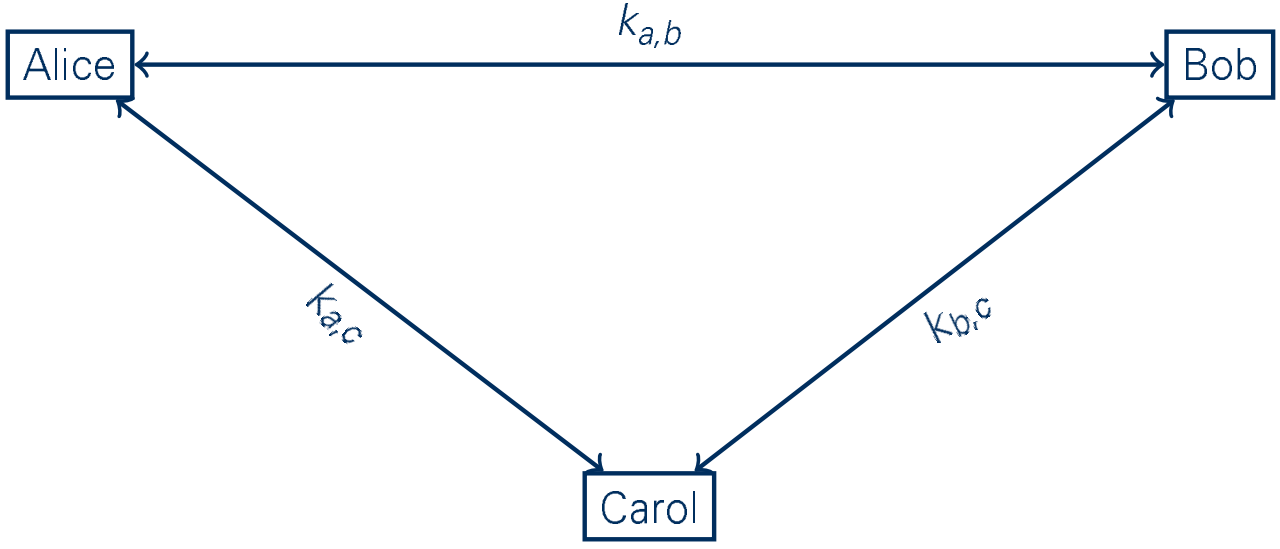
W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

Superposed Sending



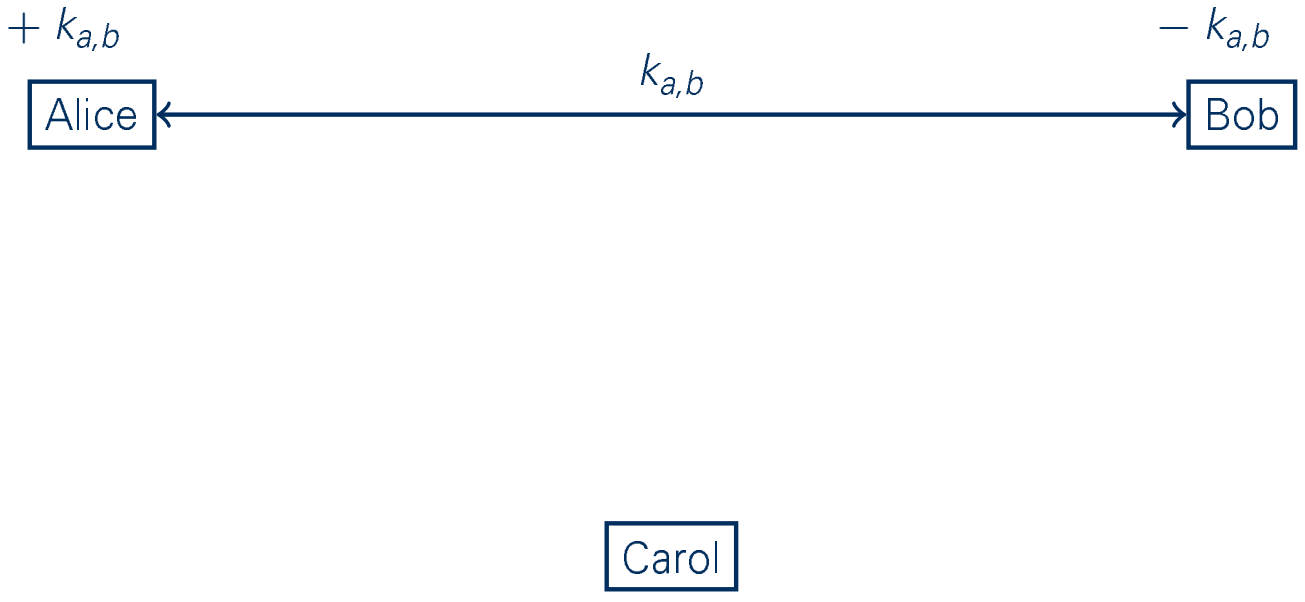
D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

Superposed Sending



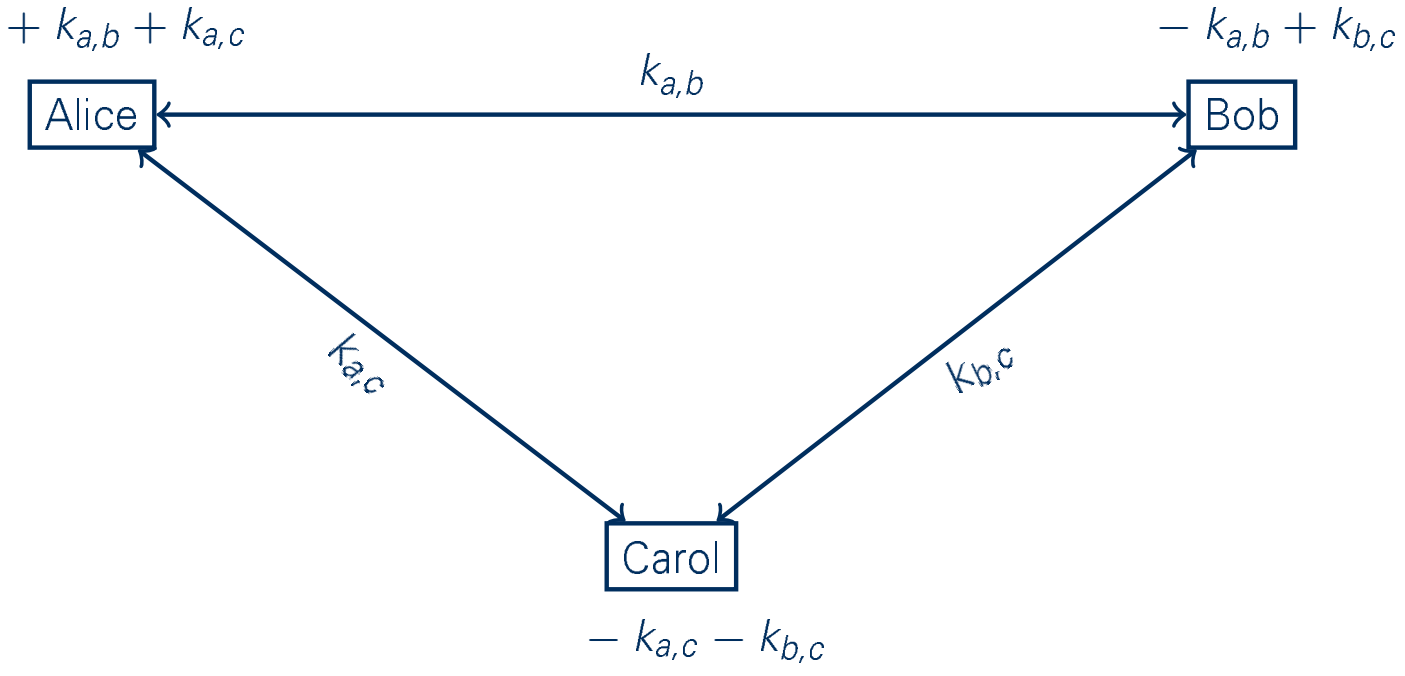
D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

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

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

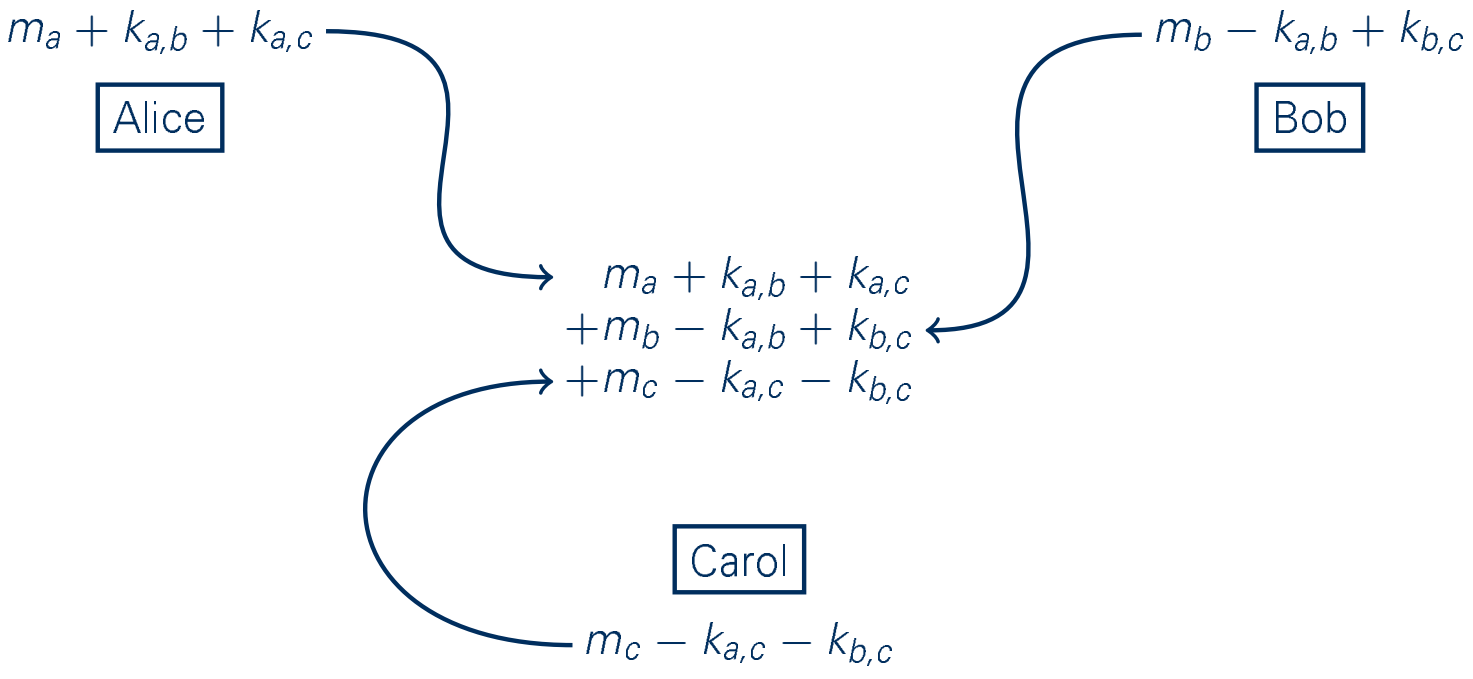
Bob

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

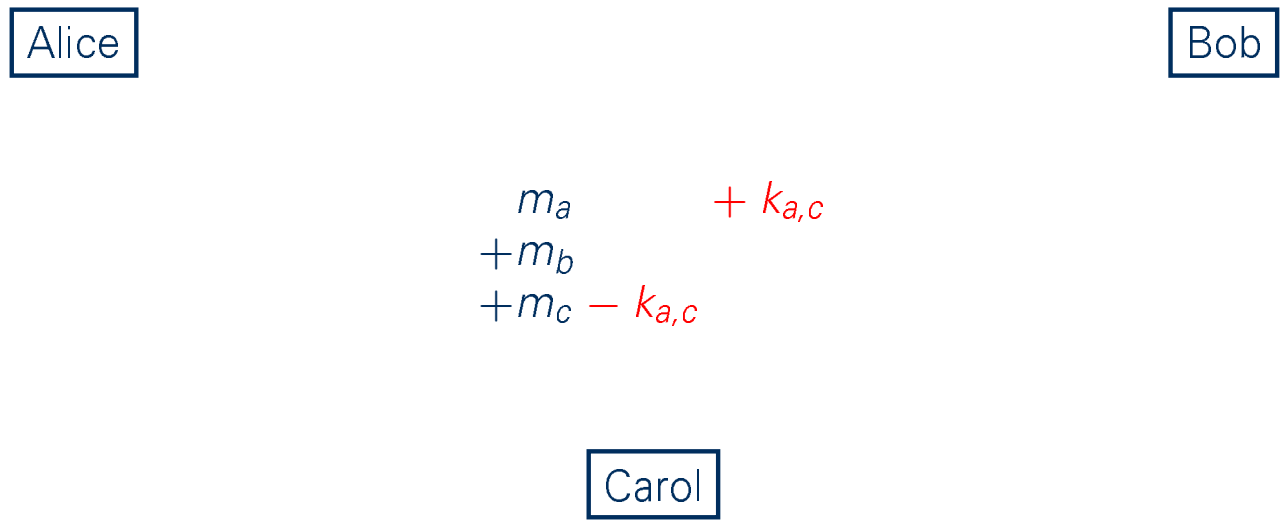
Bob

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

Carol

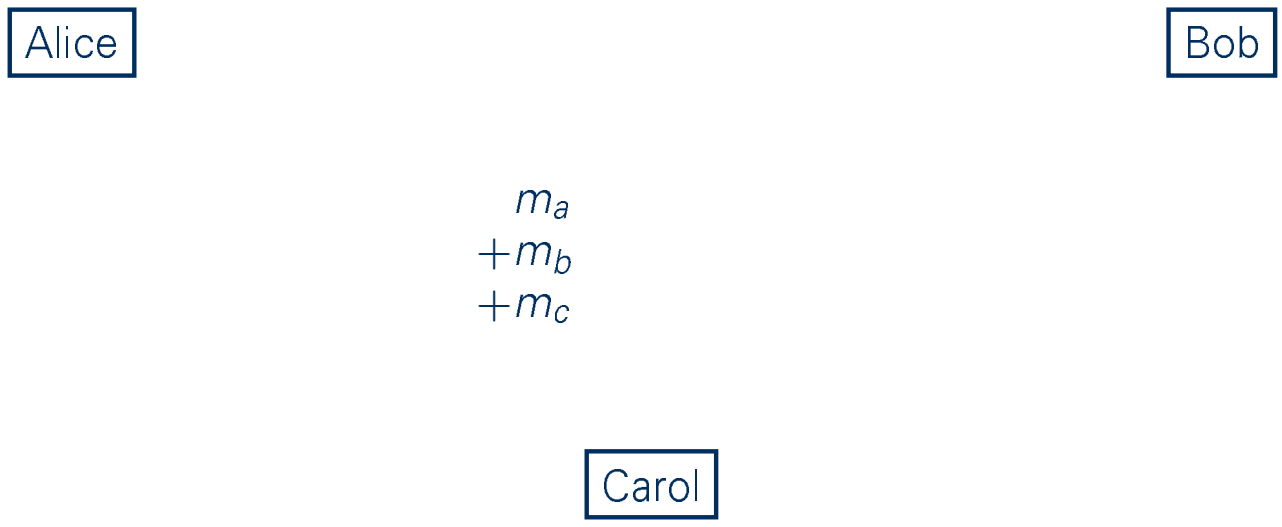
D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

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

Bookmarklet als Schlüsselspeicherung

```
1  document.getElementById('key').value='0xDEADBEEF'
```

Bookmarklet als Schlüsselspeicherung

```
1  document.getElementById('key').value='0xDEADBEEF'
```

```
1  <a href="javascript:void(document.getElementById('key')
2  .value='0xDEADBEEF')">insert key</a>
```

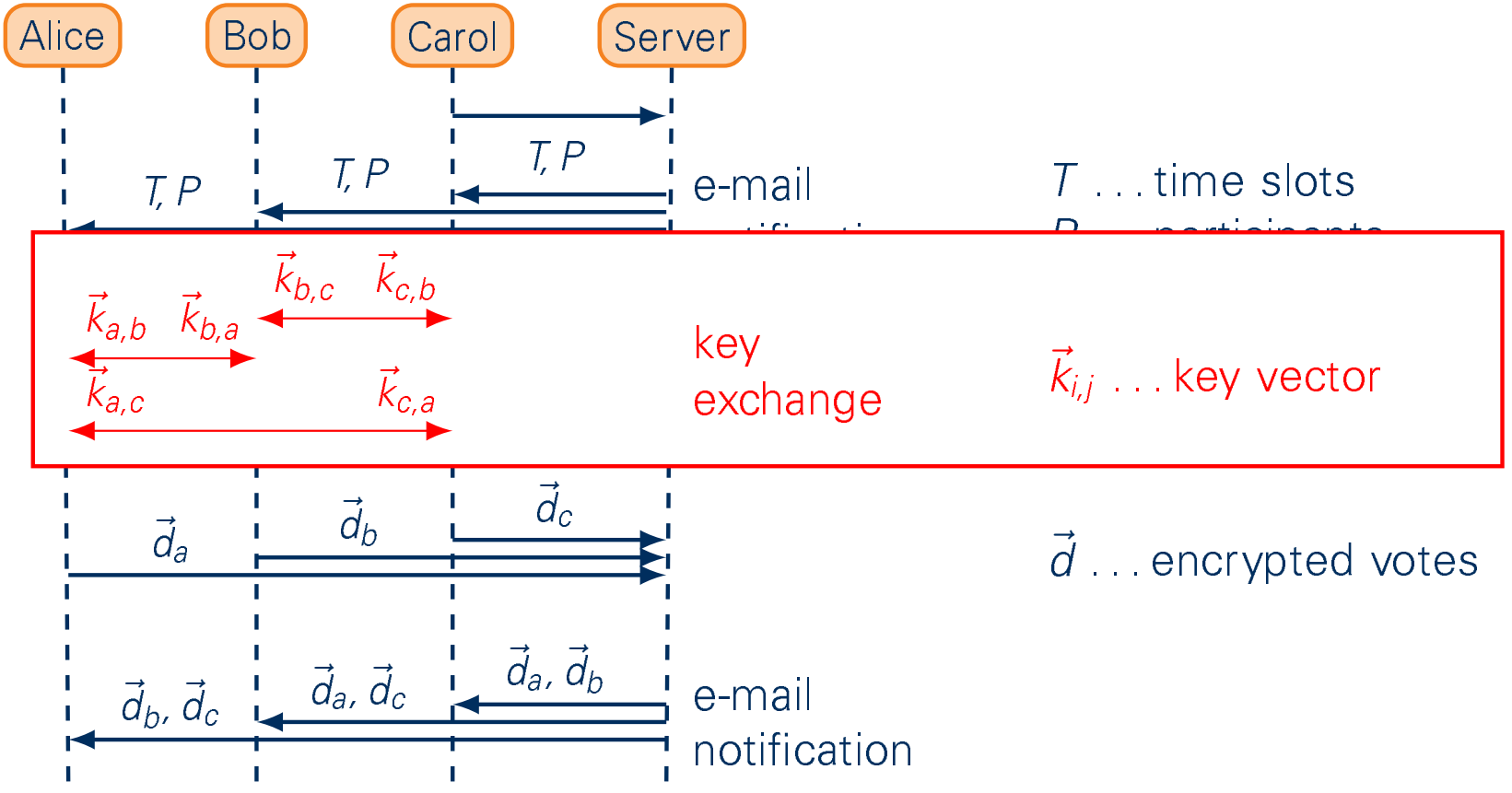
Bookmarklet als Schlüsselspeicherung

```
1  document.getElementById('key').value='0xDEADBEEF'
```

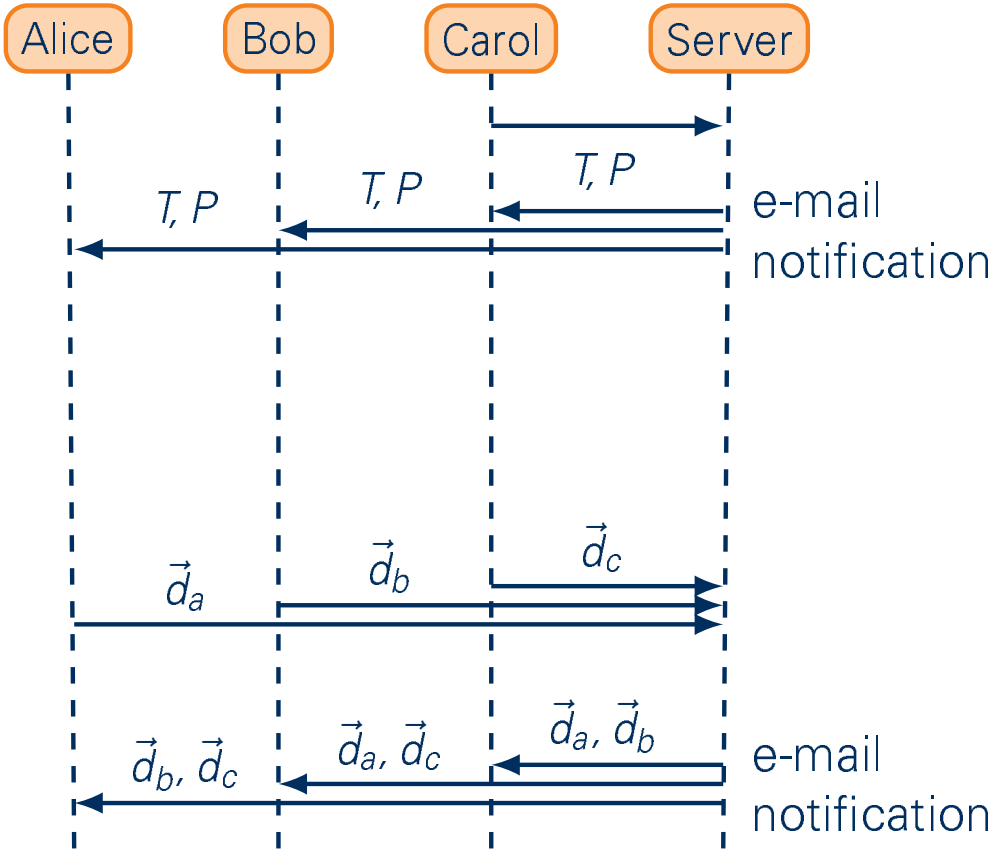
```
1  <a href="javascript:void(document.getElementById('key')
2  .value='0xDEADBEEF')">insert key</a>
```

```
1  <a href="javascript:void(document.getElementById('key')
2  .value='0xDEADBEEF')" onClick="help()">insert key</a>
```

Vereinfachung des Schlüsselaustauschs



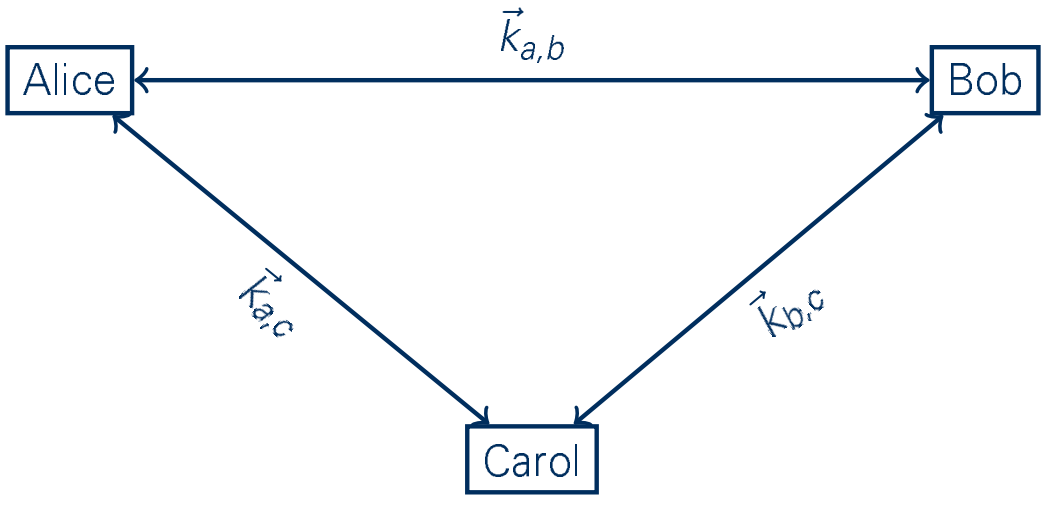
Vereinfachung des Schlüsselaustauschs



T . . . time slots
P . . . participants

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

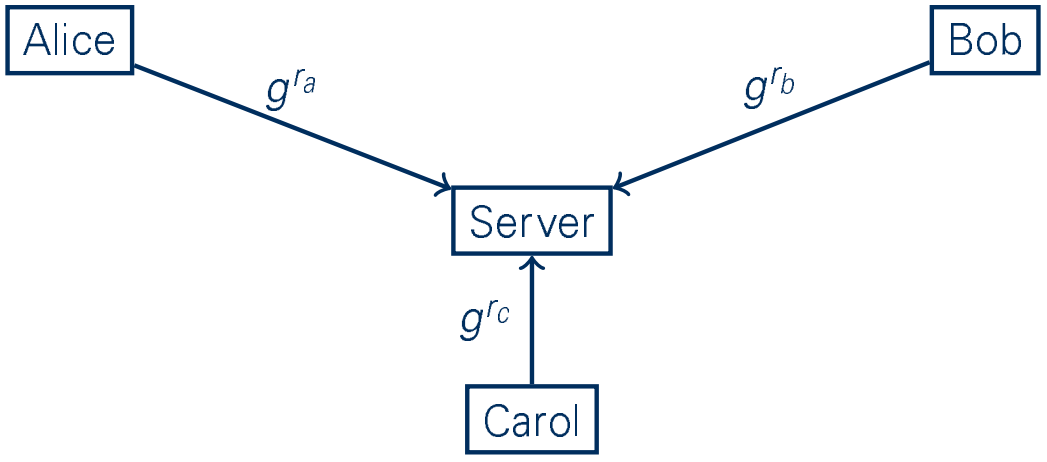
Vereinfachung des Schlüsselaustauschs



Schlüsselaustausch

Vereinfachung des Schlüsselaustauschs

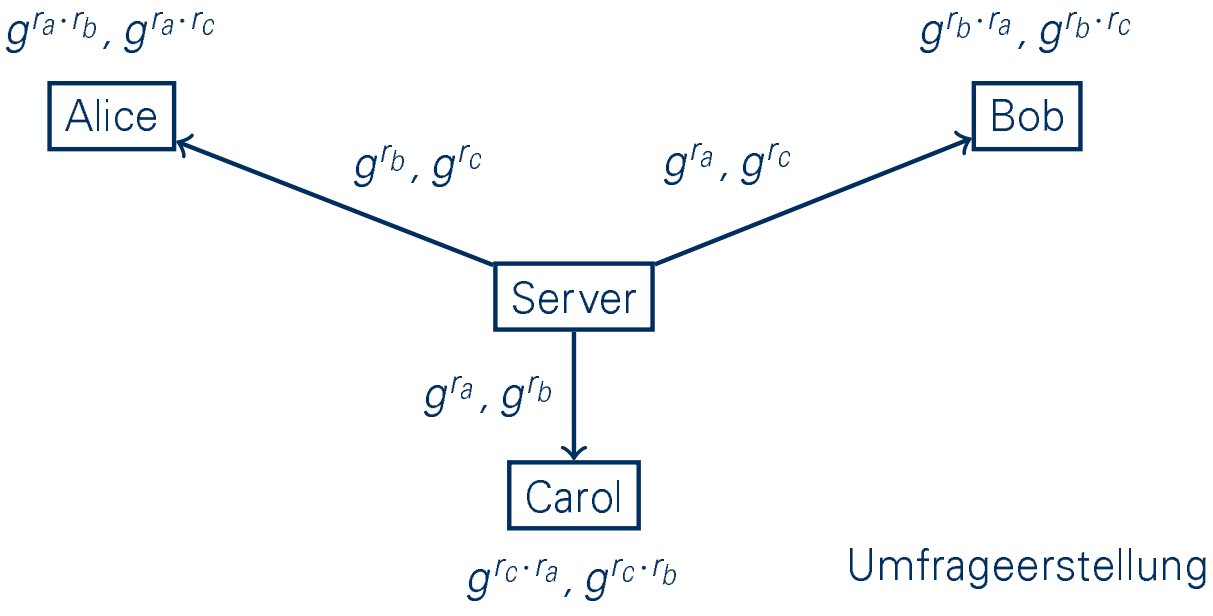
Diffie–Hellman



Registrierung

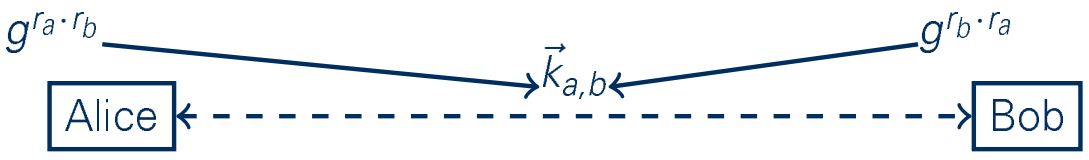
Vereinfachung des Schlüsselaustauschs

Diffie–Hellman



Vereinfachung des Schlüsselaustauschs

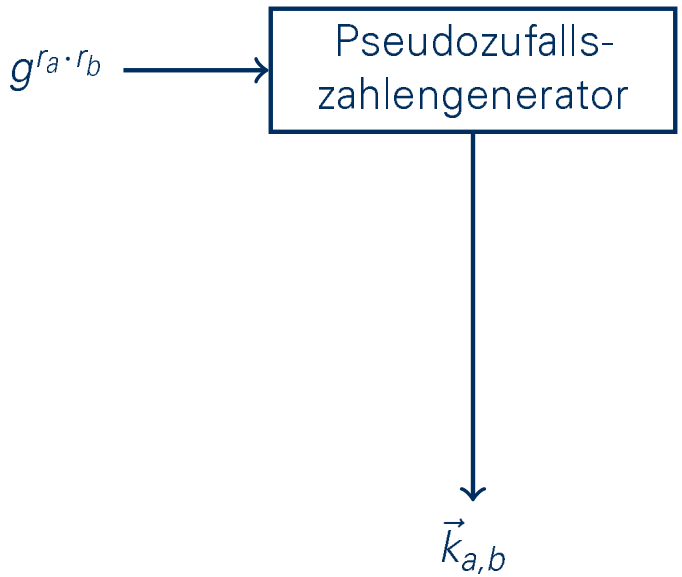
Diffie–Hellman



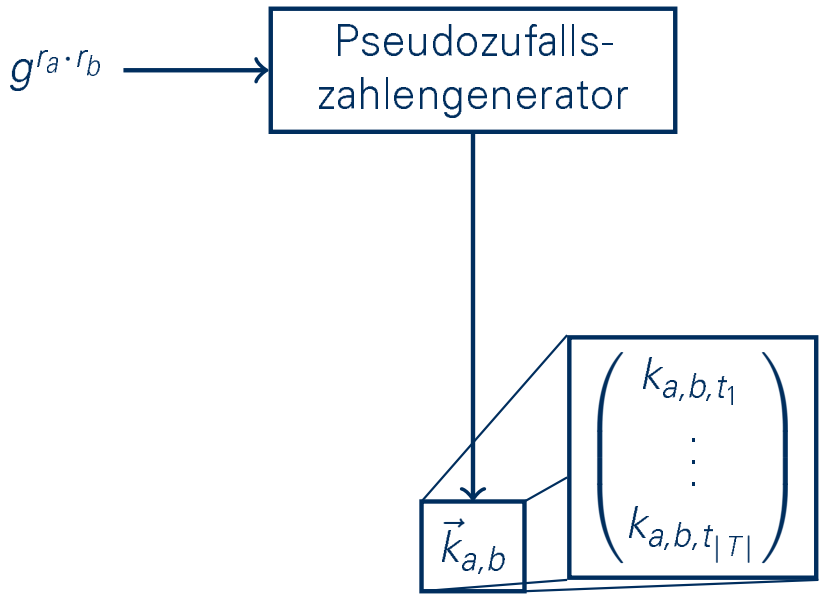
Carol

Umfrageerstellung

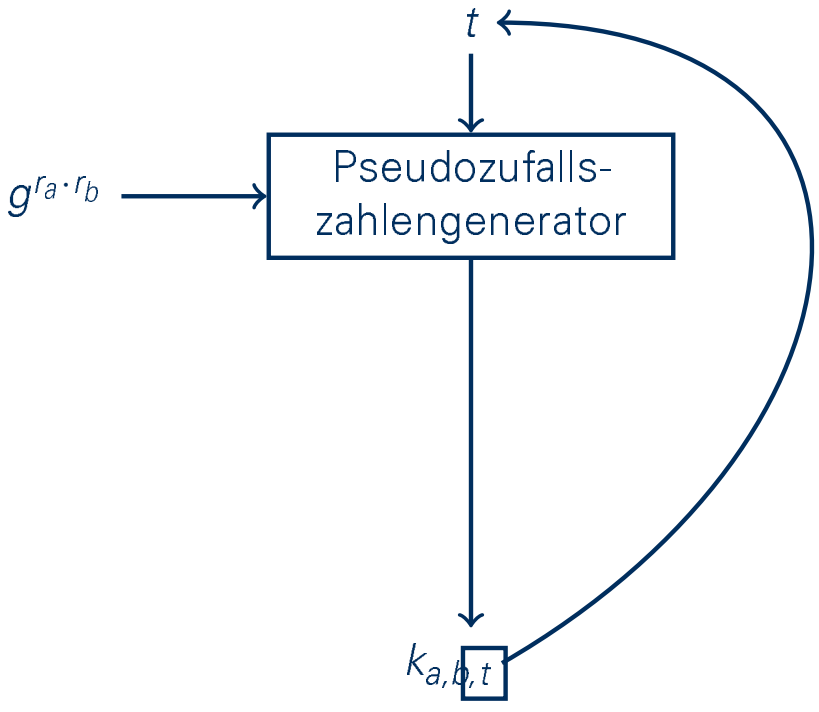
Vereinfachung des Schlüsselaustauschs



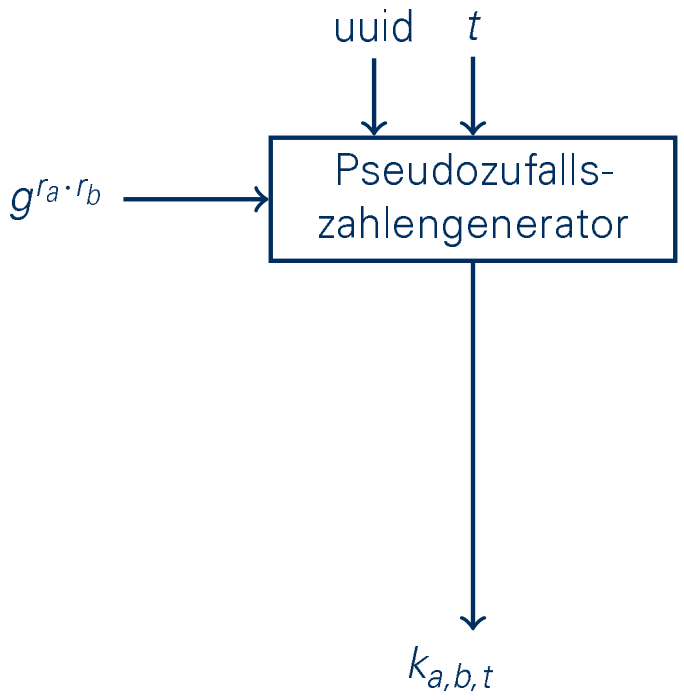
Vereinfachung des Schlüsselaustauschs



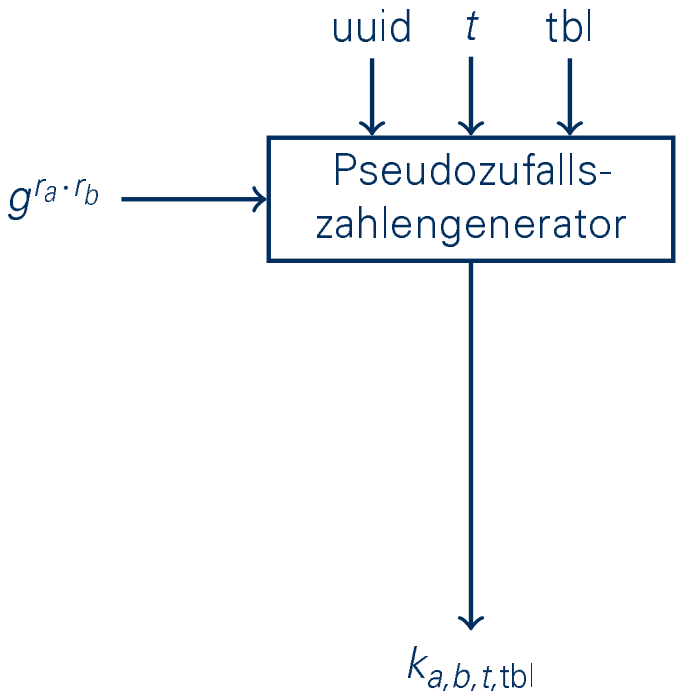
Vereinfachung des Schlüsselaustauschs



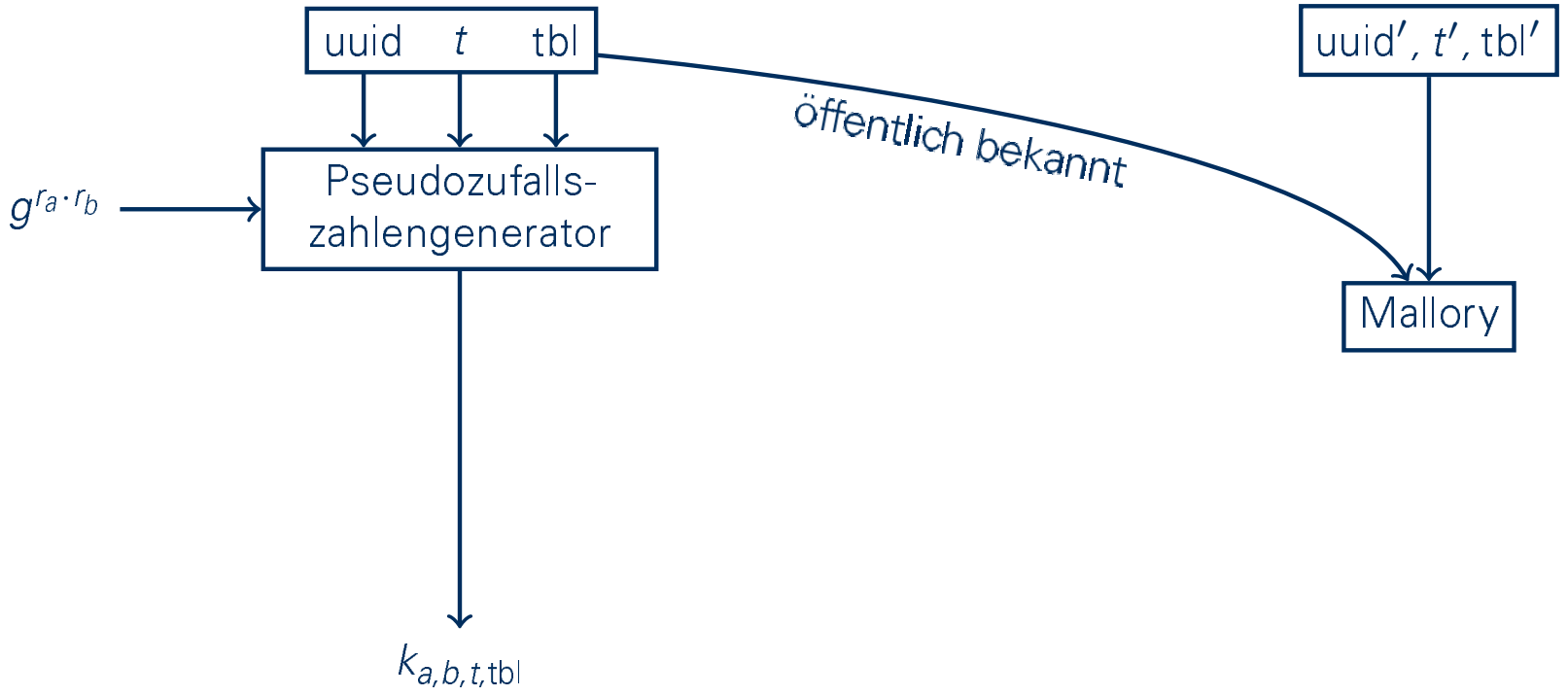
Vereinfachung des Schlüsselaustauschs



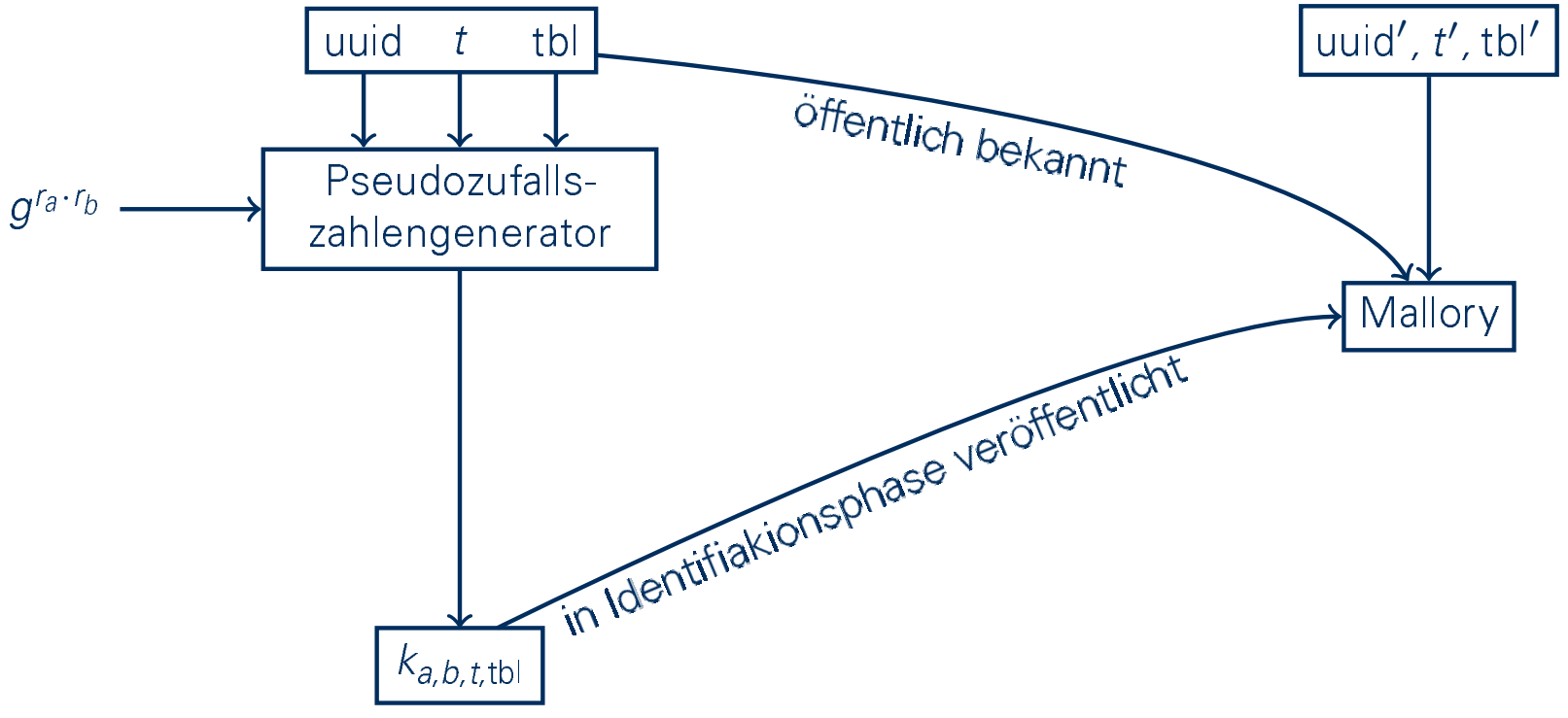
Vereinfachung des Schlüsselaustauschs



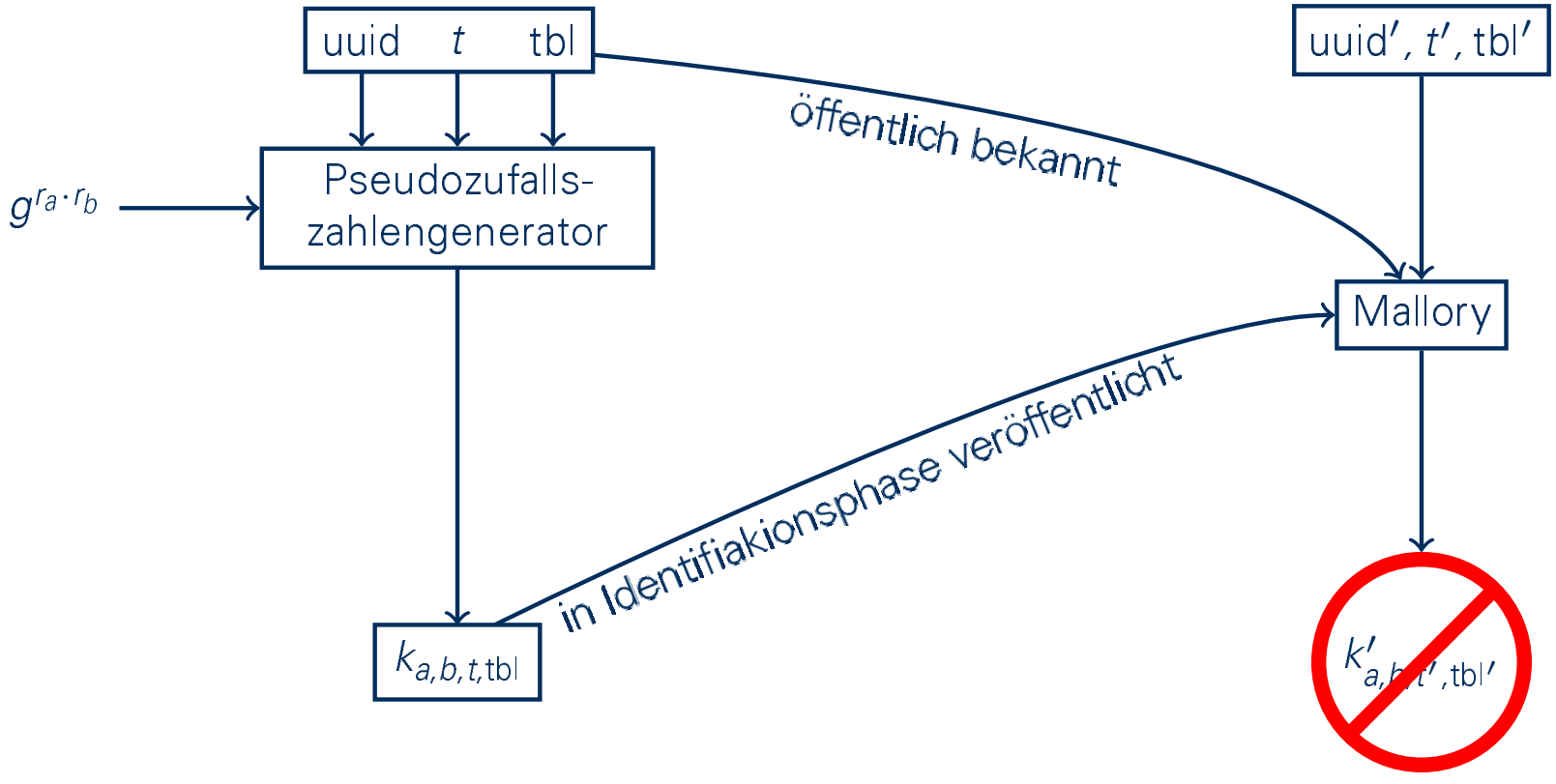
Vereinfachung des Schlüsselaustauschs



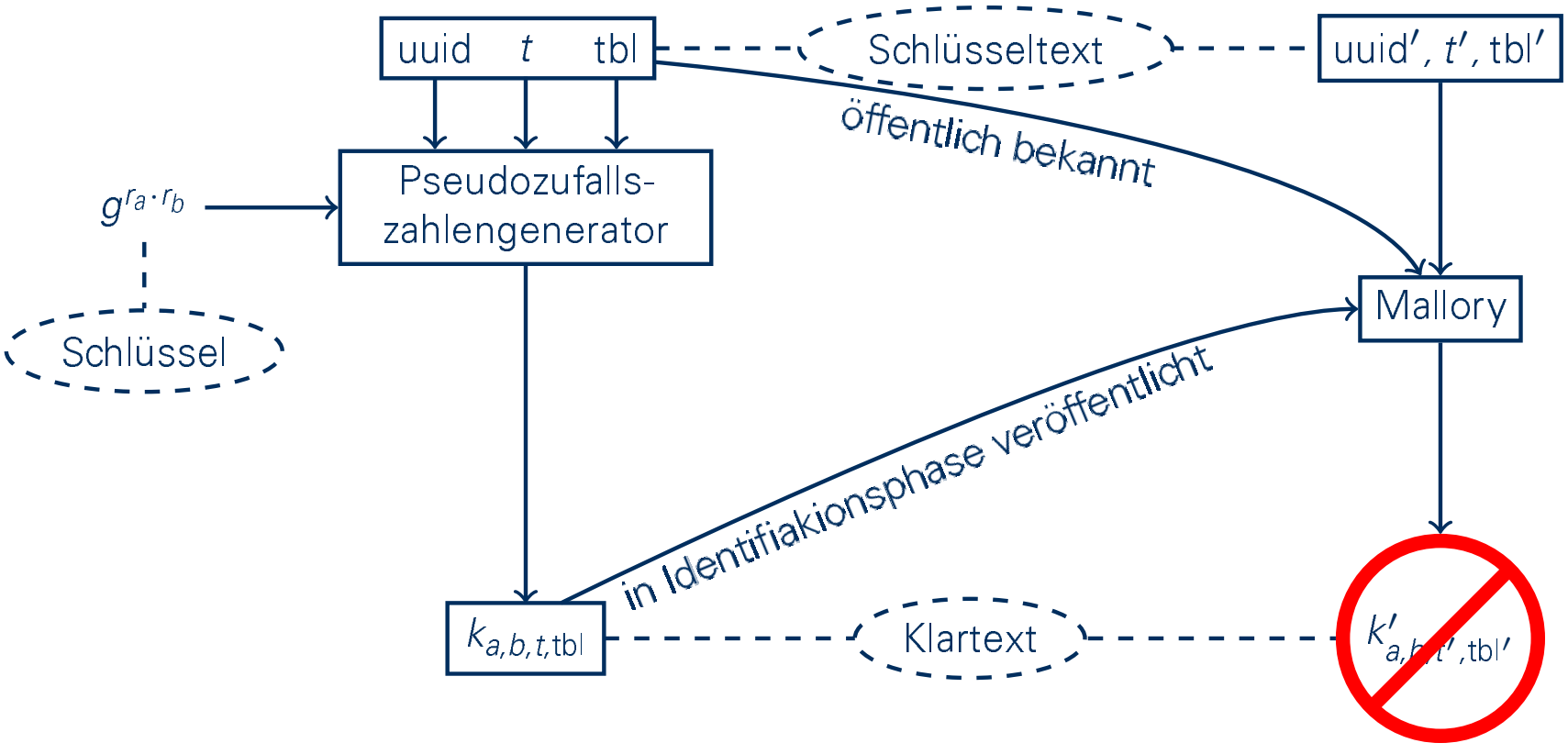
Vereinfachung des Schlüsselaustauschs



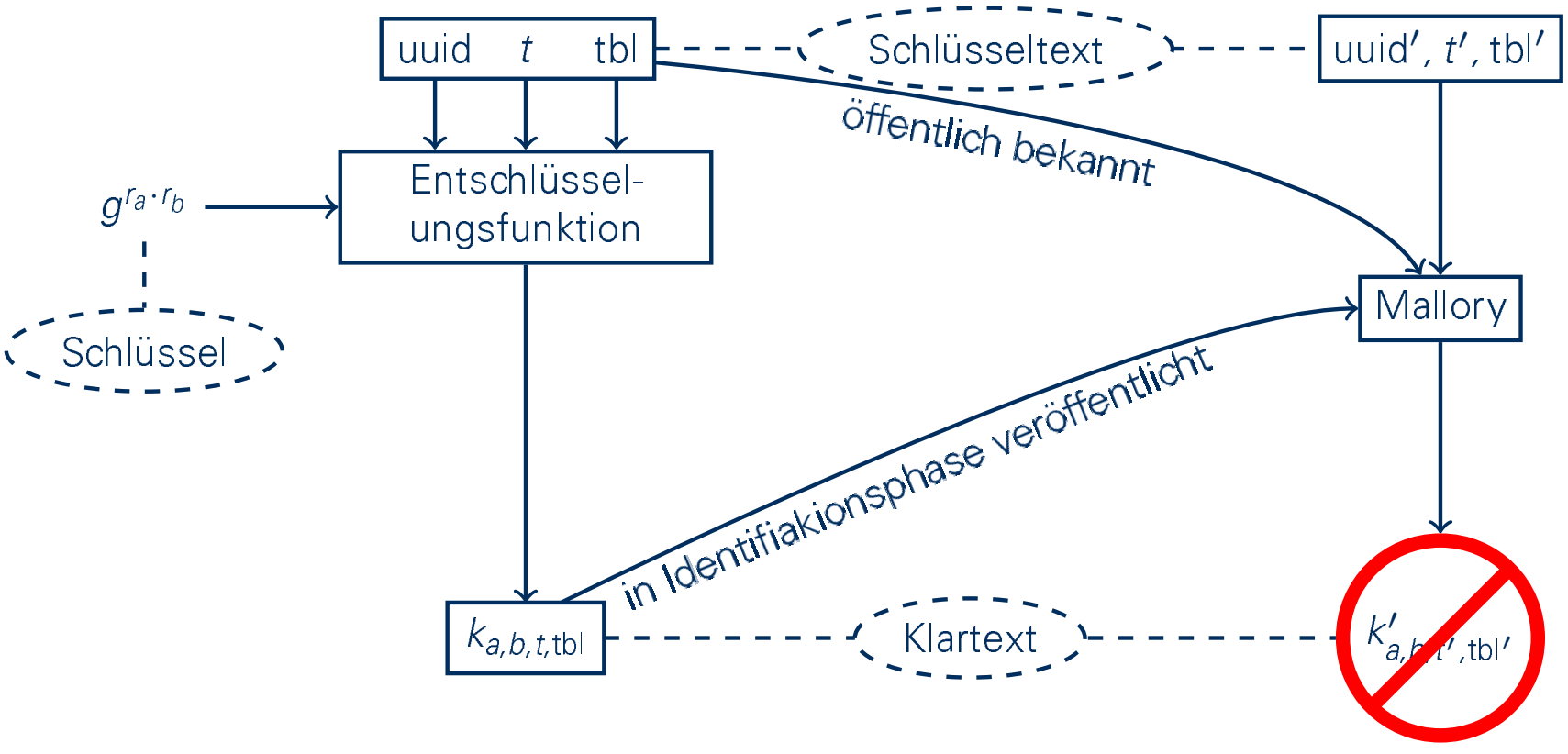
Vereinfachung des Schlüsselaustauschs



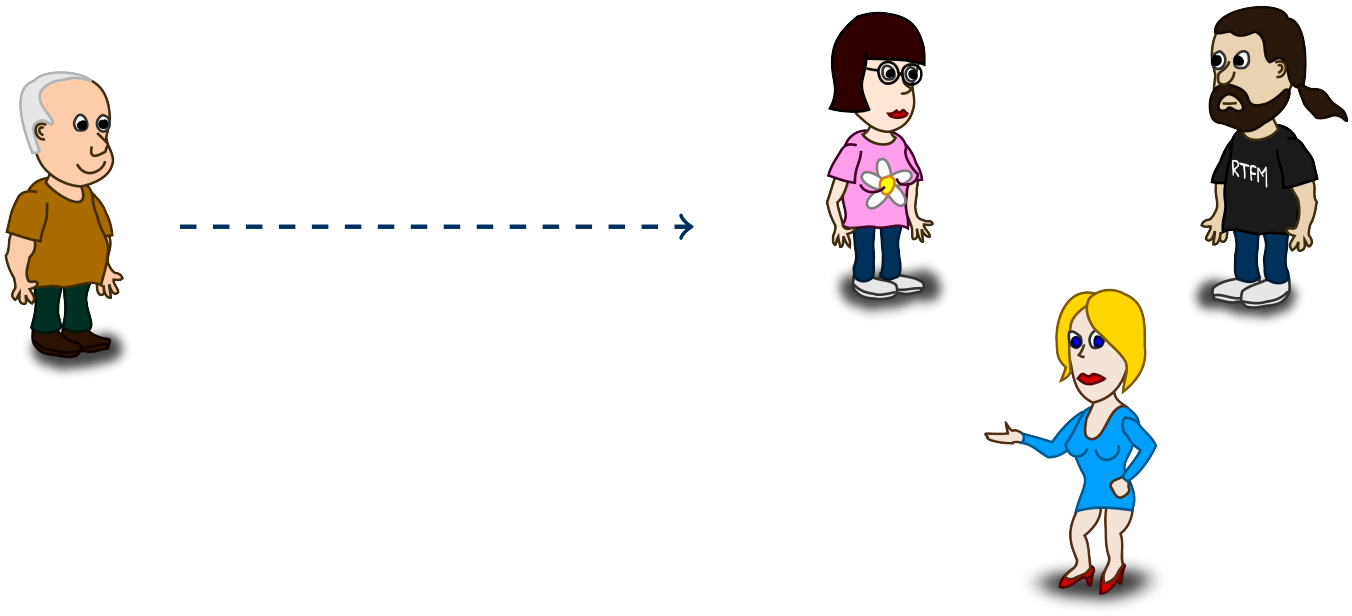
Vereinfachung des Schlüsselaustauschs



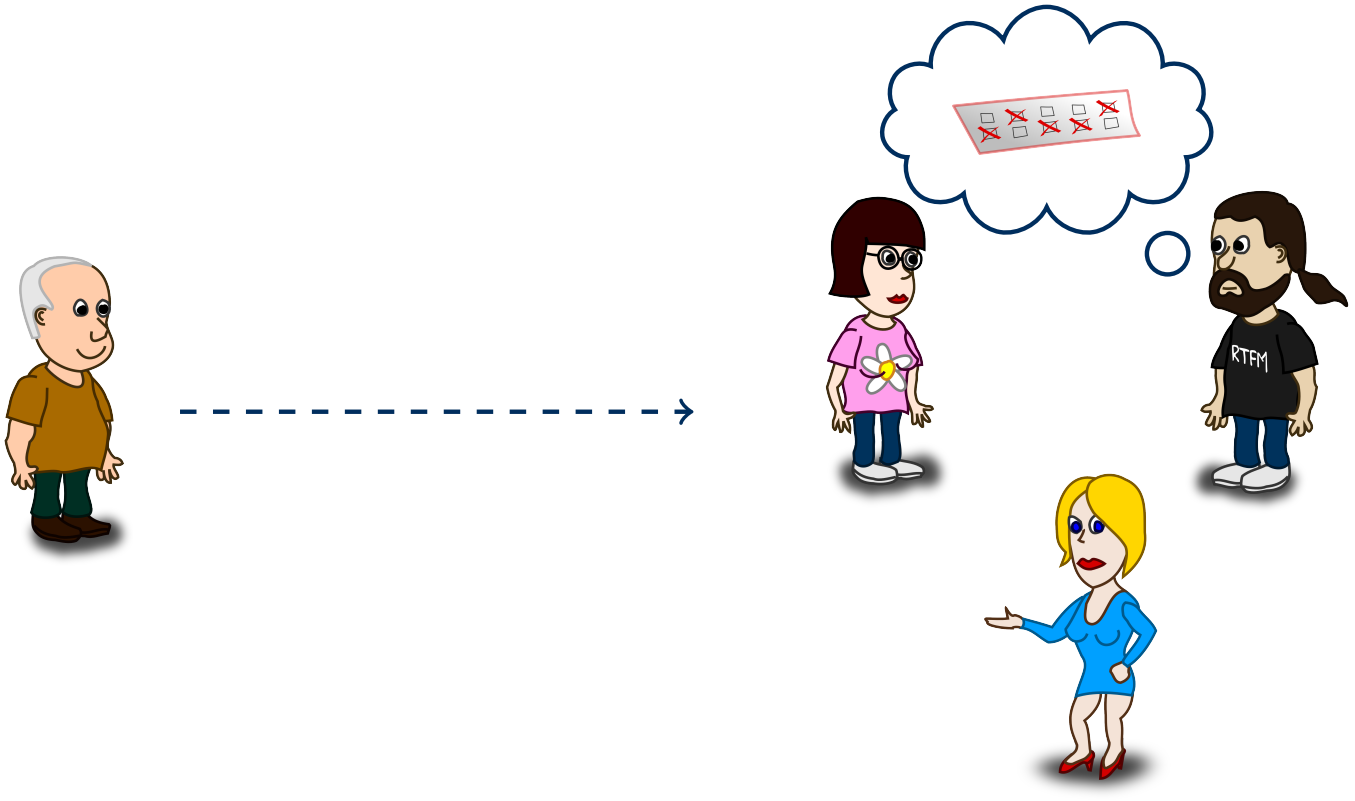
Vereinfachung des Schlüsselaustauschs



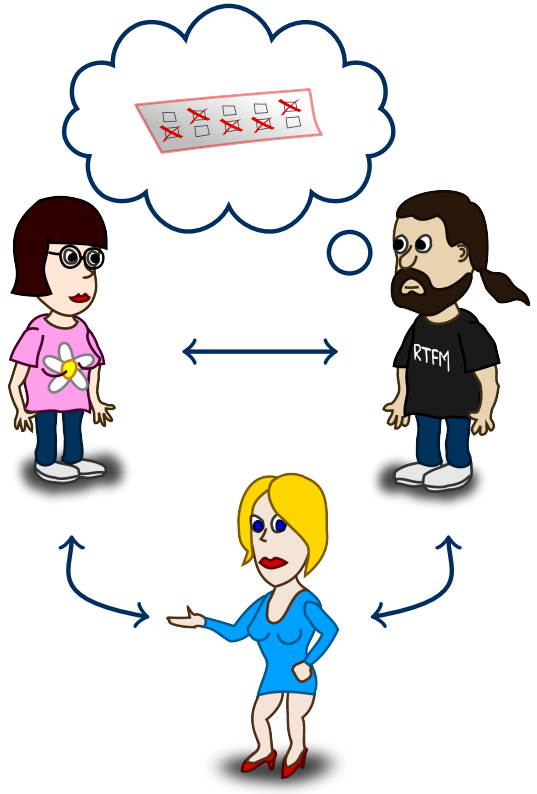
Dynamic Joining



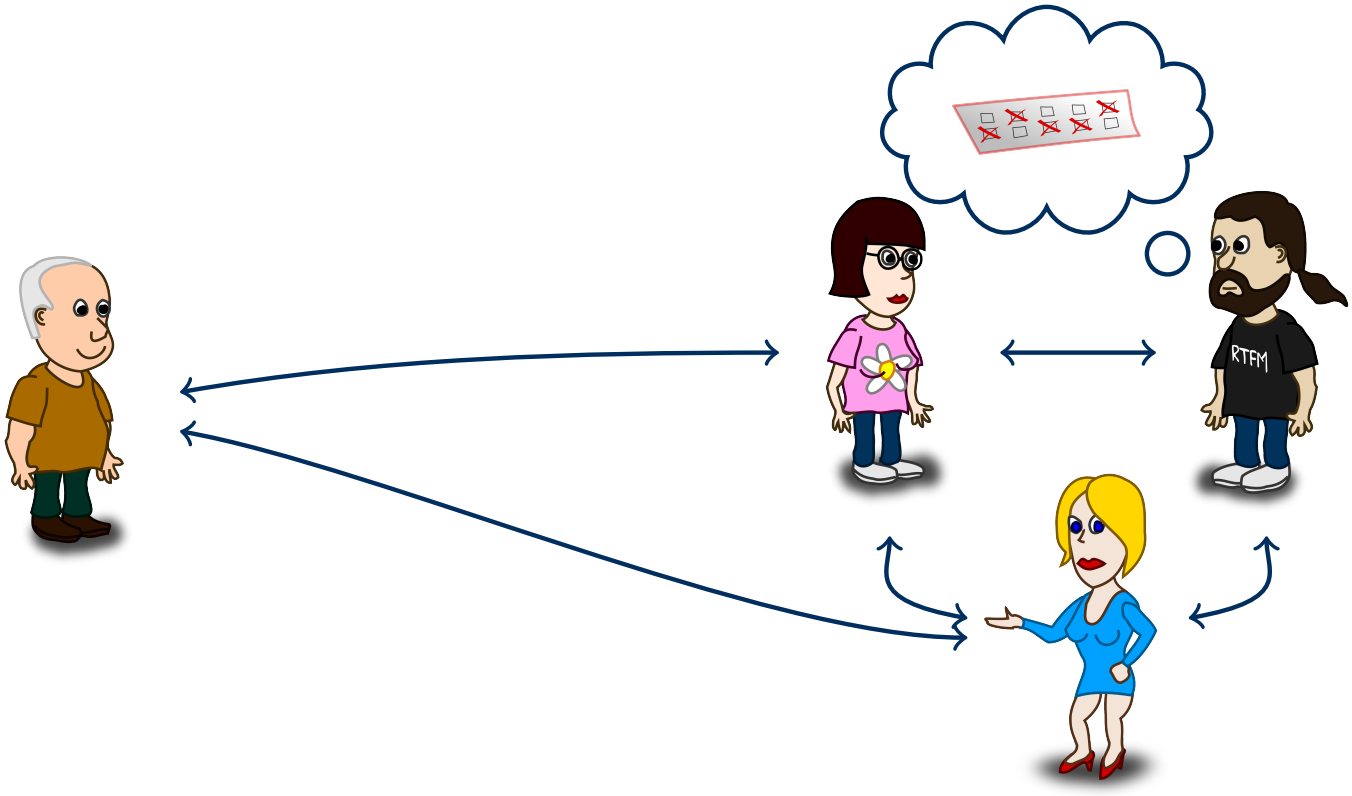
Dynamic Joining



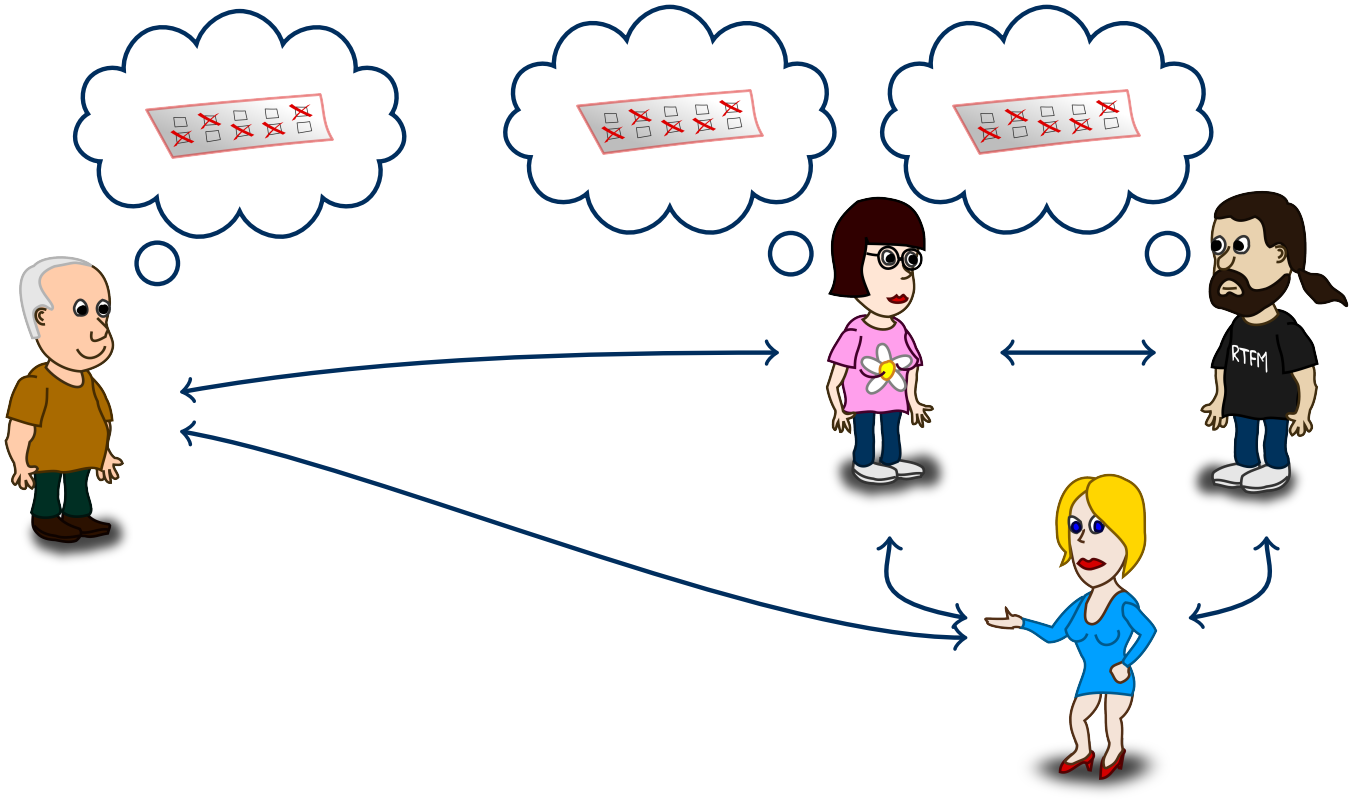
Dynamic Joining



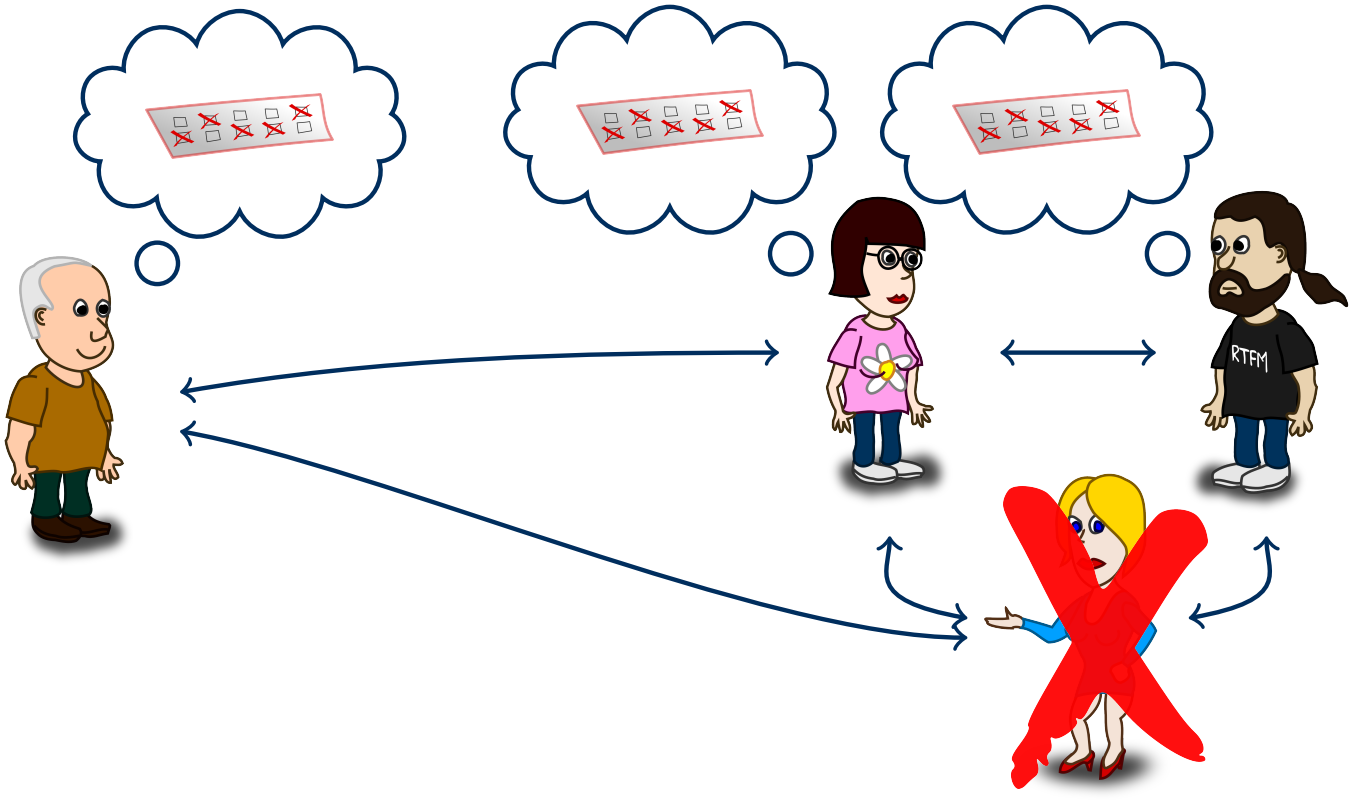
Dynamic Joining



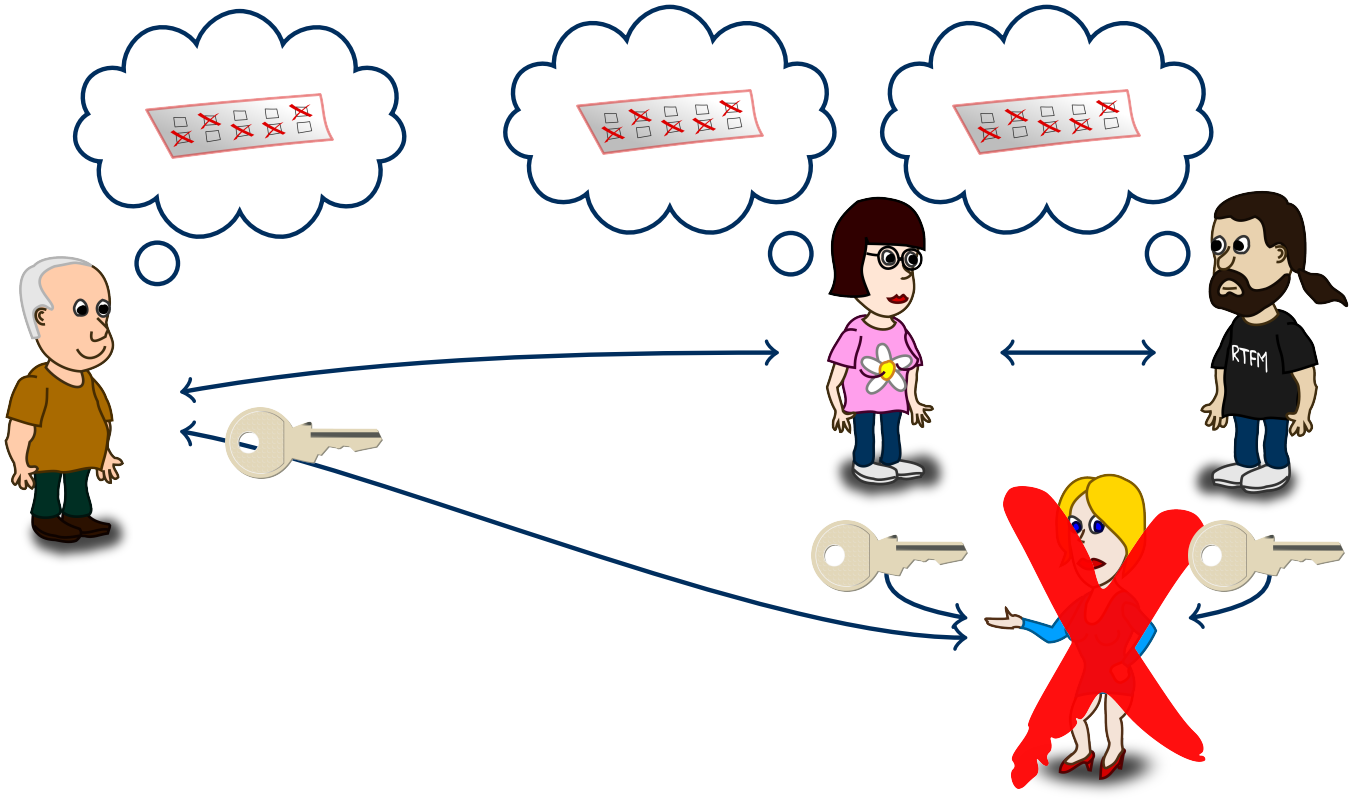
Dynamic Leaving



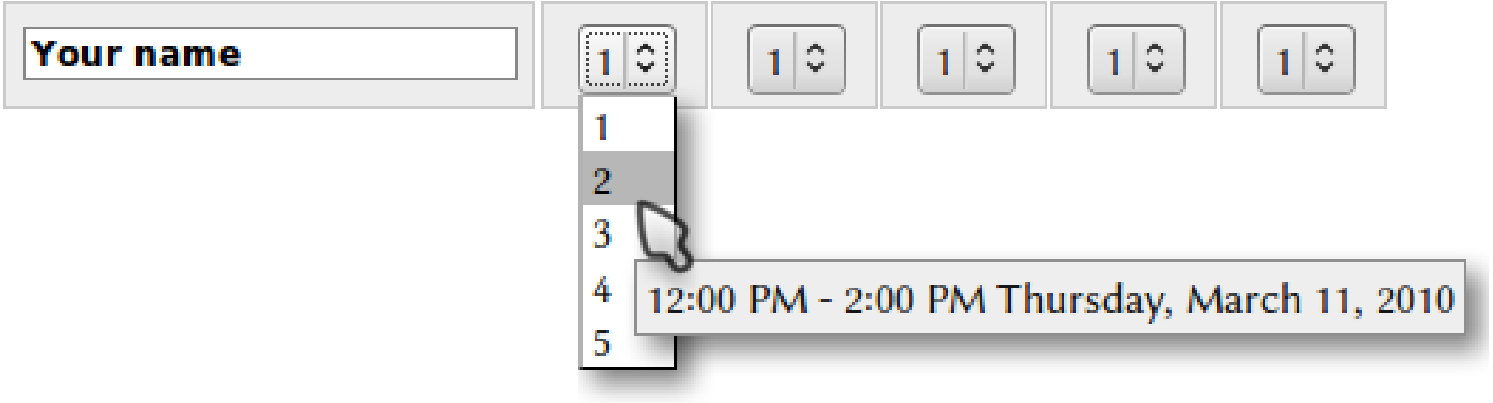
Dynamic Leaving



Dynamic Leaving



Preferences instead of Binary Choice



Updating / Revoking Votes

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
Alice	OK		OK	OK	OK
Bob		OK		OK	OK
Carol	OK	OK		OK	
Dave		OK	OK	OK	OK
Your name	☐	☐	☐	☐	☐
Count	2	3	2	**4**	3

Existing PKI usage

PGP

GnuPG