TECHNISCHE UNIVERSITÄT DRESDEN

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

Datenschutzfreundliche Terminplanung

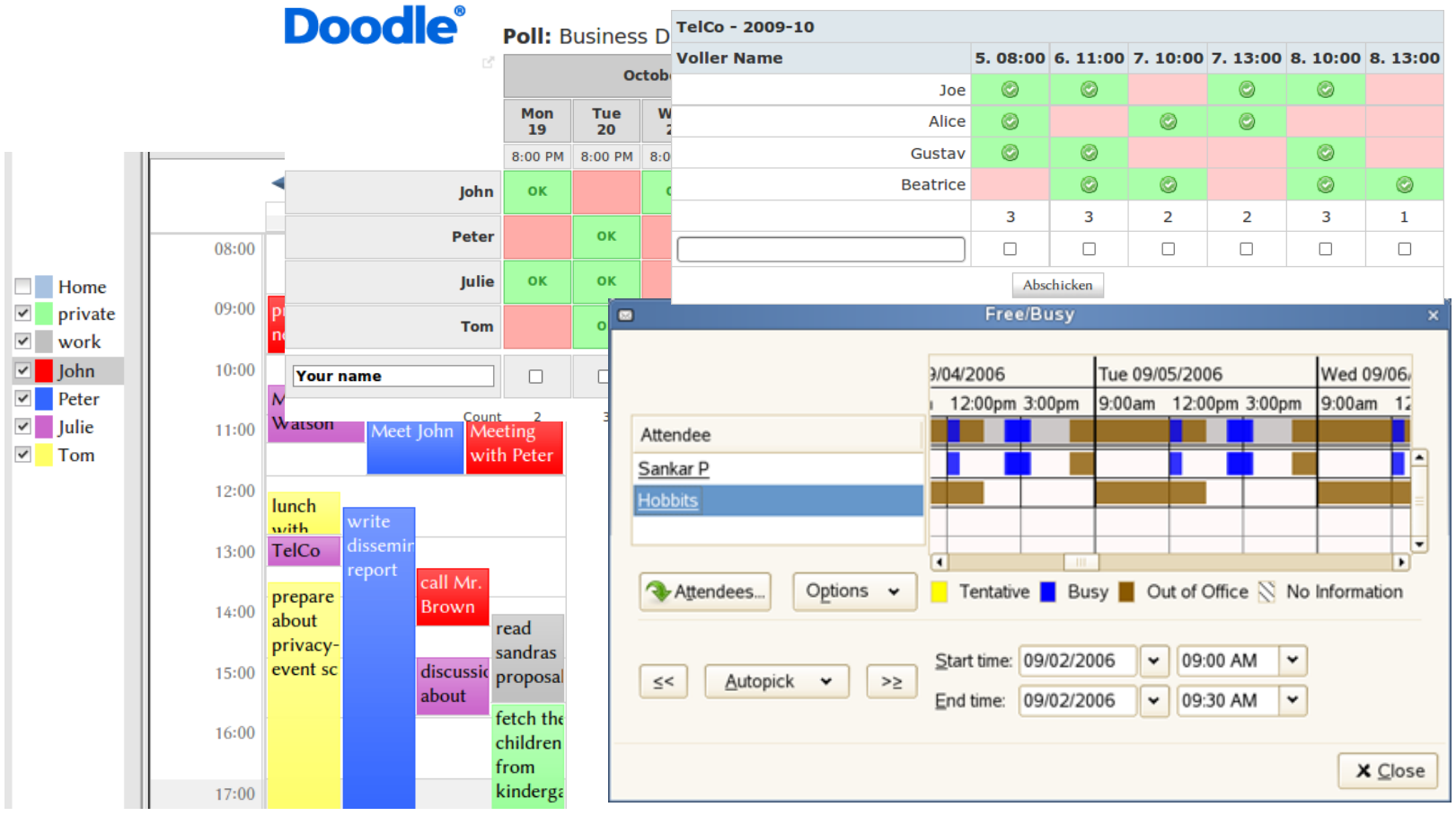
Benjamin.Kellermann@tu-dresden.de

D19E 04A8 8895 020A 8DF6

0092 3501 1A32 491A 3D9C

Dresden, 3. Oktober 2009

Terminplanung



Datenschutzprobleme

Direkte Folgerungen

Wird mein Mann für unseren Hochzeitstag stimmen?

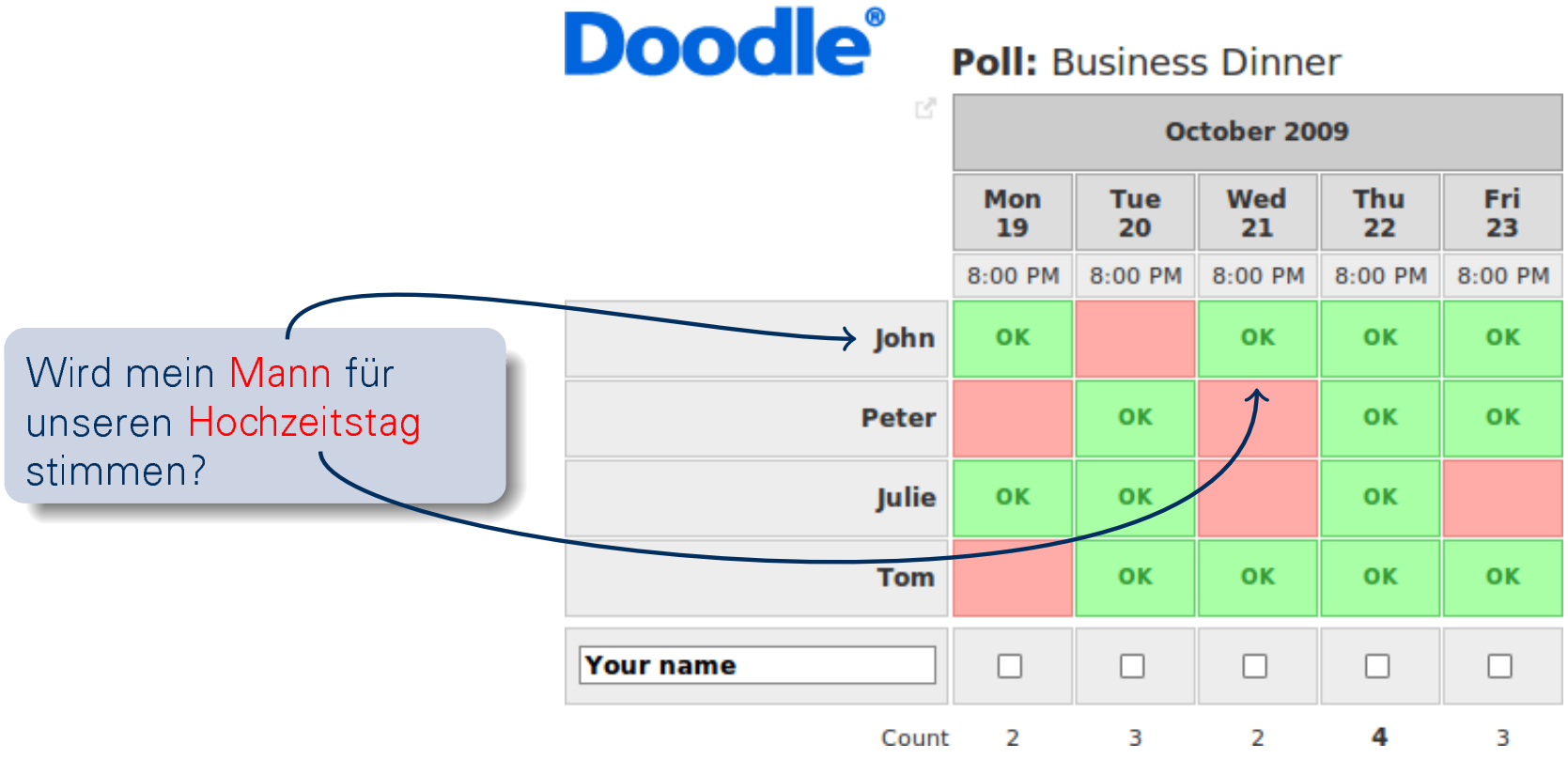
Doodle®

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

Datenschutzprobleme

Direkte Folgerungen



Datenschutzprobleme

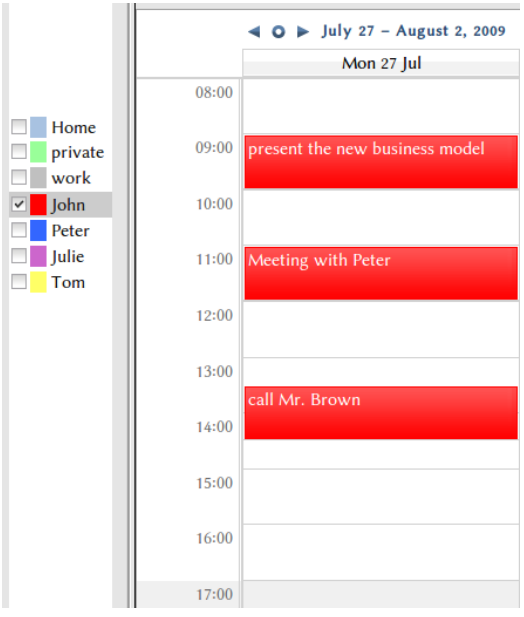
Indirekte Folgerungen

Das Verfügbarkeitsmuster des Benutzers bunny23 sieht aber verdächtig ähnlich zu dem meines Angestellten John Doe aus!

Doodle®

Poll: Chat

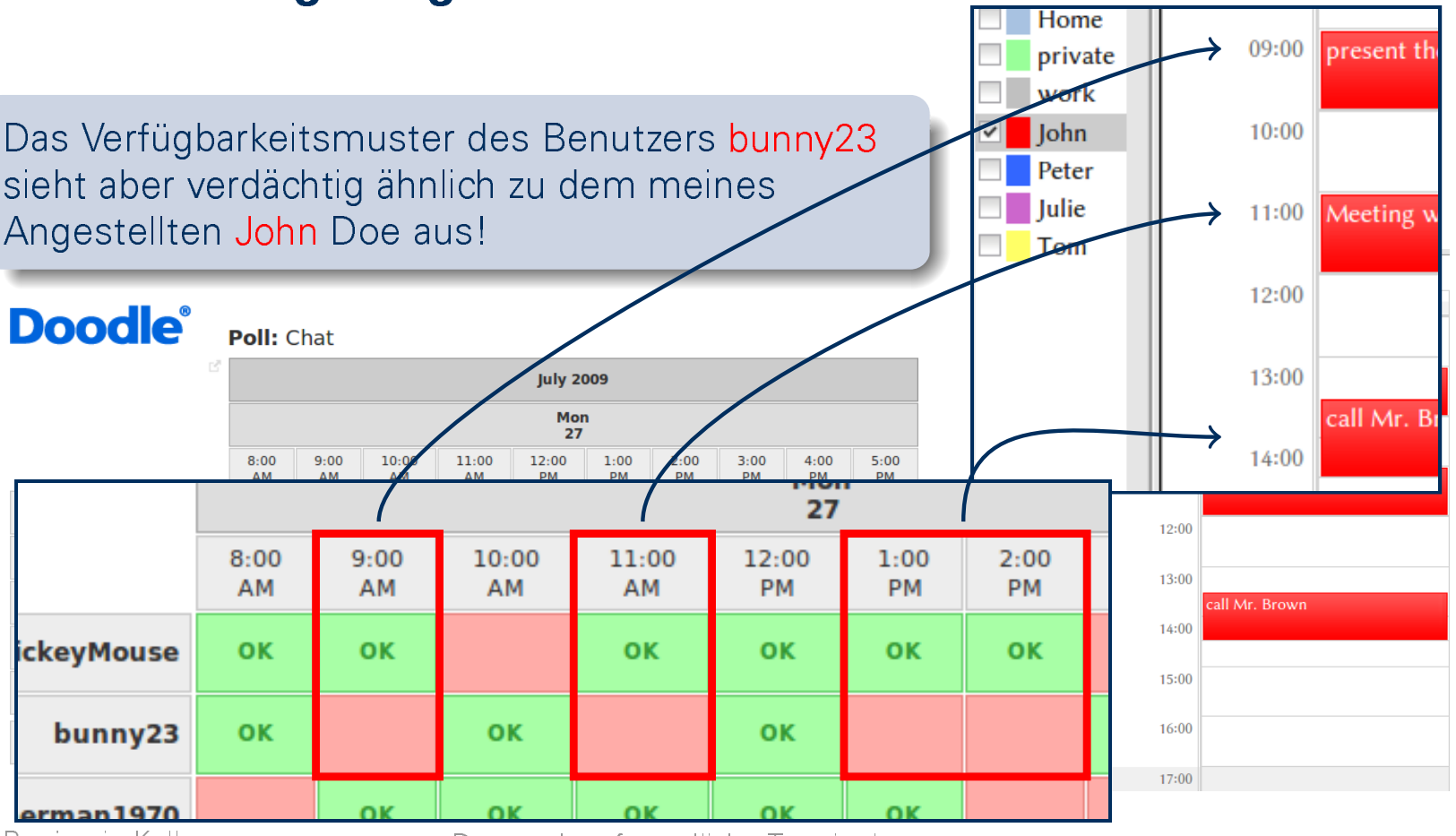
	July 2009									
	Mon 27									
	8:00 AM	9:00 AM	10:00 AM	11:00 AM	12:00 PM	1:00 PM	2:00 PM	3:00 PM	4:00 PM	5:00 PM
MickeyMouse	OK	OK		OK	OK	OK	OK			
bunny23	OK		OK		OK			OK	OK	OK
superman1970		OK	OK	OK	OK	OK				
Snoopy		OK	OK	OK	OK	OK	OK		OK	OK
little_girl				OK	OK	OK		OK	OK	
Your name	☐	☐	☐	☐	☐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



Datenschutzprobleme

Indirekte Folgerungen

Das Verfügbarkeitsmuster des Benutzers bunny23 sieht aber verdächtig ähnlich zu dem meines Angestellten John Doe aus!



Inhalt

Problembeschreibung

Schema

Erweiterungen

Evaluation

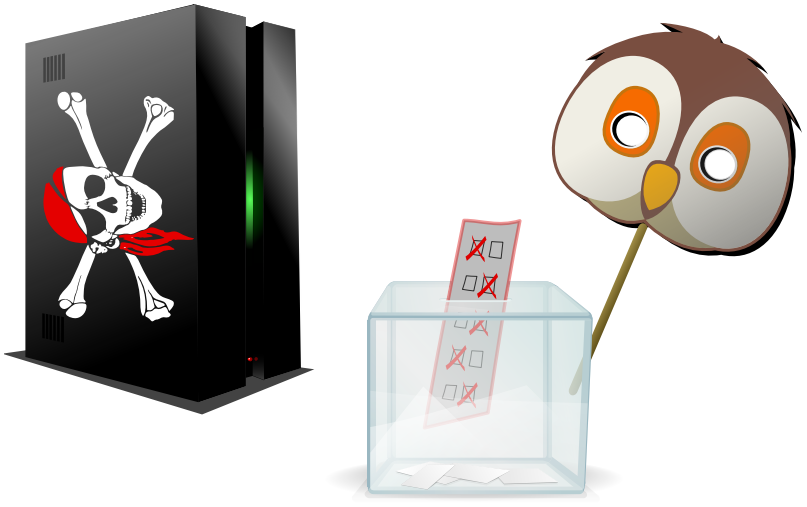
Zusammenfassung und Ausblick

Anforderungen

- nicht vertrauenswürdiger Server

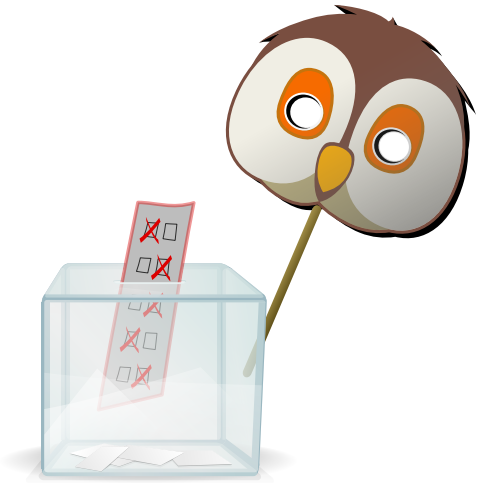
Anforderungen

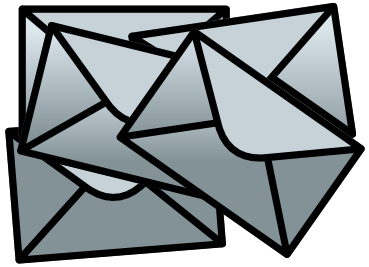
- nicht vertrauenswürdiger Server
- Datenschutz
- Überprüfbarkeit



Anforderungen

- nicht vertrauenswürdiger Server
- Datenschutz
- Überprüfbarkeit
- weniger Kommunikationsschritte
- geringer Berechnungsaufwand





E-Voting vs. Terminplanung

	Stimme
Kandidat #1	
Kandidat #2	✘
⋮	
Kandidat #10	

	Datum #1	Datum #2	. . .	Datum #320
Ja	✘			✘
Nein		✘		

ein Kreuz pro Spalte

E-Voting vs. Terminplanung

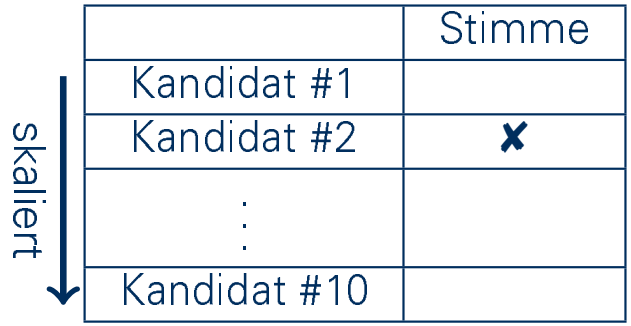
skaliert

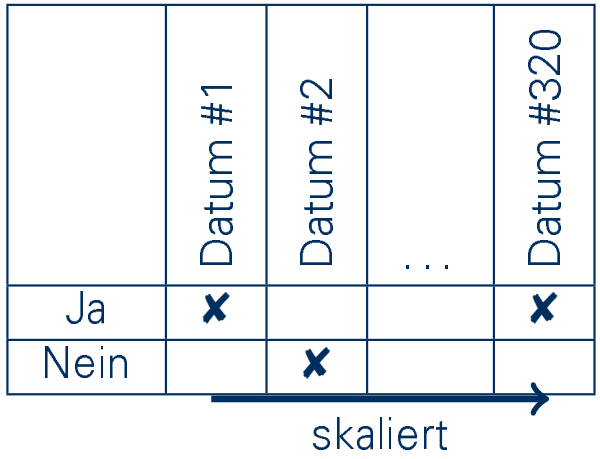
	Stimme
Kandidat #1	
Kandidat #2	✘
⋮	
Kandidat #10	

	Datum #1	Datum #2	. . .	Datum #320
Ja	✘			✘
Nein		✘		

ein Kreuz pro Spalte

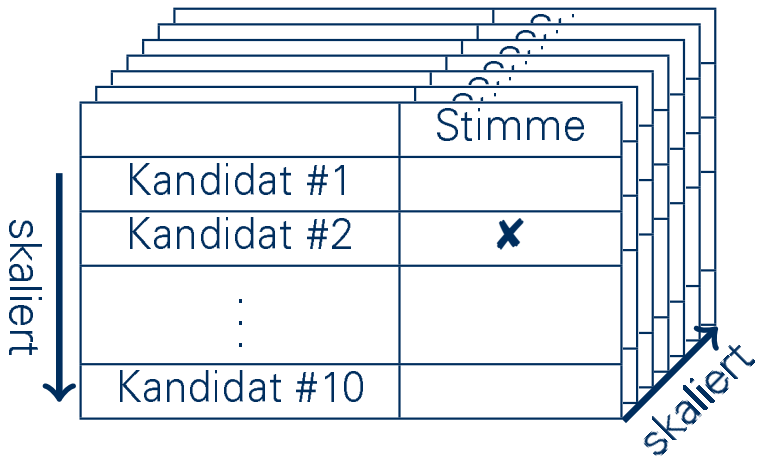
E-Voting vs. Terminplanung

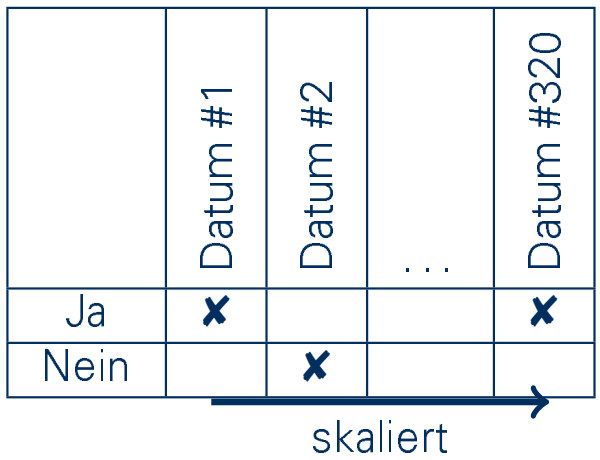




ein Kreuz pro Spalte

E-Voting vs. Terminplanung





ein Kreuz pro Spalte

TECHNISCHE UNIVERSITÄT DRESDEN

Schema

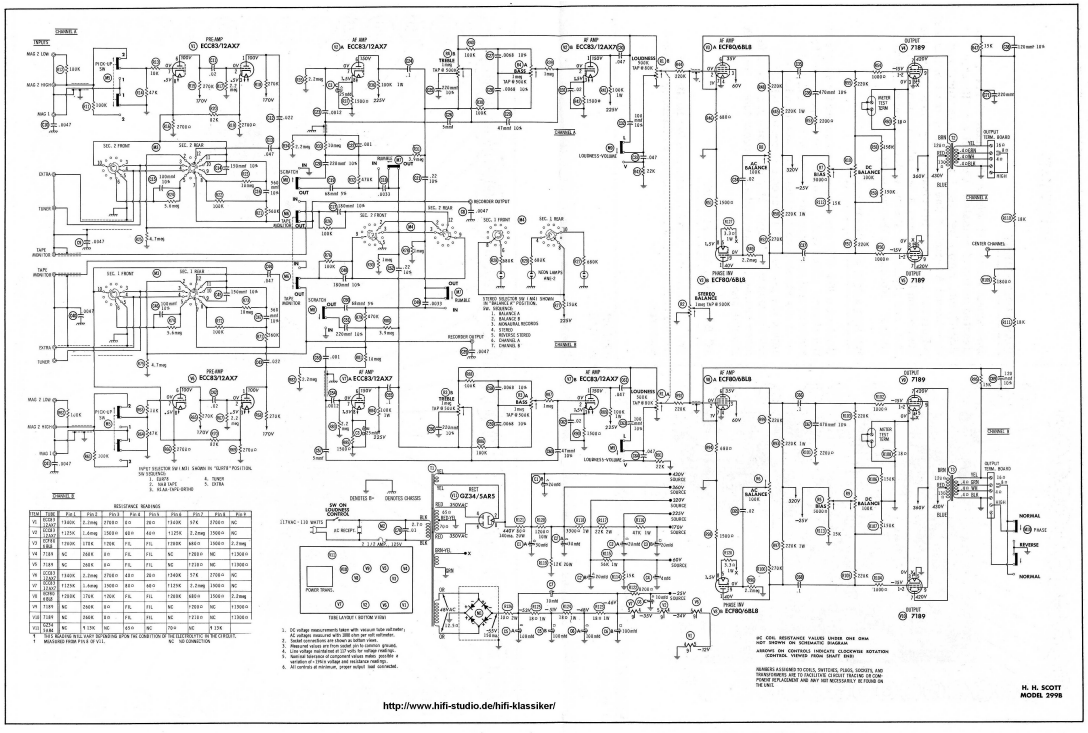
Problembeschreibung

Schema

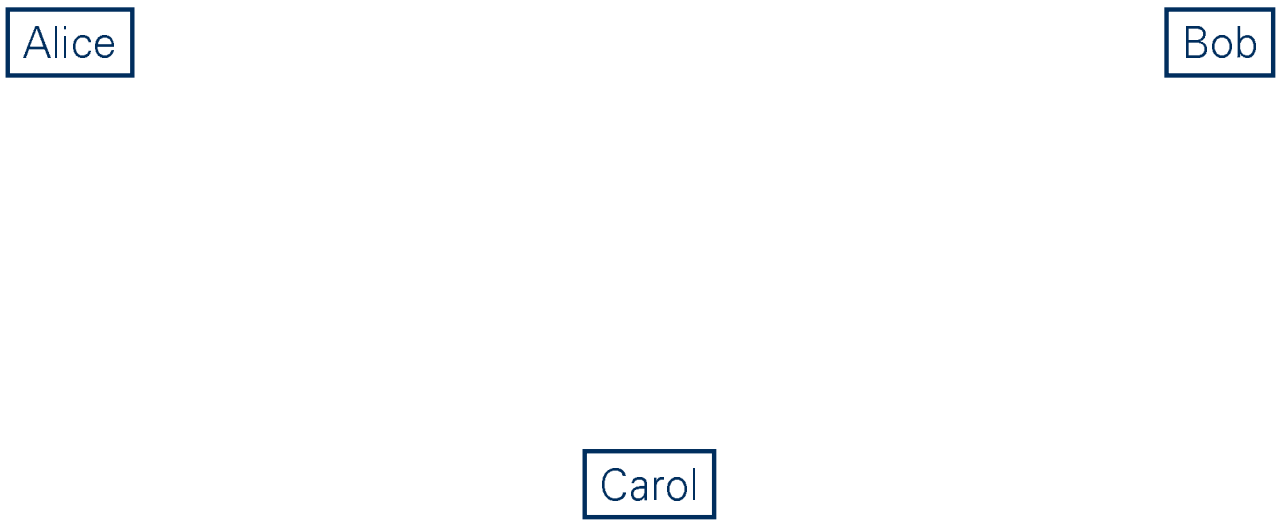
Erweiterungen

Evaluation

Zusammenfassung und Ausblick

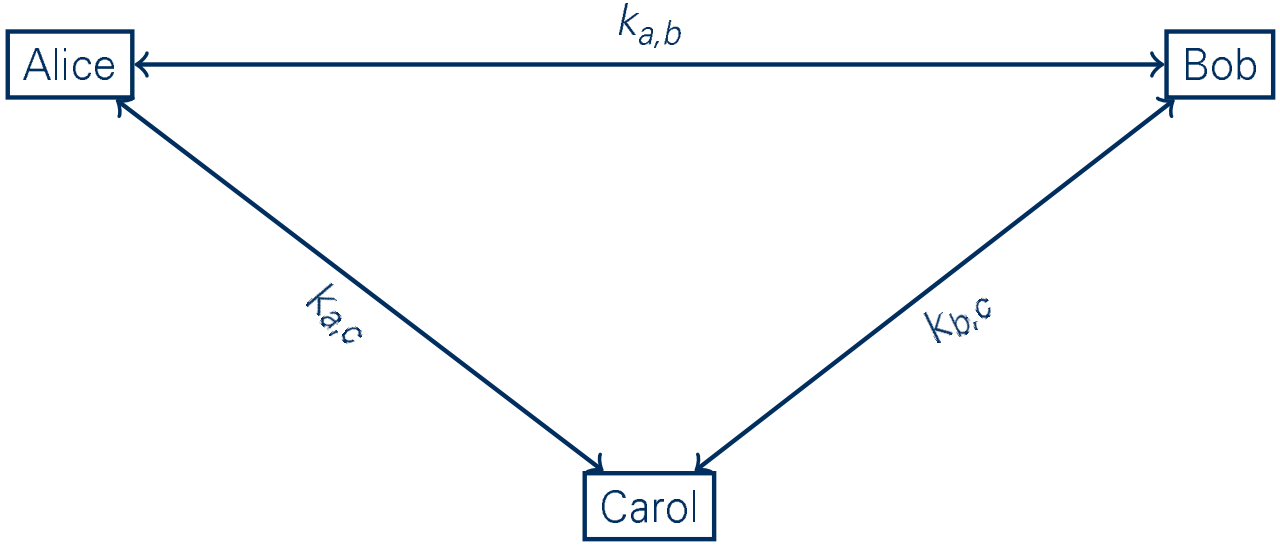


Überlagerndes Senden



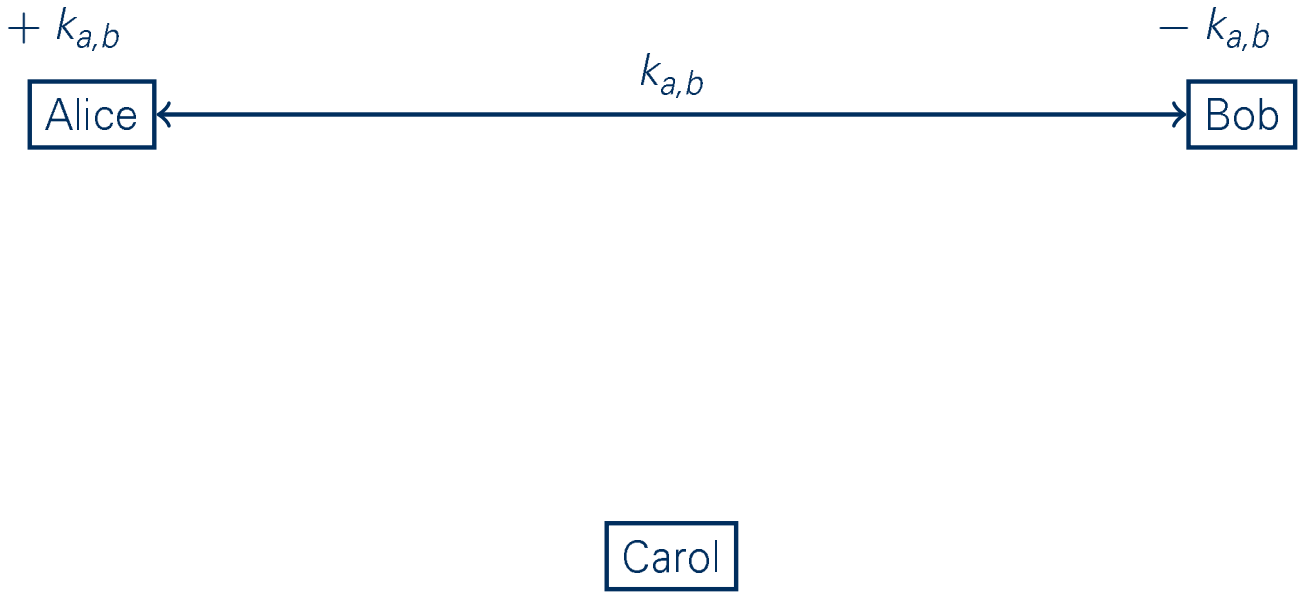
D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

Überlagerndes Senden



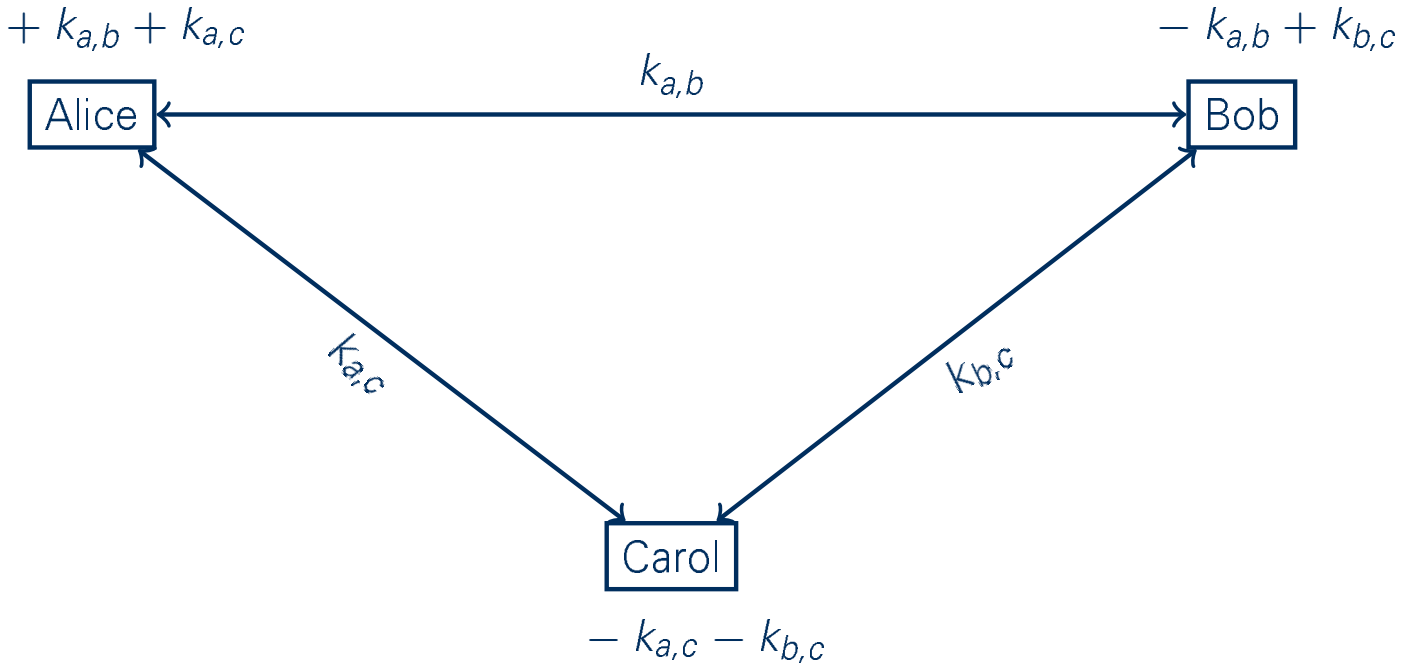
D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

Überlagerndes Senden



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

Überlagerndes Senden



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

Überlagerndes Senden

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

Alice

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

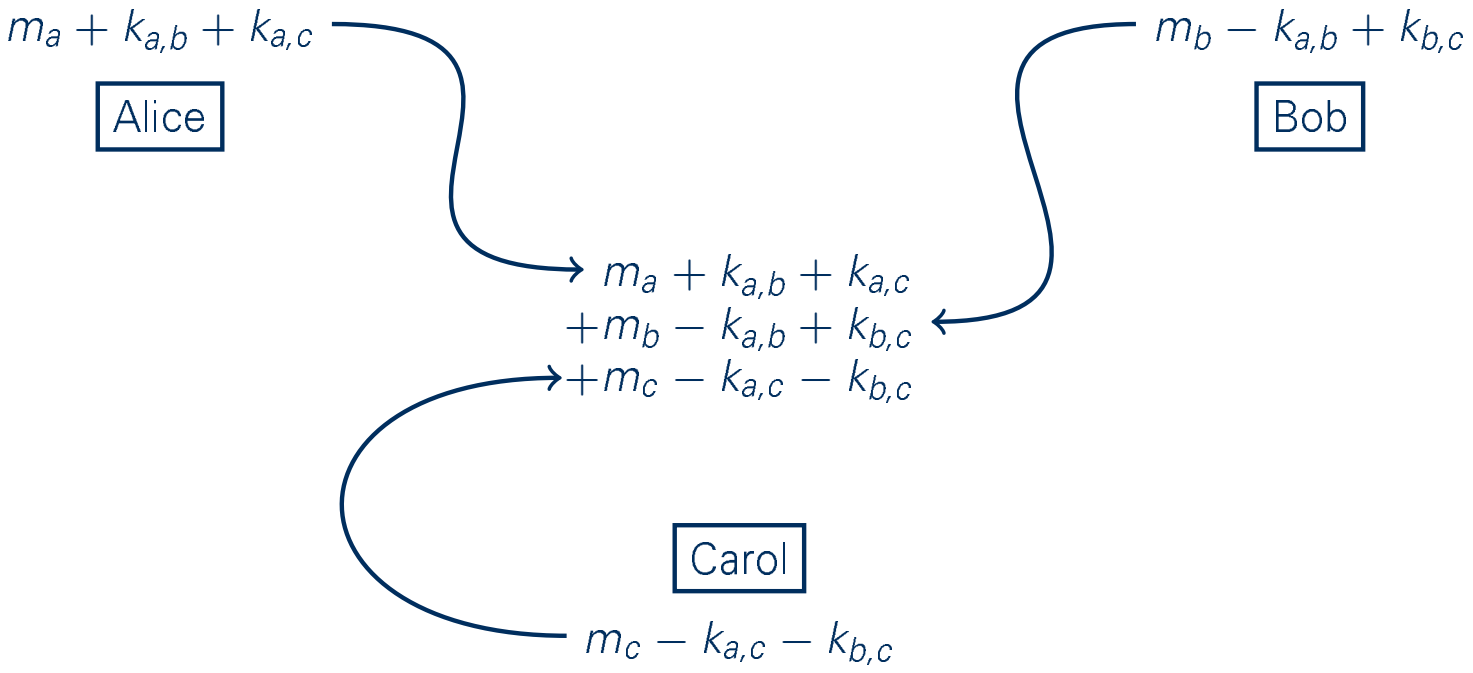
Bob

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

Überlagerndes Senden



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

Überlagerndes Senden

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

Überlagerndes Senden

Alice

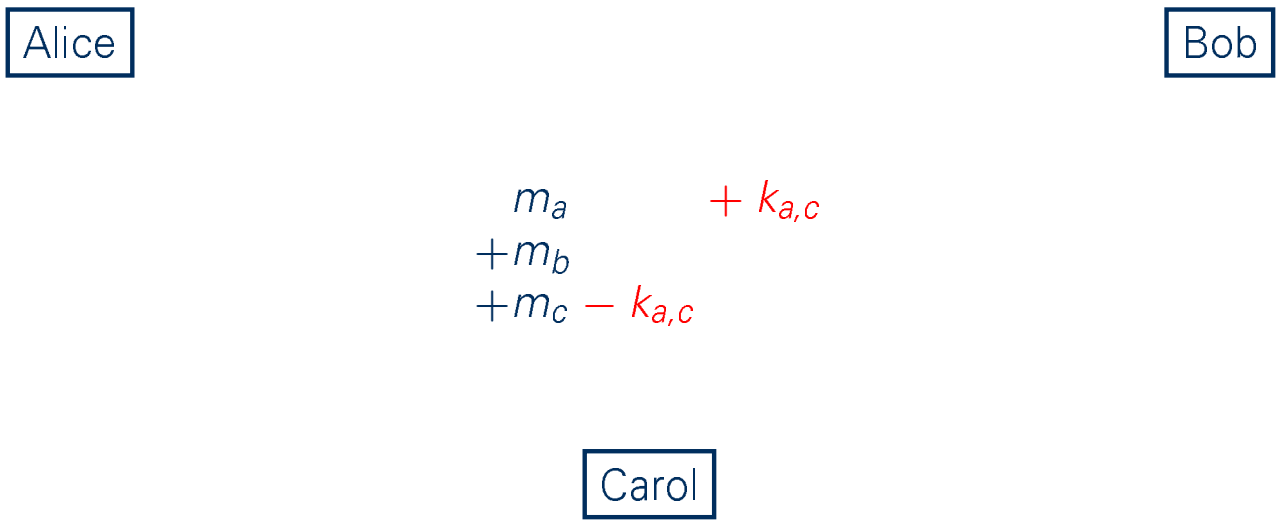
Bob

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

Carol

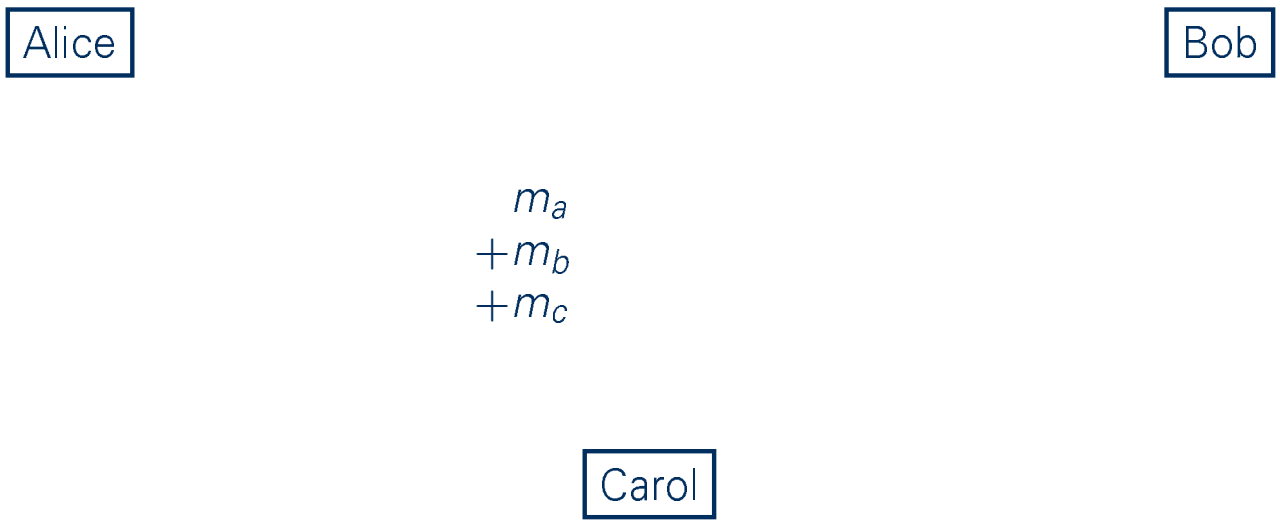
D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

Überlagerndes Senden



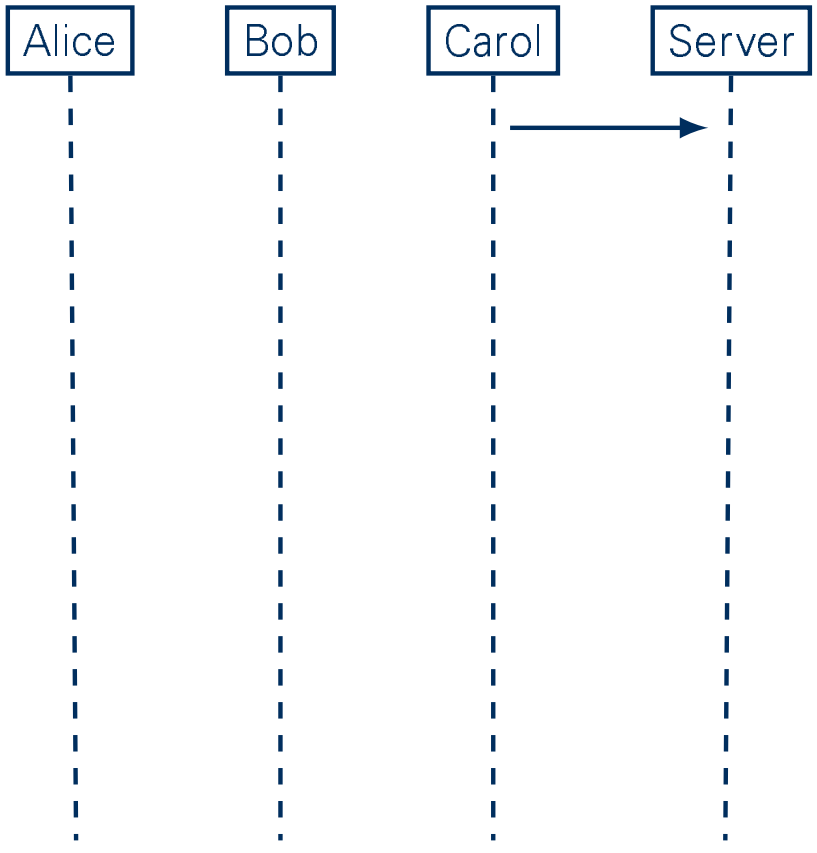
D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

Überlagerndes Senden

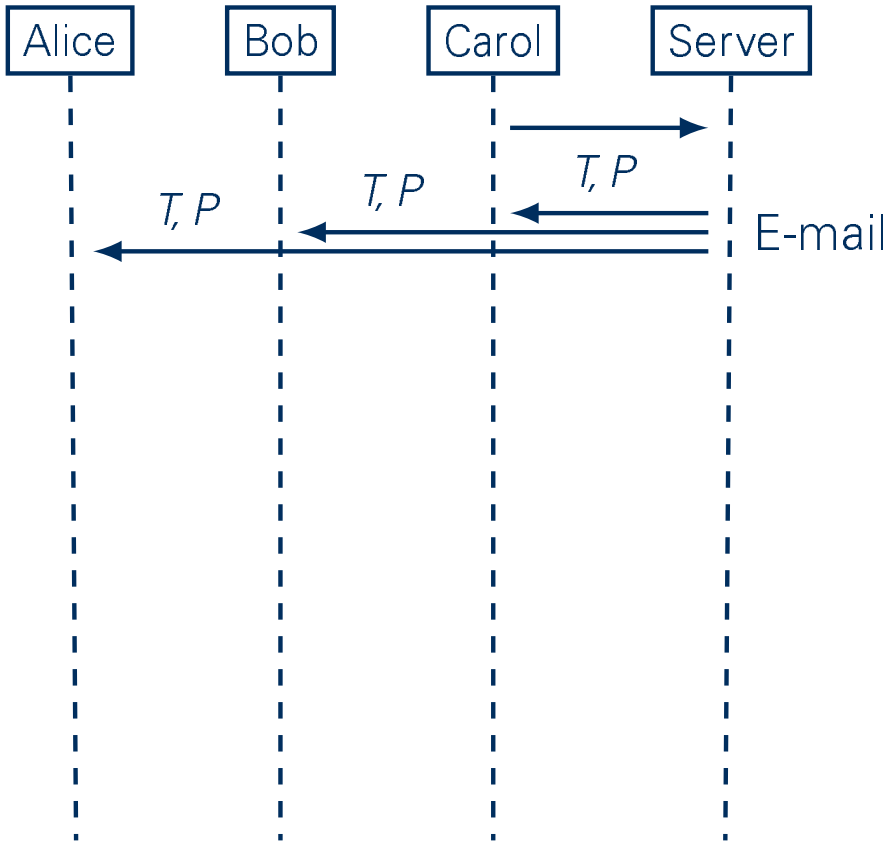


D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

Umfrageerstellung

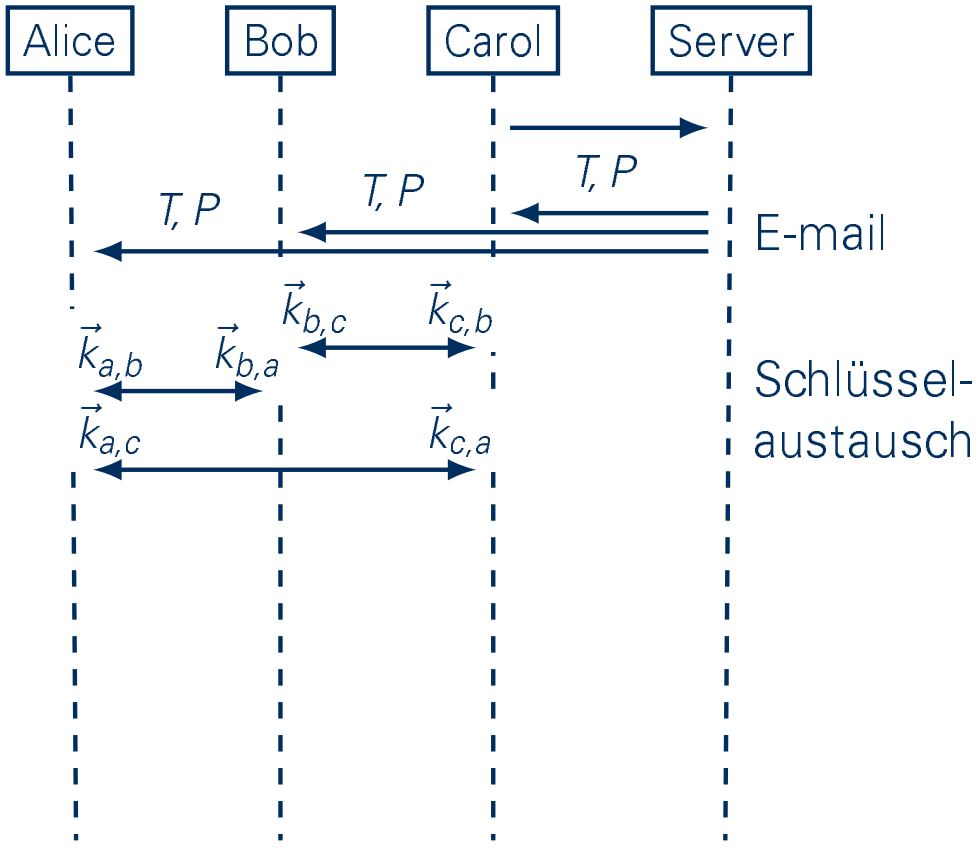


Umfrageerstellung



T . . . Zeitpunkte
P . . . voters

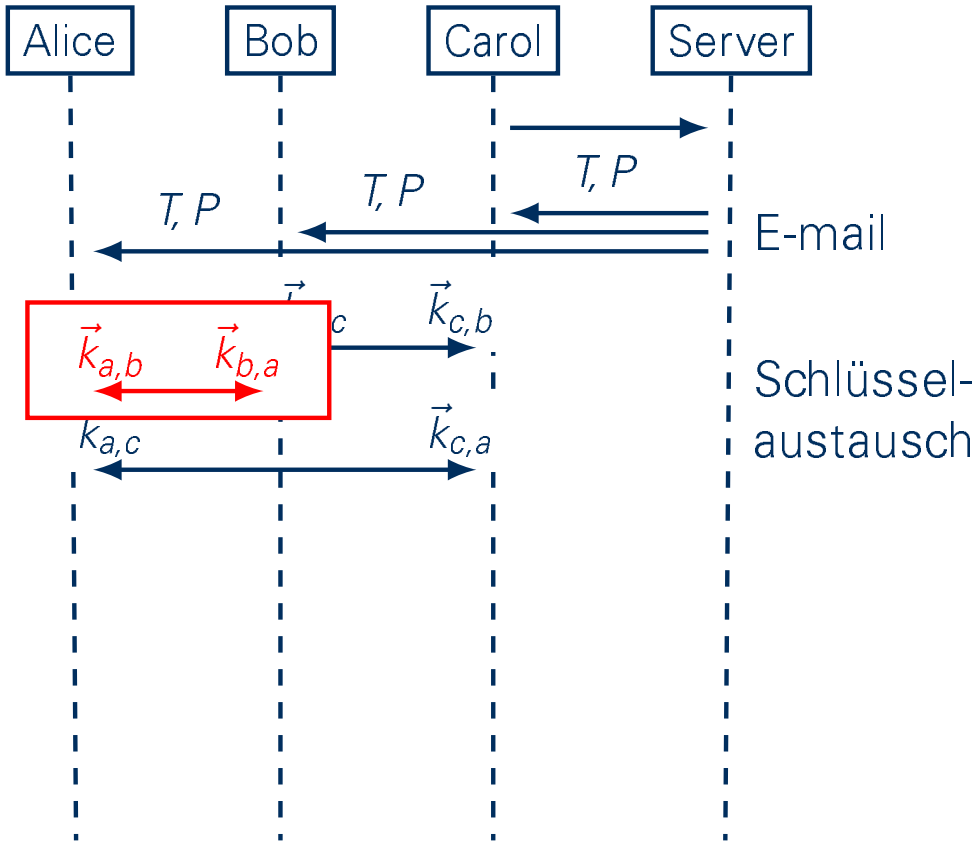
Umfrageerstellung



T . . . Zeitpunkte
P . . . voters

$\vec{k}_{i,j}$ . . . Schlüsselvektor

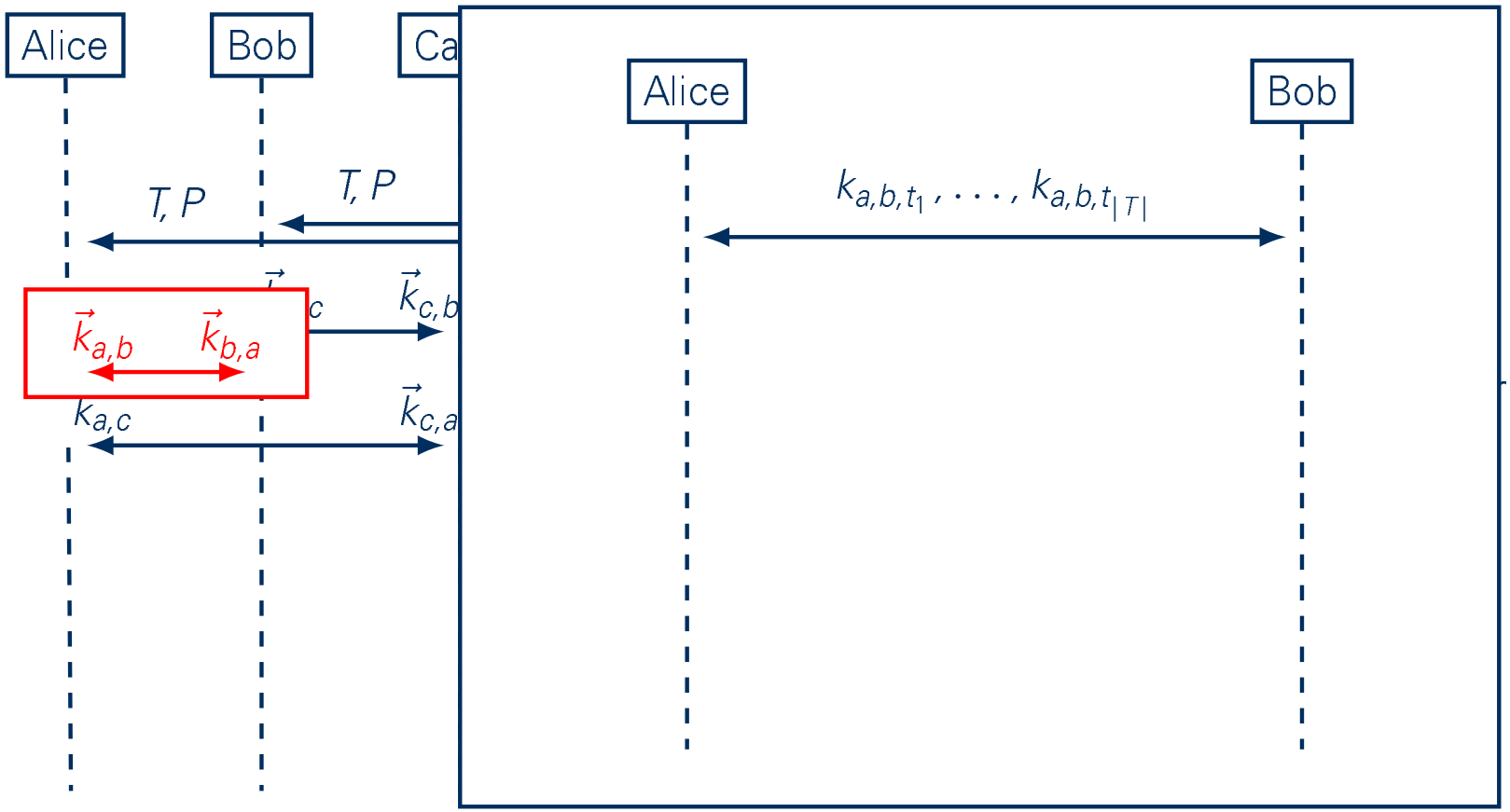
Umfrageerstellung



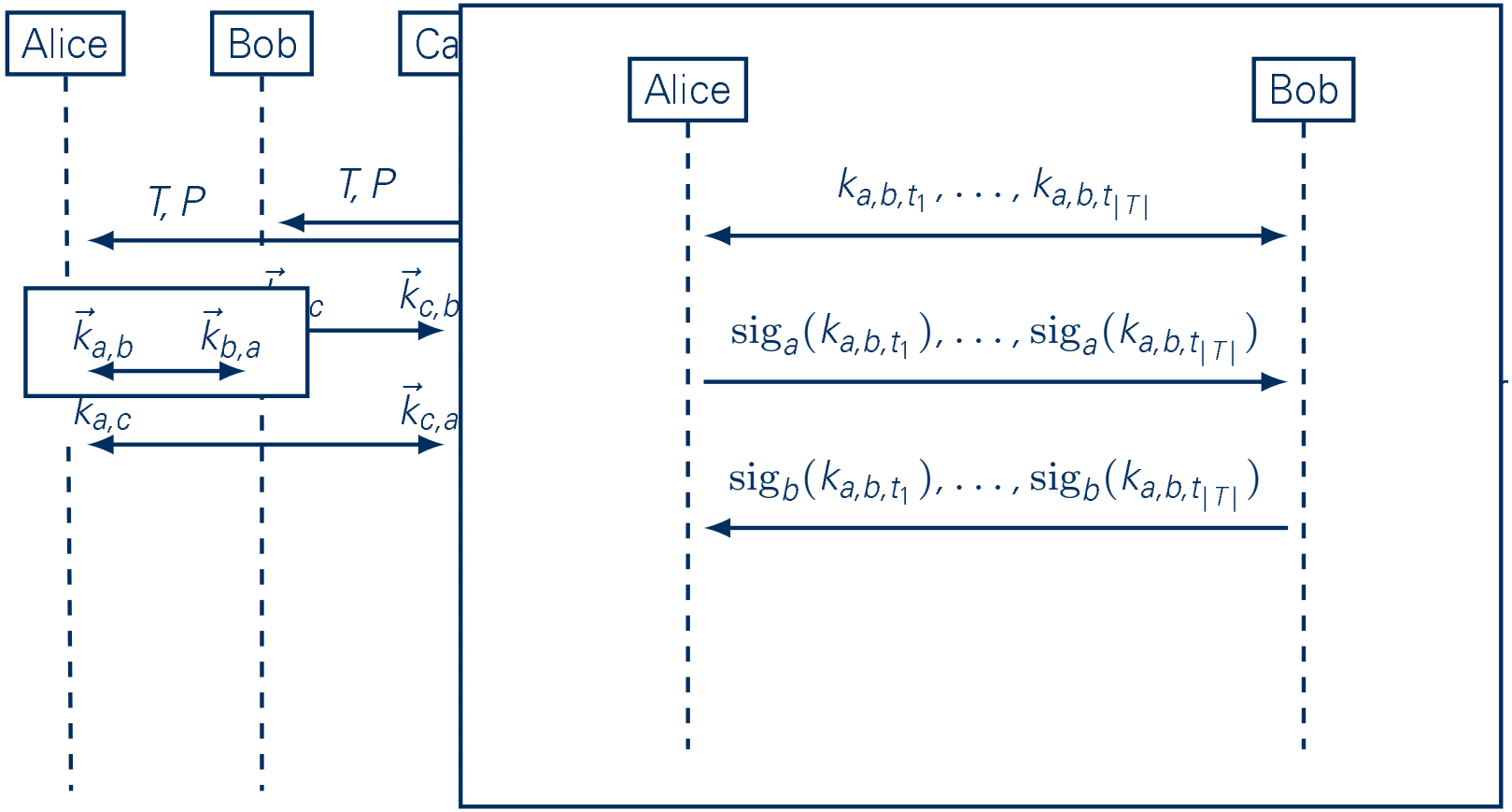
T . . . Zeitpunkte
P . . . voters

$\vec{k}_{i,j}$ . . . Schlüsselvektor

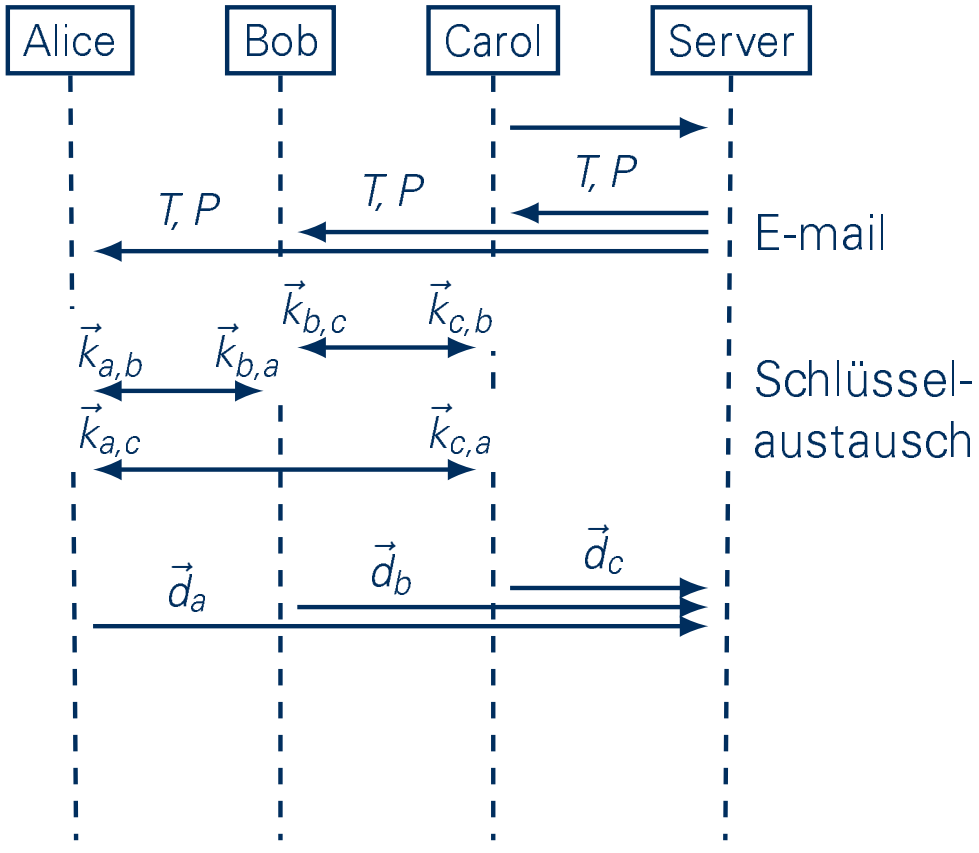
Umfrageerstellung



Umfrageerstellung



Stimmenabgabe

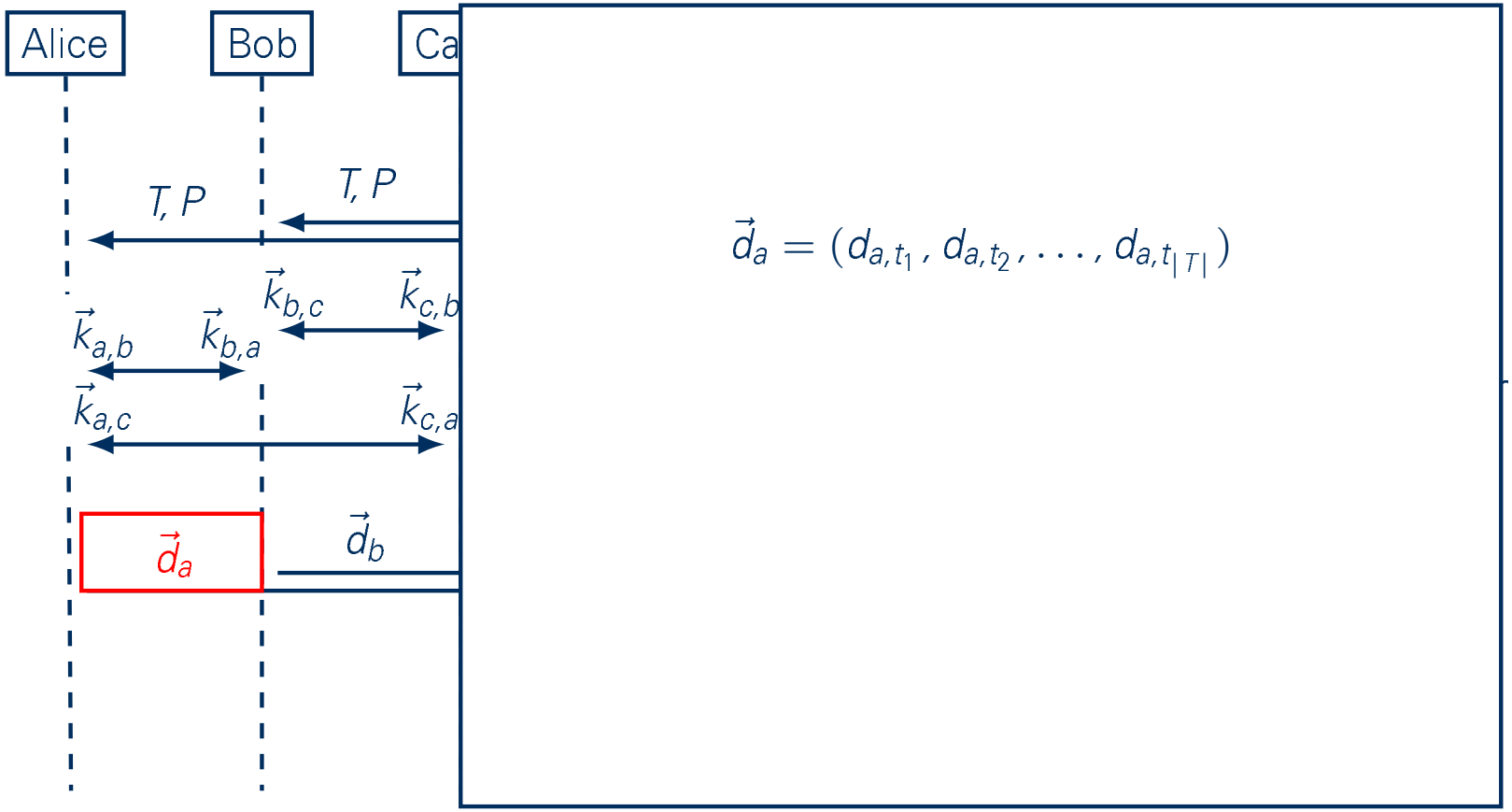


T . . . Zeitpunkte
P . . . voters

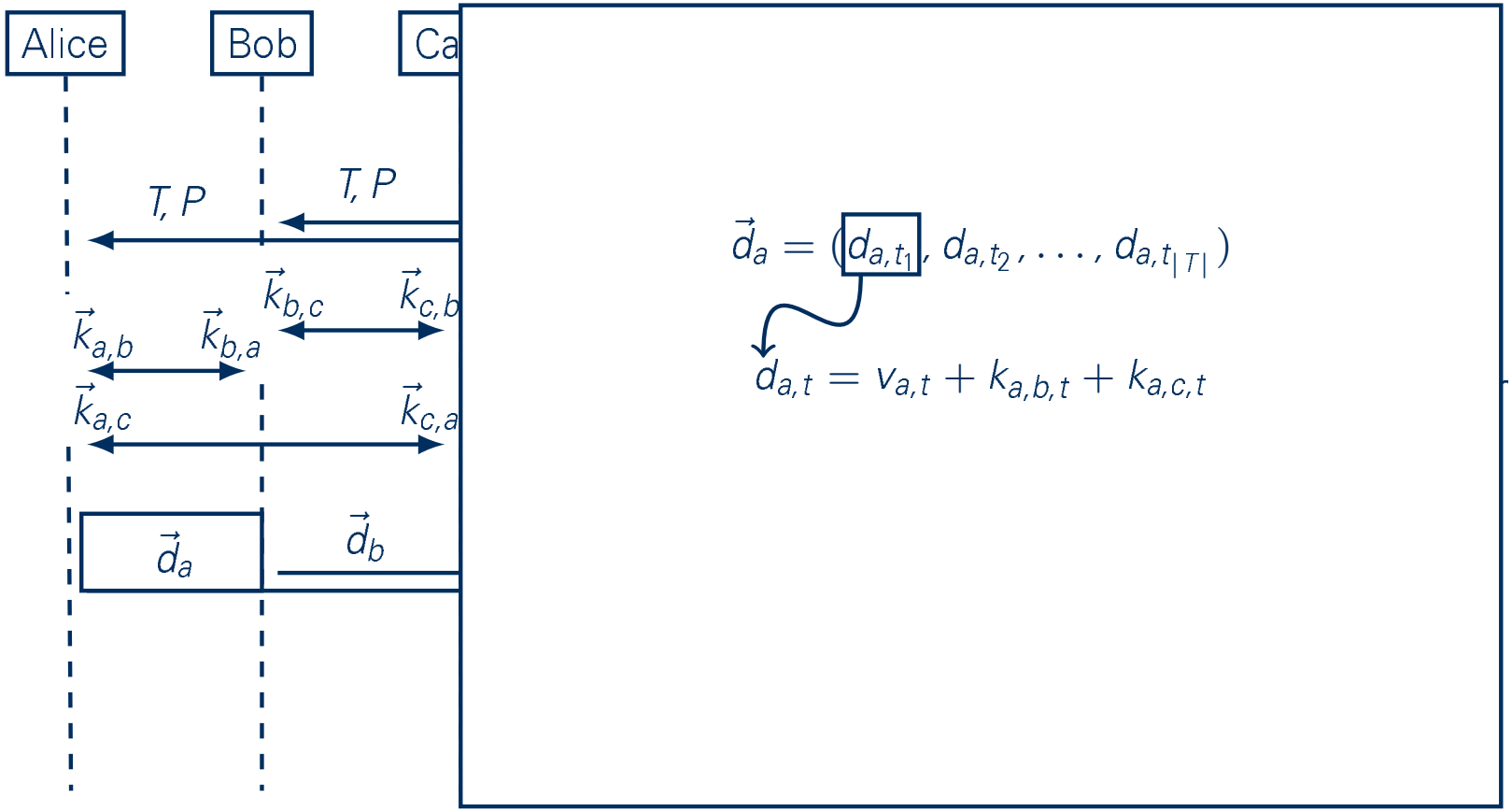
$\vec{k}_{i,j}$ . . . Schlüsselvektor

$\vec{d}$ . . . verschlüsselte Stimme

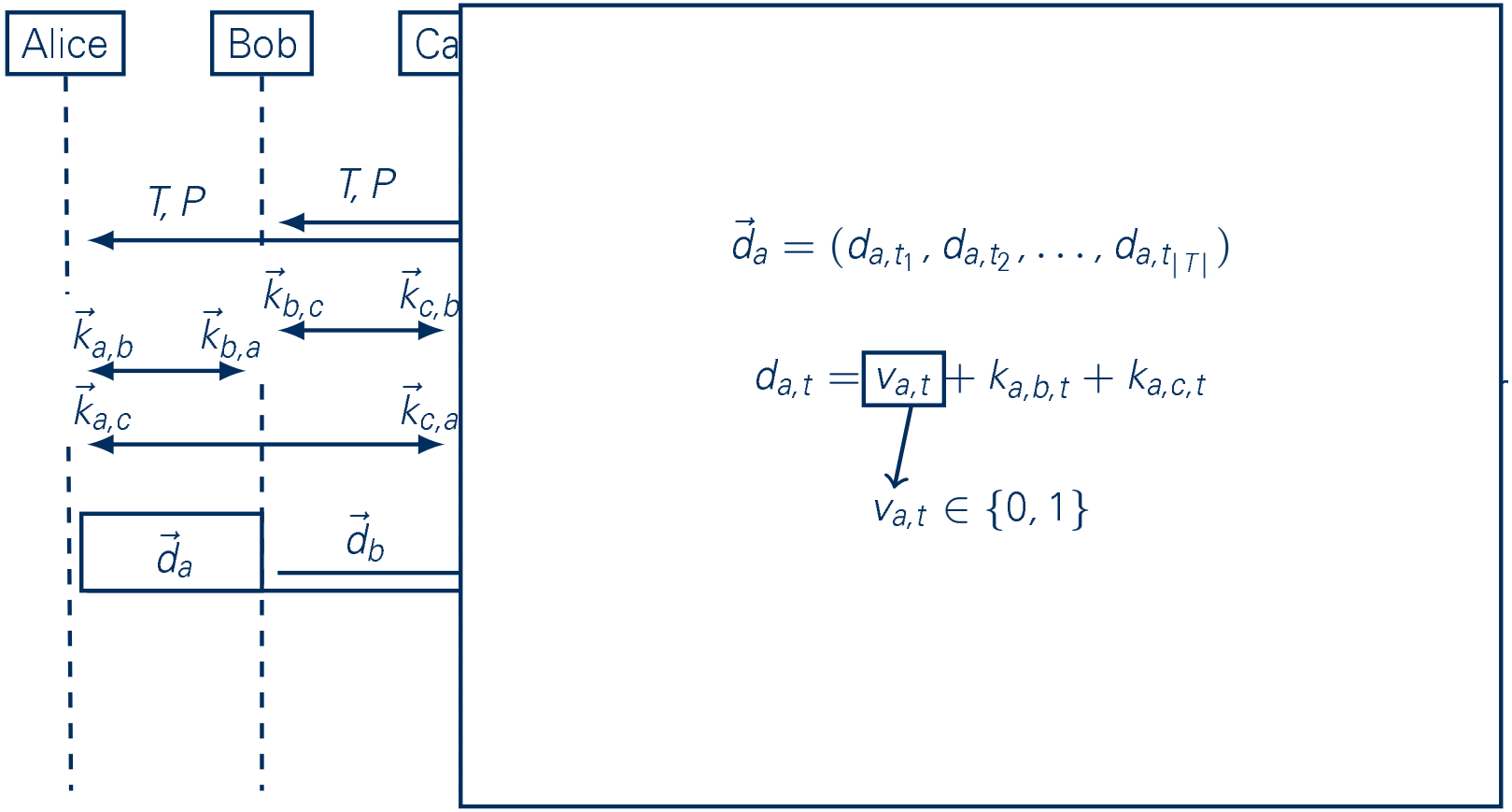
Stimmenabgabe



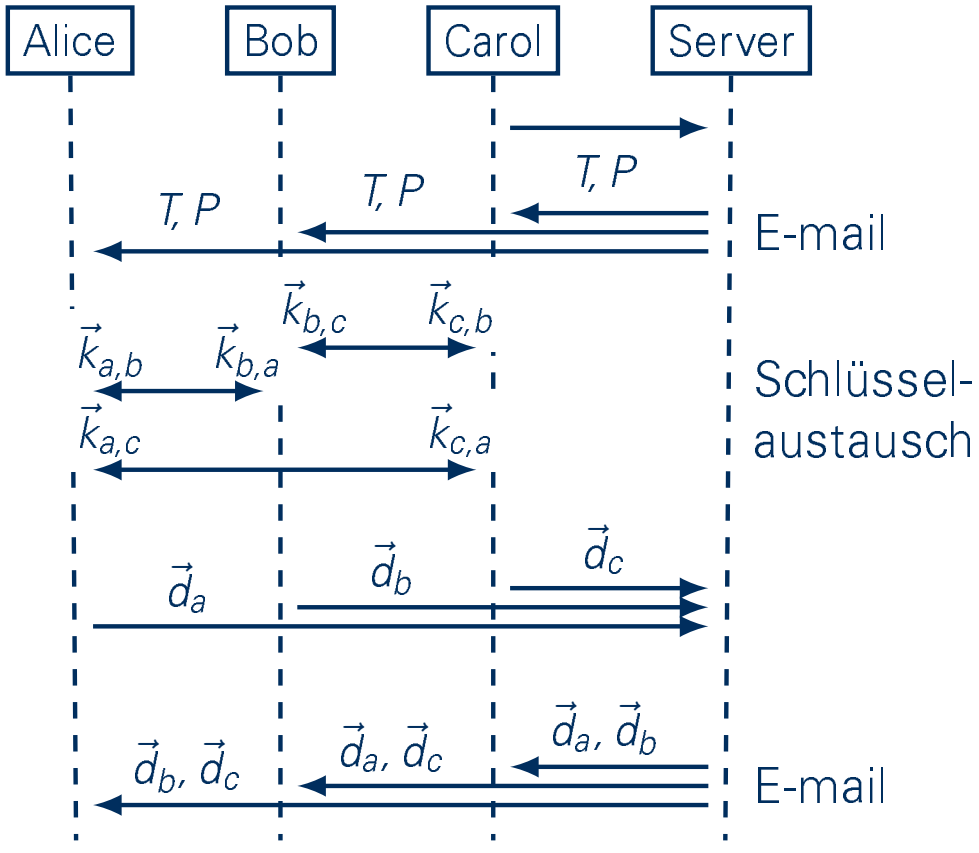
Stimmenabgabe



Stimmenabgabe



Ergebnisveröffentlichung

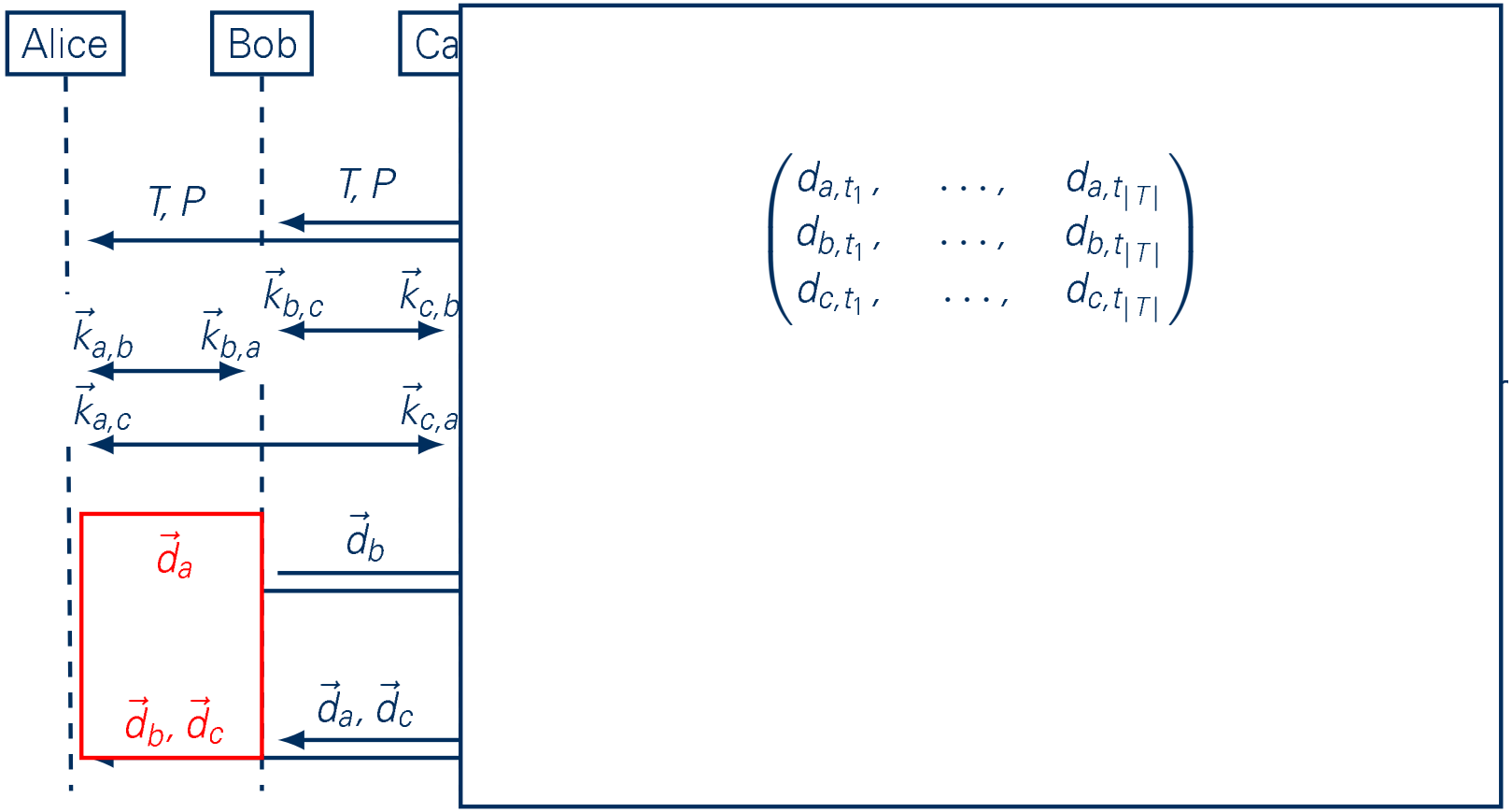


T . . . Zeitpunkte
P . . . voters

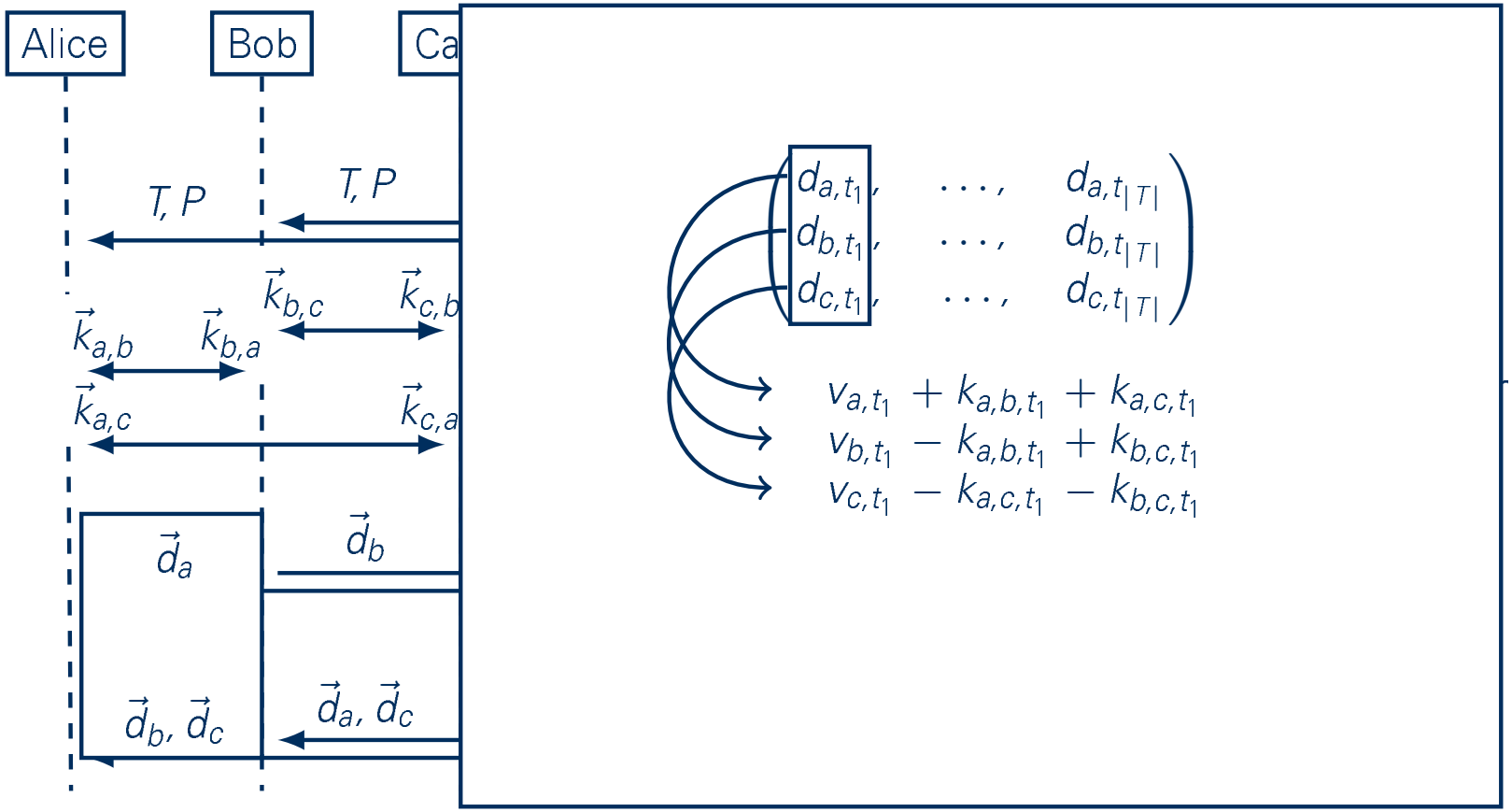
$\vec{k}_{i,j}$ . . . Schlüsselvektor

$\vec{d}$ . . . verschlüsselte Stimme

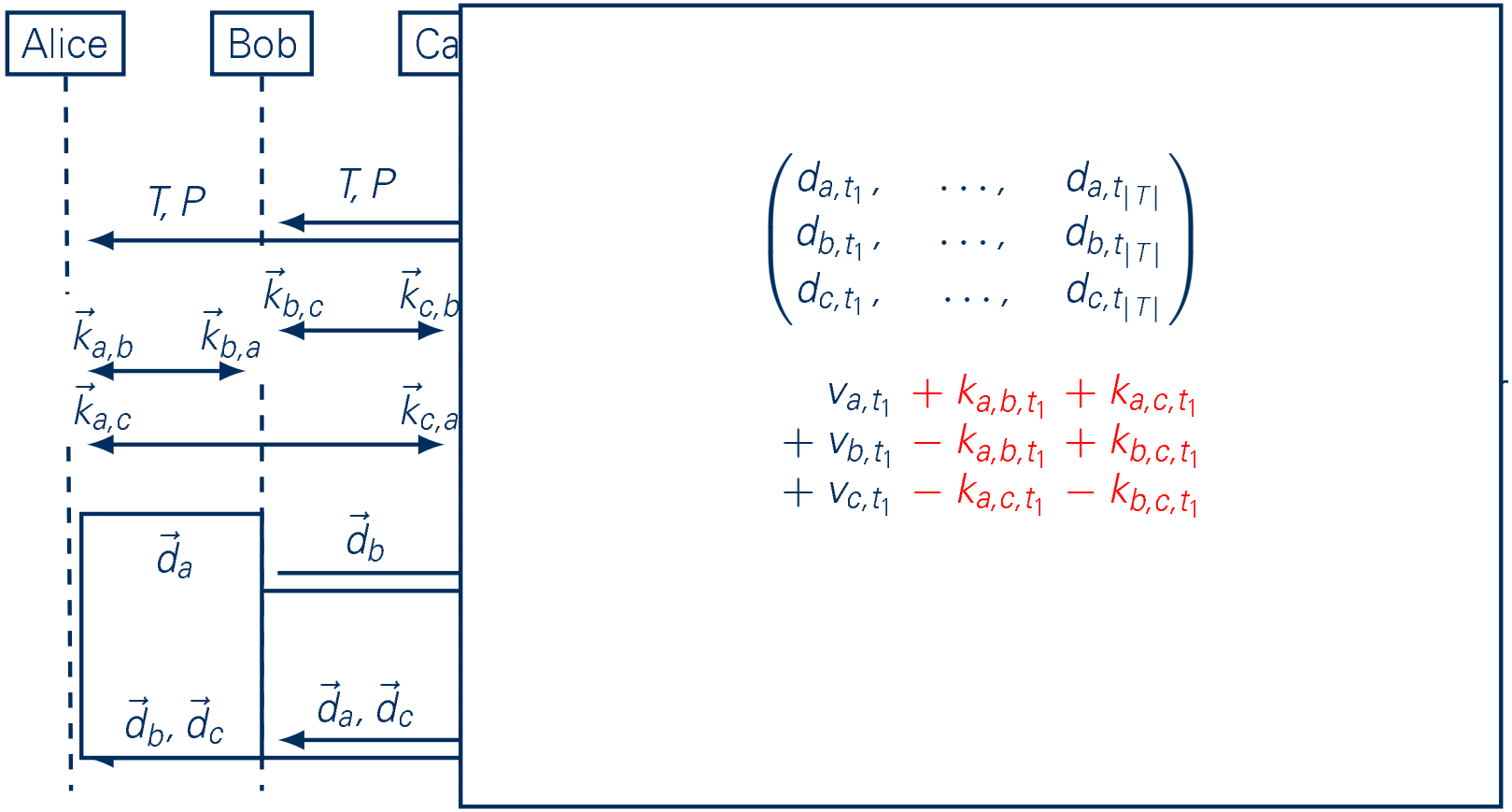
Ergebnisveröffentlichung



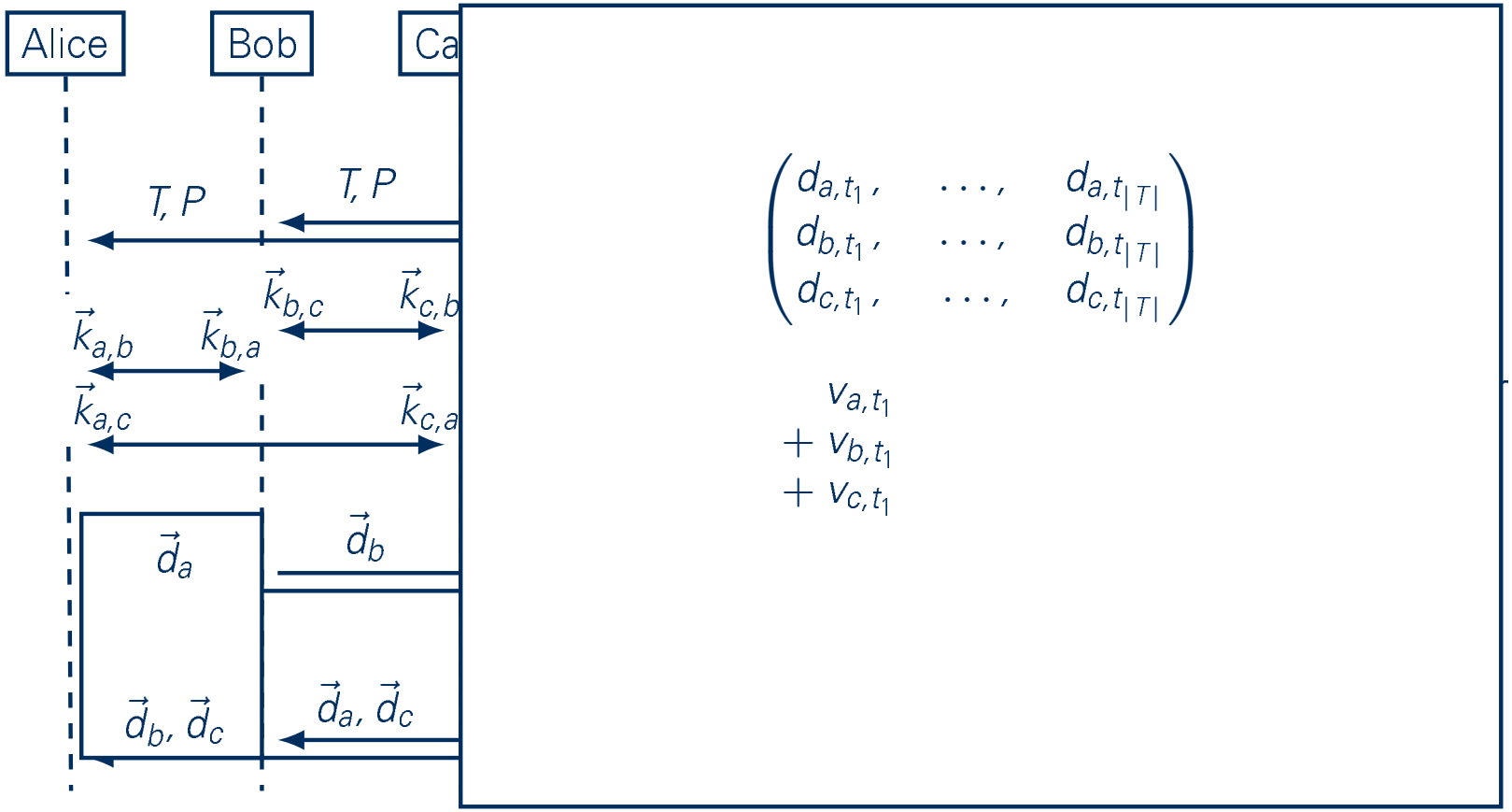
Ergebnisveröffentlichung



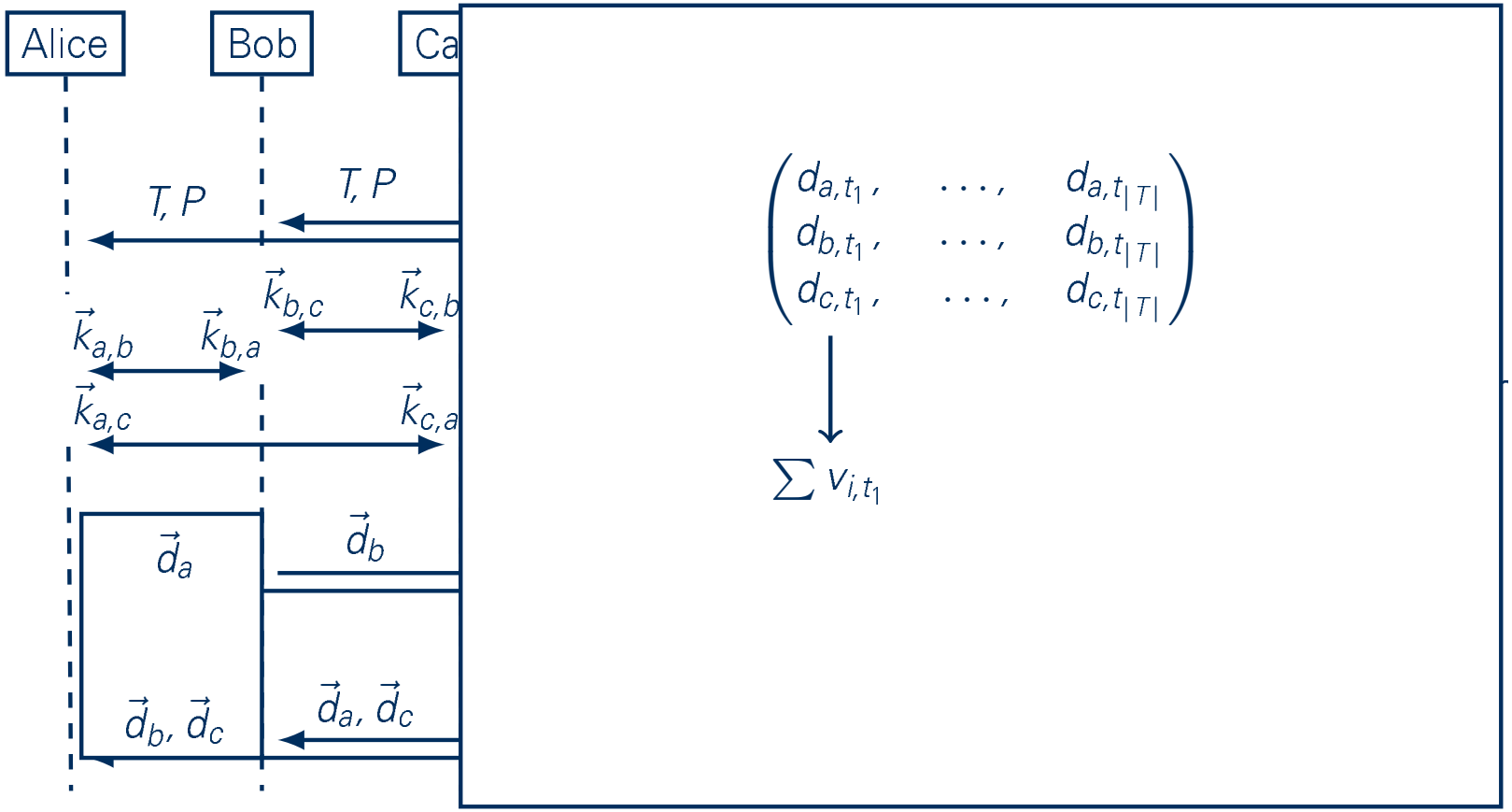
Ergebnisveröffentlichung



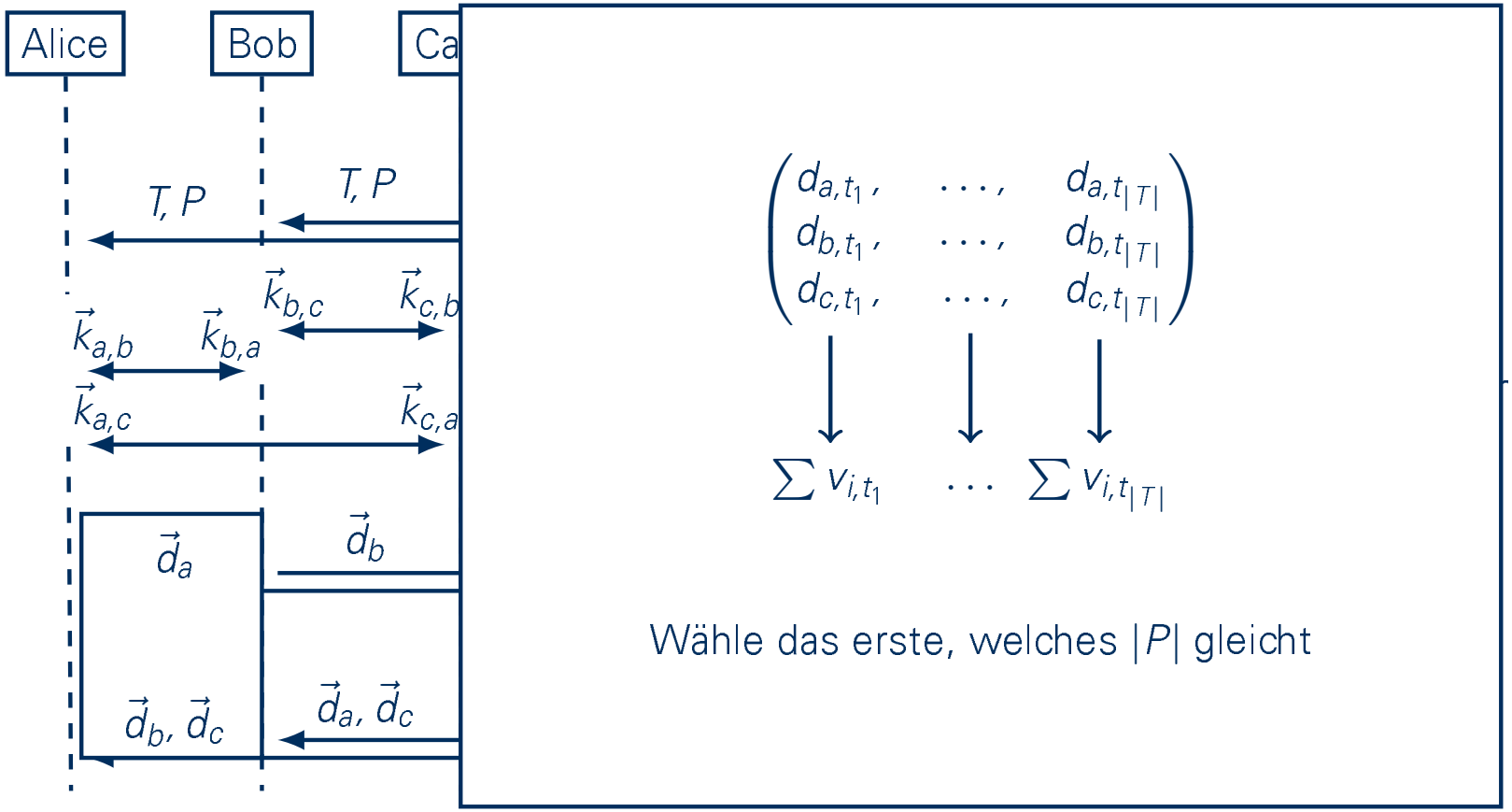
Ergebnisveröffentlichung



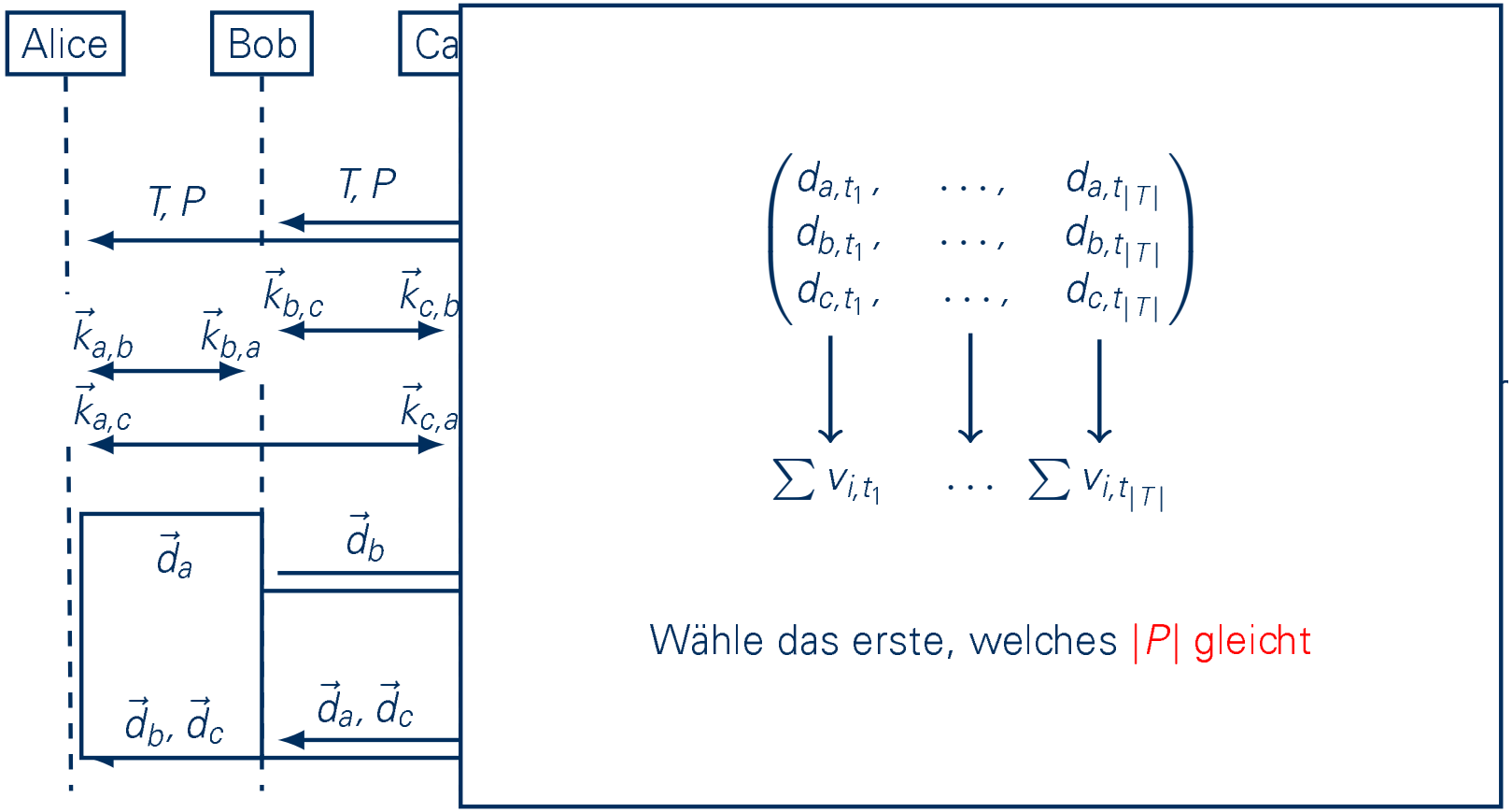
Ergebnisveröffentlichung



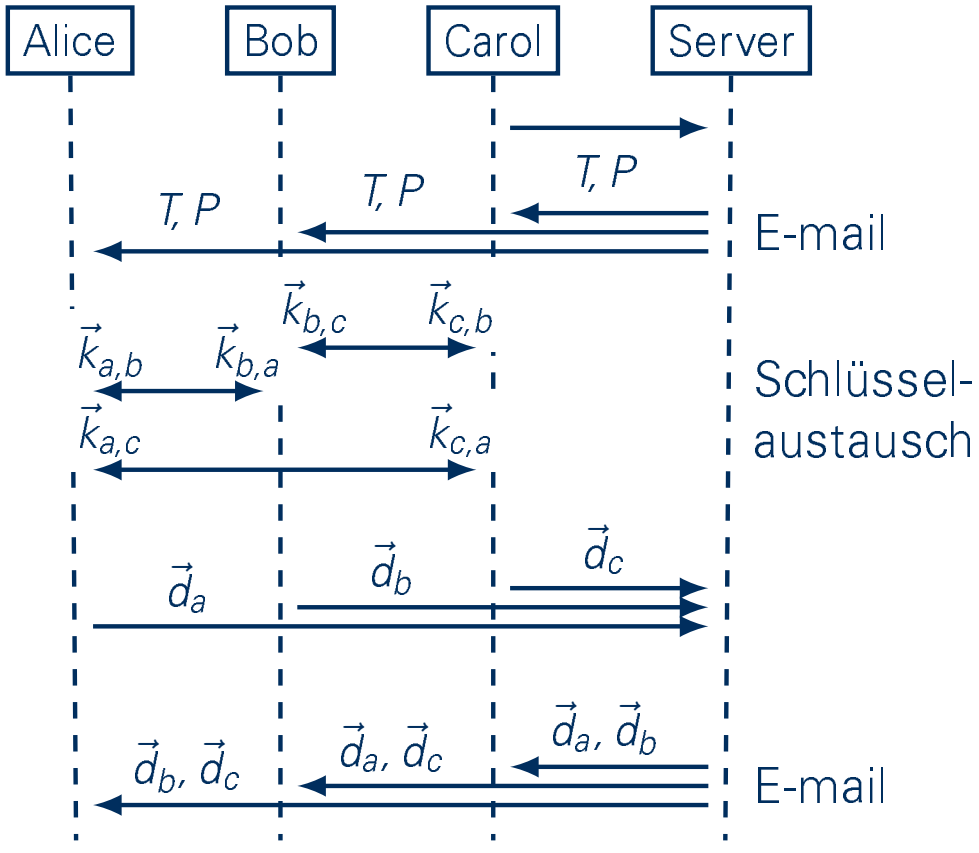
Ergebnisveröffentlichung



Ergebnisveröffentlichung



Cheating

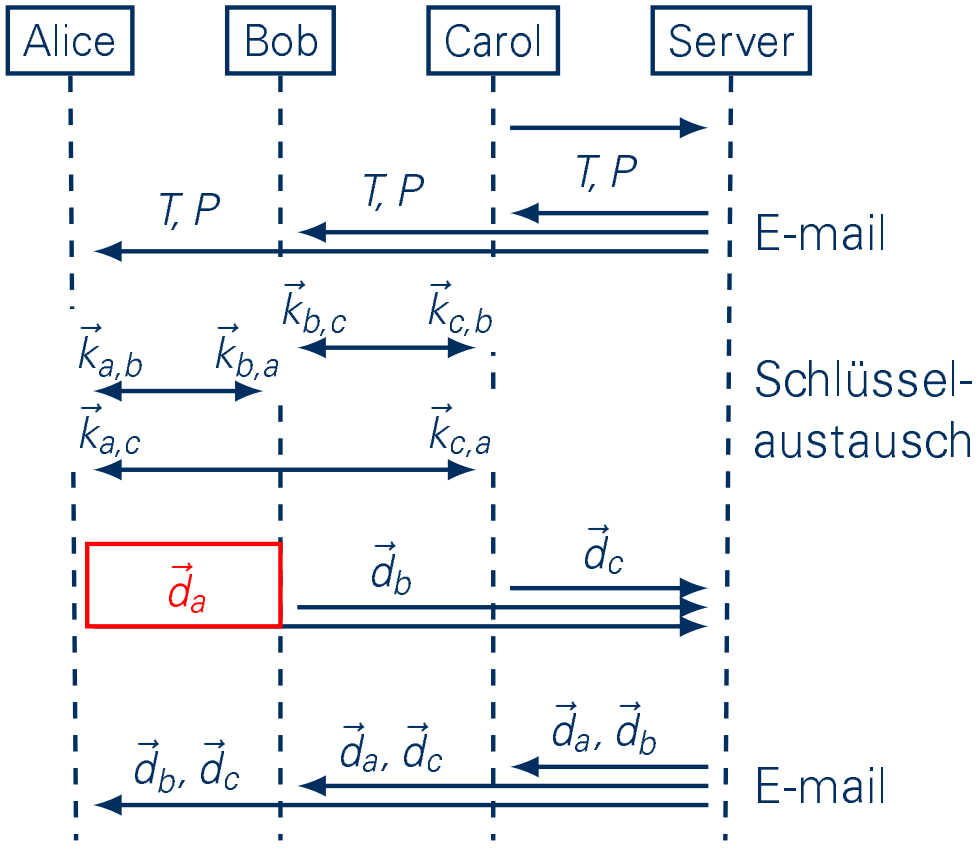


T . . . Zeitpunkte
P . . . voters

$\vec{k}_{i,j}$ . . . Schlüsselvektor

$\vec{d}$ . . . verschlüsselte Stimme

Cheating

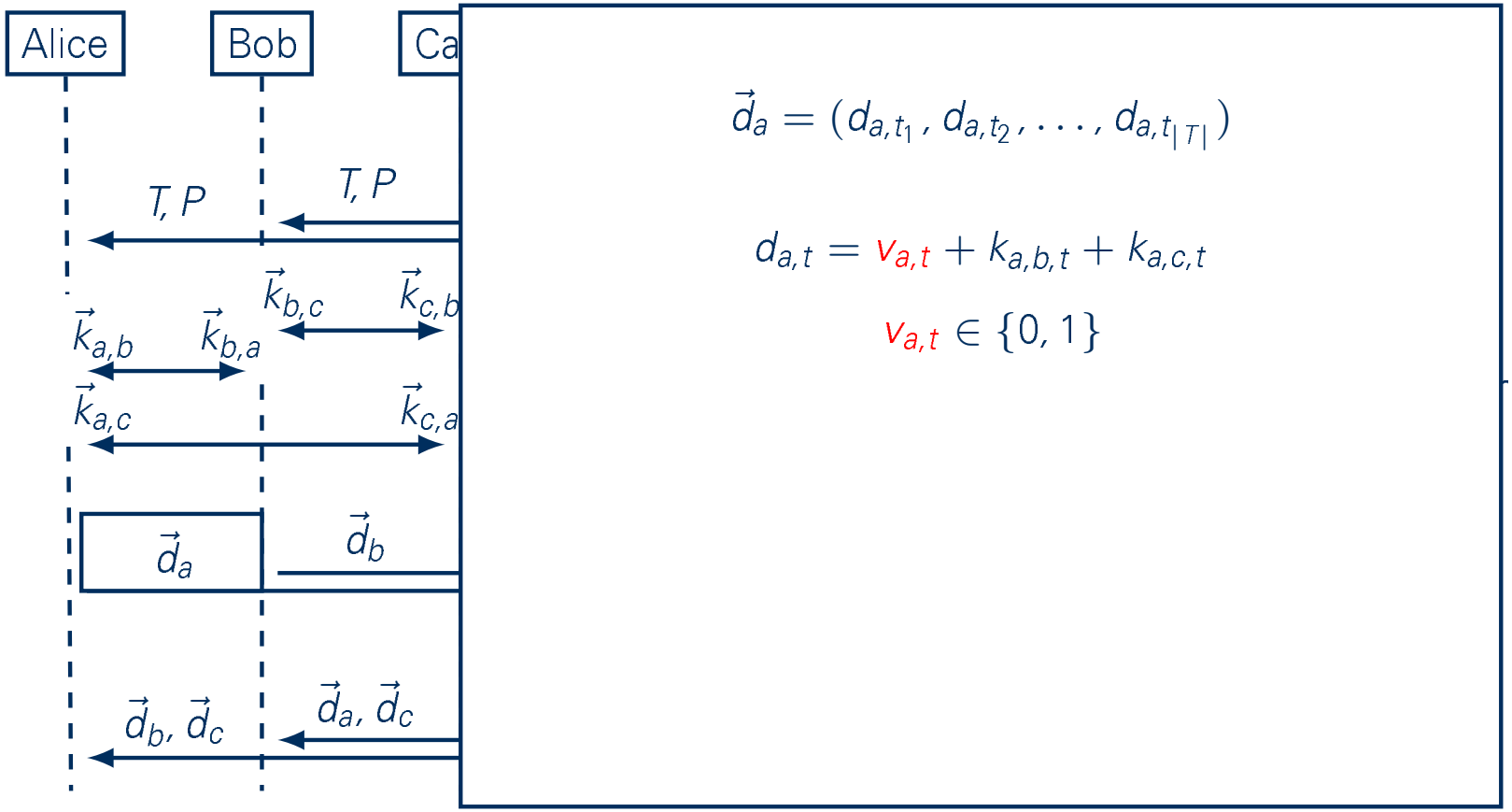


T . . . Zeitpunkte
P . . . voters

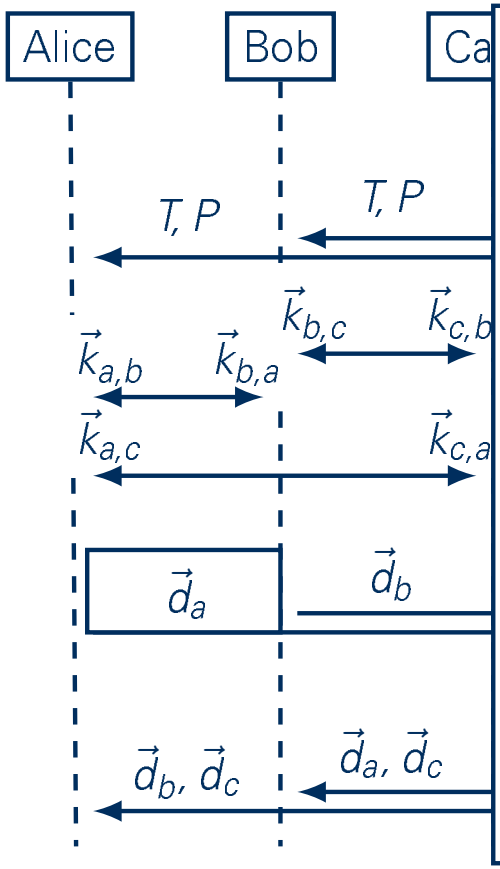
$\vec{k}_{i,j}$ . . . Schlüsselvektor

$\vec{d}$ . . . verschlüsselte Stimme

Cheating


Alice
Bob
Ca
T, P
T, P
$\vec{k}_{b,c}$
$\vec{k}_{c,b}$
$\vec{k}_{a,b}$
$\vec{k}_{b,a}$
$\vec{k}_{a,c}$
$\vec{k}_{c,a}$
$\vec{d}_a$
$\vec{d}_b$
$\vec{d}_b, \vec{d}_c$
$\vec{d}_a, \vec{d}_c$
$\vec{d}_a = (d_{a,t_1}, d_{a,t_2}, \ldots, d_{a,t_{|T|}})$
$d_{a,t} = v_{a,t} + k_{a,b,t} + k_{a,c,t}$
$v_{a,t} \in \{0, 1\}$

Cheating



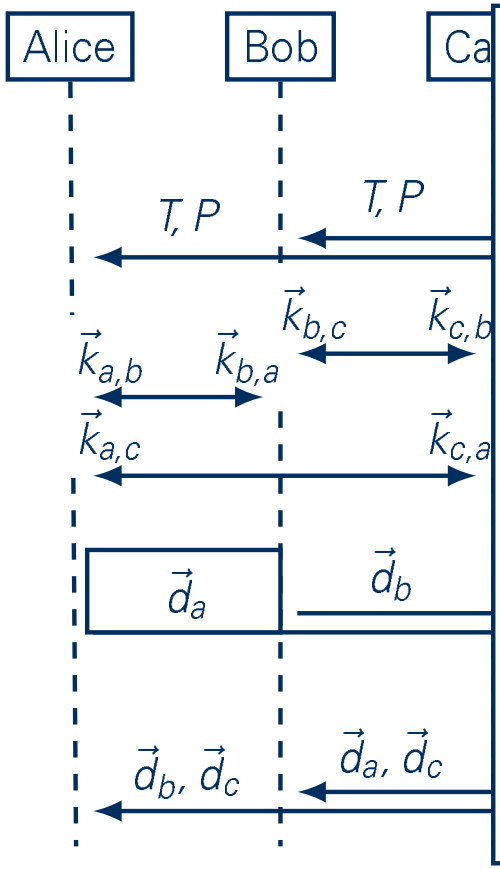
$$\vec{d}_a = (d_{a,t_1}, d_{a,t_2}, \ldots, d_{a,t_{|T|}})$$

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

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

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

Cheating



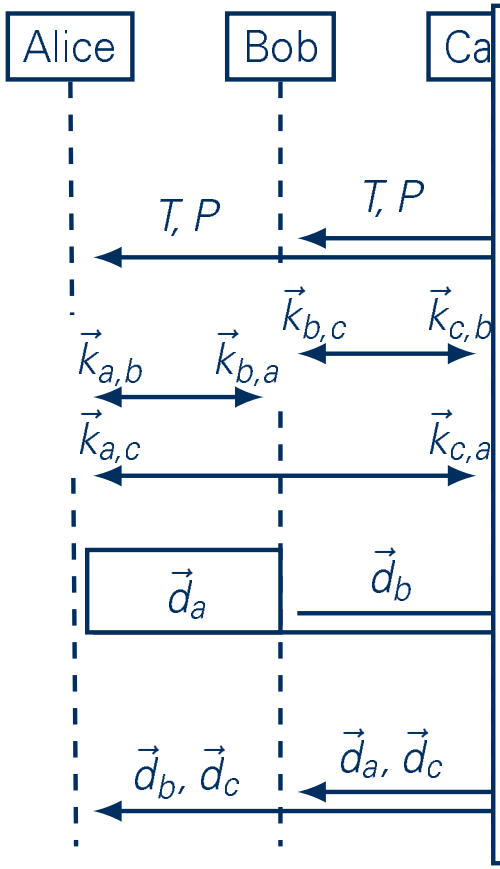
$$\vec{d}_a = (d_{a,t_1}, d_{a,t_2}, \ldots, d_{a,t_{|T|}})$$

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

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

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

Cheating



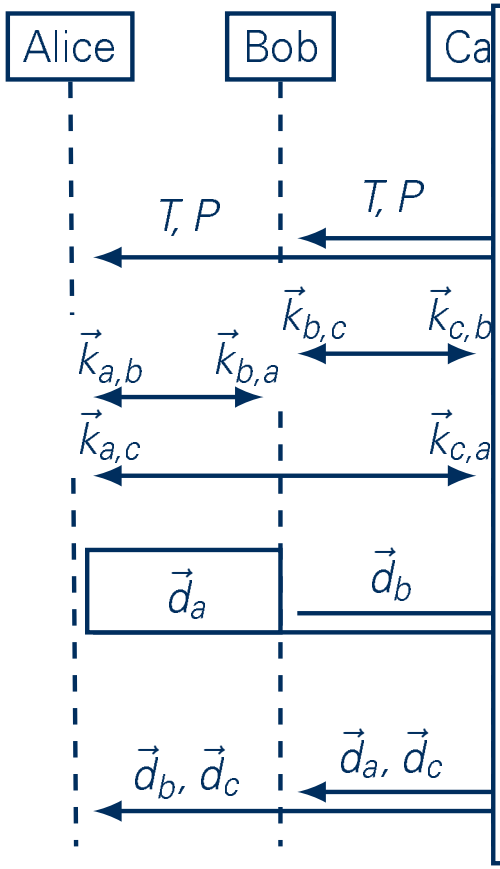
$$\vec{d}_a = (d_{a,t_1}, d_{a,t_2}, \ldots, d_{a,t_{|T|}})$$

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

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

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

Cheating



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

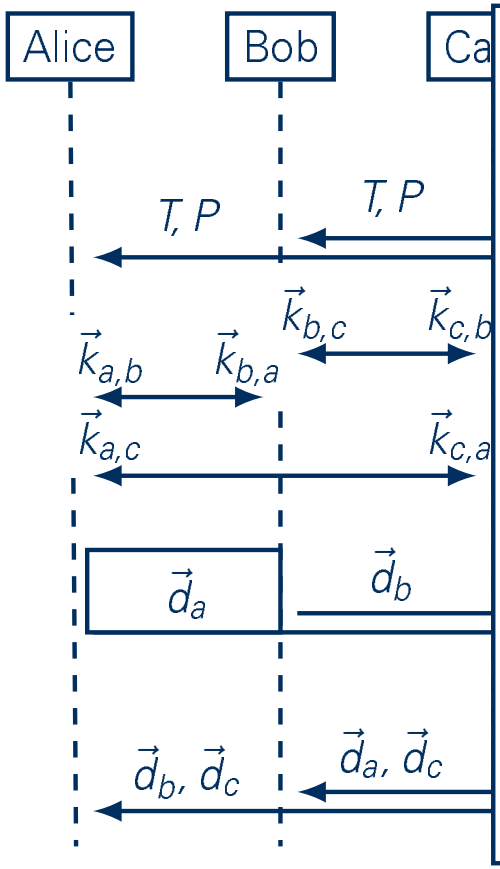
$$d_{a,t} = v_{a,t} + k_{a,b,t} + k_{a,c,t}$$

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

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

Wähle das erste, welches $|P|$ gleicht

Cheating



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

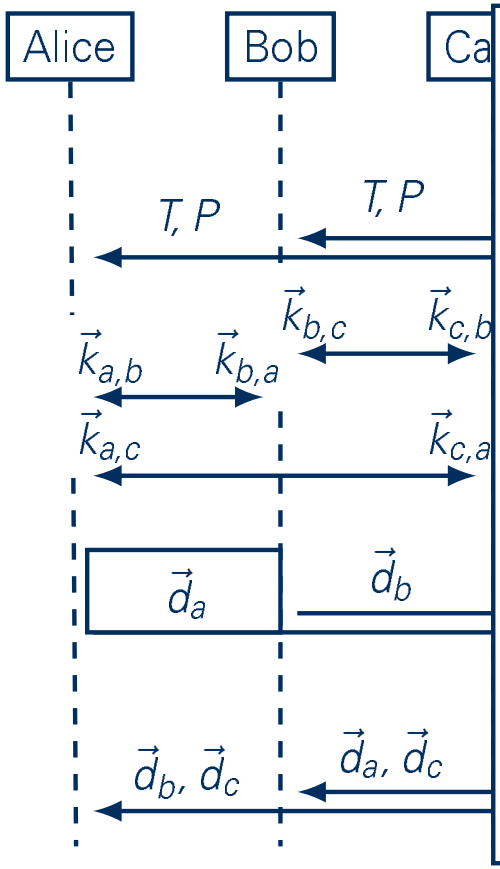
$$d_{a,t} = v_{a,t} + k_{a,b,t} + k_{a,c,t}$$

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

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

Wähle das erste, welches $|P|$ gleicht

Cheating



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

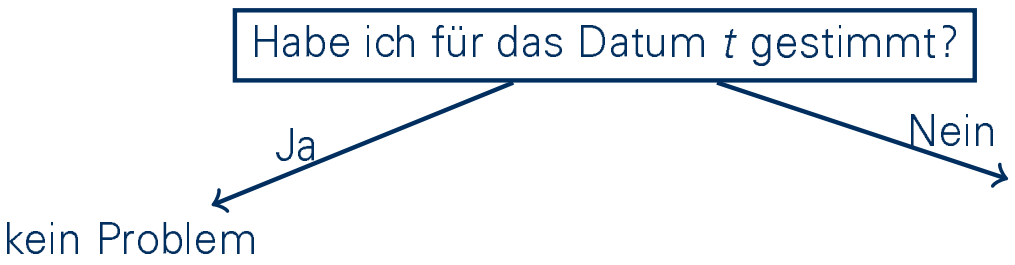
$$d_{a,t} = v_{a,t} + k_{a,b,t} + k_{a,c,t}$$

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

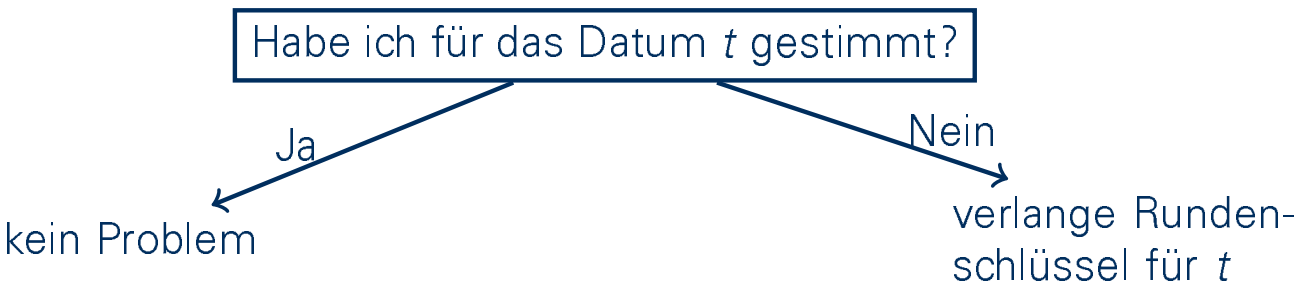
Alice	0	2	1	1	1	0
Bob	1	0	1	1	0	0
Carol	1	1	1	1	0	1
$\sum$	2	3	3	3	1	1

Ergebnis Verifikation

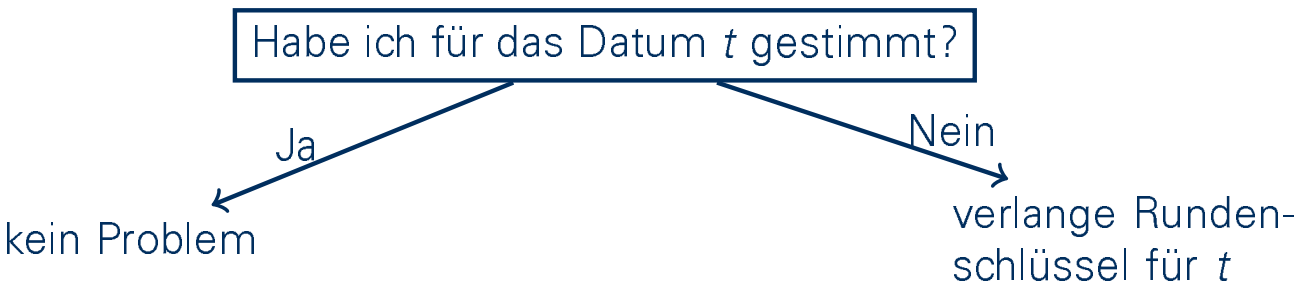
Ergebnis Verifikation



Ergebnis Verifikation



Ergebnis Verifikation



- Einzelstimmen können entschlüsselt werden ($v_{i,t}$)
- Ehrliche Teilnehmer sollten 1 gewählt haben
- cheaten wird durch Signaturen verhindert

Erweiterungen

Problembeschreibung

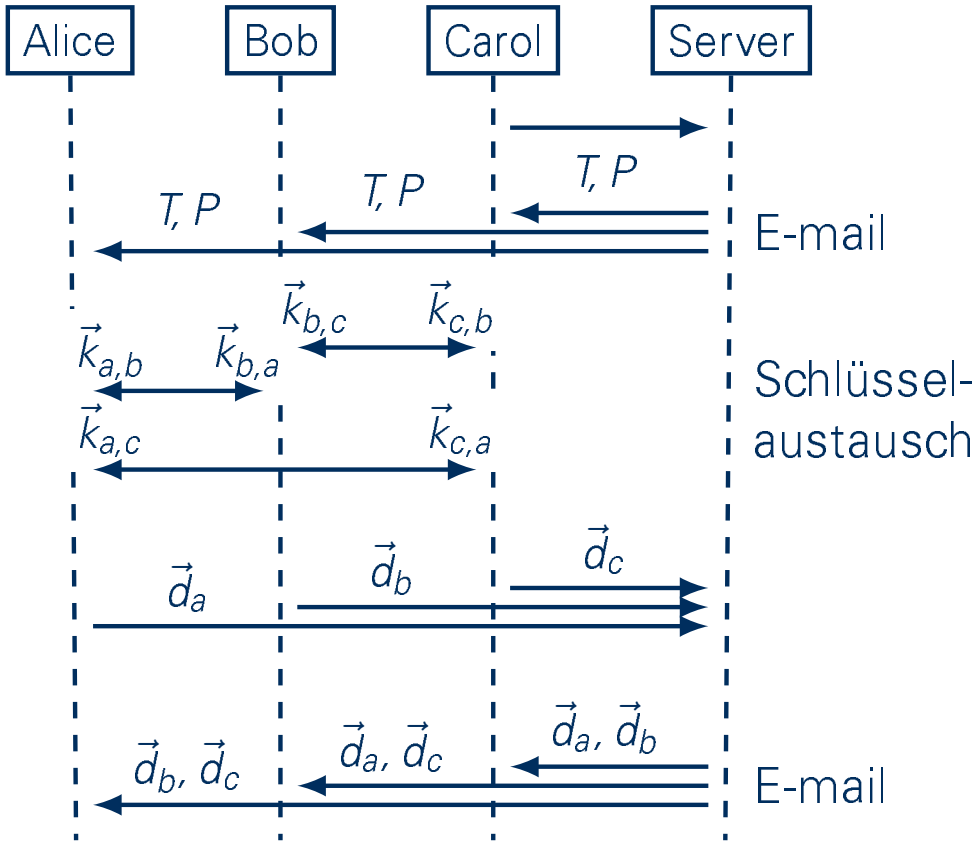
Schema

Erweiterungen

Evaluation

Zusammenfassung und Ausblick

Vereinfachung des Schlüsselaustauschs

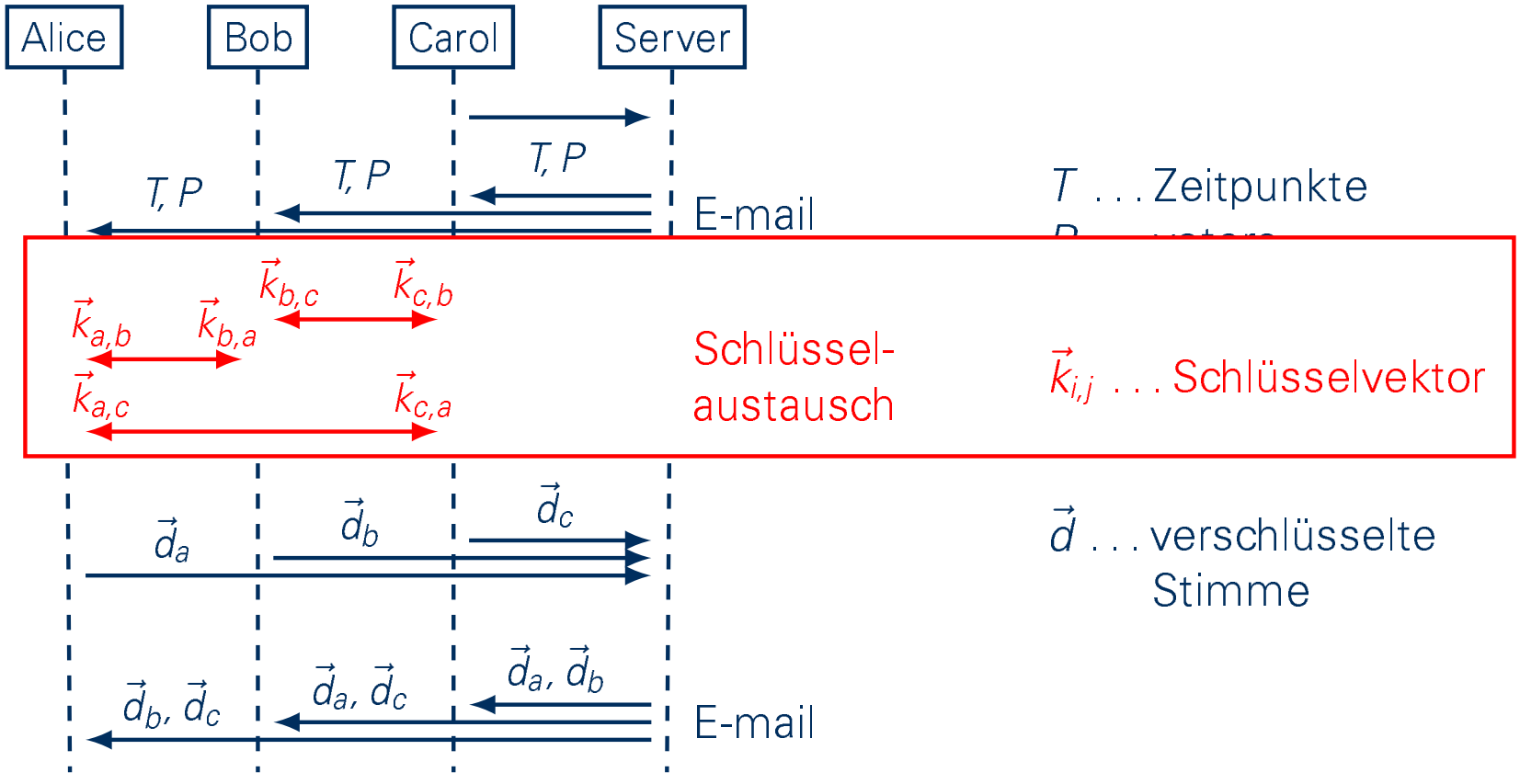


T . . . Zeitpunkte
P . . . voters

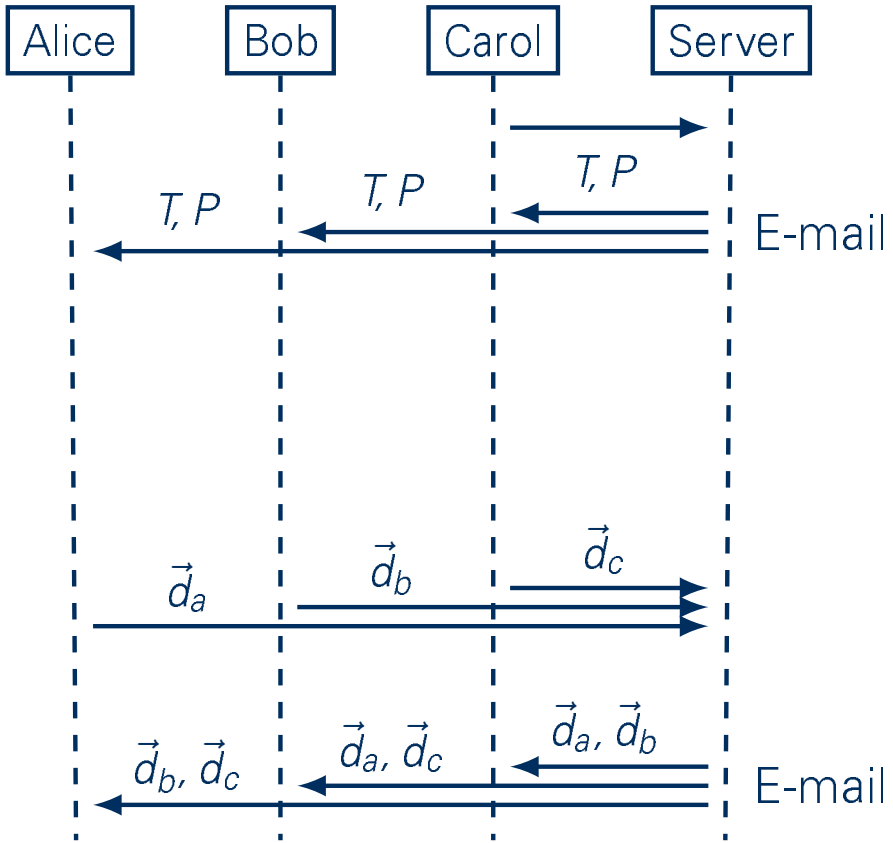
$\vec{k}_{i,j}$ . . . Schlüsselvektor

$\vec{d}$ . . . verschlüsselte Stimme

Vereinfachung des Schlüsselaustauschs



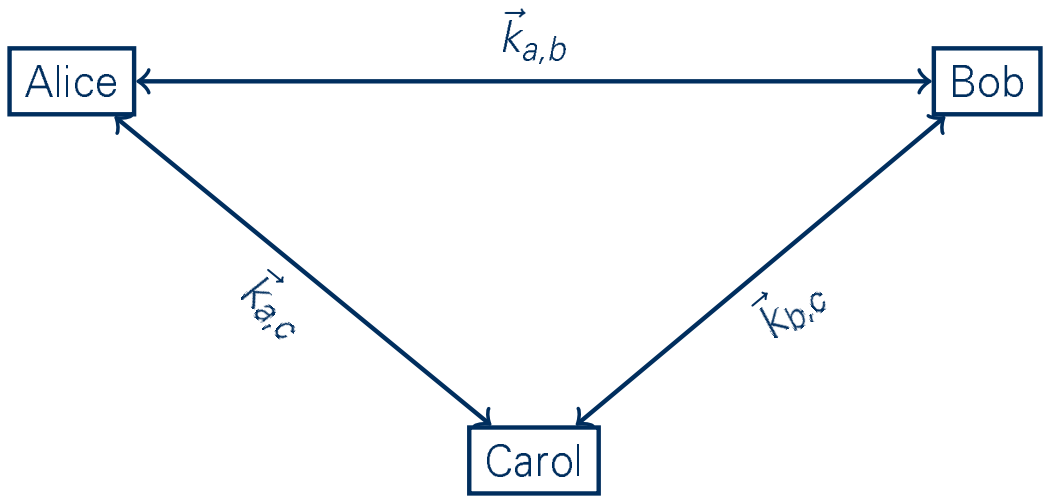
Vereinfachung des Schlüsselaustauschs



T . . . Zeitpunkte
P . . . voters

$\vec{d}$ . . . verschlüsselte Stimme

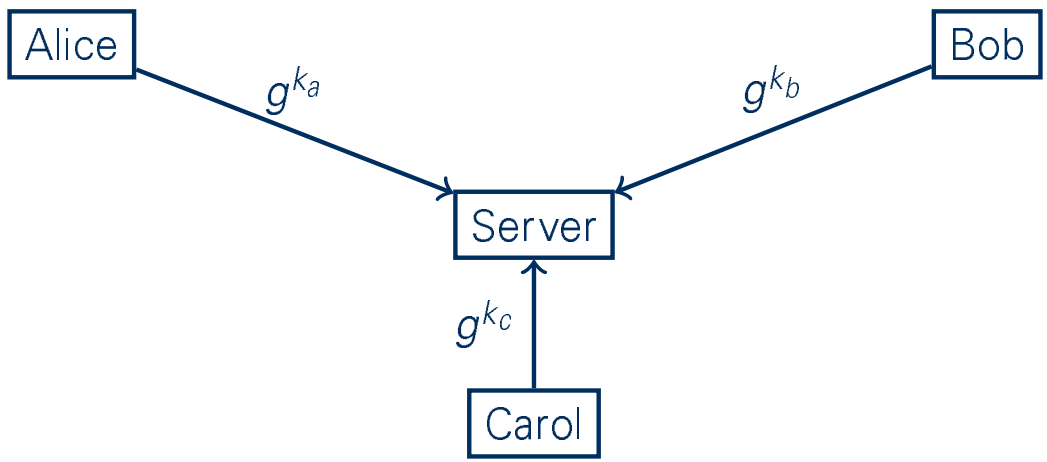
Vereinfachung des Schlüsselaustauschs



Schlüsselaustausch

Vereinfachung des Schlüsselaustauschs

Diffie–Hellman

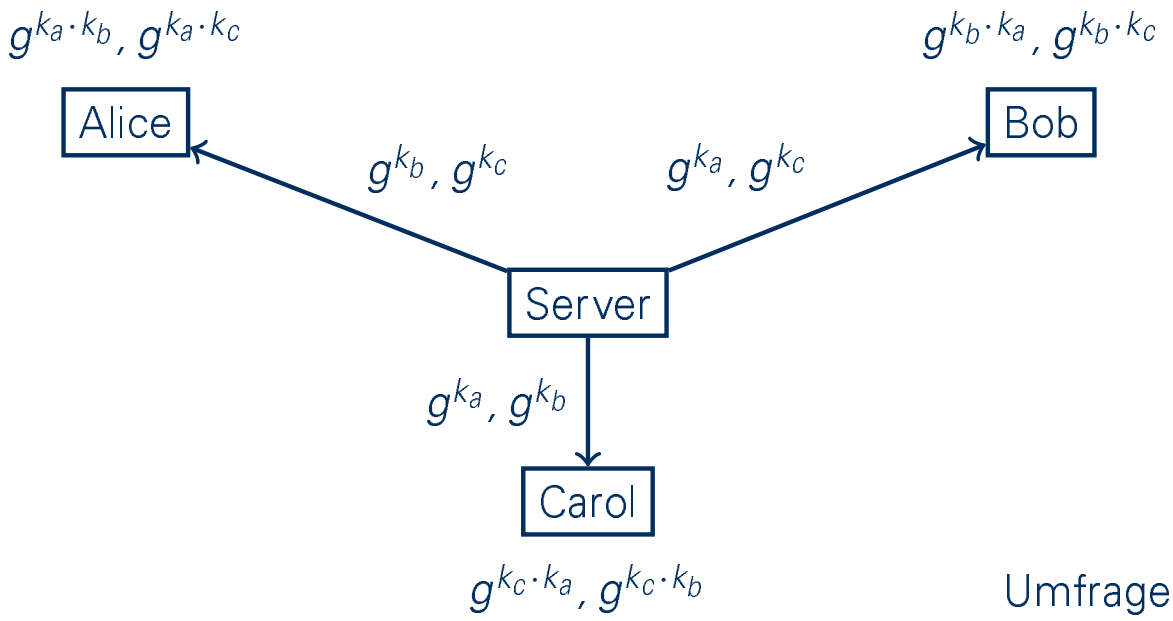


Registrierung

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

Vereinfachung des Schlüsselaustauschs

Diffie–Hellman

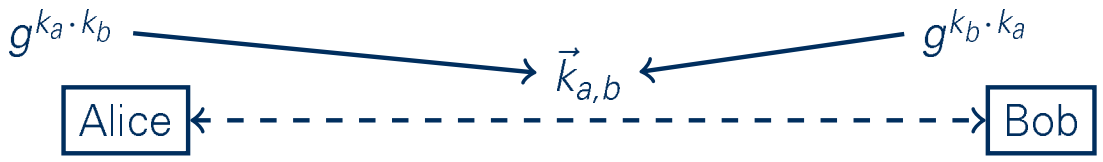


Umfrageerstellung

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

Vereinfachung des Schlüsselaustauschs

Diffie–Hellman



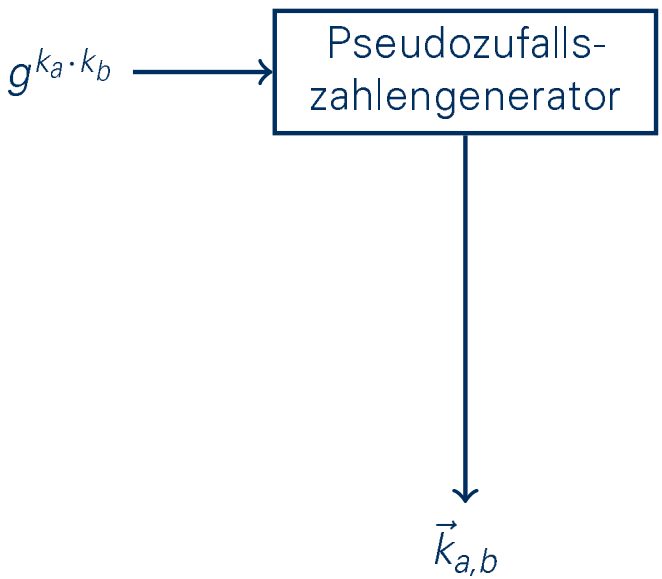
Carol

Umfrageerstellung

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

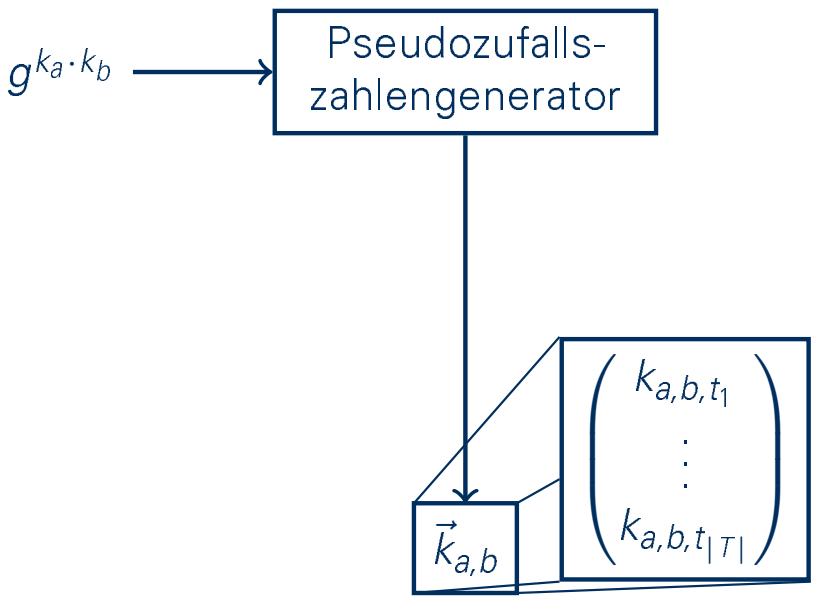
Vereinfachung des Schlüsselaustauschs

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



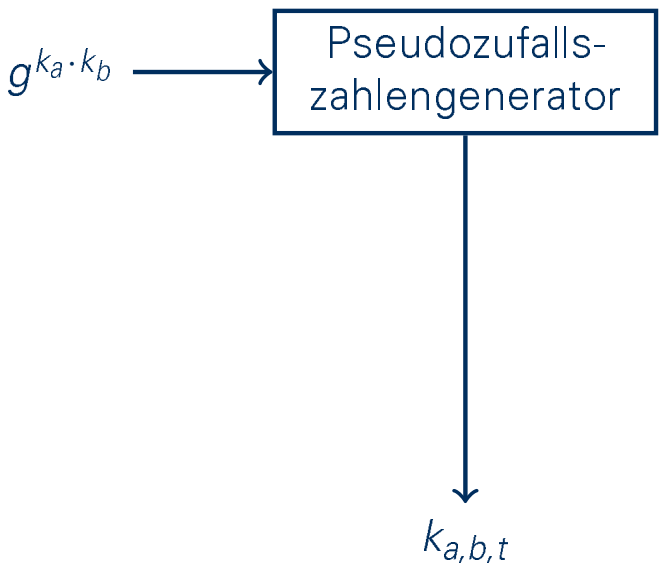
Vereinfachung des Schlüsselaustauschs

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



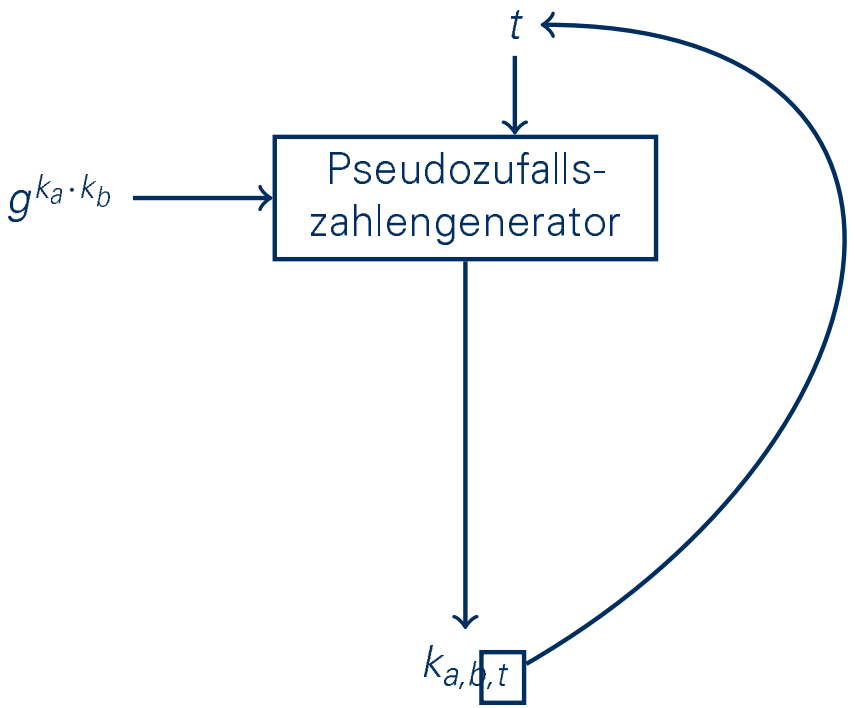
Vereinfachung des Schlüsselaustauschs

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



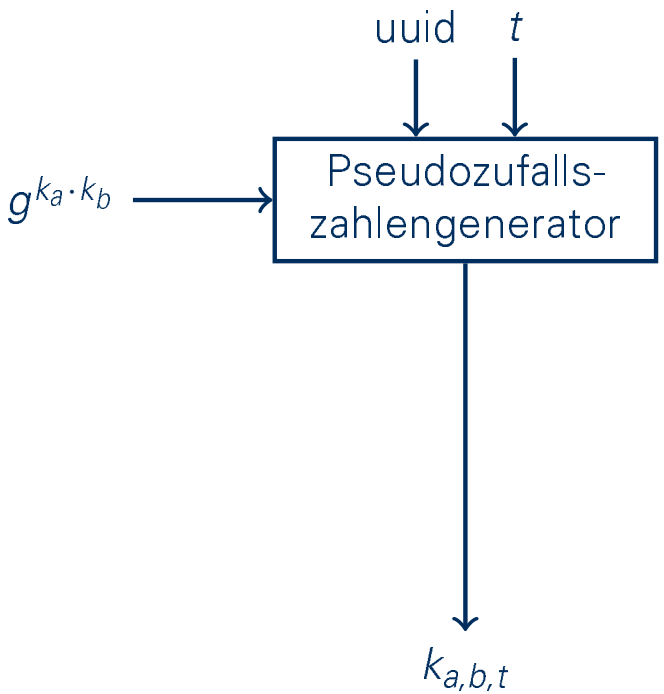
Vereinfachung des Schlüsselaustauschs

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



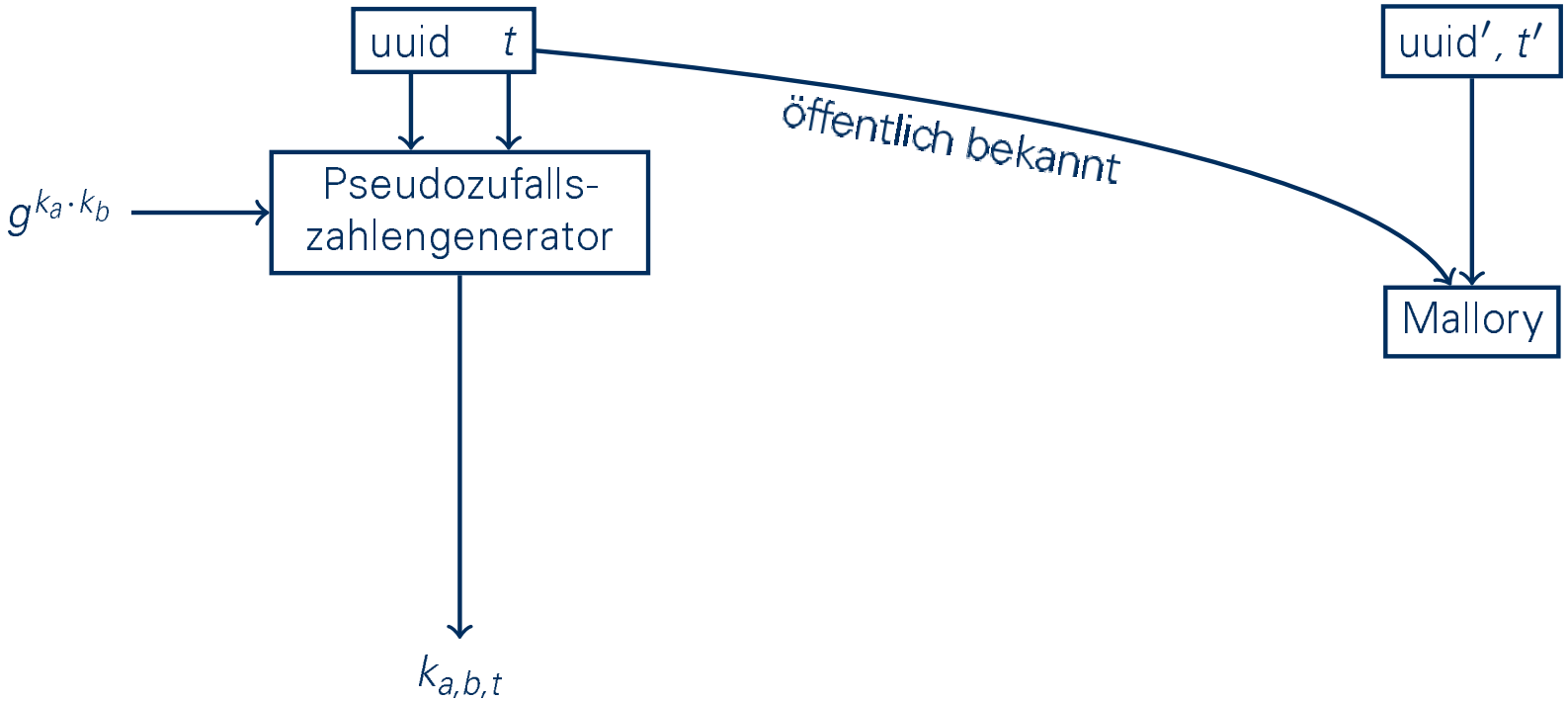
Vereinfachung des Schlüsselaustauschs

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



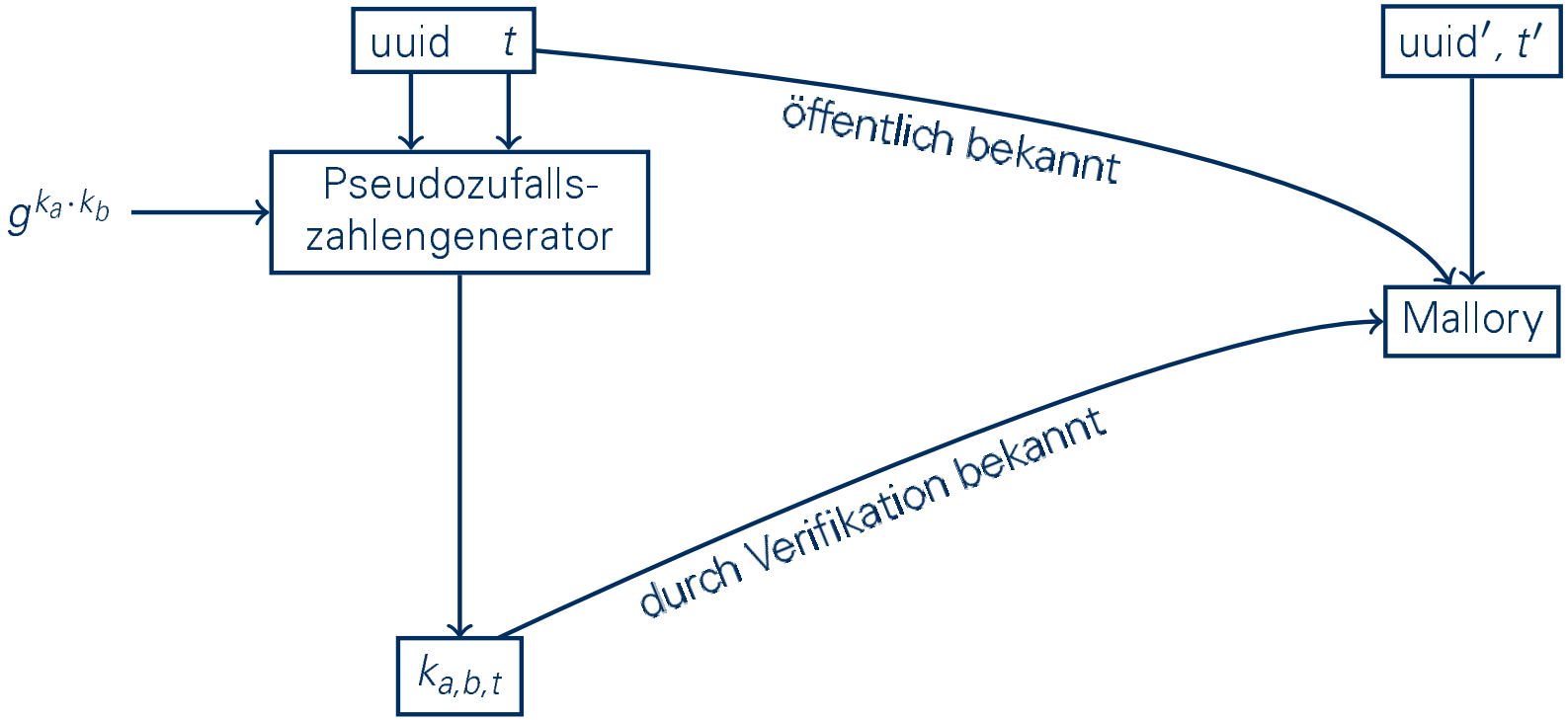
Vereinfachung des Schlüsselaustauschs

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



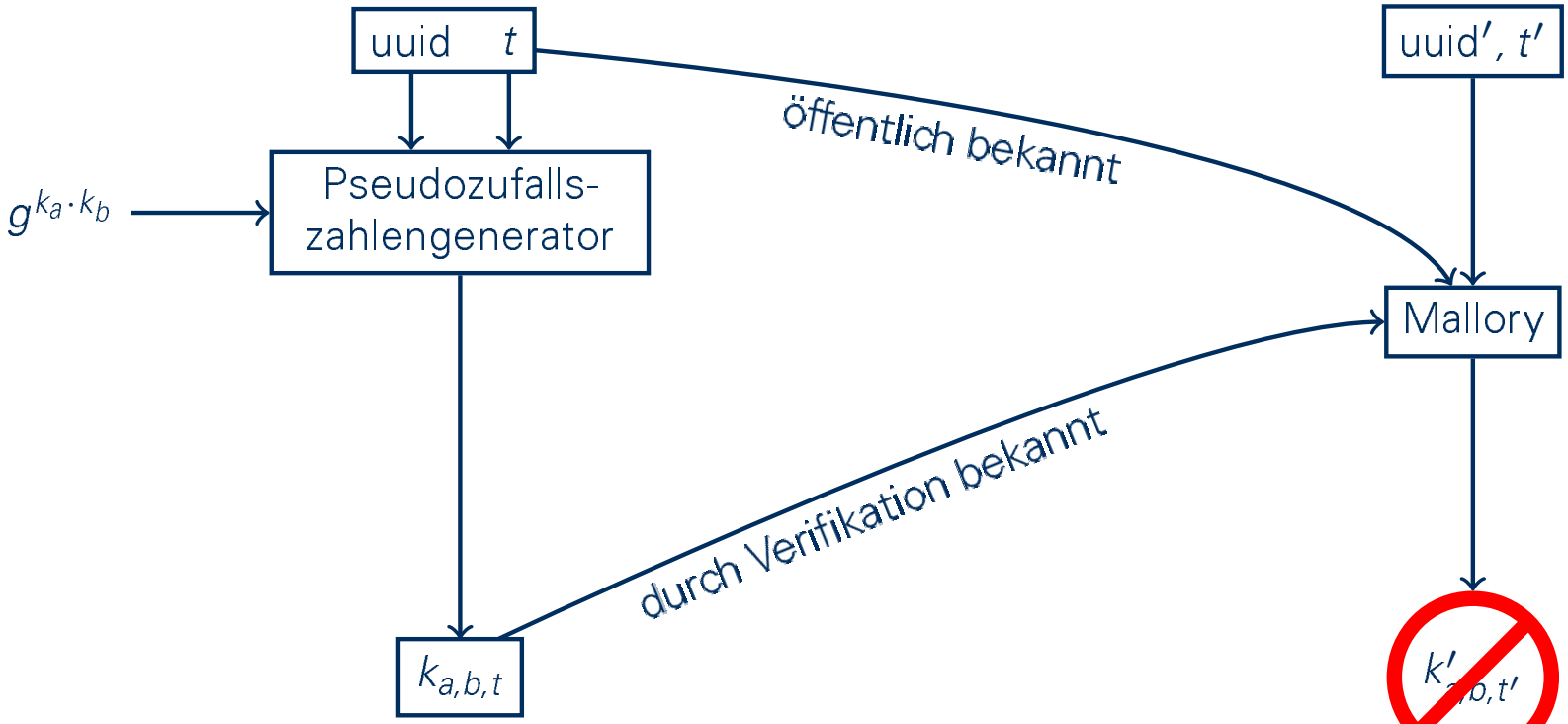
Vereinfachung des Schlüsselaustauschs

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



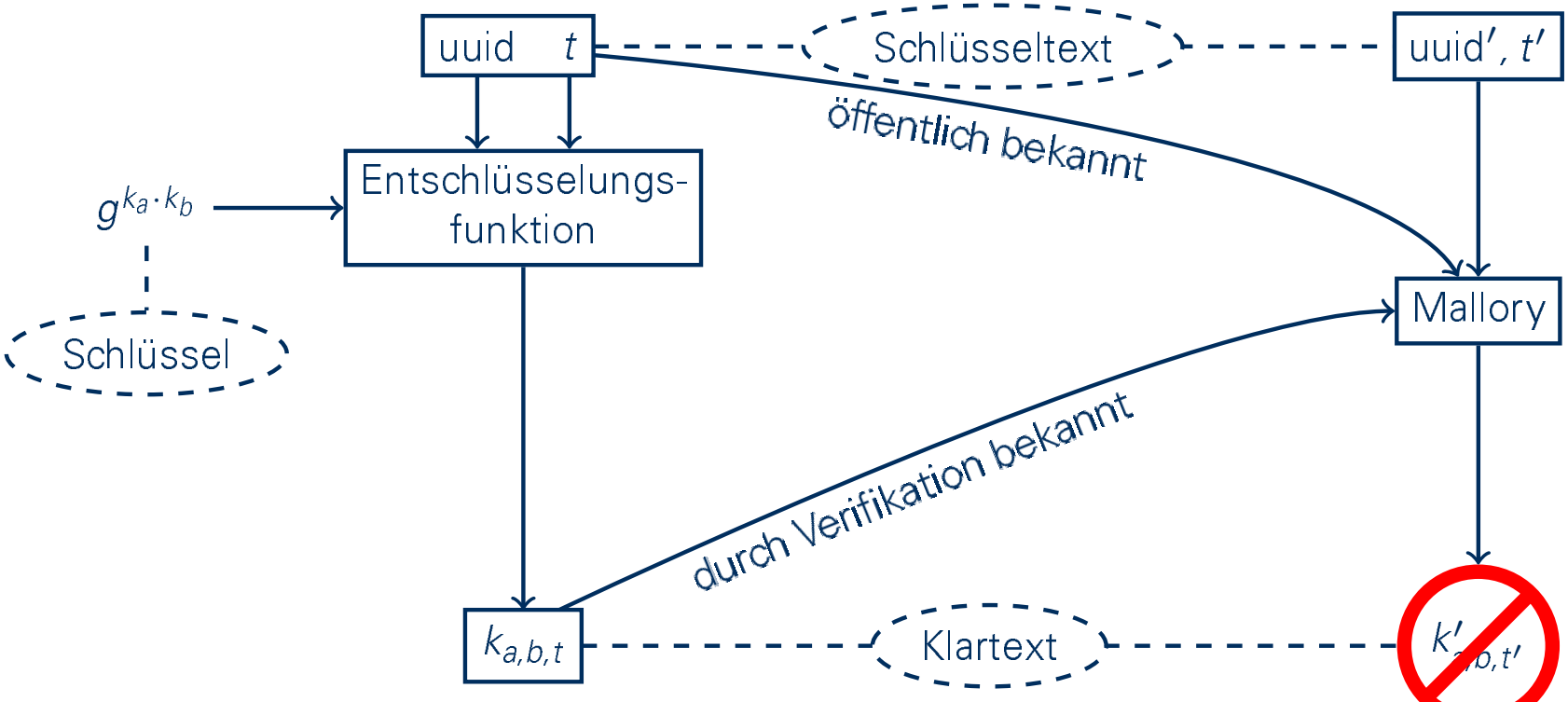
Vereinfachung des Schlüsselaustauschs

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



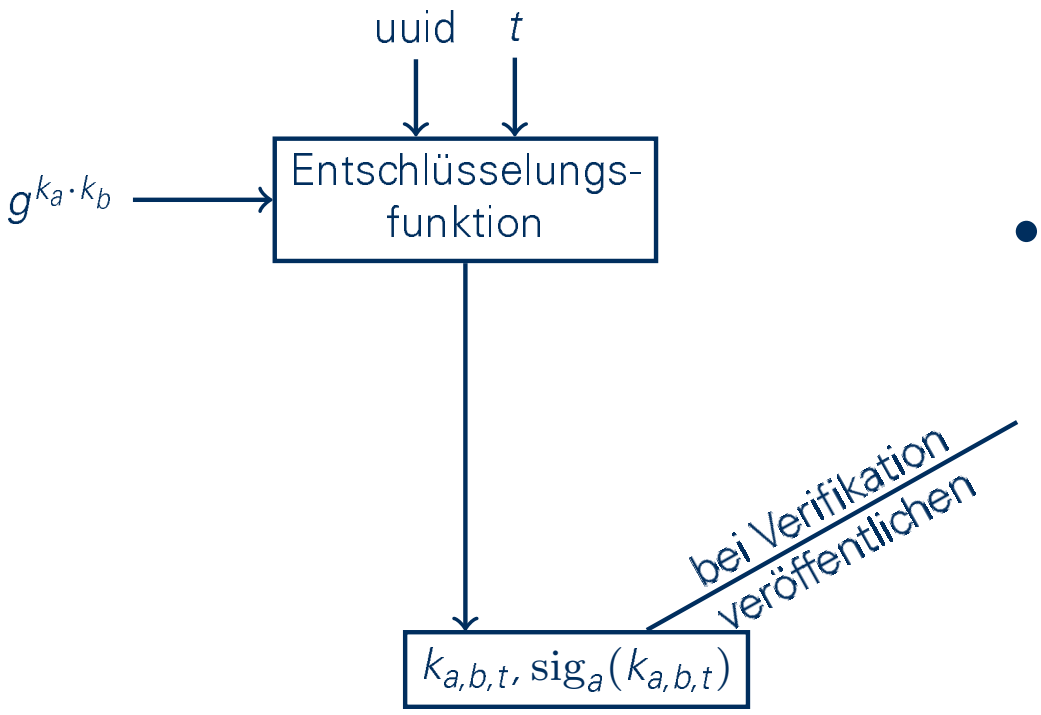
Vereinfachung des Schlüsselaustauschs

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



Verzicht auf die Signaturen

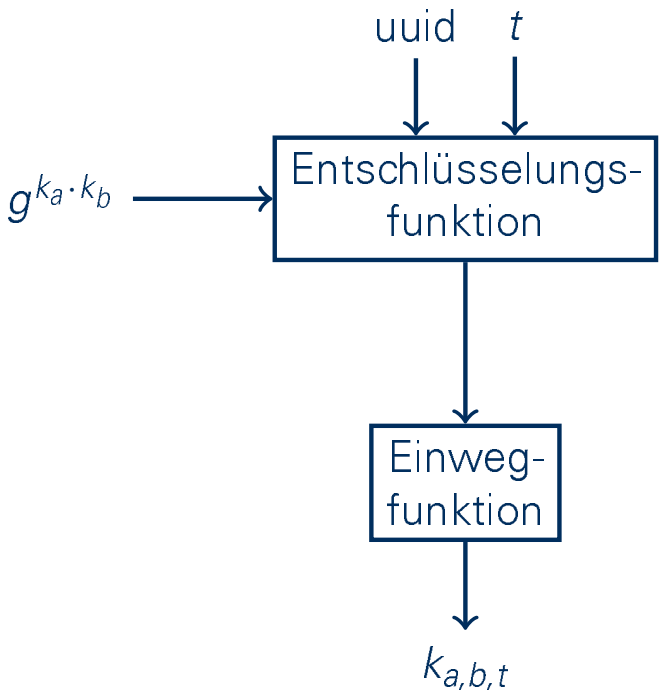
$$\mathrm{decr}_{g^{k_a \cdot k_b}}(\mathrm{uuid}||t) = k_{a,b,t}$$



- Signaturen verhindern cheaten beim Offenlegen der Schlüssel

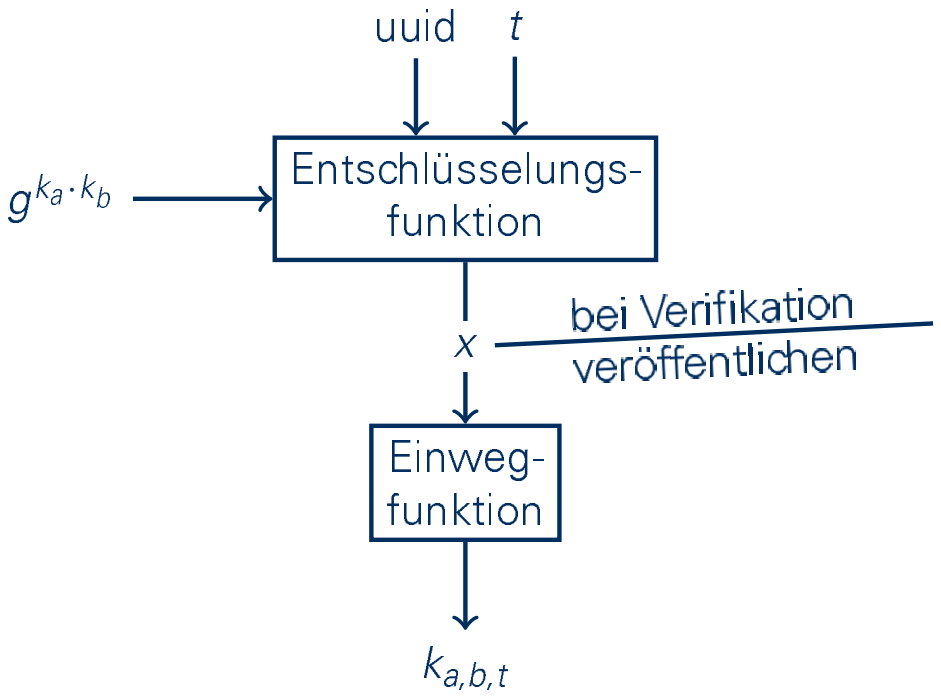
Verzicht auf die Signaturen

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



Verzicht auf die Signaturen

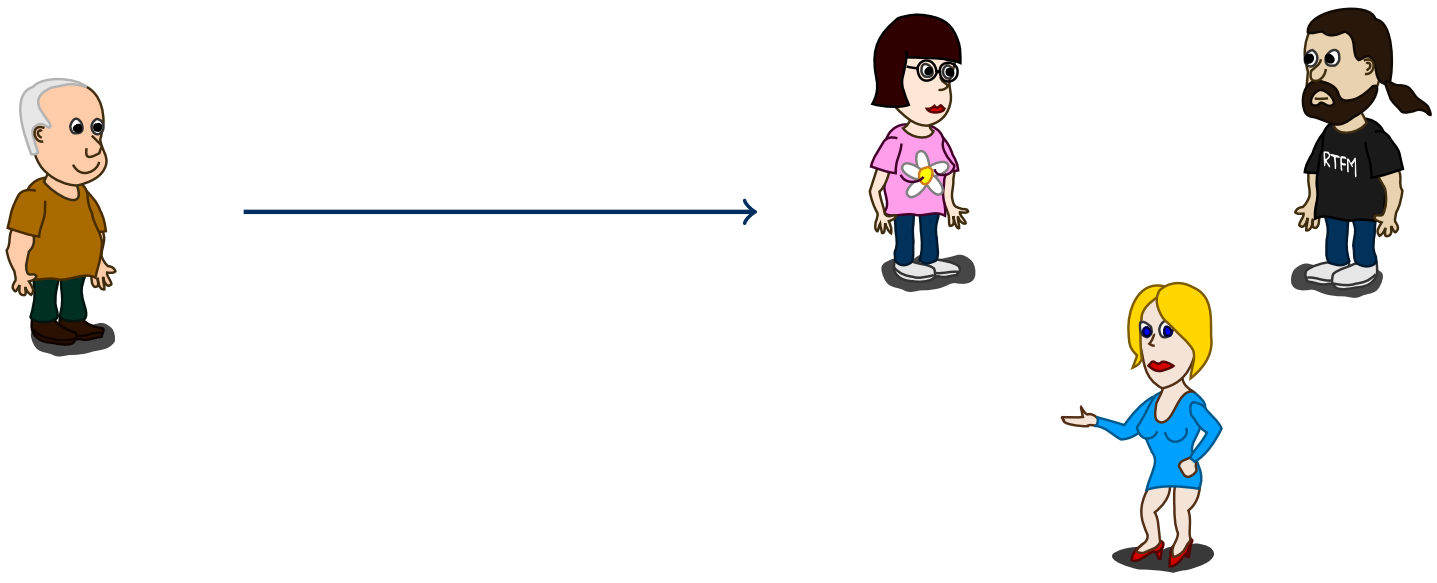
$$\mathrm{h}(\mathrm{decr}_{g^{k_a \cdot k_b}}(\mathrm{uuid}||t)) = k_{a,b,t}$$



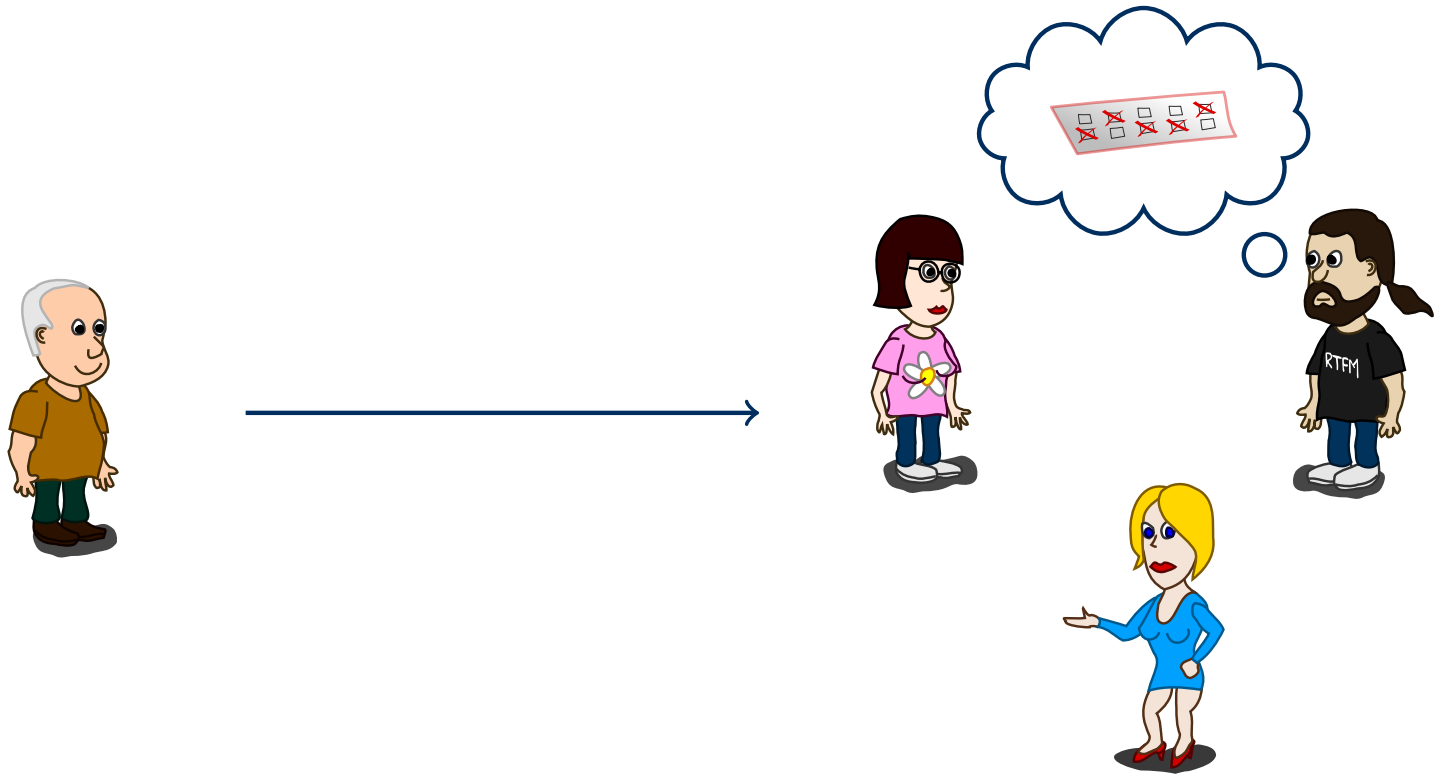
- pre-image resistancy verhindert cheaten beim Offenlegen der Schlüssel

Demo

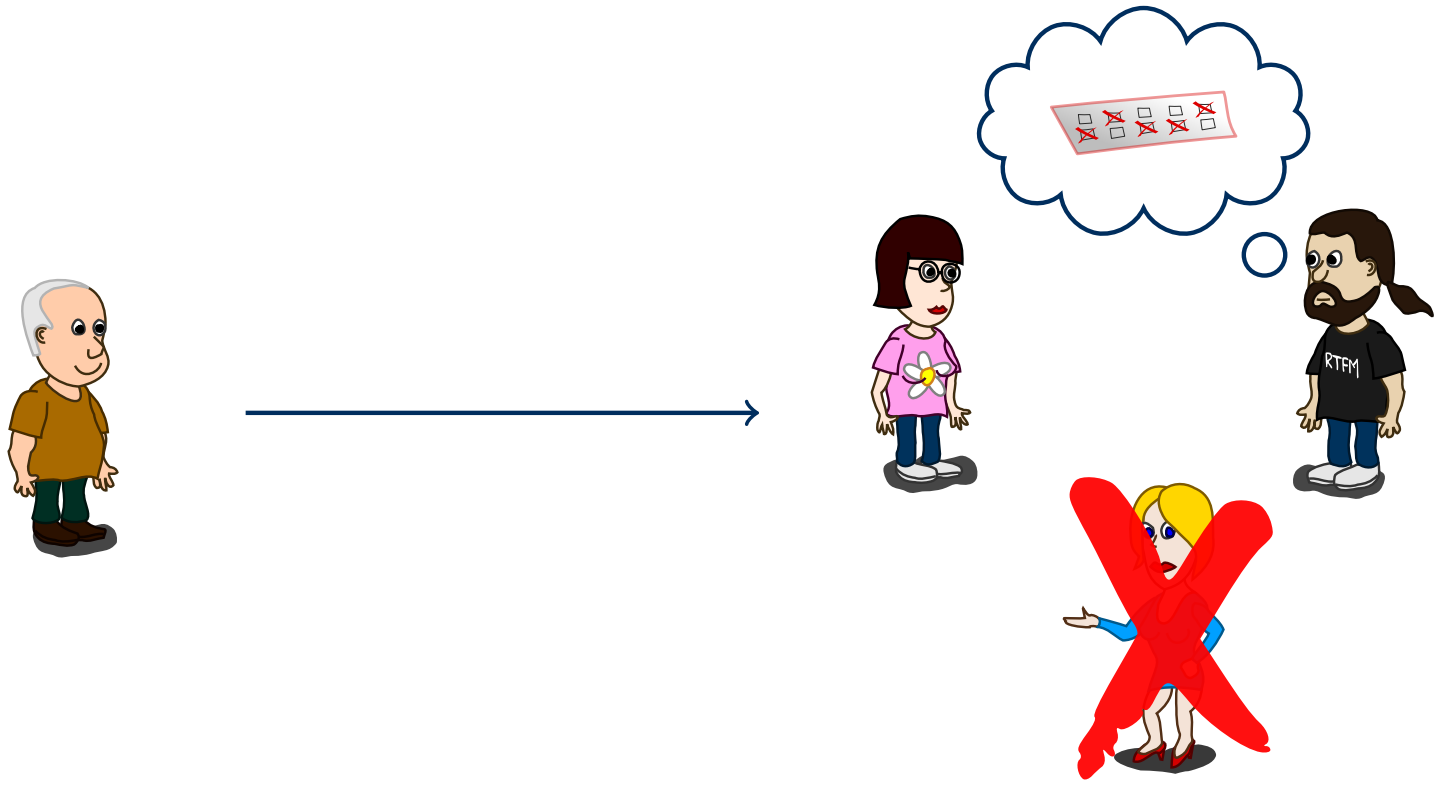
Dynamisches Hinzufügen



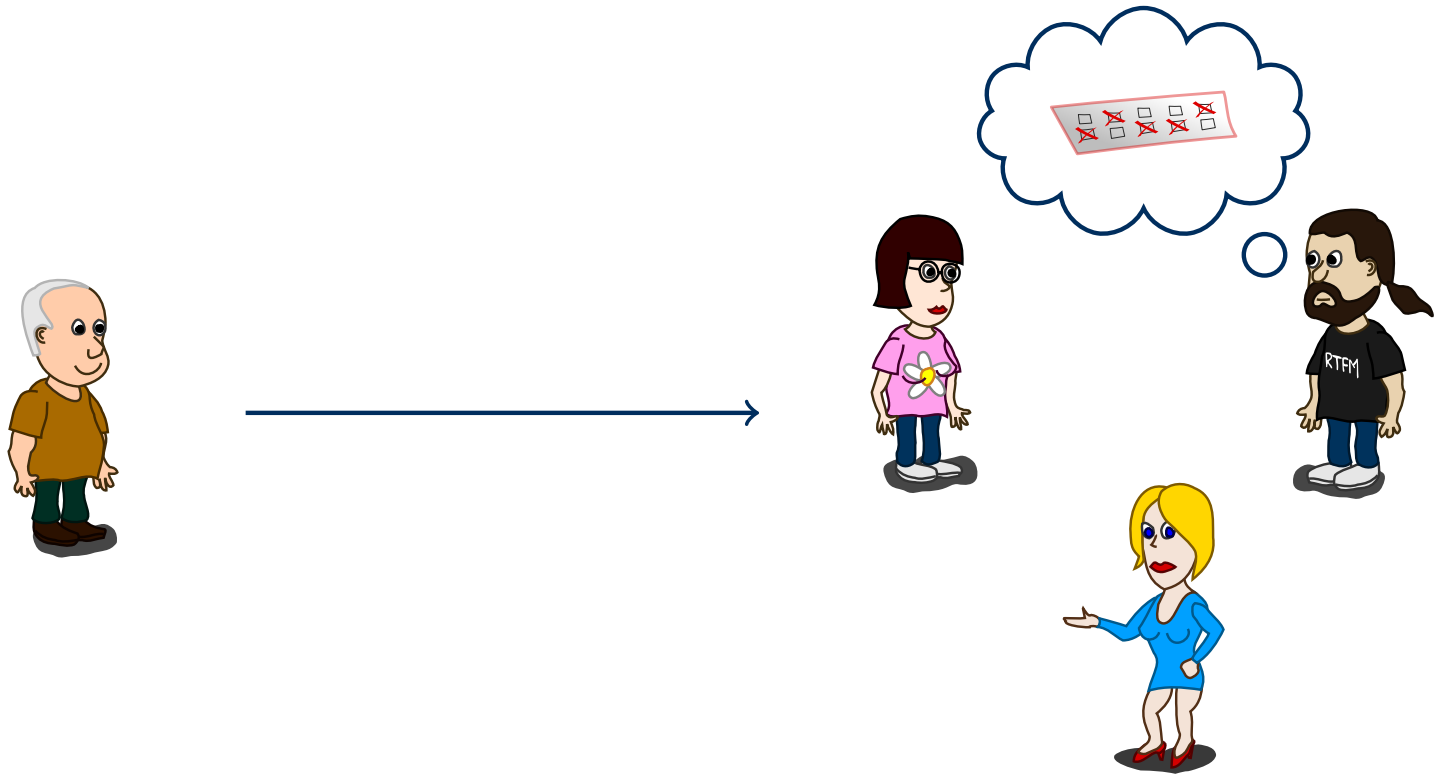
Dynamisches Hinzufügen



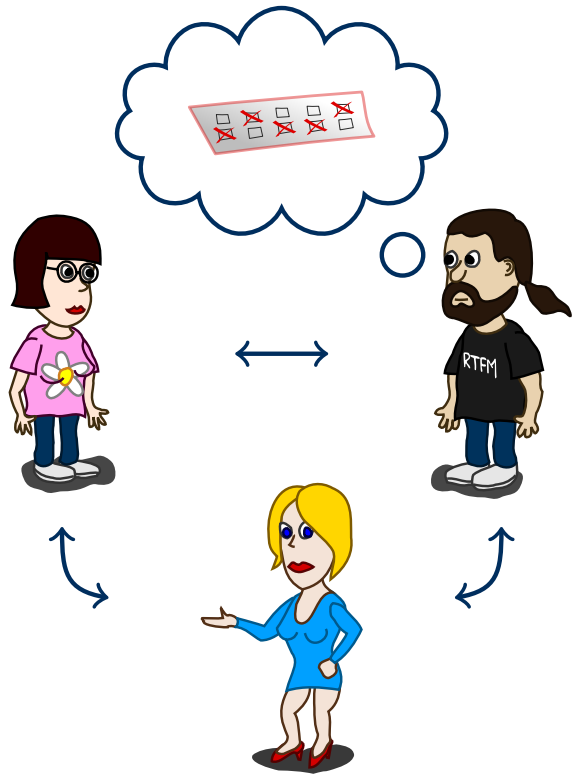
Dynamisches Hinzufügen/Verlassen



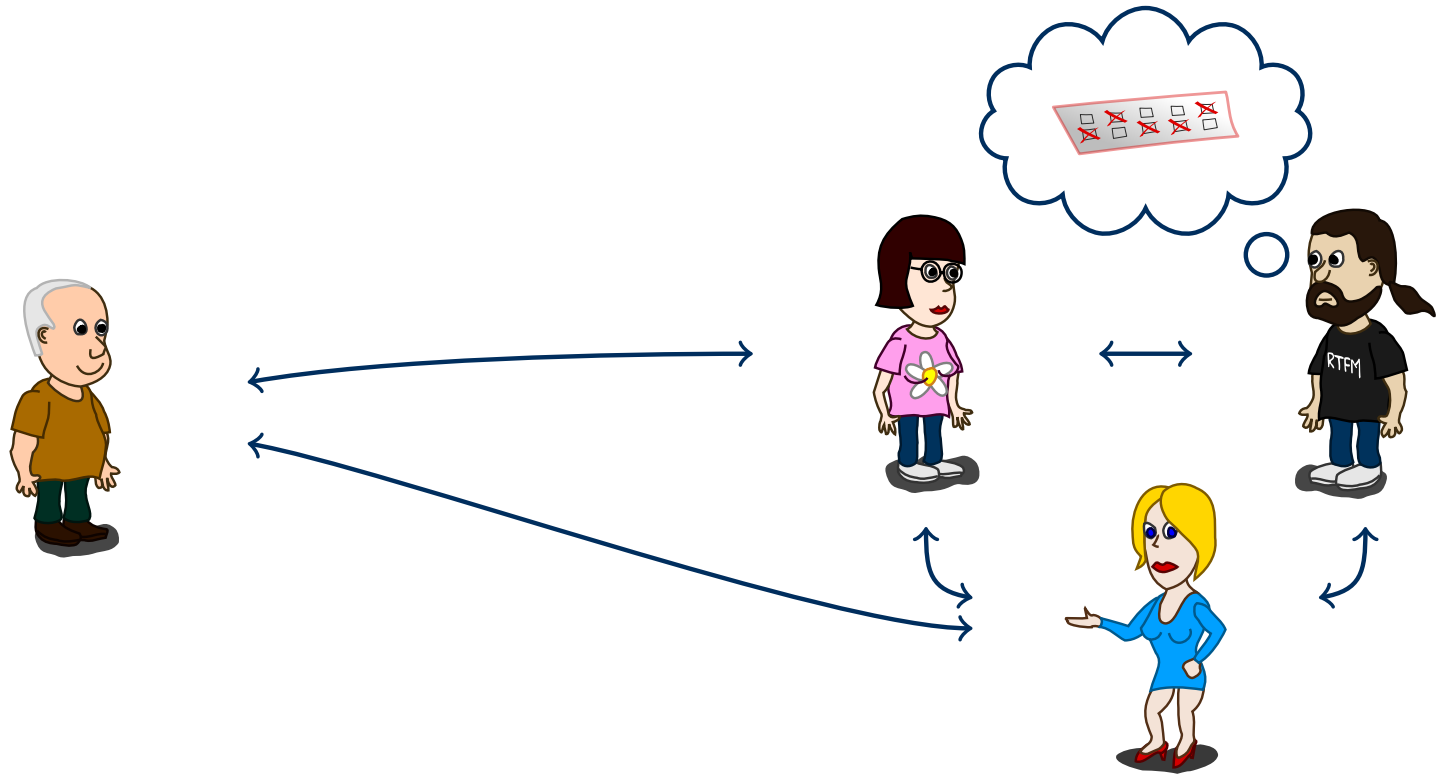
Dynamisches Hinzufügen



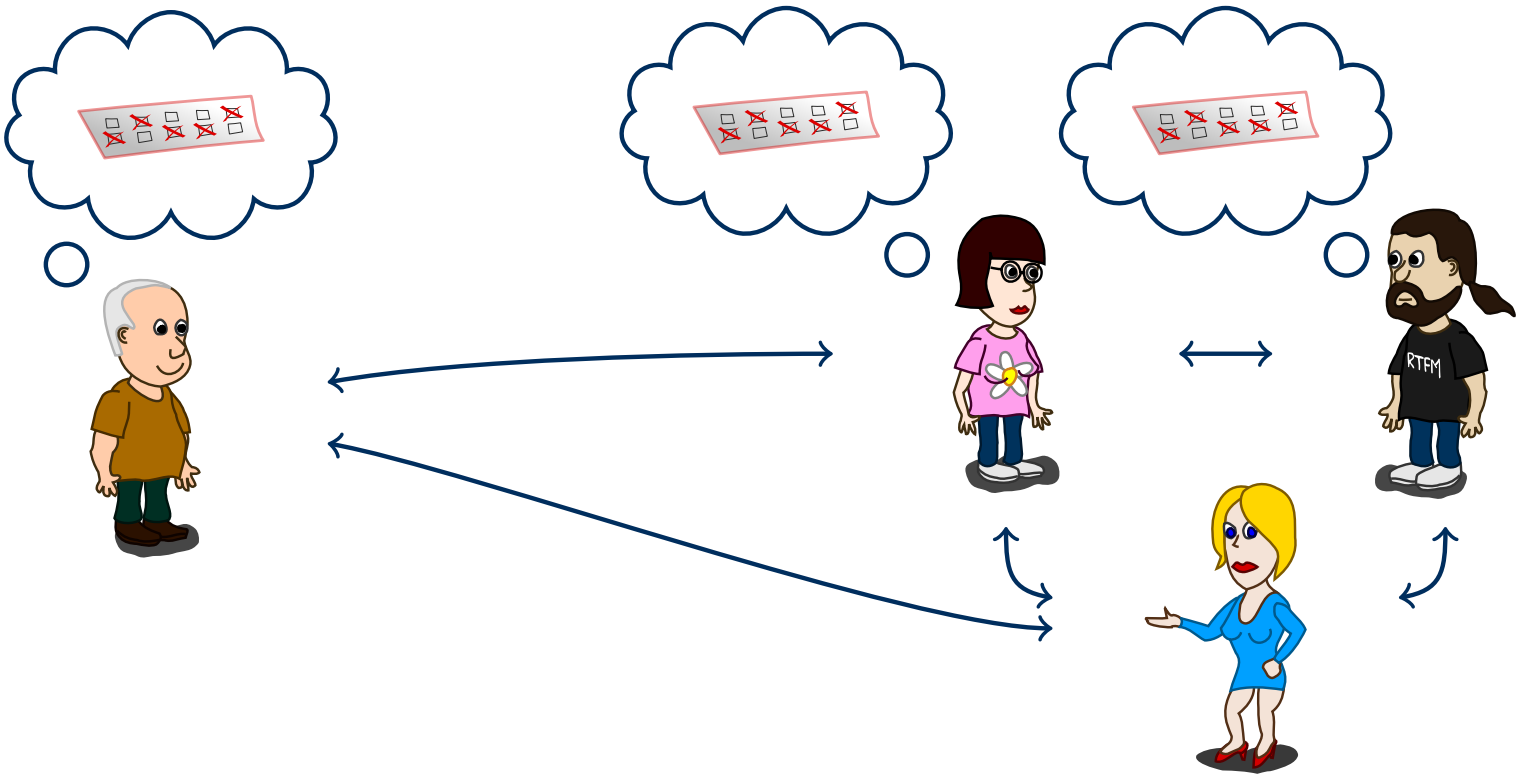
Dynamisches Hinzufügen



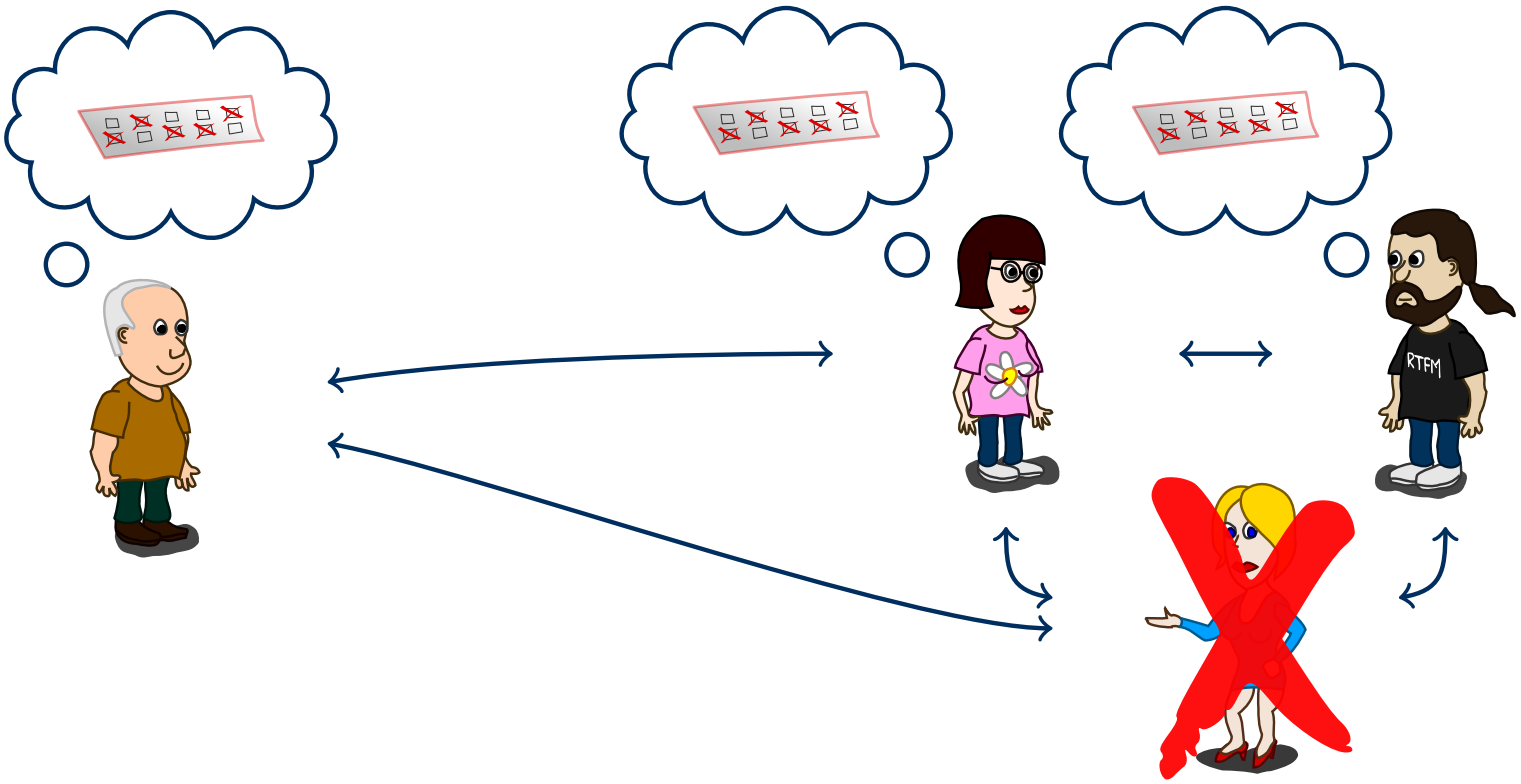
Dynamisches Hinzufügen



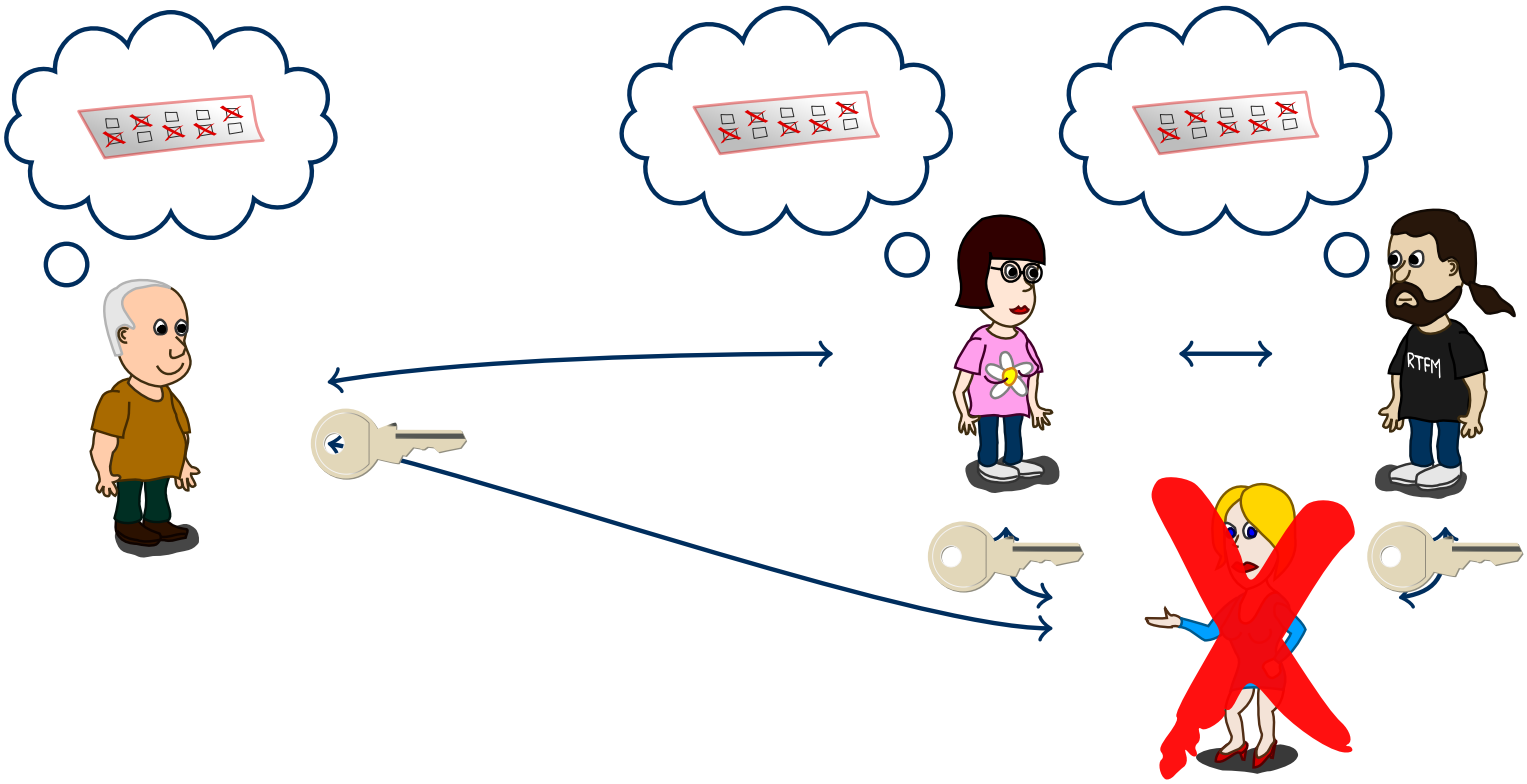
Dynamisches Verlassen



Dynamisches Verlassen



Dynamisches Verlassen



Demo

Evaluation

Problembeschreibung

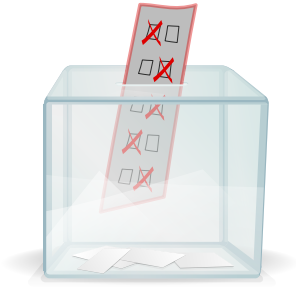
Schema

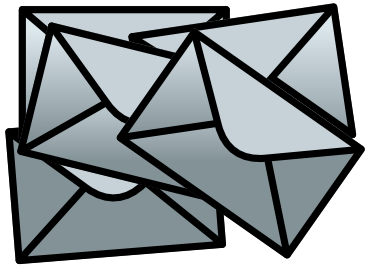
Erweiterungen

Evaluation

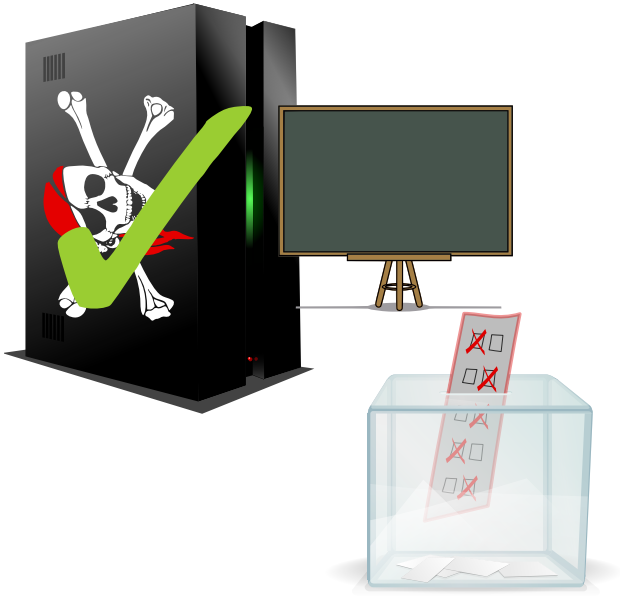
Zusammenfassung und Ausblick

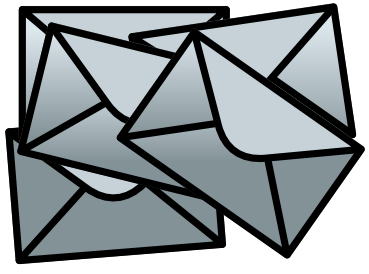
Evaluation



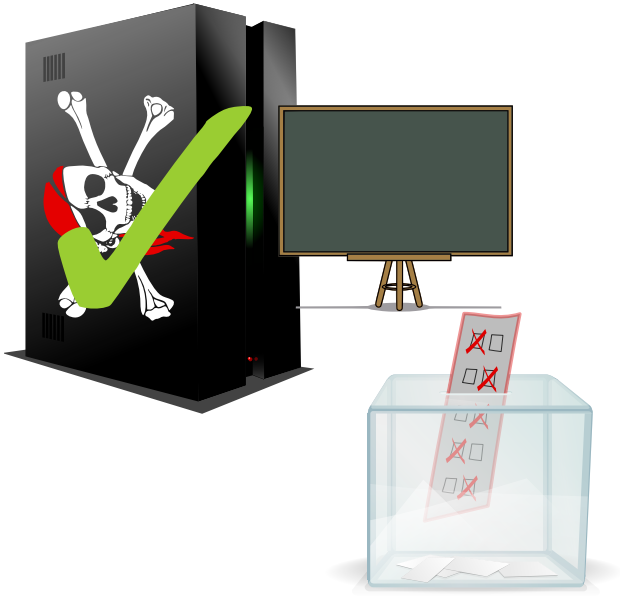


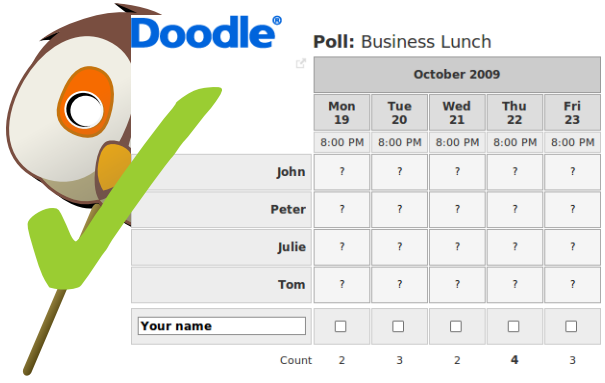
Evaluation

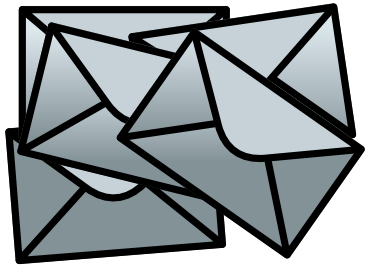




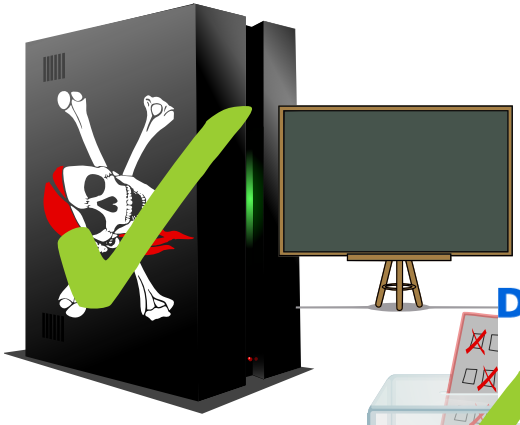
Evaluation




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



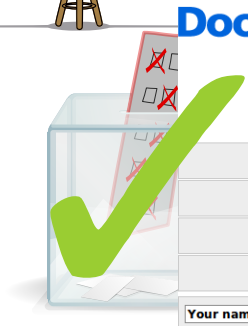
Evaluation



Doodle®

Poll: Business Lunch

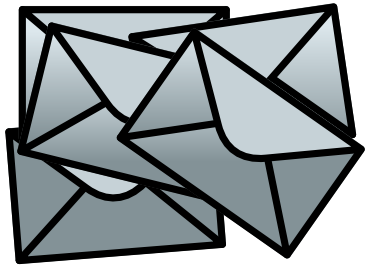
	October 2009				
	Mon 19	Tue 20	Wed 21	Thu 22	Fri 23
	8:00 PM	8:00 PM	8:00 PM	8:00 PM	8:00 PM
John	?	?	?	?	?
Peter	?	?	?	?	?
Julie	?	?	?	?	?
Tom	?	?	?	?	?
Your name	☐	☐	☐	☐	☐
Count	2	3	2	4	3



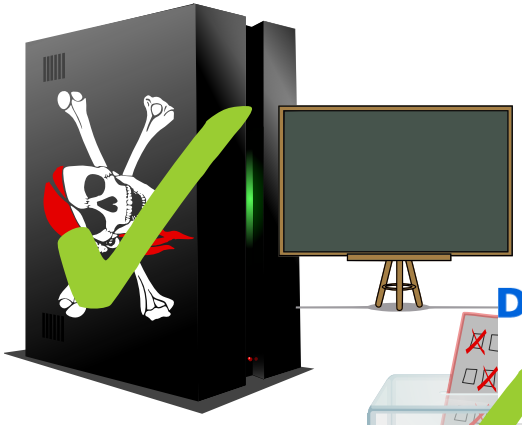
Doodle®

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



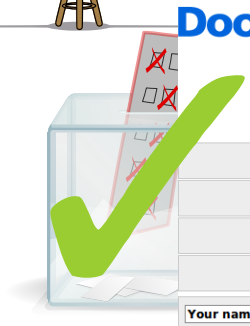
Evaluation



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



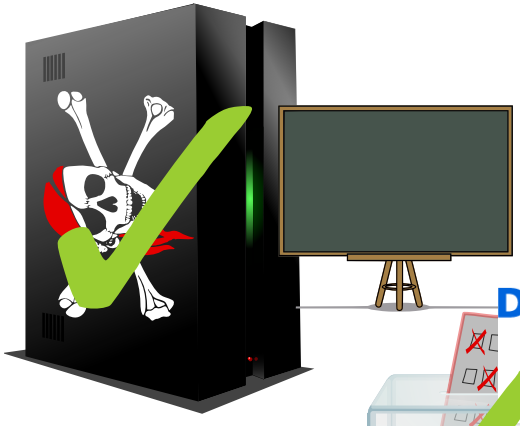
Doodle®

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 Kommuni-
kationsschritte
pro Teilnehmer

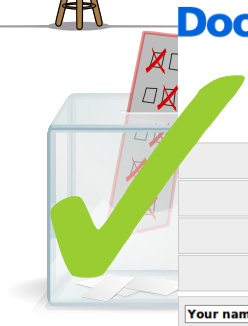
Evaluation



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 Kommunikationsschritte pro Teilnehmer

	Datum #1	. . .	Datum #240
Ja			✘
Nein	✘		

skaliert
($|P|$ — 1 asym. operationen pro Teilnehmer)

Zusammenfassung und Ausblick

- neues Schema für Datenschutzfreundliche Terminplanung
  - ➠ skaliert mit der Anzahl der Zeitpunkte
  - ➠ keine zentrale vertrauenswürdige Partei
- teilweise als Web 2.0 Anwendung implementiert

- fehlende Features implementieren
- Performance validieren
- mehr Features
  - ➠ nicht nur Einstimmigkeit
  - ➠ . . .

TECHNISCHE UNIVERSITÄT DRESDEN

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

Vielen Dank für die Aufmerksamkeit!

Fragen/Diskussion

Benjamin.Kellermann@tu-dresden.de

D19E 04A8 8895 020A 8DF6

0092 3501 1A32 491A 3D9C

Dresden, 3. Oktober 2009

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)
$\|P\| - 1$	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