TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik Institut für Systemarchitektur, Lehrstuhl für Datenschutz und Datensicherheit

Dudle: Mehrseitig sichere Web 2.0-Terminabstimmung

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

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

Dresden, 16. Dezember 2011

Inhalt

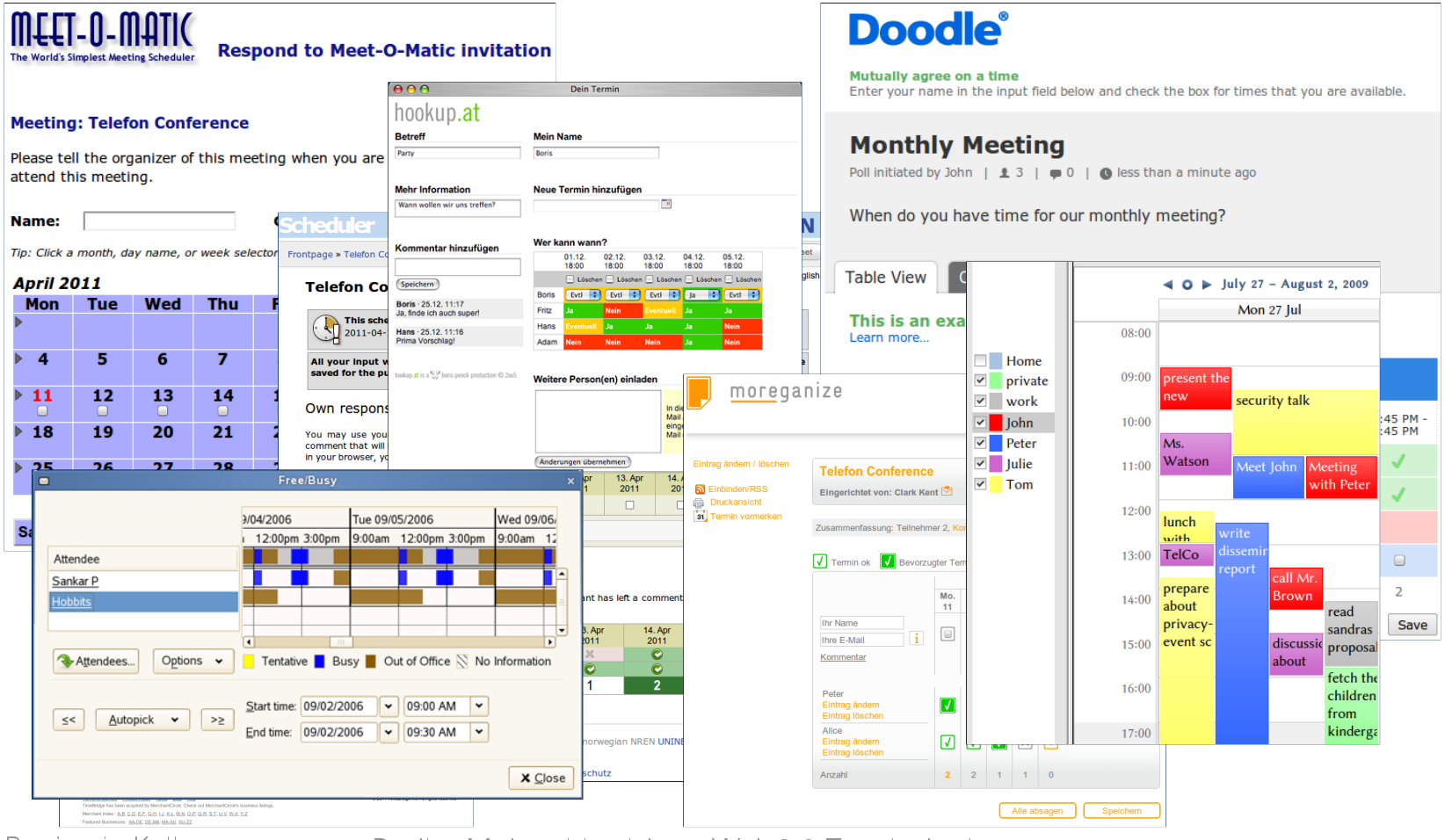
Begriffe / Anforderungen

Neue Protokolle

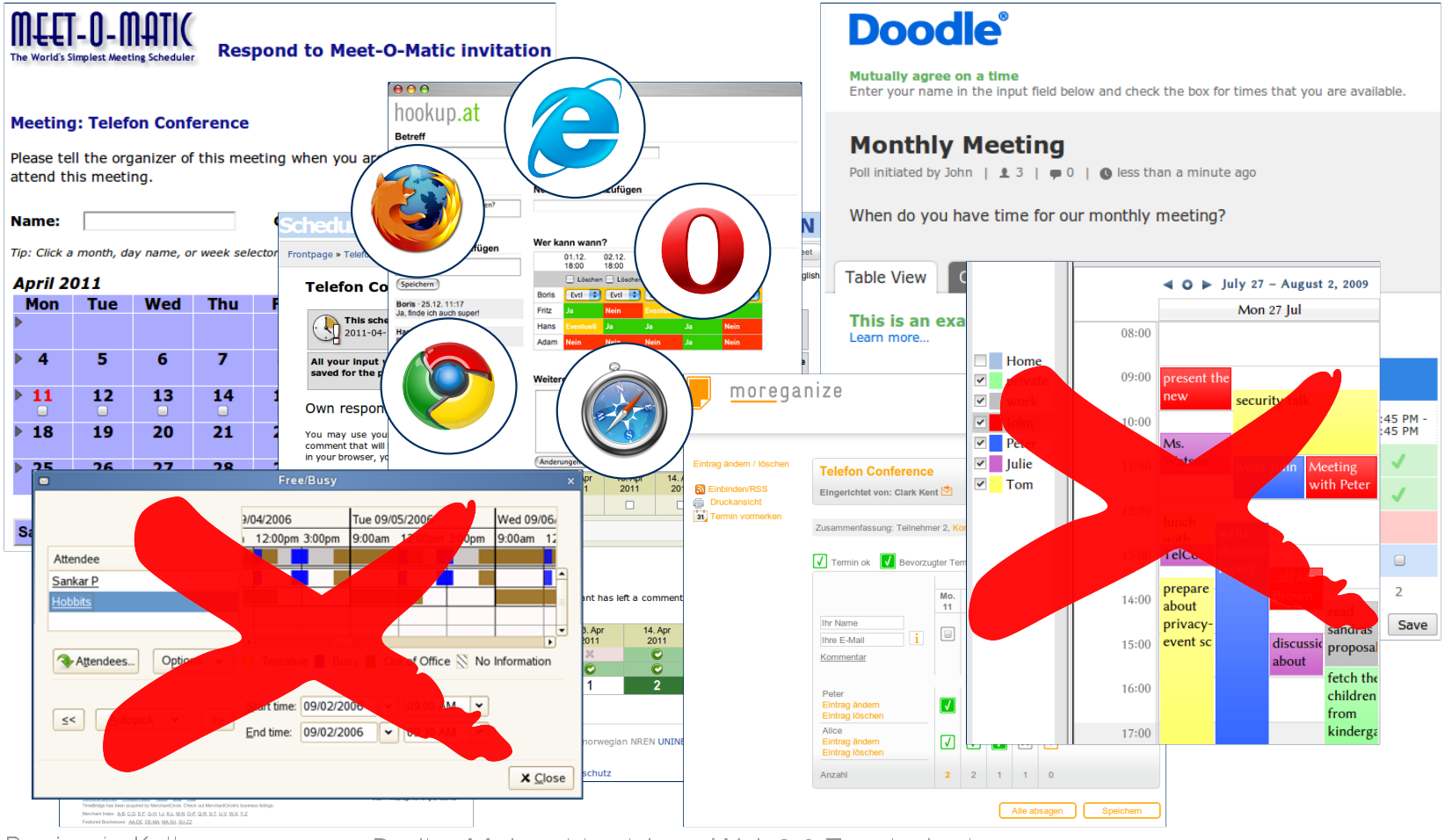
Implementierung

Zusammenfassung / Ausblick

Mehrseitig sichere Web 2.0-Terminabstimmung

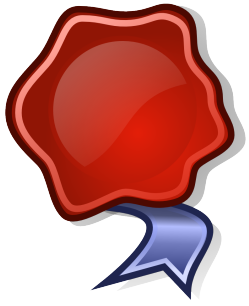


Mehrseitig sichere **Web 2.0**-Terminabstimmung



Mehrseitig **sichere** Web 2.0-Terminabstimmung

Vertraulichkeit
Datenminimierung



Integrität
jeder soll Manipulationen erkennen

Verfügbarkeit
integeres Ergebnis nach angemessener Zeit

Vertraulichkeit

Direkter Informationsgewinn

Ist meinem Doktorvater eine Fakultätsberatung wichtiger als meine Arbeit?

FAKULTÄTSBERATUNG

		Jun 2011											
		Mo, 13				Di, 14				Mi, 15			
	Name ▾▴	09:20 ▾▴	11:10 ▾▴	13:00 ▾▴	14:50 ▾▴	09:20 ▾▴	11:10 ▾▴	13:00 ▾▴	14:50 ▾▴	09:20 ▾▴	11:10 ▾▴	13:00 ▾▴	14:50 ▾▴
✎ | ✖	Lehner	✔	✘	✔	✘	✔	✔	✔	✔	✘	✔	✔	?
✎ | ✖	Aßmann	✔	✘	✔	✔	?	✘	?	✔	?	✘	✔	✔
✎ | ✖	Schill	✔	✘	✘	✔	✘	✘	✘	✘	✔	✔	✘	✔
✎ | ✖	Hochberger	?	✔	✔	✔	✘	✔	✔	✘	✘	?	✔	✘
✎ | ✖	Nagel	✔	✔	✔	✘	✘	✔	✔	✘	✔	✘	?	✔
		○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔
		◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘
		○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?
	Summe	4	2	4	3	1	3	3	2	2	2	3	3

Vertraulichkeit

Direkter Informationsgewinn

Ist meinem Doktorvater eine Fakultätsberatung wichtiger als meine Arbeit?

Dienstag 11:30 Uhr Termin mit Prof. Schill

FAKULTÄTSBERATUNG

	Jun 2011											
	Mo, 13				Di, 14				Mi,			
Name	09:20	11:10	13:00	14:50	09:20	11:10	13:00	14:50	09:20	11:10	13:00	14:50
Lehner	✓	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	?
Aßmann	✓	✗	✓	✓	?	✗	?	✓	?	✗	✓	✓
Schill	✓	✗	✗	✓	✗	✗	✗	✗	✓	✓	✗	✓
Hochberger	?	✓	✓	✓	✗	✓	✓	✗	✗	?	✓	✗
Nagel	✓	✓	✓	✗	✗	✓	✓	✗	✓	✗	?	✓
	○ ✓	○ ✓	○ ✓	○ ✓	○ ✓	○ ✓	○ ✓	○ ✓	○ ✓	○ ✓	○ ✓	○ ✓
	◉ ✗	◉ ✗	◉ ✗	◉ ✗	◉ ✗	◉ ✗	◉ ✗	◉ ✗	◉ ✗	◉ ✗	◉ ✗	◉ ✗
	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?
Summe	4	2	4	3	1	3	3	2	2	2	3	3

Vertraulichkeit

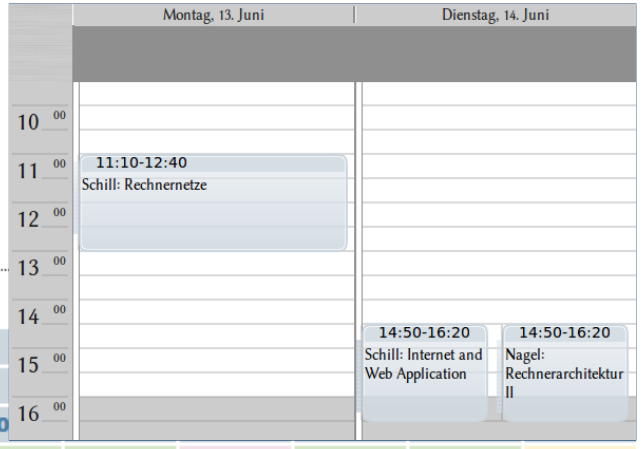
Indirekter Informationsgewinn

FAKULTÄTSBERATUNG

	Jun 2011											
	Mo, 13				Di, 14				Mi, 15			
Name ▾▴	09:20 ▾▴	11:10 ▾▴	13:00 ▾▴	14:50 ▾▴	09:20 ▾▴	11:10 ▾▴	13:00 ▾▴	14:50 ▾▴	09:20 ▾▴	11:10 ▾▴	13:00 ▾▴	14:50 ▾▴
✎ | ✖ Anonymous #1	✔	✘	✔	✘	✔	✔	✔	✔	✘	✔	✔	?
✎ | ✖ Anonymous #2	✔	✘	✔	✔	?	✘	?	✔	?	✘	✔	✔
✎ | ✖ Anonymous #3	✔	✘	✘	✔	✘	✘	✘	✘	✔	✔	✘	✔
✎ | ✖ Anonymous #4	?	✔	✔	✔	✘	✔	✔	✘	✘	?	✔	✘
✎ | ✖ Anonymous #5	✔	✔	✔	✘	✘	✔	✔	✘	✔	✘	?	✔
	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔
	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘
	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?
Summe	4	2	4	3	1	3	3	2	2	2	3	3

Vertraulichkeit

Indirekter Informationsgewinn

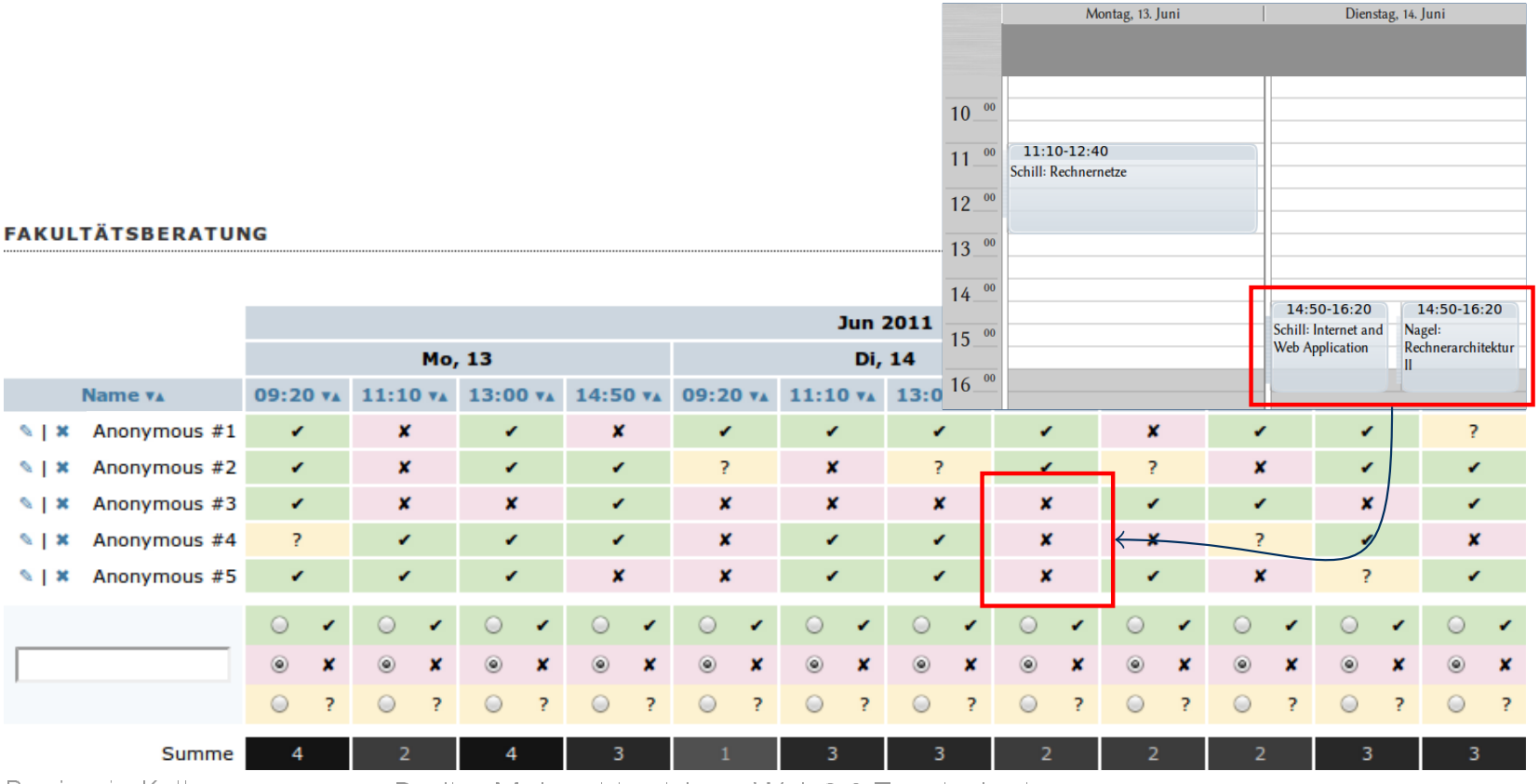


FAKULTÄTSBERATUNG

	Jun 2011											
	Mo, 13				Di, 14							
Name	09:20	11:10	13:00	14:50	09:20	11:10	13:0					
Anonymous #1	✔	✘	✔	✘	✔	✔	✔	✔	✘	✔	✔	?
Anonymous #2	✔	✘	✔	✔	?	✘	?	✔	?	✘	✔	✔
Anonymous #3	✔	✘	✘	✔	✘	✘	✘	✘	✔	✔	✘	✔
Anonymous #4	?	✔	✔	✔	✘	✔	✔	✘	✘	?	✔	✘
Anonymous #5	✔	✔	✔	✘	✘	✔	✔	✘	✔	✘	?	✔
Summe	4	2	4	3	1	3	3	2	2	2	3	3

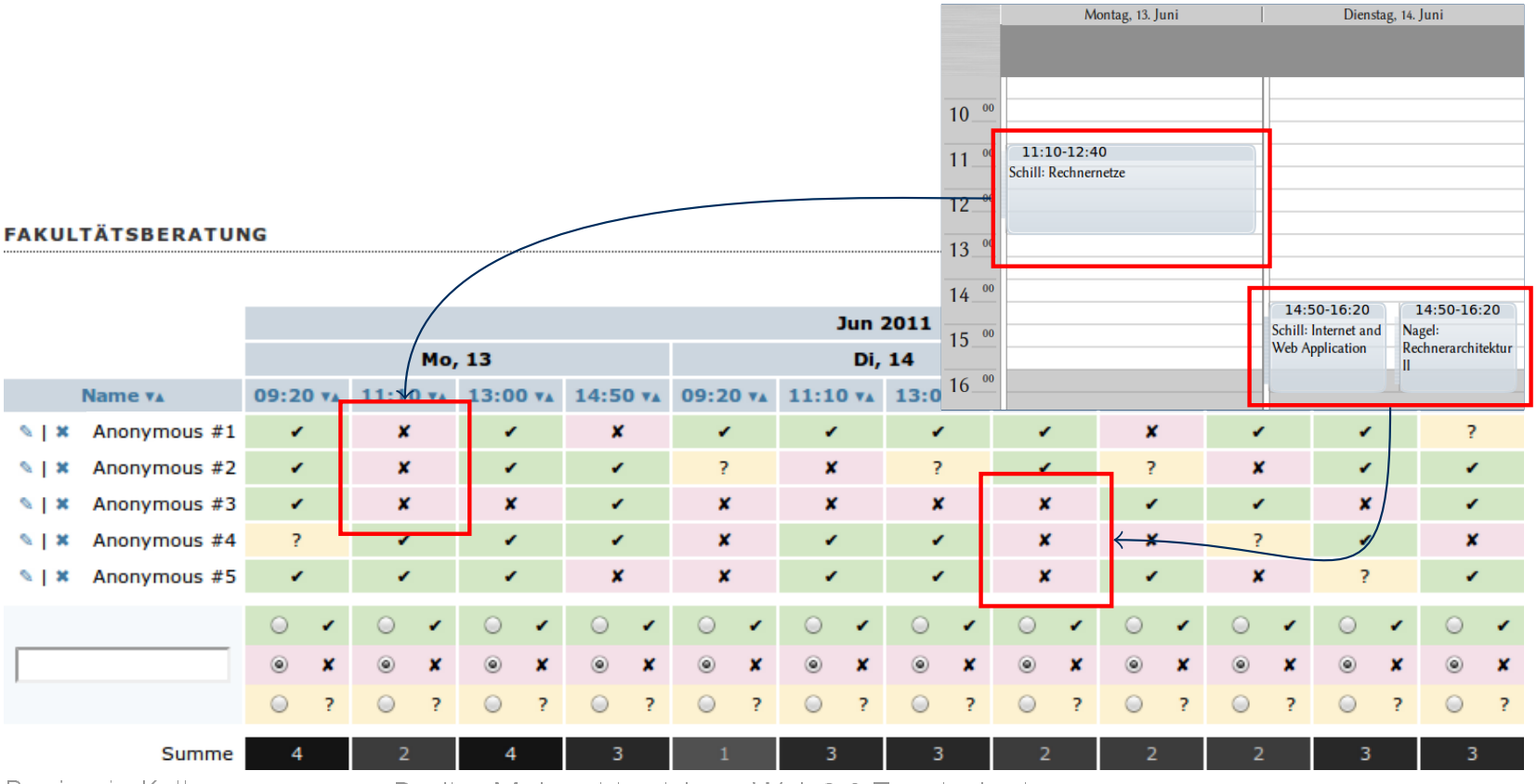
Vertraulichkeit

Indirekter Informationsgewinn



Vertraulichkeit

Indirekter Informationsgewinn



Integrität

PRÜFUNGSVORBEREITUNG

		Mrz 2011									
		Mo, 14					Di, 15				
	Name ▾▴	07:30 ▾▴	09:20 ▾▴	11:10 ▾▴	13:00 ▾▴	14:30 ▾▴	07:30 ▾▴	09:20 ▾▴	11:10 ▾▴	13:00 ▾▴	14:30 ▾▴
✎ | ✖	s2342005	✘	✔	✘	✔	✔	✘	✔	✘	✔	✔
✎ | ✖	Anonymous #1	✘	✔	✘	✘	?	✔	✘	✘	✔	✘
✎ | ✖	Tom	✘	✘	✔	✔	✔	✘	✘	✔	✔	✔
✎ | ✖	Oskar	✘	✔	?	✔	✔	✘	✔	✔	✘	✘
✎ | ✖	Anonymous #2	✘	✔	✘	✔	✘	✔	✔	✘	✘	✘
✎ | ✖	Jörg	✘	?	✔	✔	✔	✘	✔	✘	✔	✘
✎ | ✖	Anonymous #3	✘	✔	✘	✘	✘	✘	✘	✘	✘	✘
✎ | ✖	Anonymous #4	✘	✔	✘	✘	✘	✘	✘	✘	✘	✘
✎ | ✖	Anonymous #5	✘	✔	✘	✘	✘	✘	✘	✘	✘	✘
✎ | ✖	Anonymous #6	✘	✔	✘	✘	✘	✘	✘	✘	✘	✘
✎ | ✖	Anonymous #7	✘	✔	✘	✘	✘	✘	✘	✘	✘	✘
✎ | ✖	Anonymous #8	✘	✔	✘	✘	✘	✘	✘	✘	✘	✘
✎ | ✖	Alex	✘	?	✔	✔	?	✔	✘	✘	✘	✘
✎ | ✖	Arthur	✘	✘	✔	?	✔	✔	✘	✘	✔	✔
✎ | ✖	s4711007	✘	✔	✘	✔	✘	✔	✘	✔	✔	✘

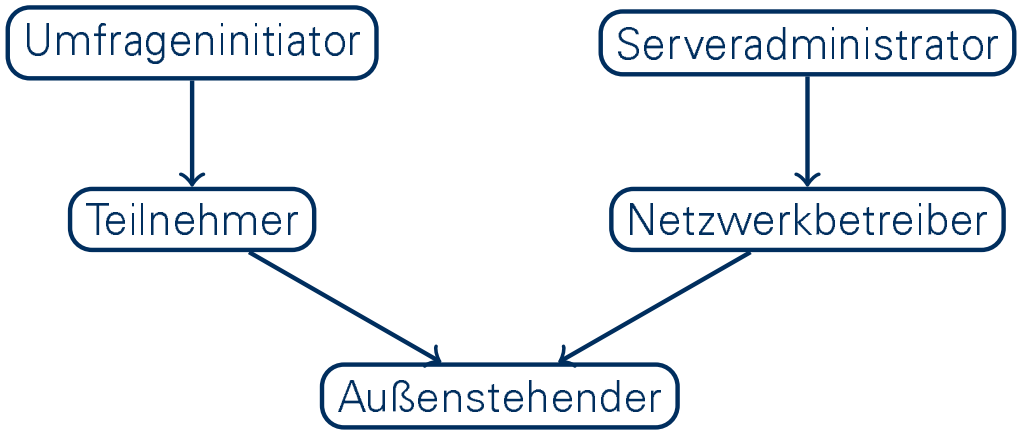
Integrität

PRÜFUNGSVORBEREITUNG

		Mrz 2011									
		Mo, 14					Di, 15				
	Name ▾▴	07:30 ▾▴	09:20 ▾▴	11:10 ▾▴	13:00 ▾▴	14:30 ▾▴	07:30 ▾▴	09:20 ▾▴	11:10 ▾▴	13:00 ▾▴	14:30 ▾▴
✎ | ✖	s2342005	✘	✔	✘	✔	✔	✘	✔	✘	✔	✔
✎ | ✖	Anonymous #1	✘	✔	✘	✘	?	✔	✘	✘	✔	✘
✎ | ✖	Tom	✘	✘	✔	✔	✔	✘	✘	✔	✔	✔
✎ | ✖	Oskar	✘	✔	?	✔	✔	✘	✔	✔	✘	✘
✎ | ✖	Anonymous #2	✘	✔	✘	✔	✘	✔	✔	✘	✘	✘
✎ | ✖	Jörg	✘	?	✔	✔	✔	✘	✔	✘	✔	✘
✎ | ✖	Anonymous #3	✘	✔	✘	✘	✘	✘	✘	✘	✘	✘
✎ | ✖	Anonymous #4	✘	✔	✘	✘	✘	✘	✘	✘	✘	✘
✎ | ✖	Anonymous #5	✘	✔	✘	✘	✘	✘	✘	✘	✘	✘
✎ | ✖	Anonymous #6	✘	✔	✘	✘	✘	✘	✘	✘	✘	✘
✎ | ✖	Anonymous #7	✘	✔	✘	✘	✘	✘	✘	✘	✘	✘
✎ | ✖	Anonymous #8	✘	✔	✘	✘	✘	✘	✘	✘	✘	✘
✎ | ✖	Alex	✘	?	✔	✔	?	✔	✘	✘	✘	✘
✎ | ✖	Arthur	✘	✘	✔	?	✔	✔	✘	✘	✔	✔
✎ | ✖	s4711007	✘	✔	✘	✔	✘	✔	✘	✔	✔	✘

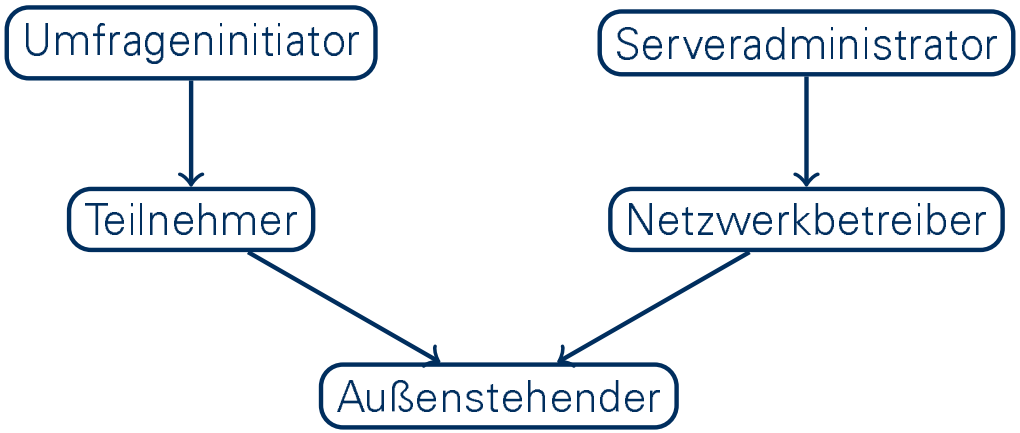
Mehrseitig sichere Web 2.0-Terminabstimmung

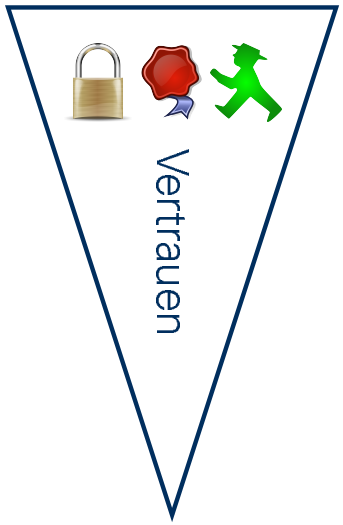
Involvierte Parteien



Mehrseitig sichere Web 2.0-Terminabstimmung

Involvierte Parteien





Flexibilität

FAKULTÄTSBERATUNG

		Jun 2011											
		Mo, 13				Di, 14				Mi, 15			
Name ▾▴		09:20 ▾▴	11:10 ▾▴	13:00 ▾▴	14:50 ▾▴	09:20 ▾▴	11:10 ▾▴	13:00 ▾▴	14:50 ▾▴	09:20 ▾▴	11:10 ▾▴	13:00 ▾▴	14:50 ▾▴
✎ | ✖	Lehner	✔	✘	✔	✘	✔	✔	✔	✔	✘	✔	✔	?
✎ | ✖	Aßmann	✔	✘	✔	✔	?	✘	?	✔	?	✘	✔	✔
✎ | ✖	Schill	✔	✘	✘	✔	✘	✘	✘	✘	✔	✔	✘	✔
✎ | ✖	Hochberger	?	✔	✔	✔	✘	✔	✔	✘	✘	?	✔	✘
✎ | ✖	Nagel	✔	✔	✔	✘	✘	✔	✔	✘	✔	✘	?	✔
		○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔
		◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘
		○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?
	Summe	4	2	4	3	1	3	3	2	2	2	3	3

Flexibilität

FAKULTÄTSBERATUNG

	Jun 2011											
	Mo, 13				Di, 14				Mi, 15			
Name ▾▴	09:20 ▾▴	11:10 ▾▴	13:00 ▾▴	14:50 ▾▴	09:20 ▾▴	11:10 ▾▴	13:00 ▾▴	14:50 ▾▴	09:20 ▾▴	11:10 ▾▴	13:00 ▾▴	14:50 ▾▴
✎ | ✖ Lehner	✔	✘	✔	✘	✔	✔	✔	✔	✘	✔	✔	?
✎ | ✖ Aßmann	✔	✘	✔	✔	?	✘	?	✔	?	✘	✔	✔
✎ | ✖ Schill	✔	✘	✘	✔	✘	✘	✘	✘	✔	✔	✘	✔
✎ | ✖ Hochberger	?	✔	✔	✔	✘	✔	✔	✘	✘	?	✔	✘
✎ | ✖ Nagel	✔	✔	✔	✘	✘	✔	✔	✘	✔	✘	?	✔
	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔	○ ✔
	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘	◉ ✘
	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?	○ ?
Summe	4	2	4	3	1	3	3	2	2	2	3	3

Flexibilität

FAKULTÄTSBERATUNG

Flexibilität

FAKULTÄTSBERATUNG

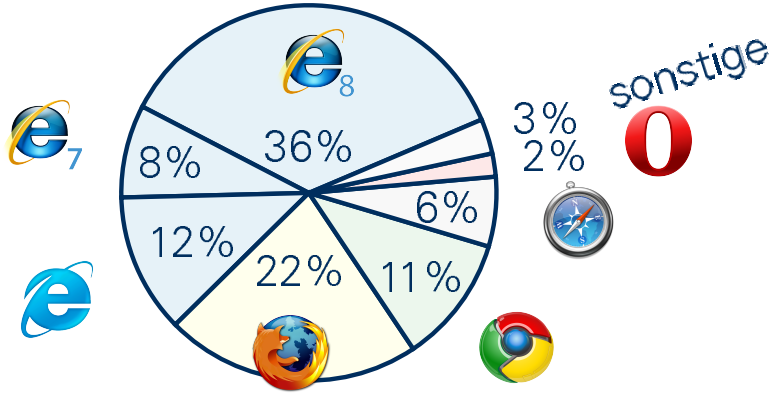
Terminauswahlfunktion?

Berechnungskomplexität

	 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

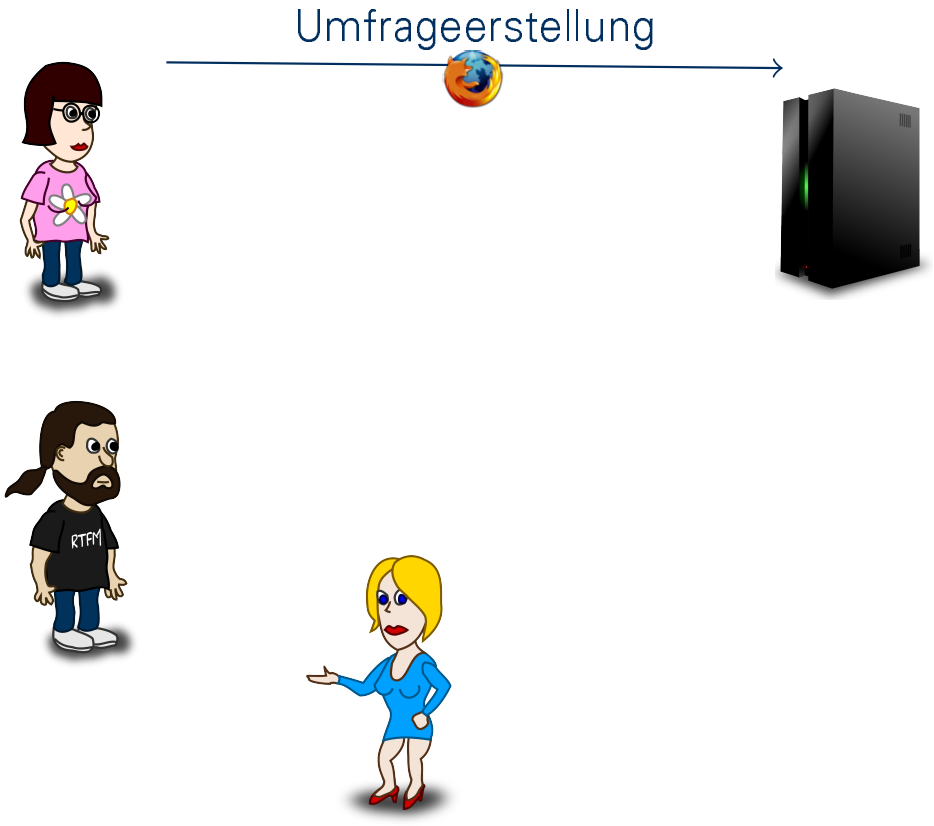
Berechnungskomplexität

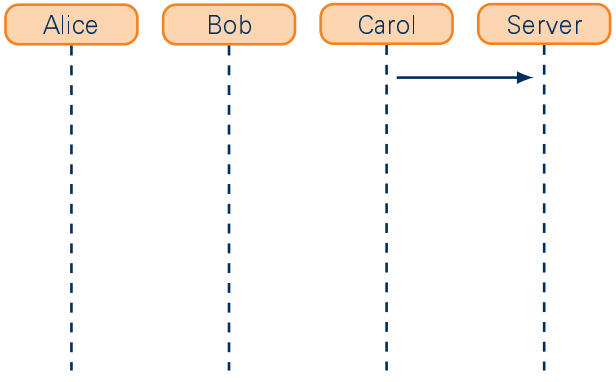
	8.0	7.0	6.0	3.6.13	9.0.597	5.0.3	11.01
modPow() – JS-Wu	**4,89 s**	**5,39 s**	**5,49 s**	1,74 s	**0,18 s**	1,49 s	0,52 s
modPow() – JS-Baird	8,46 s	13,43 s	13,56 s	**0,76 s**	0,25 s	**0,25 s**	**0,30 s**
modPow() – Java	0,03 s	0,04 s	0,03 s	0,04 s	0,04 s	0,03 s	0,03 s
1000 × AES256	1,02 s	2,51 s	2,52 s	0,35 s	0,04 s	0,08 s	0,07 s



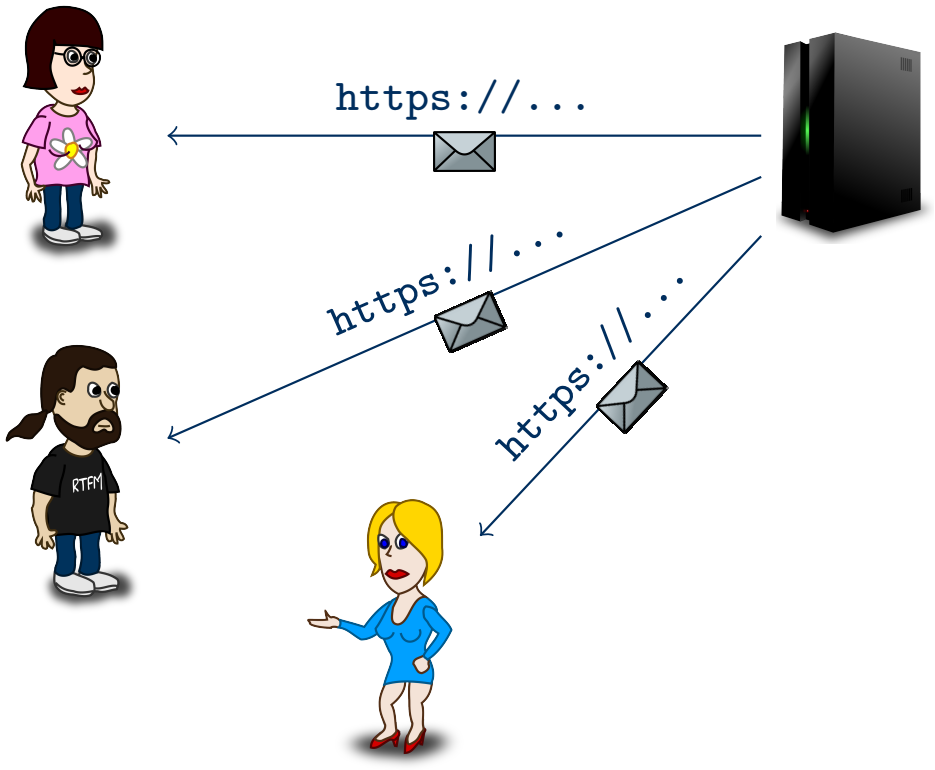
Web-Browser Marktanteil
(Februar 2011)

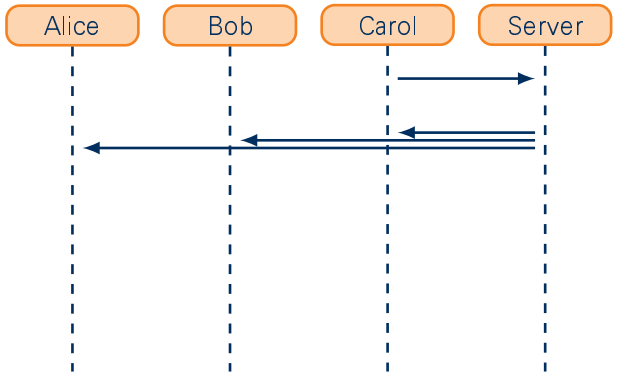
Notwendige Kommunikationsschritte



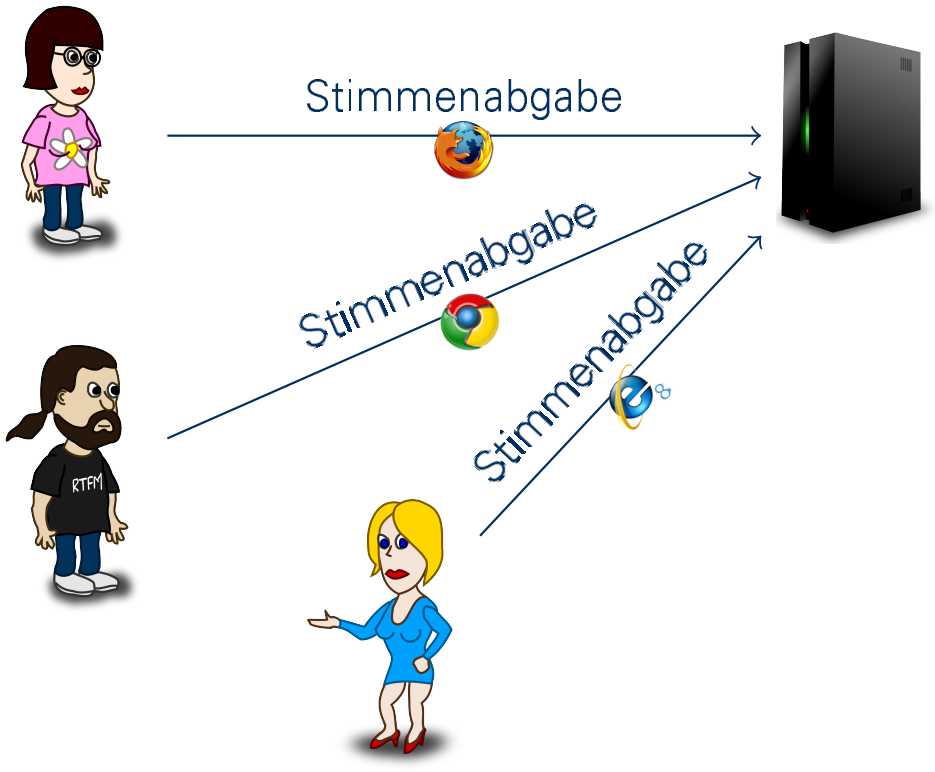


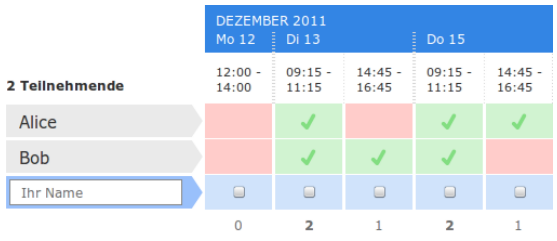
Notwendige Kommunikationsschritte

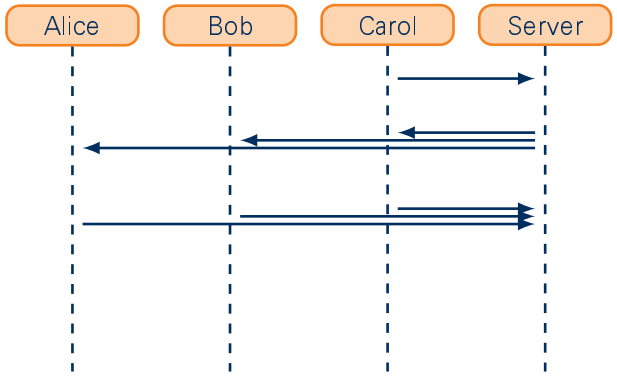




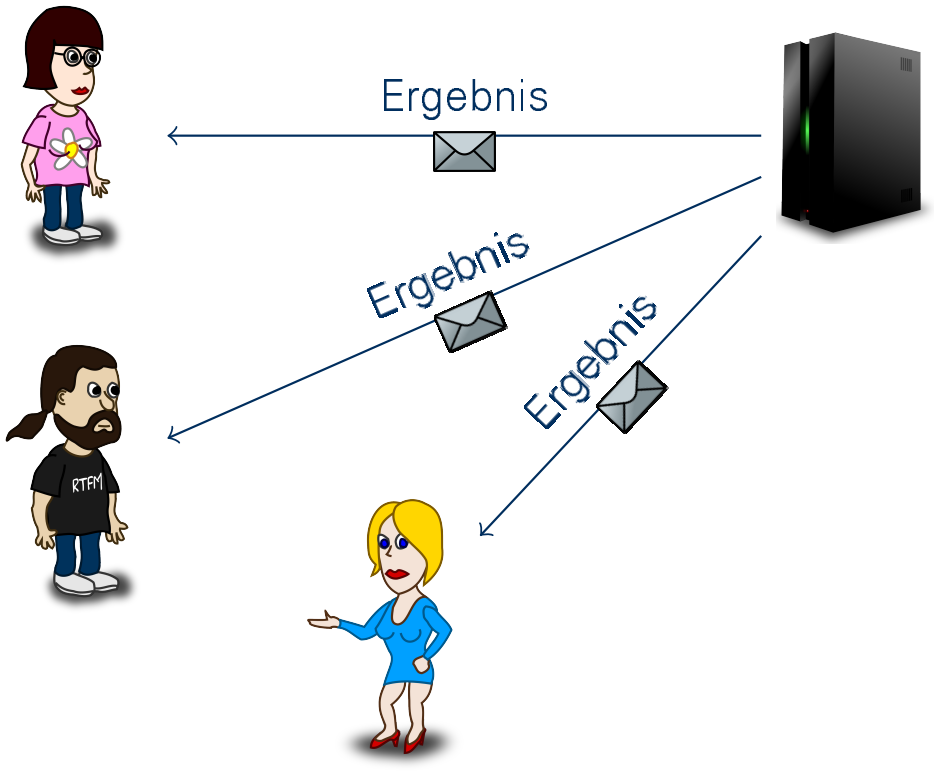
Notwendige Kommunikationsschritte

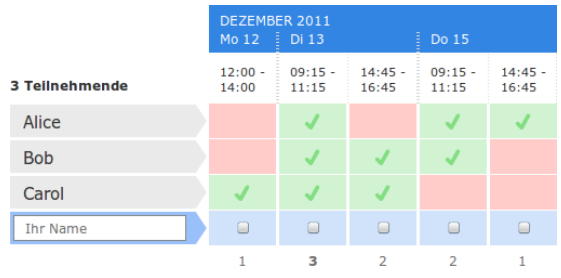


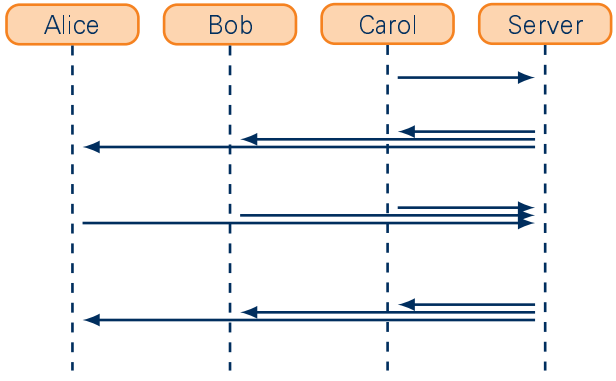




Notwendige Kommunikationsschritte







Inhalt

- Anforderungen
  - Sicherheit ()
  - Flexibilität (Terminauswahl)
  - Berechnungsaufwand ()
  - Protokollrunden (1 Interaktion)

Neue Protokolle

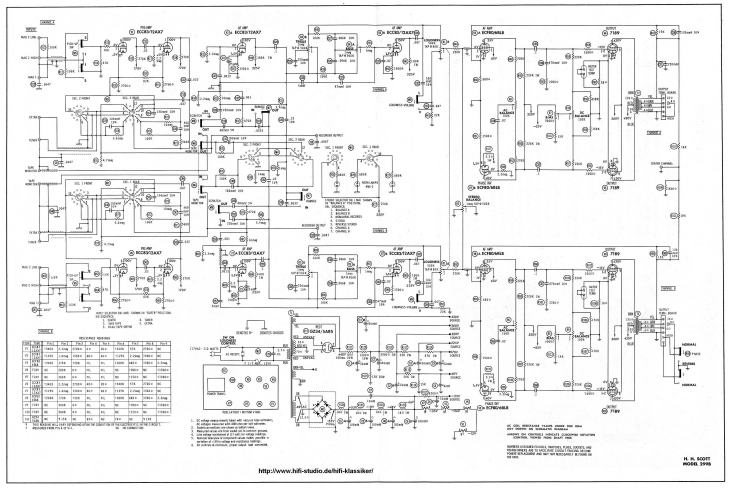
Implementierung

Zusammenfassung / Ausblick

Inhalt

Anforderungen

- Sicherheit
- Flexibilität (Terminauswahl)
- Berechnungsaufwand
- Protokollrunden (1 Interaktion)



→ Neue Protokolle

Implementierung

Zusammenfassung / Ausblick

Vertrauensmodelle

Abstimmen (Schreibzugriff)	Ergebnis anschauen (Lesezugriff)	Initiator	Teil-nehmer	Außen-stehender	Server Admin

Existierende Modelle

Vertrauensmodelle

Abstimmen (Schreibzugriff)	Ergebnis anschauen (Lesezugriff)	Initiator	Teil-nehmer	Außen-stehender	Server Admin
—	—				

Existierende Modelle

Vertrauensmodelle

Abstimmen (Schreibzugriff)	Ergebnis anschauen (Lesezugriff)	Initiator	Teil-nehmer	Außen-stehender	Server Admin
—	—				
Abstimmungspasswort	Abstimmungspasswort				

Existierende Modelle

Vertrauensmodelle

Abstimmen (Schreibzugriff)	Ergebnis anschauen (Lesezugriff)	Initiator	Teil-nehmer	Außen-stehender	Server Admin
—	—				
Abstimmungspasswort	Abstimmungspasswort				
Benutzerpasswort	Abstimmungspasswort				

Existierende Modelle

Vertrauensmodelle

Abstimmen (Schreibzugriff)	Ergebnis anschauen (Lesezugriff)	Initiator	Teil-nehmer	Außen-stehender	Server Admin
—	—				
Abstimmungspasswort	Abstimmungspasswort				
Benutzerpasswort	Abstimmungspasswort				
Benutzerpasswort	Initiatorpasswort				

Existierende Modelle

Vertrauensmodelle

Abstimmen (Schreibzugriff)	Ergebnis anschauen (Lesezugriff)	Initiator	Teil-nehmer	Außen-stehender	Server Admin
—	—				
Abstimmungspasswort	Abstimmungspasswort			🔒🔴	
Benutzerpasswort	Abstimmungspasswort	🔴	🔴	🔒🔴	
Benutzerpasswort	Initiatorpasswort		🔒🔴	🔒🔴	
Benutzerpasswort	Nur die Summe wird angezeigt	🔒	🔒🔴	🔒🔴	

Existierende Modelle

Vertrauensmodelle

Abstimmen (Schreibzugriff)	Ergebnis anschauen (Lesezugriff)	Initiator	Teil-nehmer	Außen-stehender	Server Admin
—	—				
Abstimmungspasswort	Abstimmungspasswort			🔒🔴	
Benutzerpasswort	Abstimmungspasswort	🔴	🔴	🔒🔴	
Benutzerpasswort	Initiatorpasswort		🔒🔴	🔒🔴	
Benutzerpasswort	Nur die Summe wird angezeigt	🔒	🔒🔴	🔒🔴	

Existierende Modelle

Vertrauensmodelle

Abstimmen (Schreibzugriff)	Ergebnis anschauen (Lesezugriff)	Initiator	Teil-nehmer	Außen-stehender	Server Admin
—	—				
Abstimmungspasswort	Abstimmungspasswort			🔒 🔴	
Symmetrische Authentifikation	Symmetrische Verschlüsselung			🔒 🔴	🔒 🔴
Benutzerpasswort	Abstimmungspasswort	🔴	🔴	🔒 🔴	
Benutzerpasswort	Initiatorpasswort		🔒 🔴	🔒 🔴	
Benutzerpasswort	Nur die Summe wird angezeigt	🔒	🔒 🔴	🔒 🔴	

Existierende Modelle

Im Rahmen dieser Dissertation entstandene Modelle

Vertrauensmodelle

Abstimmen (Schreibzugriff)	Ergebnis anschauen (Lesezugriff)	Initiator	Teil-nehmer	Außen-stehender	Server Admin
—	—				
Abstimmungspasswort	Abstimmungspasswort			🔒🔴	
Symmetrische Authentifikation	Symmetrische Verschlüsselung			🔒🔴	🔒🔴
Benutzerpasswort	Abstimmungspasswort	🔴	🔴	🔒🔴	
Digitale Signatur	Symmetrische Verschlüsselung	🔴	🔴	🔒🔴	🔒🔴
Benutzerpasswort	Initiatorpasswort		🔒🔴	🔒🔴	
Benutzerpasswort	Nur die Summe wird angezeigt	🔒	🔒🔴	🔒🔴	

Existierende Modelle

Im Rahmen dieser Dissertation entstandene Modelle

Vertrauensmodelle

Abstimmen (Schreibzugriff)	Ergebnis anschauen (Lesezugriff)	Initiator	Teil-nehmer	Außen-stehender	Server Admin
—	—				
Abstimmungspasswort	Abstimmungspasswort			🔒🔴	
Symmetrische Authentifikation	Symmetrische Verschlüsselung			🔒🔴	🔒🔴
Benutzerpasswort	Abstimmungspasswort	🔴	🔴	🔒🔴	
Digitale Signatur	Symmetrische Verschlüsselung	🔴	🔴	🔒🔴	🔒🔴
Benutzerpasswort	Initiatorpasswort		🔒🔴	🔒🔴	
Digitale Signatur	Asymmetrische Verschlüsselung an Initiator		🔒🔴	🔒🔴	🔒🔴
Benutzerpasswort	Nur die Summe wird angezeigt	🔒	🔒🔴	🔒🔴	

Existierende Modelle

Im Rahmen dieser Dissertation entstandene Modelle

Vertrauensmodelle

Abstimmen (Schreibzugriff)	Ergebnis anschauen (Lesezugriff)	Initiator	Teil-nehmer	Außen-stehender	Server Admin
—	—				
Abstimmungspasswort	Abstimmungspasswort			🔒🎖	
Symmetrische Authentifikation	Symmetrische Verschlüsselung			🔒🎖	🔒🎖
Benutzerpasswort	Abstimmungspasswort	🎖	🎖	🔒🎖	
Digitale Signatur	Symmetrische Verschlüsselung	🎖	🎖	🔒🎖	🔒🎖
Benutzerpasswort	Initiatorpasswort		🔒🎖	🔒🎖	
Digitale Signatur	Asymmetrische Verschlüsselung an Initiator		🔒🎖	🔒🎖	🔒🎖
Benutzerpasswort	Nur die Summe wird angezeigt	🔒	🔒🎖	🔒🎖	
Digitale Signatur	Nur die Summe kann berechnet werden	🔒🎖	🔒🎖	🔒🎖	🔒🎖

Existierende Modelle

Im Rahmen dieser Dissertation entstandene Modelle

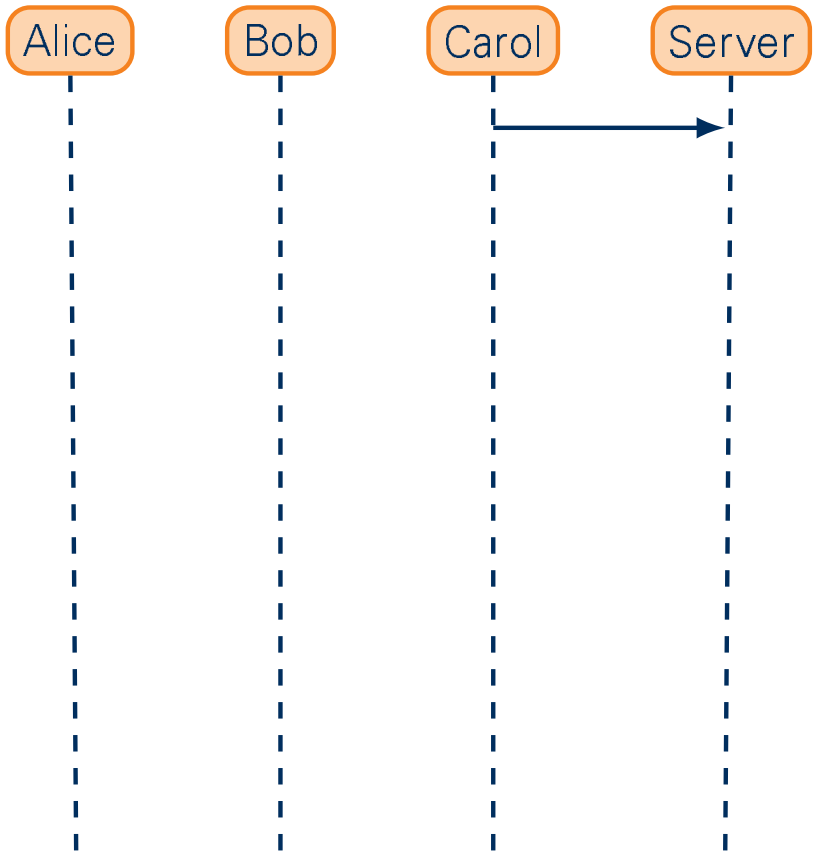
Vertrauensmodelle

Abstimmen (Schreibzugriff)	Ergebnis anschauen (Lesezugriff)	Initiator	Teil-nehmer	Außen-stehender	Server Admin
—	—				
Abstimmungspasswort	Abstimmungspasswort			🔒🎖	
Symmetrische Authentifikation	Symmetrische Verschlüsselung			🔒🎖	🔒🎖
Benutzerpasswort	Abstimmungspasswort	🎖	🎖	🔒🎖	
Digitale Signatur	Symmetrische Verschlüsselung	🎖	🎖	🔒🎖	🔒🎖
Benutzerpasswort	Initiatorpasswort		🔒🎖	🔒🎖	
Digitale Signatur	Asymmetrische Verschlüsselung an Initiator		🔒🎖	🔒🎖	🔒🎖
Benutzerpasswort	Nur die Summe wird angezeigt	🔒	🔒🎖	🔒🎖	
Digitale Signatur	Nur die Summe kann berechnet werden	🔒🎖	🔒🎖	🔒🎖	🔒🎖

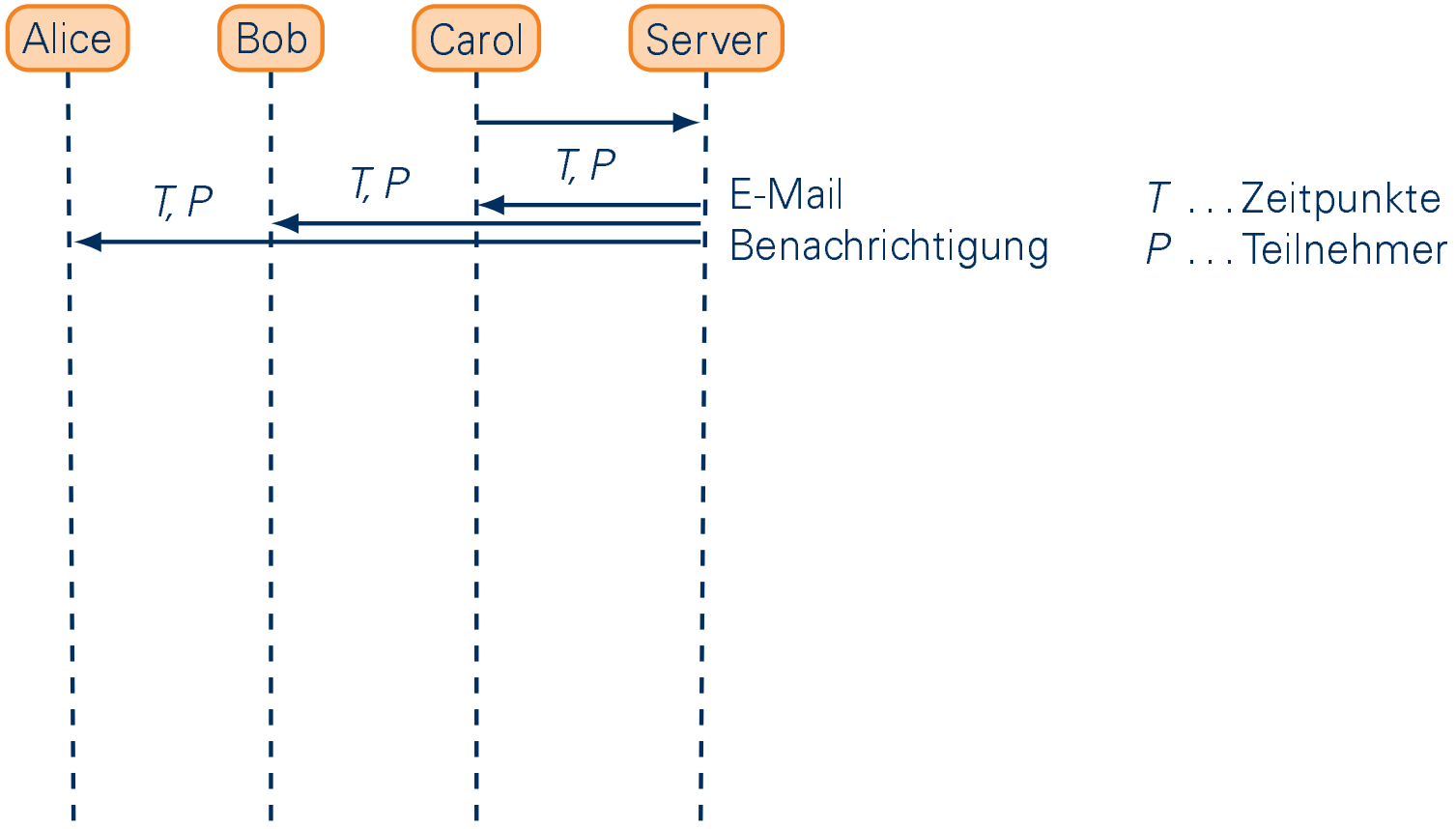
Existierende Modelle

Im Rahmen dieser Dissertation entstandene Modelle

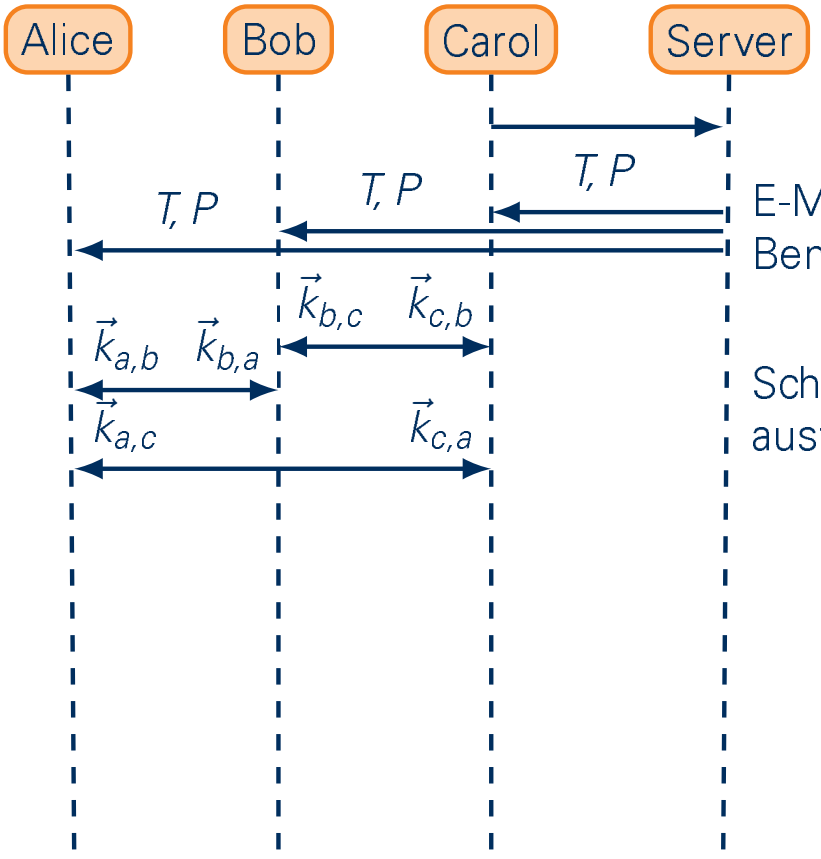
Umfrageerstellung [Kellermann, Böhme, IEEE CSE/PASSAT 2009]



Umfrageerstellung [Kellermann, Böhme, IEEE CSE/PASSAT 2009]



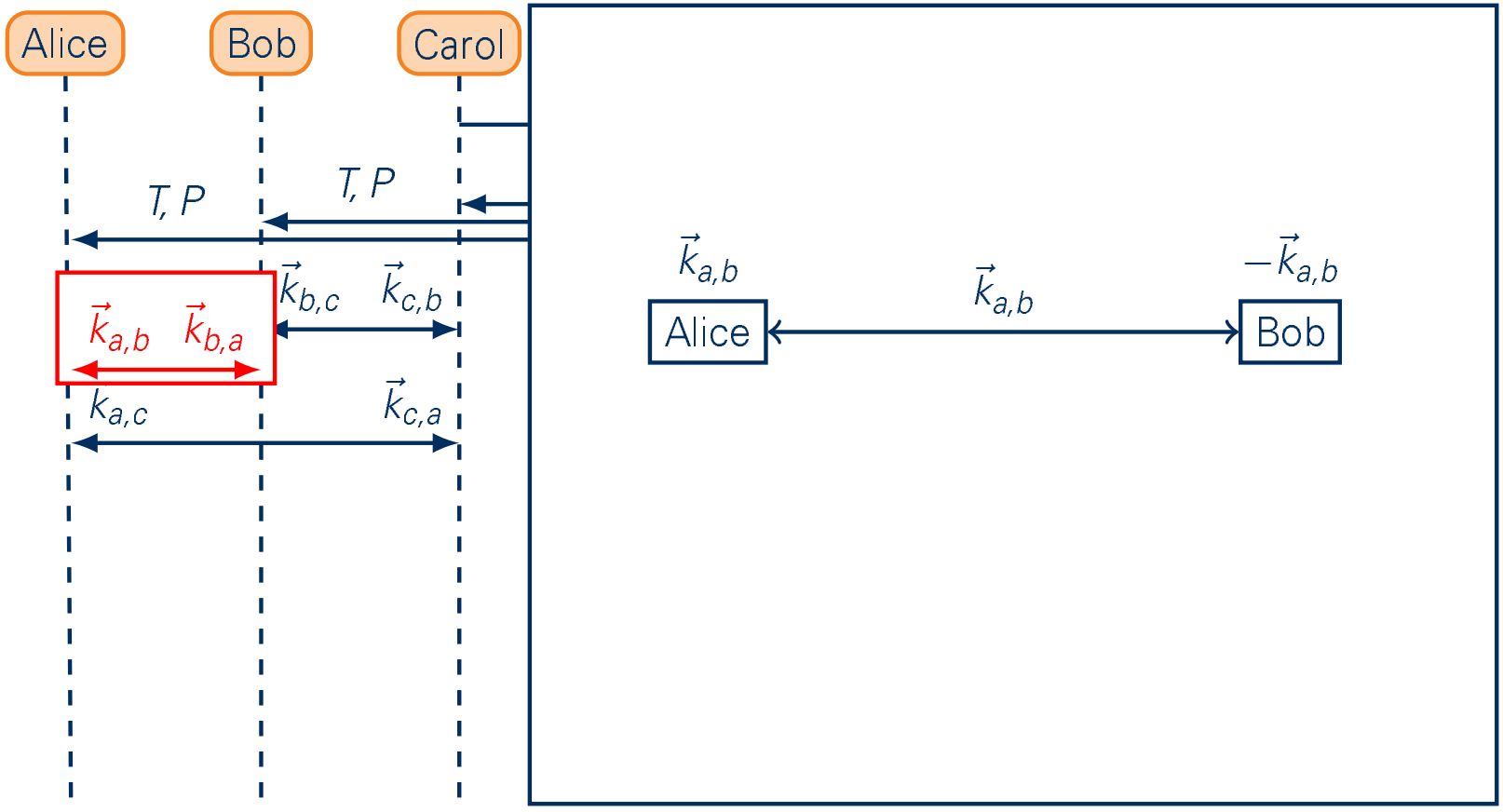
Umfrageerstellung [Kellermann, Böhme, IEEE CSE/PASSAT 2009]



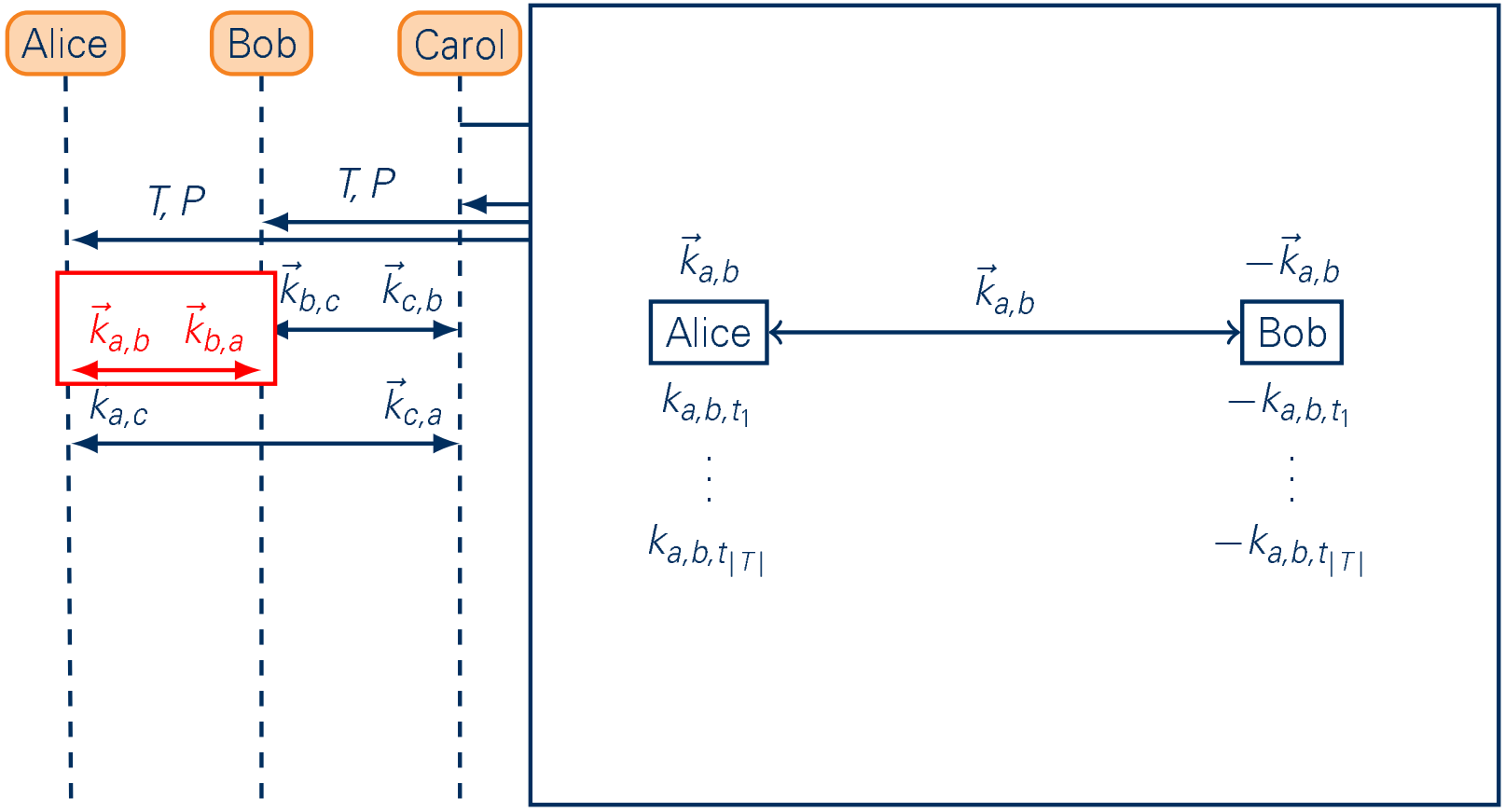
T . . . Zeitpunkte
P . . . Teilnehmer

$\vec{k}_{i,j}$ . . . Schlüsselvektor

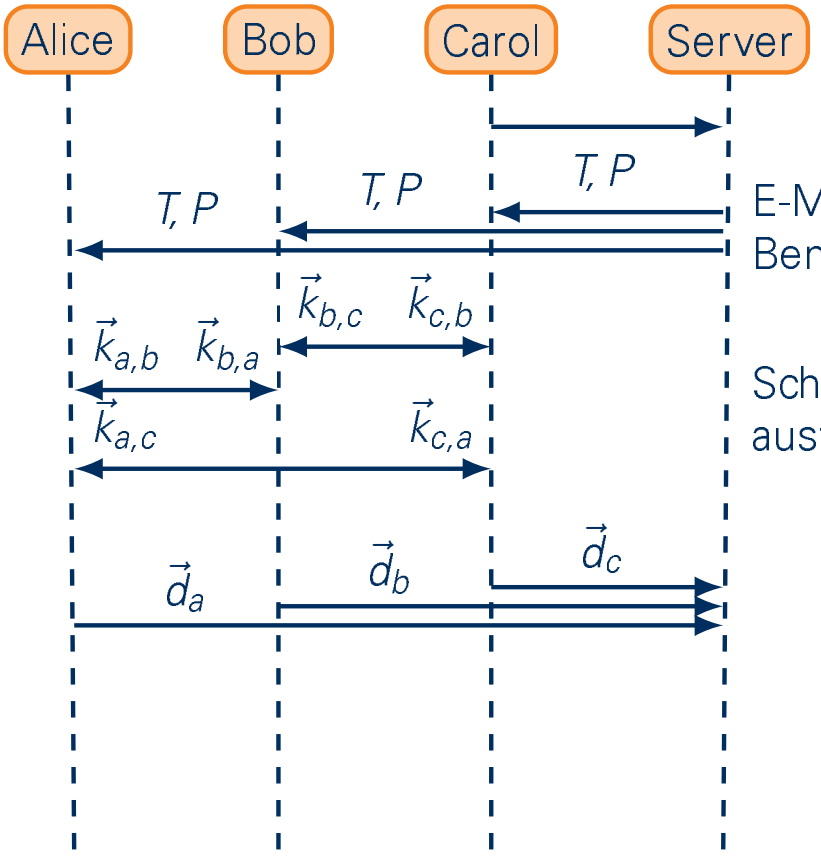
Umfrageerstellung [Kellermann, Böhme, IEEE CSE/PASSAT 2009]



Umfrageerstellung [Kellermann, Böhme, IEEE CSE/PASSAT 2009]



Stimmenabgabe [Kellermann, Böhme, IEEE CSE/PASSAT 2009]

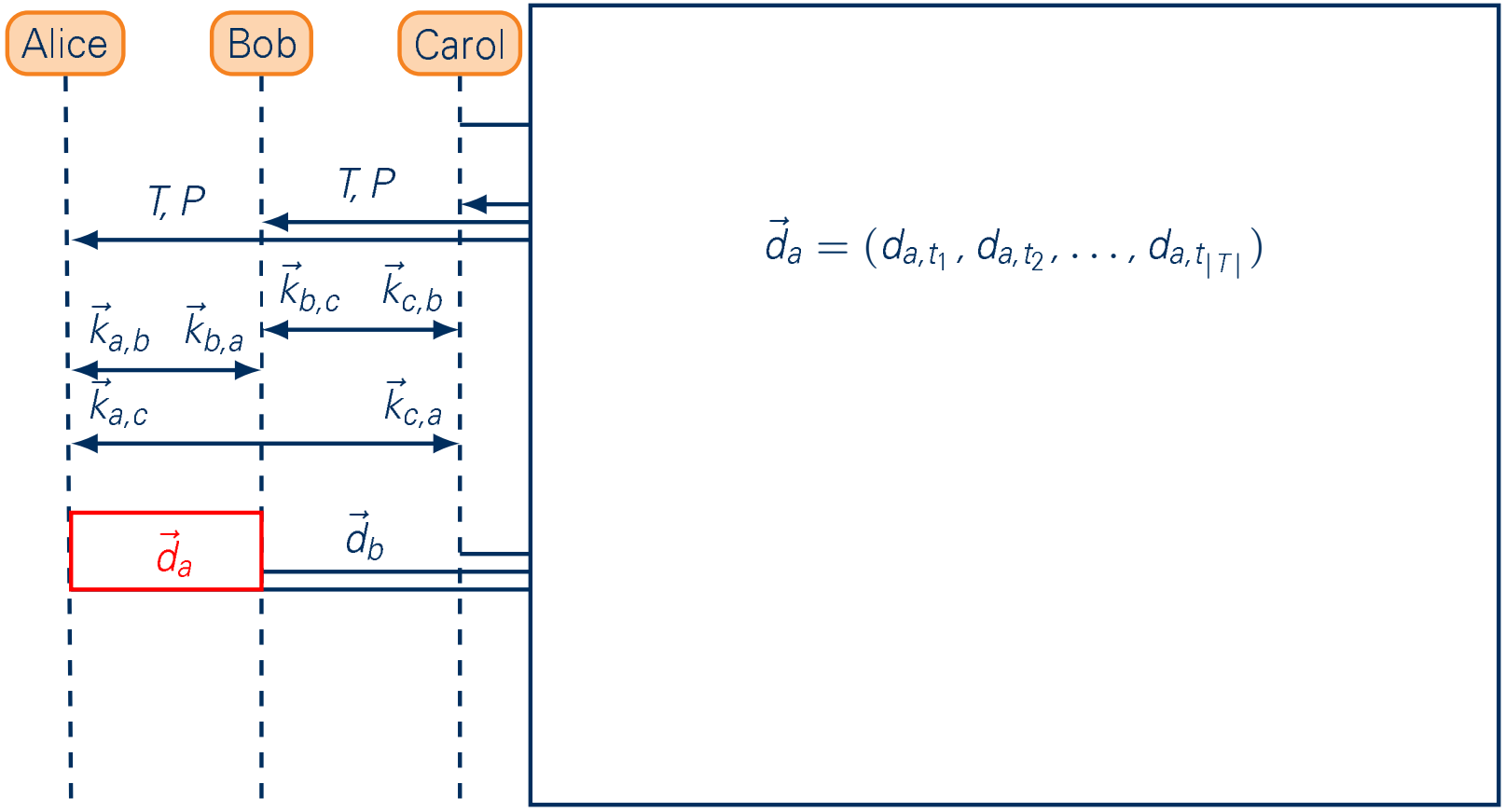


T . . . Zeitpunkte
P . . . Teilnehmer

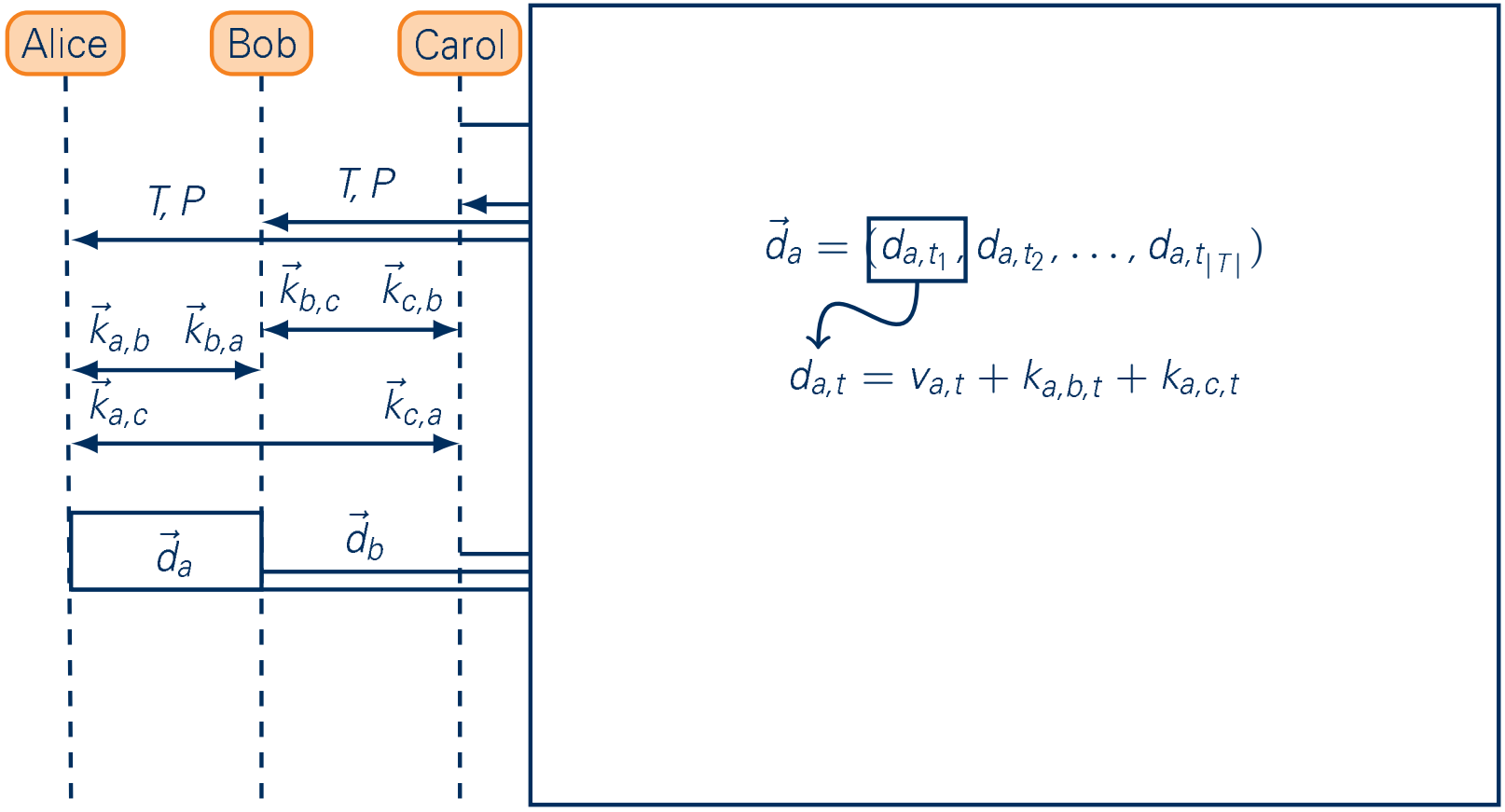
$\vec{k}_{i,j}$ . . . Schlüsselvektor

$\vec{d}$ . . . verschlüsselte Stimmen

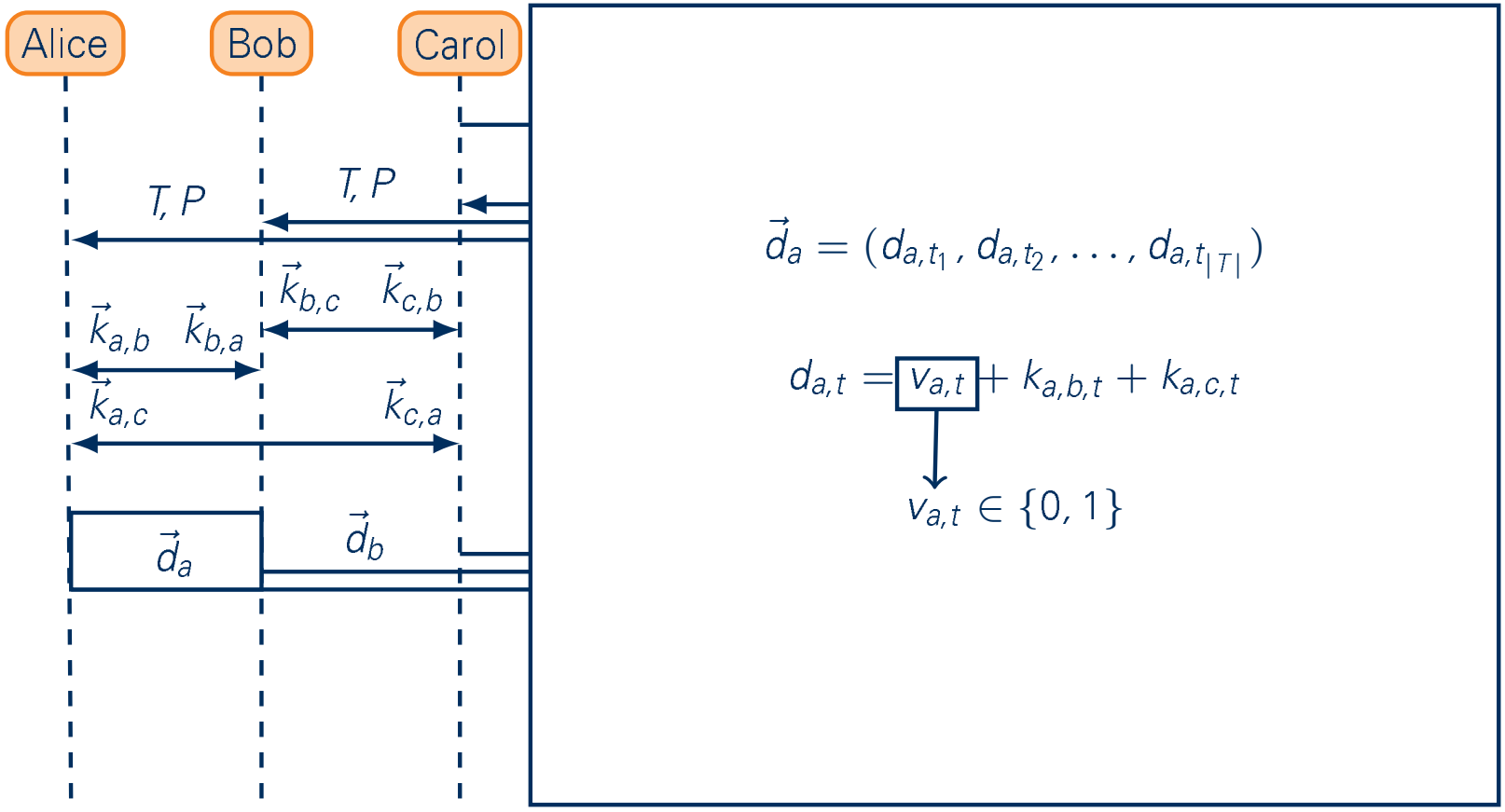
Stimmenabgabe [Kellermann, Böhme, IEEE CSE/PASSAT 2009]



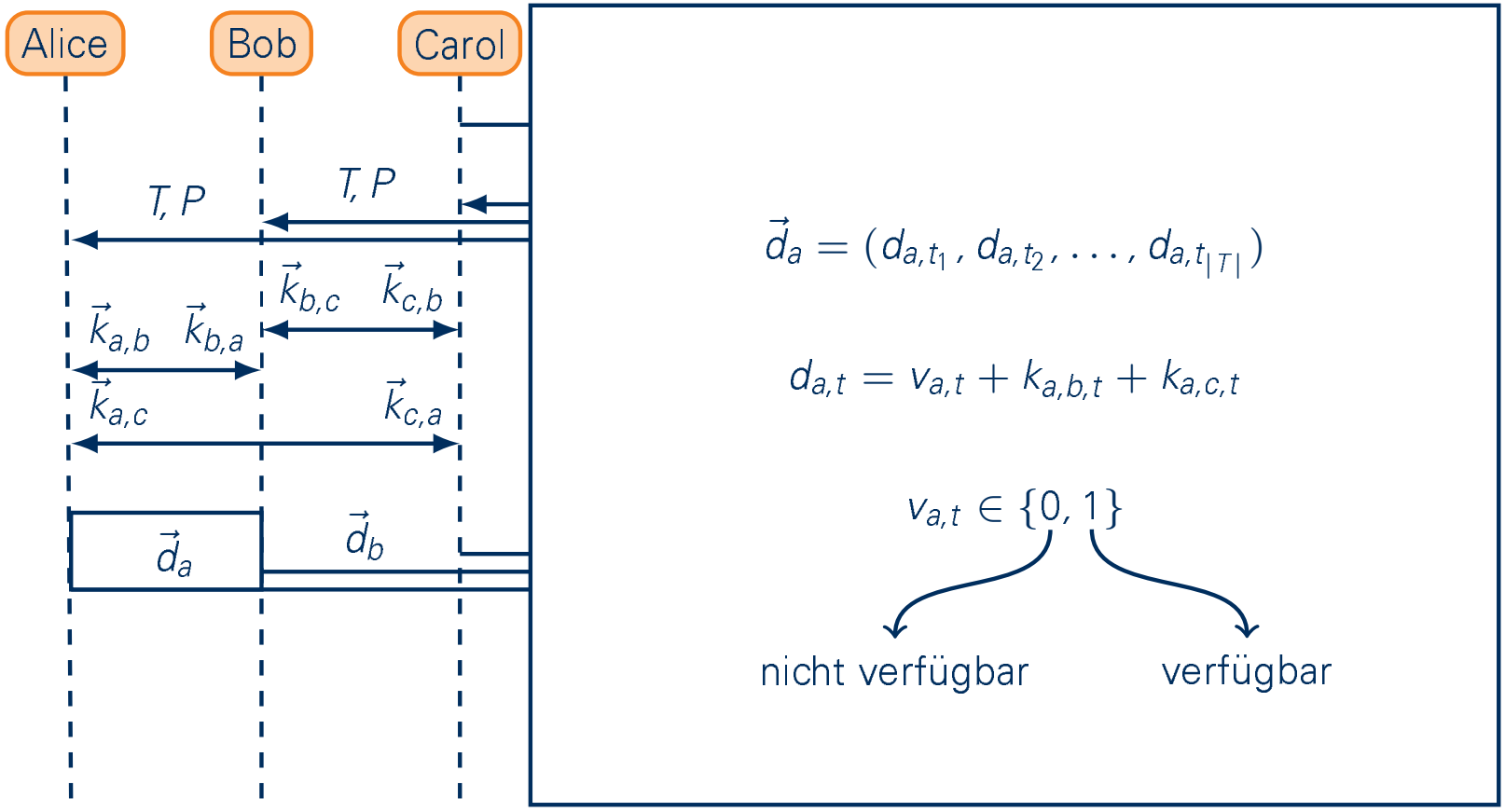
Stimmenabgabe [Kellermann, Böhme, IEEE CSE/PASSAT 2009]



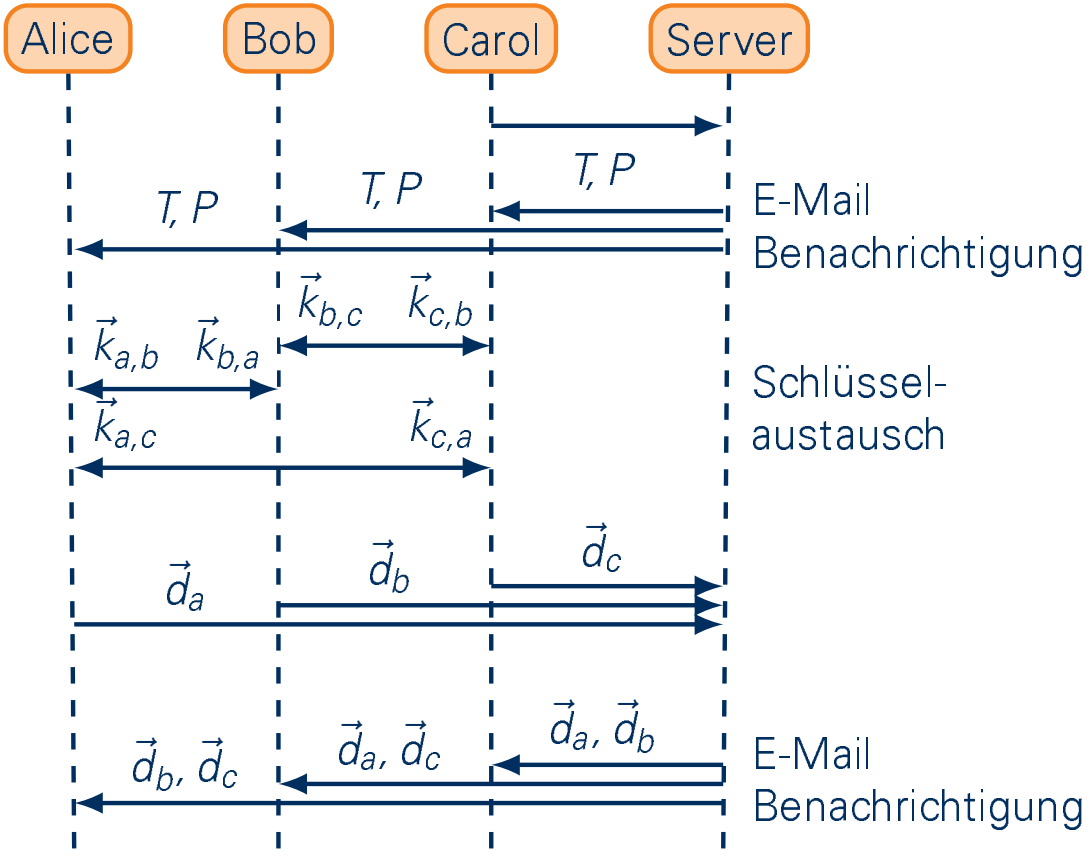
Stimmenabgabe [Kellermann, Böhme, IEEE CSE/PASSAT 2009]



Stimmenabgabe [Kellermann, Böhme, IEEE CSE/PASSAT 2009]



Ergebnisveröffentlichung [Kellermann, Böhme, IEEE CSE/PASSAT 2009]

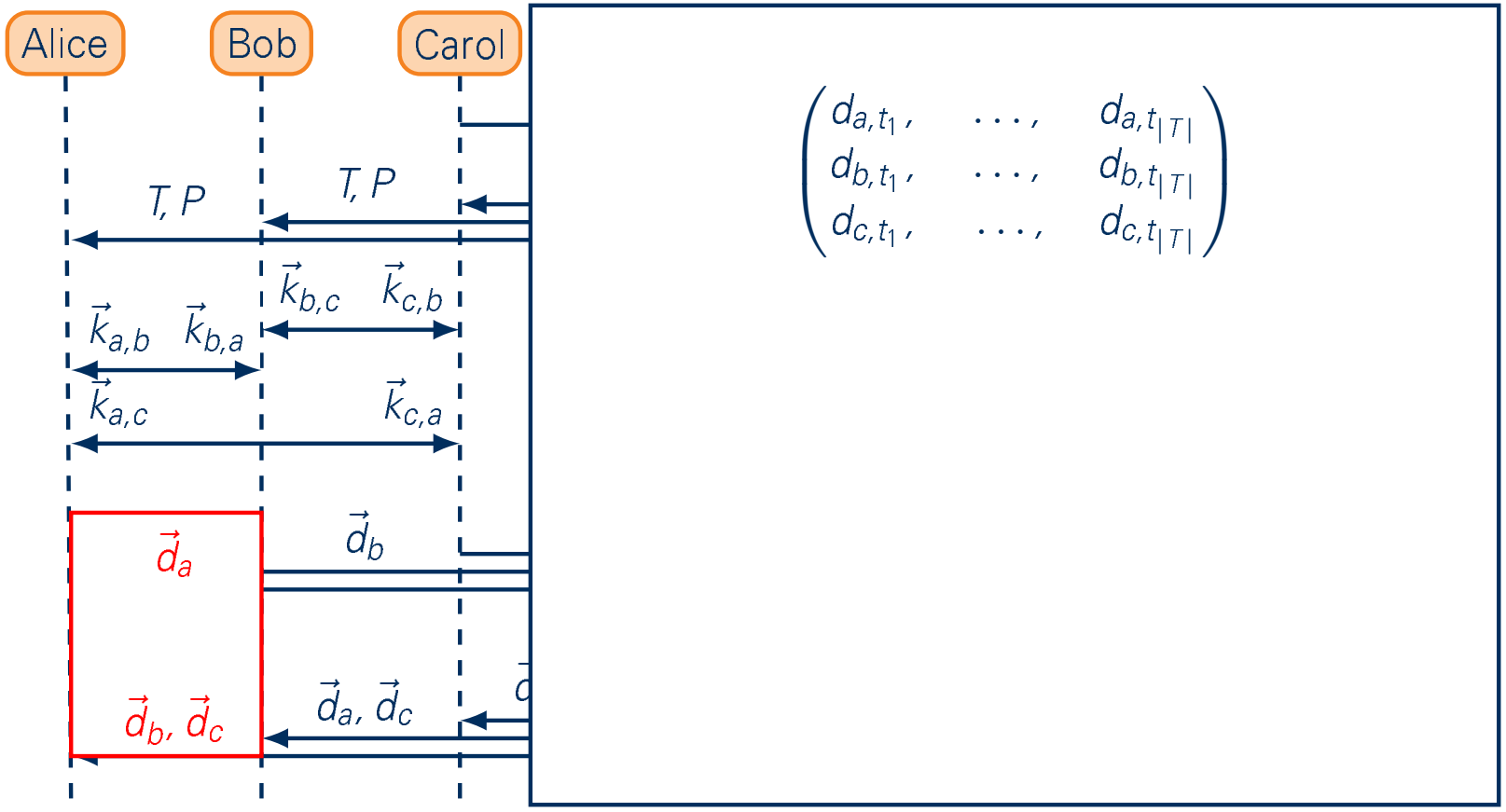


T . . . Zeitpunkte
P . . . Teilnehmer

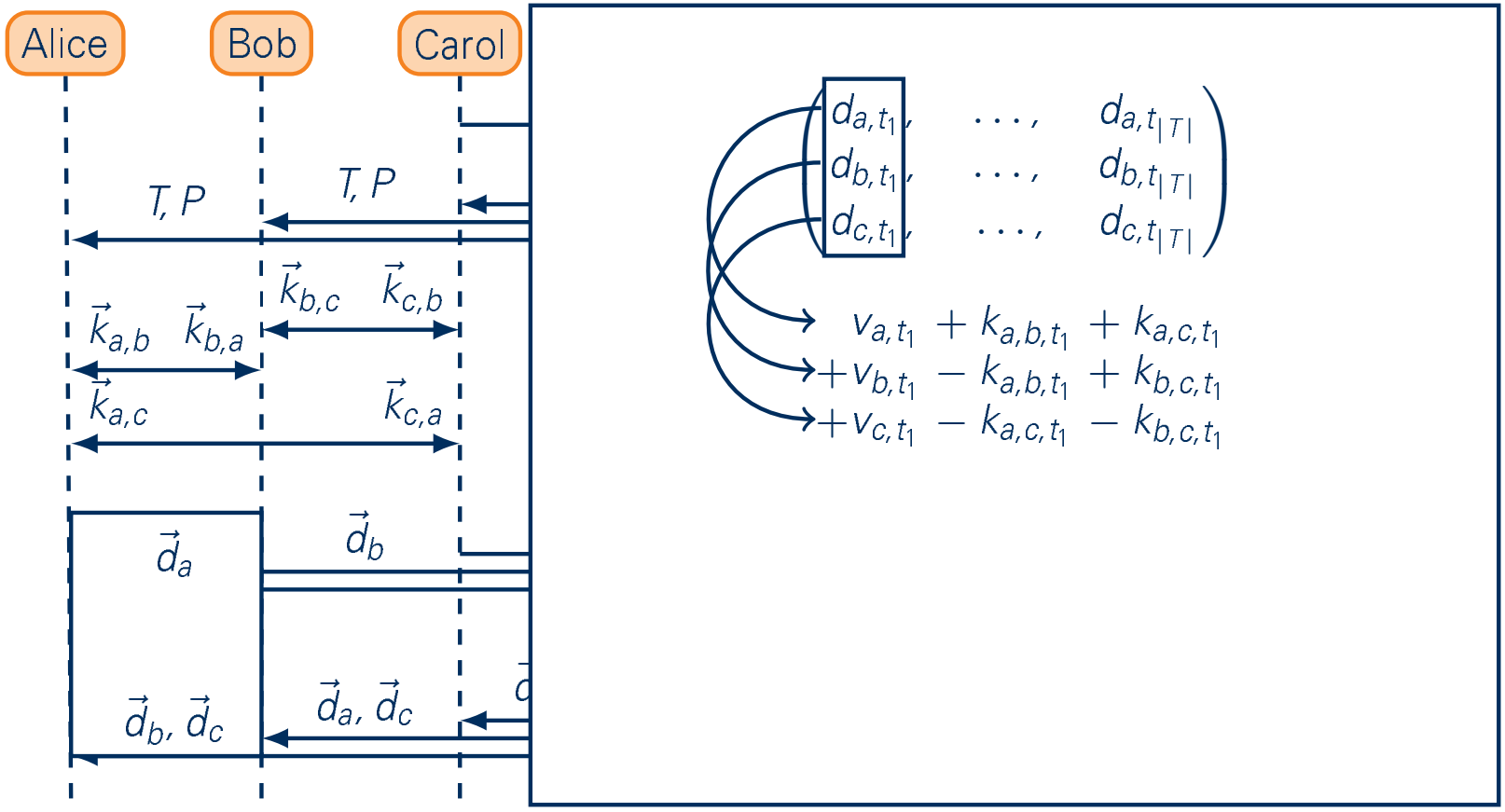
$\vec{k}_{i,j}$ . . . Schlüsselvektor

$\vec{d}$ . . . verschlüsselte Stimmen

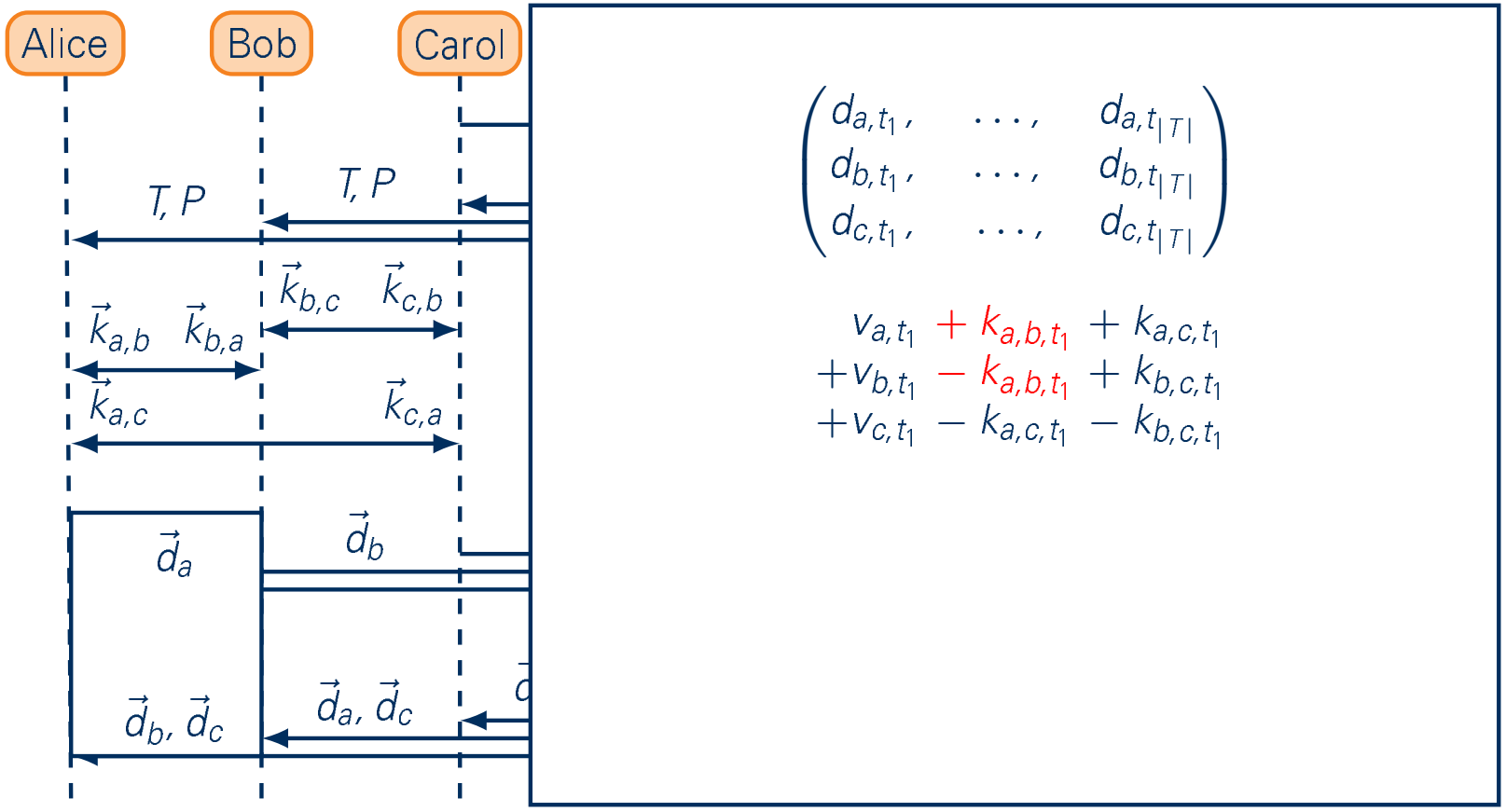
Ergebnisveröffentlichung [Kellermann, Böhme, IEEE CSE/PASSAT 2009]



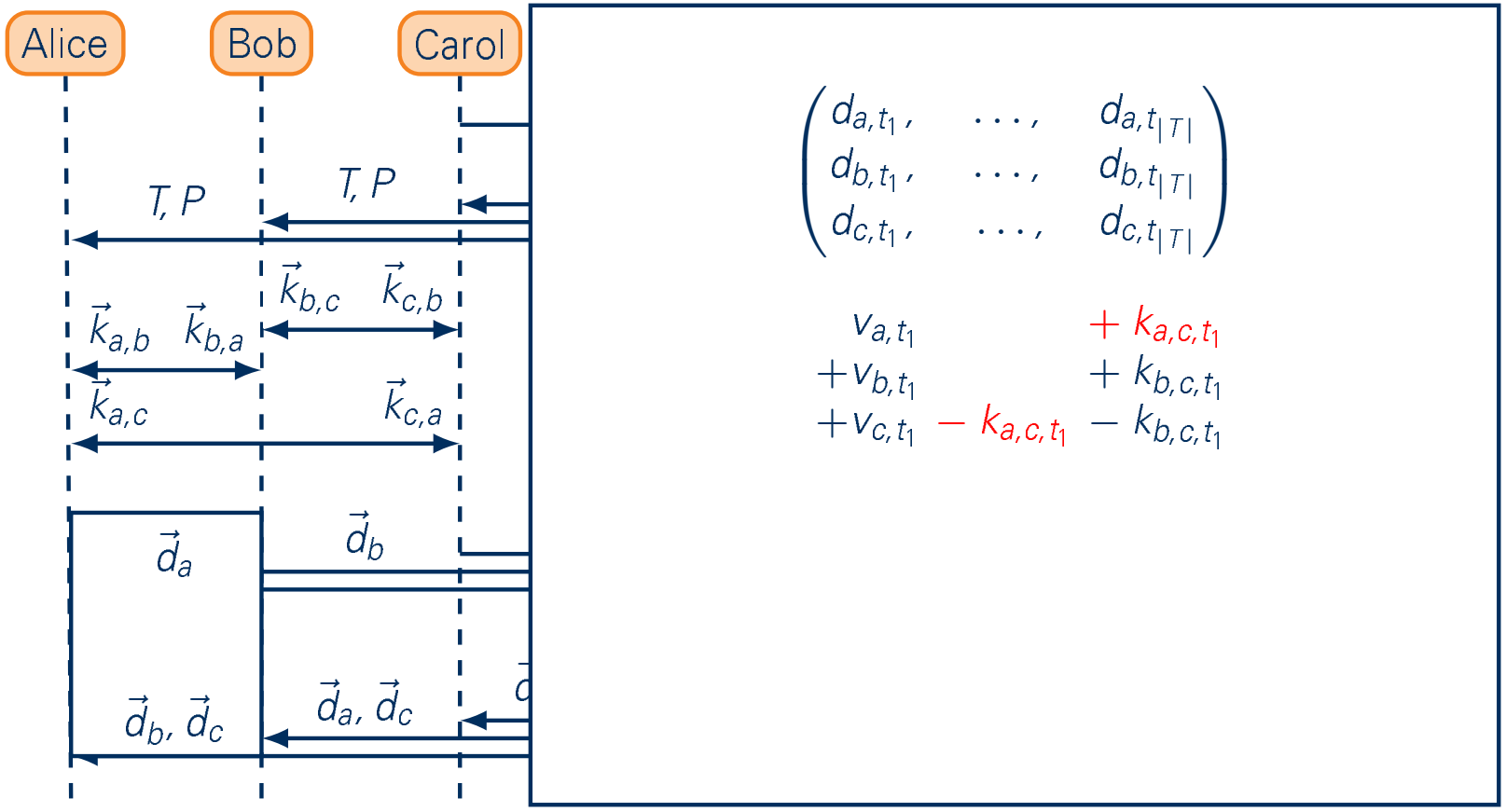
Ergebnisveröffentlichung [Kellermann, Böhme, IEEE CSE/PASSAT 2009]



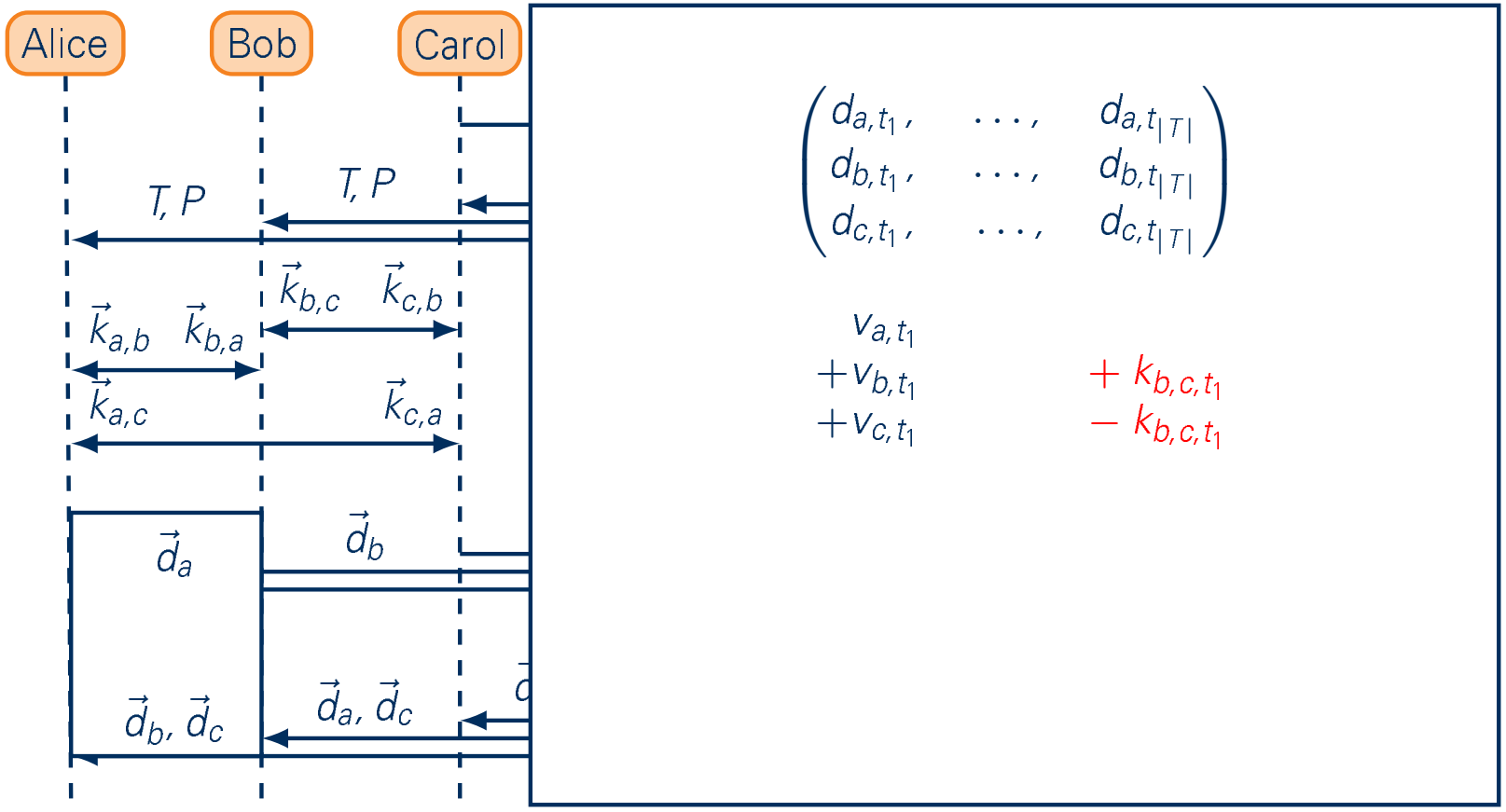
Ergebnisveröffentlichung [Kellermann, Böhme, IEEE CSE/PASSAT 2009]



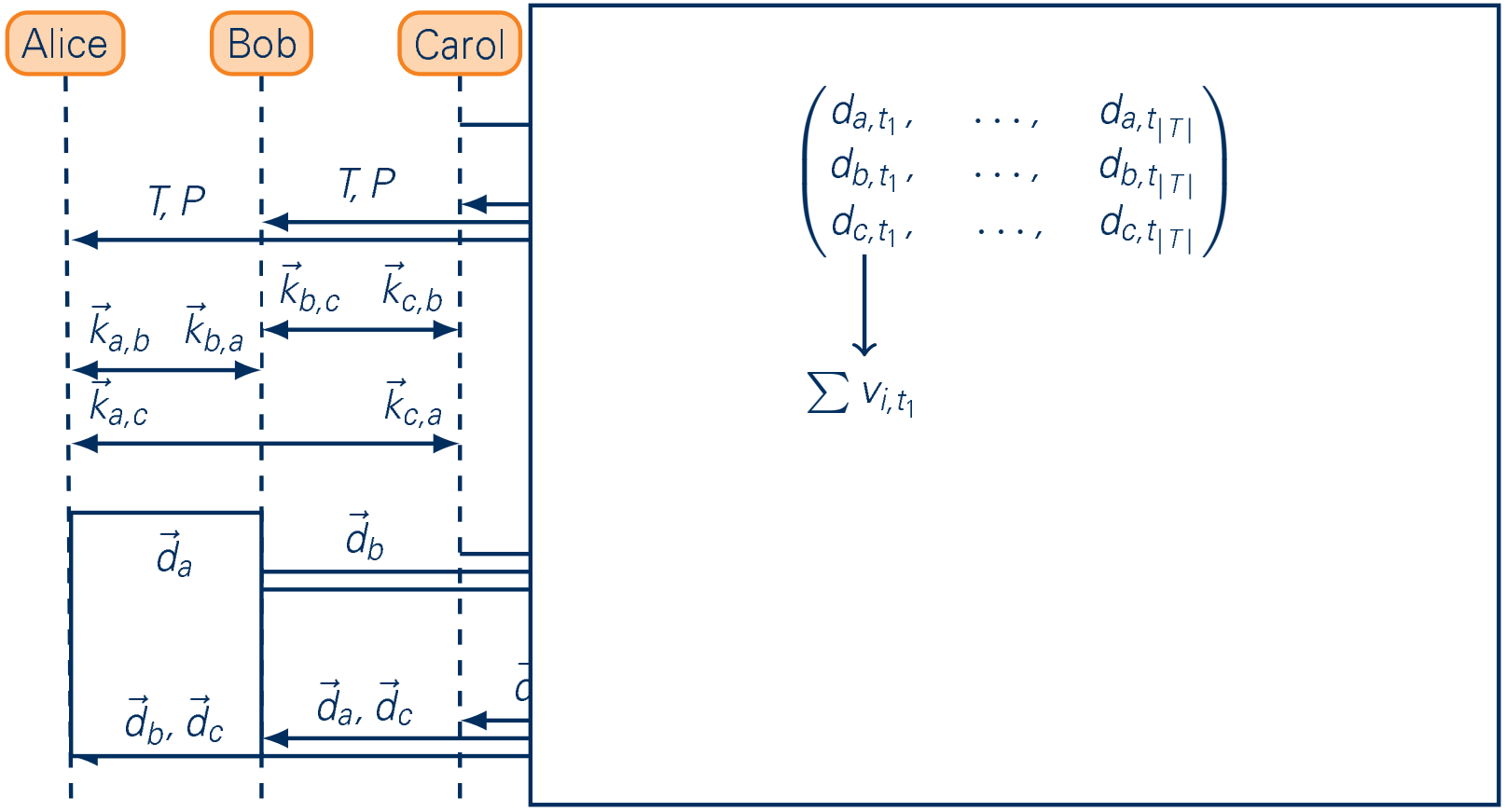
Ergebnisveröffentlichung [Kellermann, Böhme, IEEE CSE/PASSAT 2009]



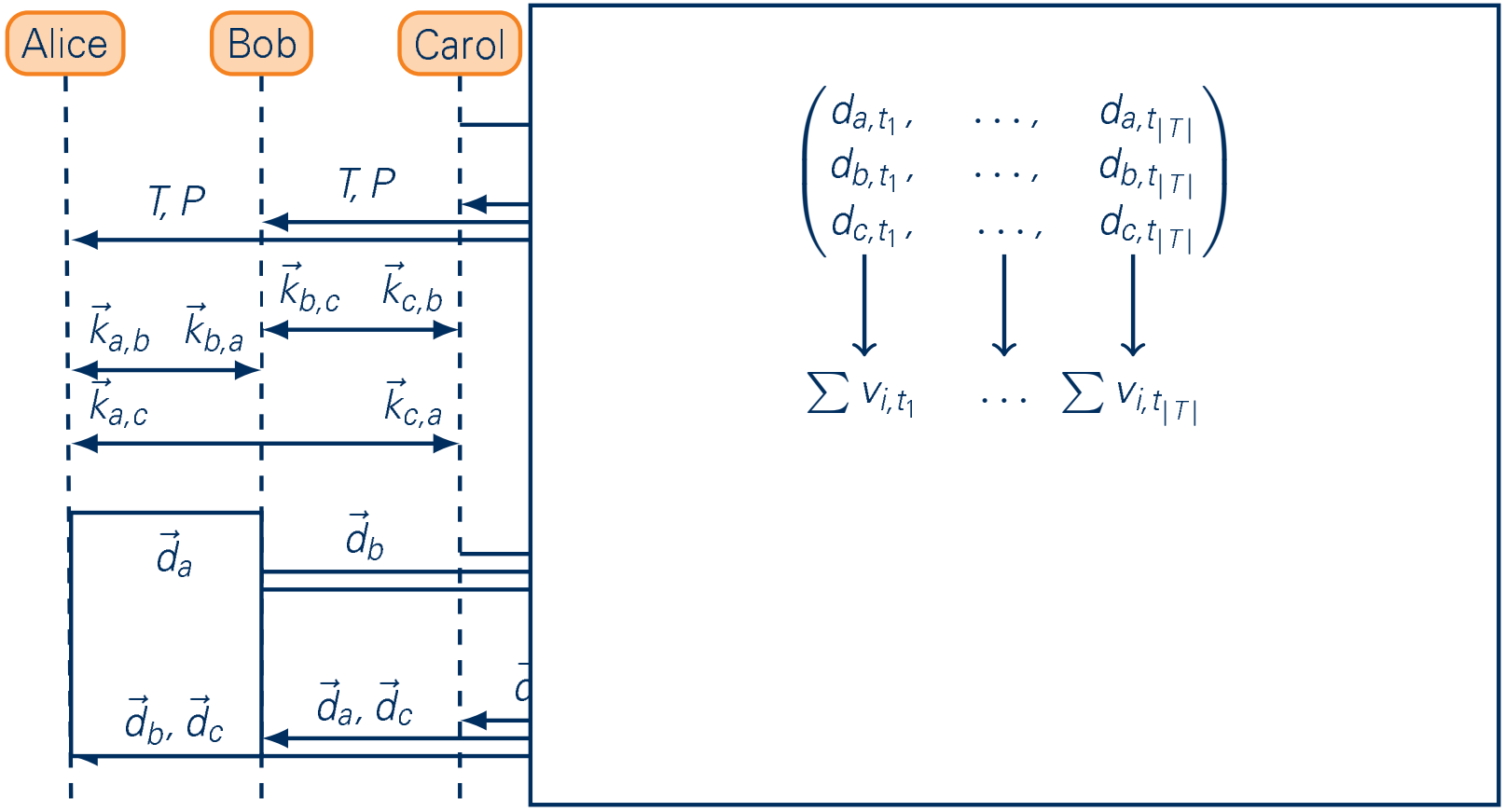
Ergebnisveröffentlichung [Kellermann, Böhme, IEEE CSE/PASSAT 2009]



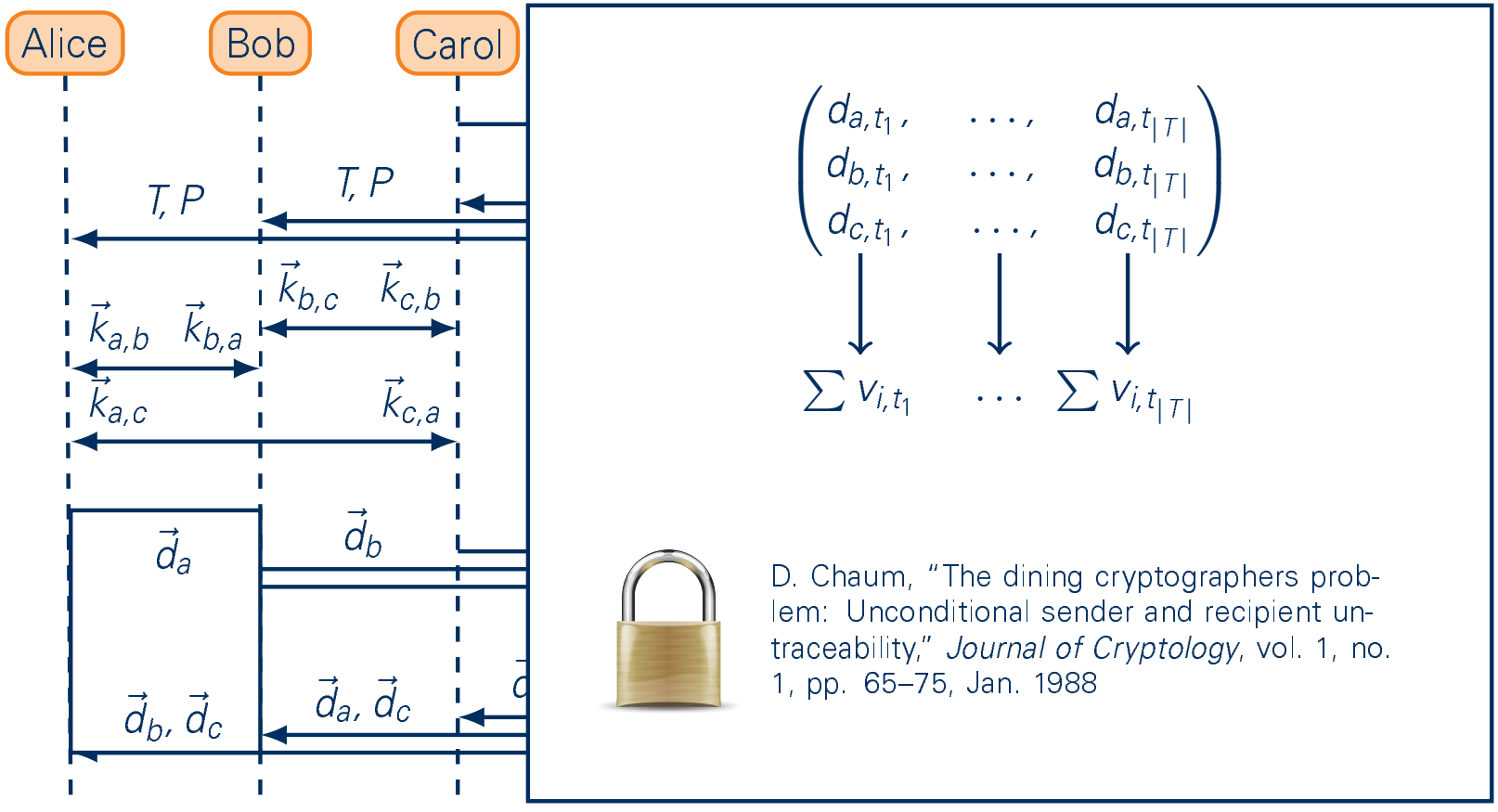
Ergebnisveröffentlichung [Kellermann, Böhme, IEEE CSE/PASSAT 2009]



Ergebnisveröffentlichung [Kellermann, Böhme, IEEE CSE/PASSAT 2009]

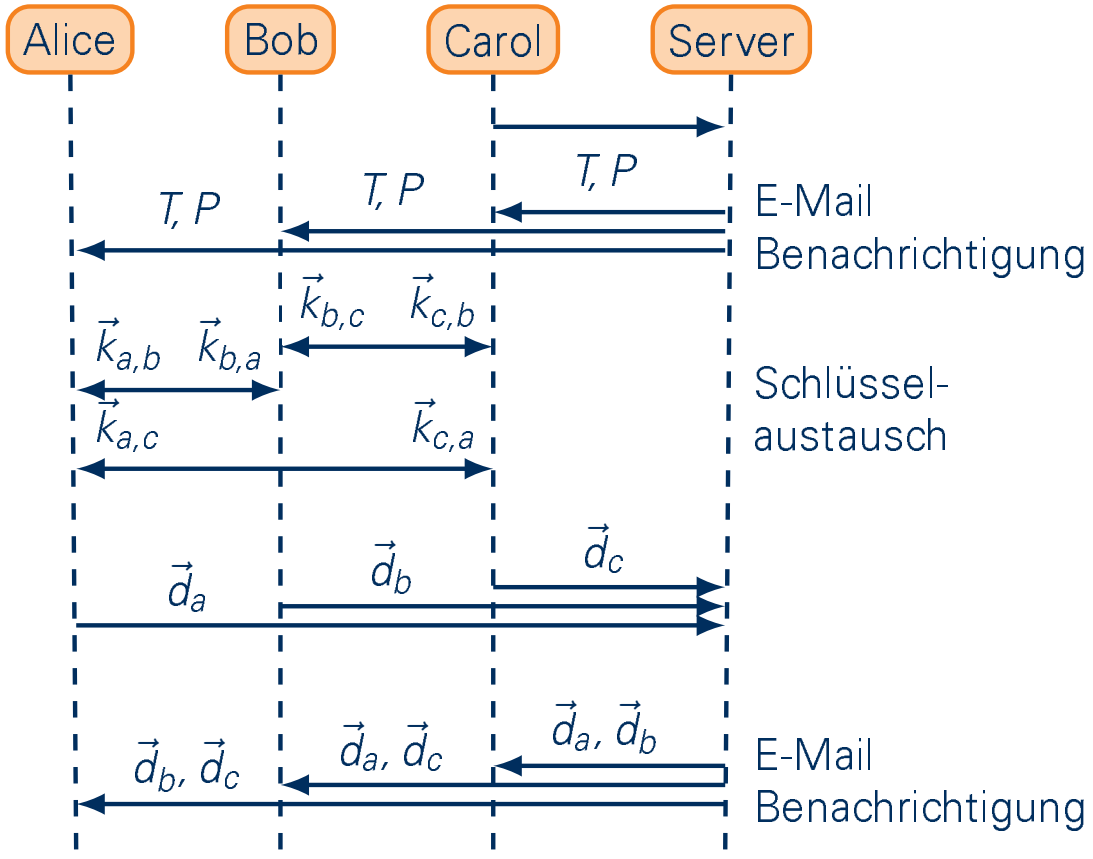


Ergebnisveröffentlichung [Kellermann, Böhme, IEEE CSE/PASSAT 2009]



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

Angreifer erkennen

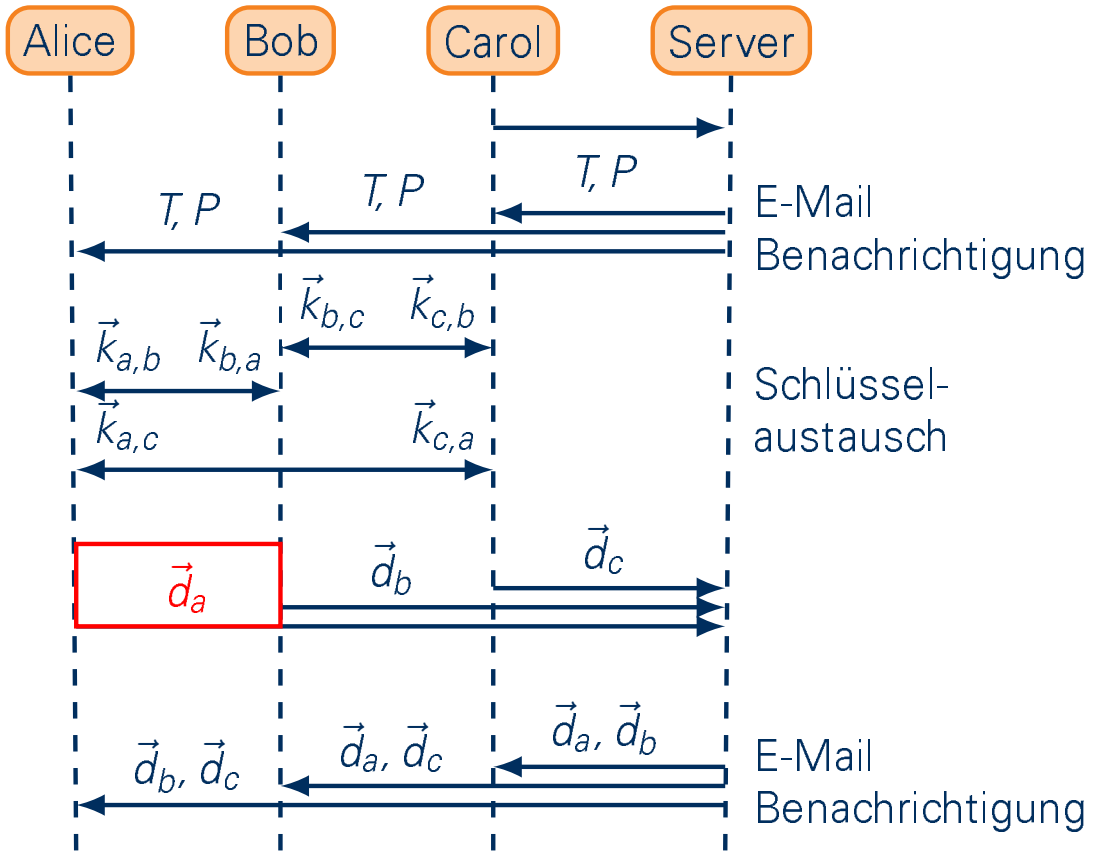


T . . . Zeitpunkte
P . . . Teilnehmer

$\vec{k}_{i,j}$ . . . Schlüsselvektor

$\vec{d}$ . . . verschlüsselte Stimmen

Angreifer erkennen

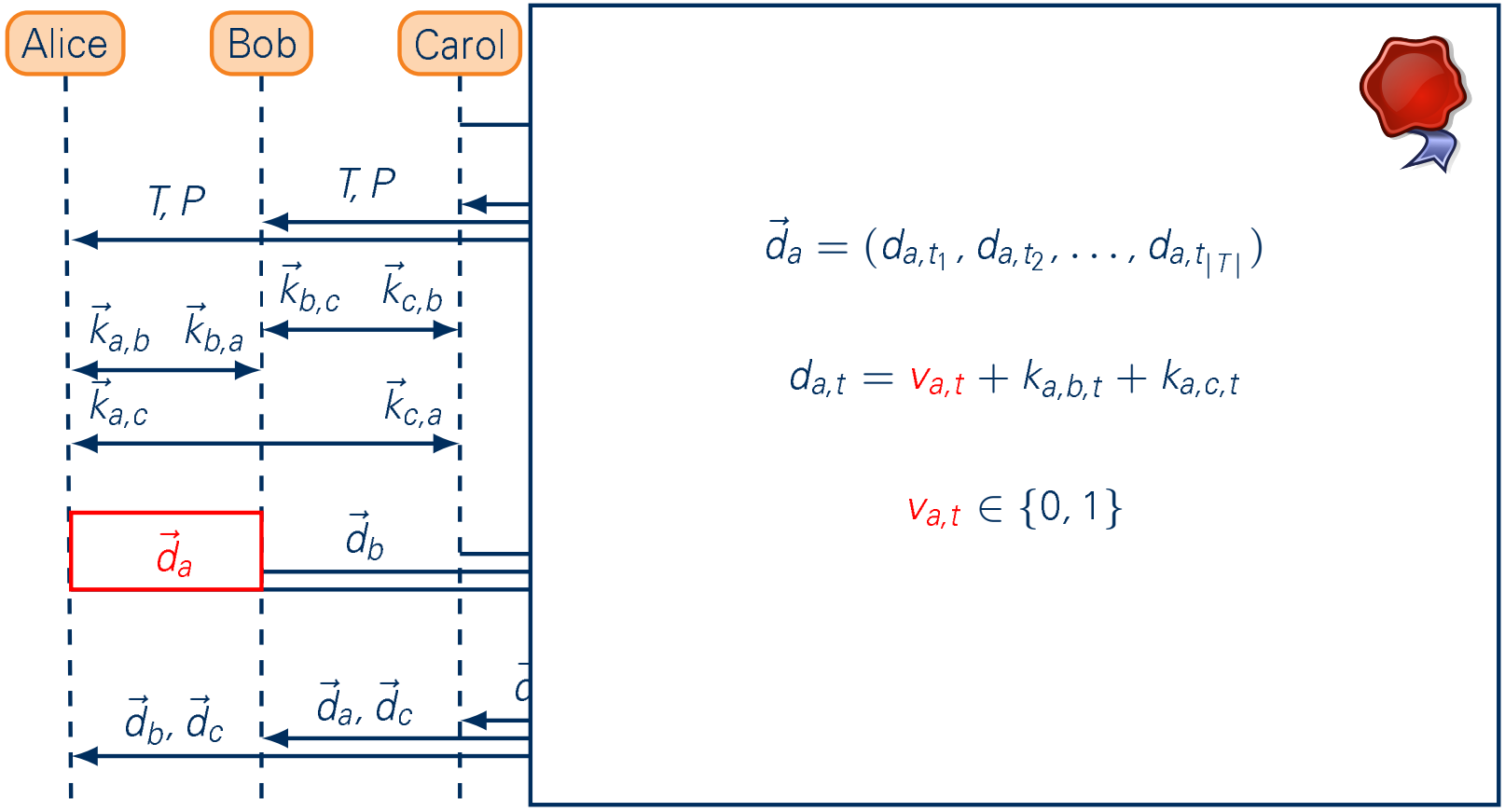


T . . . Zeitpunkte
P . . . Teilnehmer

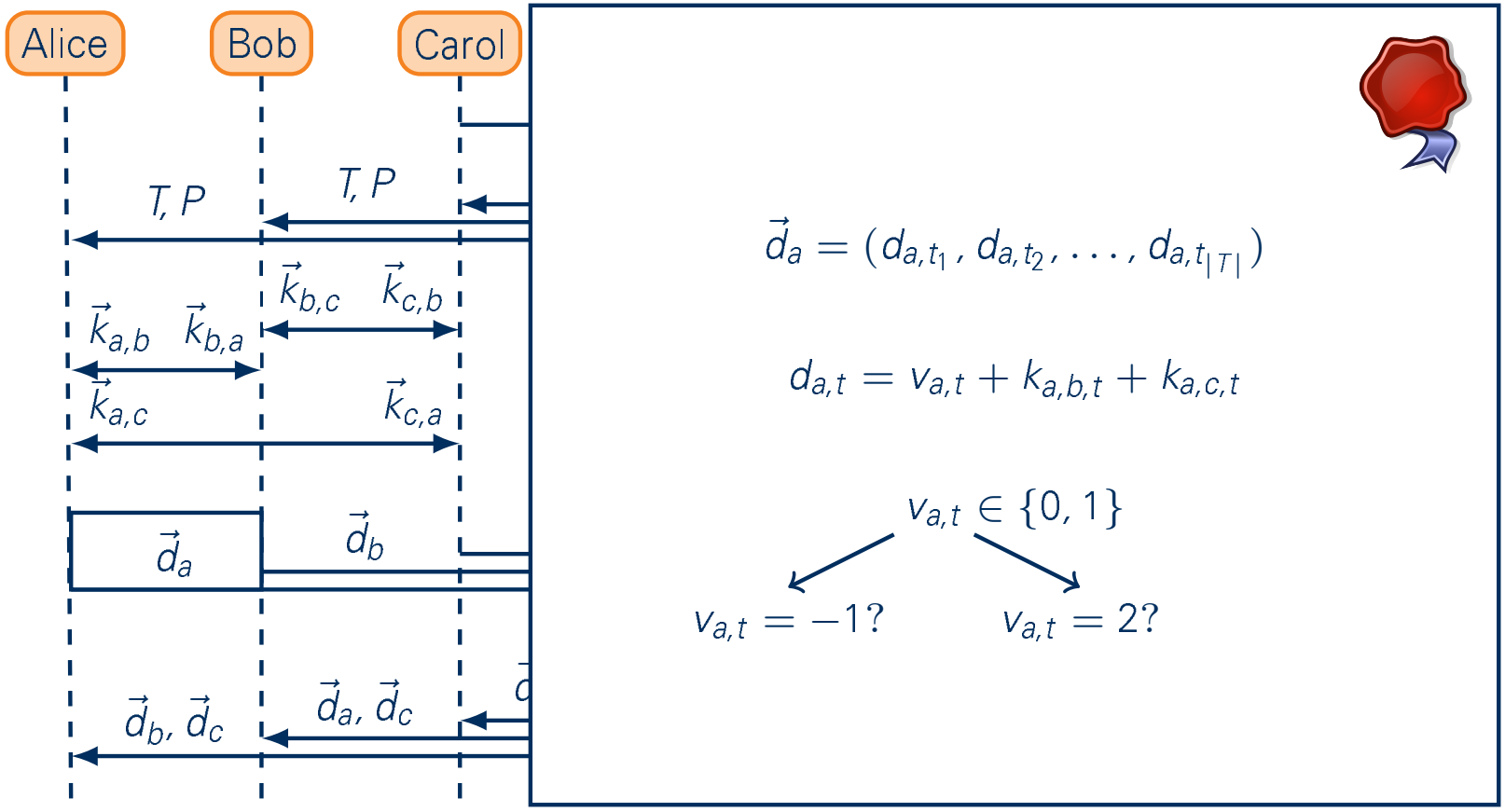
$\vec{k}_{i,j}$ . . . Schlüsselvektor

$\vec{d}$ . . . verschlüsselte Stimmen

Angreifer erkennen



Angreifer erkennen



(−1)-Angriffe erkennen [Kellermann, IFIP/SEC 2011]

	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

(−1)-Angriffe erkennen [Kellermann, IFIP/SEC 2011]

	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

(−1)-Angriffe erkennen [Kellermann, IFIP/SEC 2011]

	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

(−1)-Angriffe erkennen [Kellermann, IFIP/SEC 2011]

	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

(−1)-Angriffe erkennen [Kellermann, IFIP/SEC 2011]

	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

(−1)-Angriffe erkennen [Kellermann, IFIP/SEC 2011]

	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

Alice	0	1	0	0

Alice	1	0	0	0

$\sum$	1	1	0	0

(−1)-Angriffe erkennen [Kellermann, IFIP/SEC 2011]

	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

(−1)-Angriffe erkennen [Kellermann, IFIP/SEC 2011]

	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

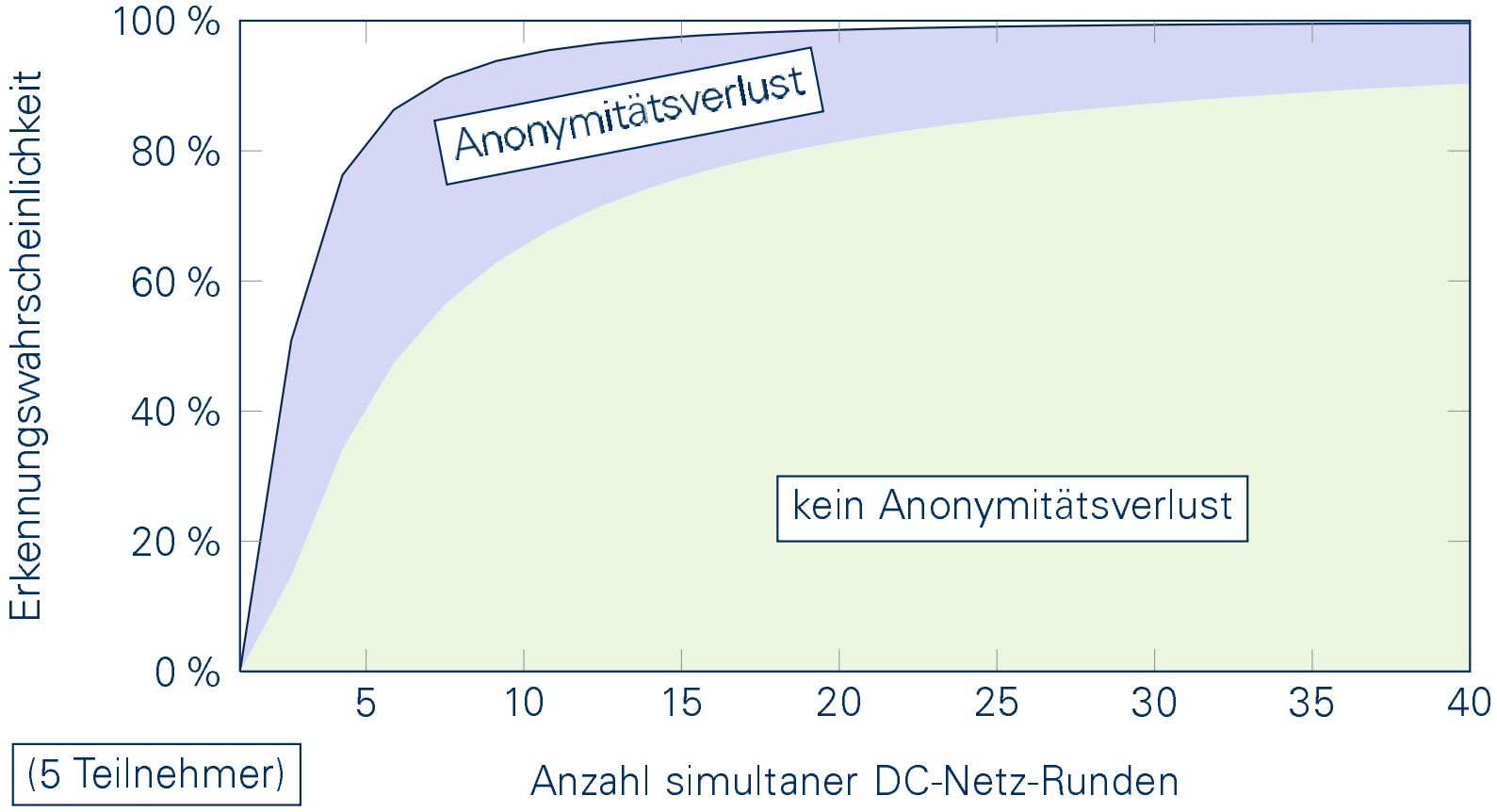
Alice	0	0	0	0
Bob	0	1	0	0
$\sum$		≥ 0?		
Alice	0	1	0	0
Bob	0	0	0	0
$\sum$		≥ 0?		
Alice	1	0	0	0
Bob	0	0	1	0
$\sum$		≥ 0?		
$\sum$	1	2	1	0

(−1)-Angriffe erkennen [Kellermann, IFIP/SEC 2011]

	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

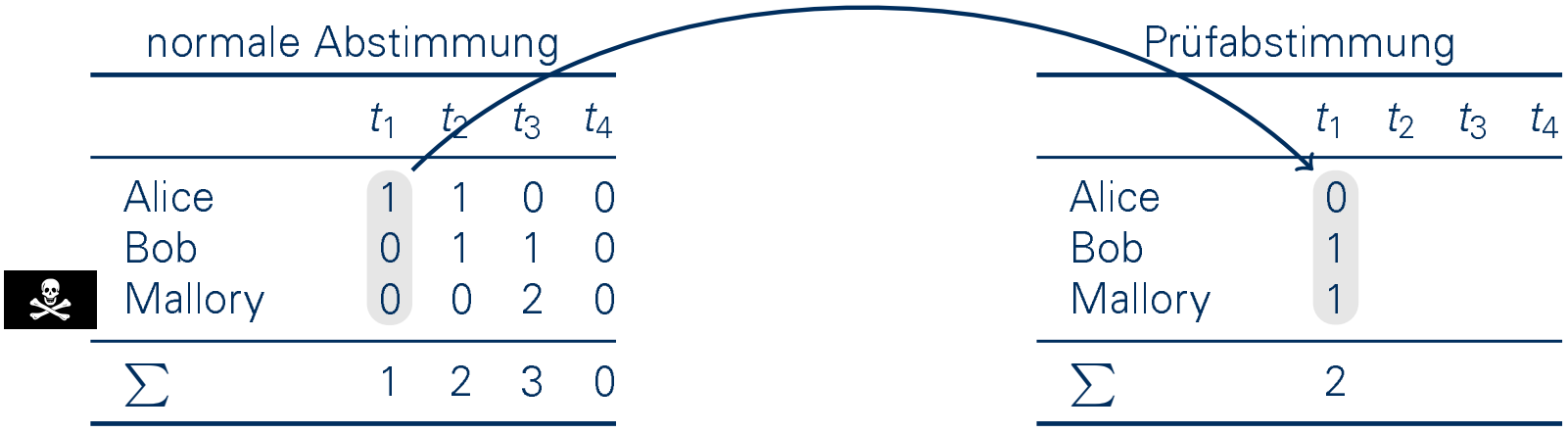
Erkennungswahrscheinlichkeiten



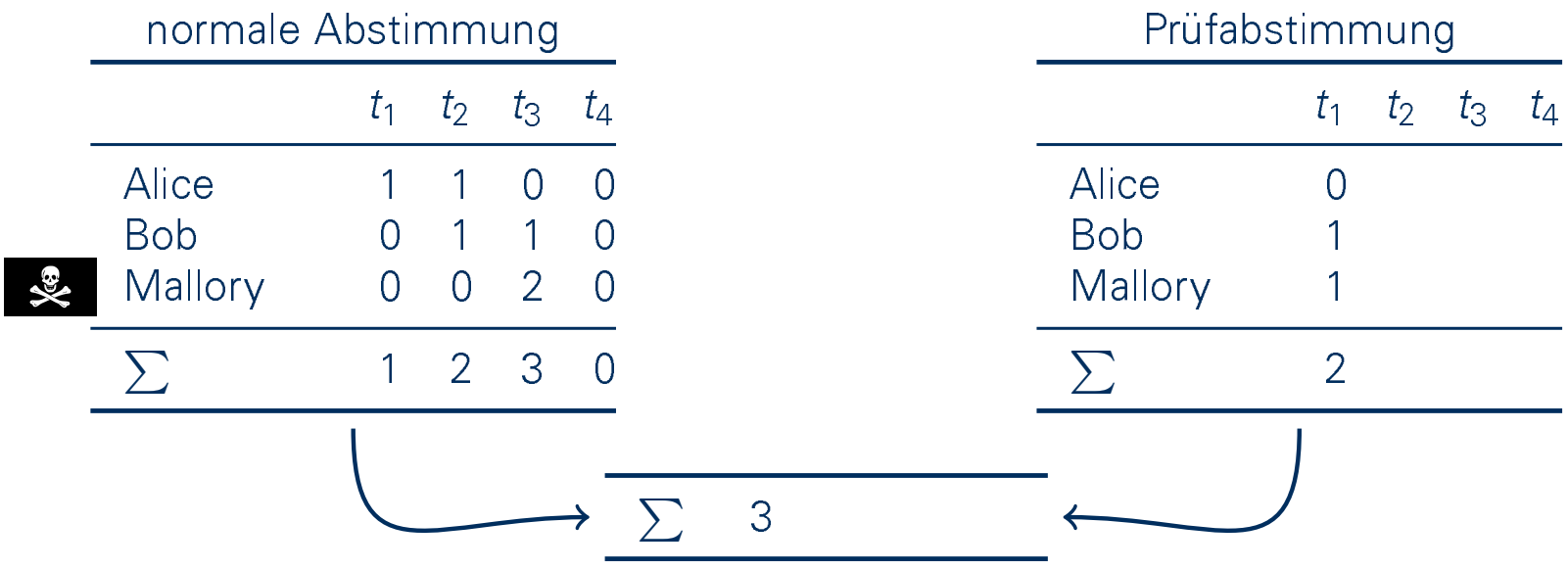
(+2)-Angriffe erkennen [Kellermann, IFIP/SEC 2011]

	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

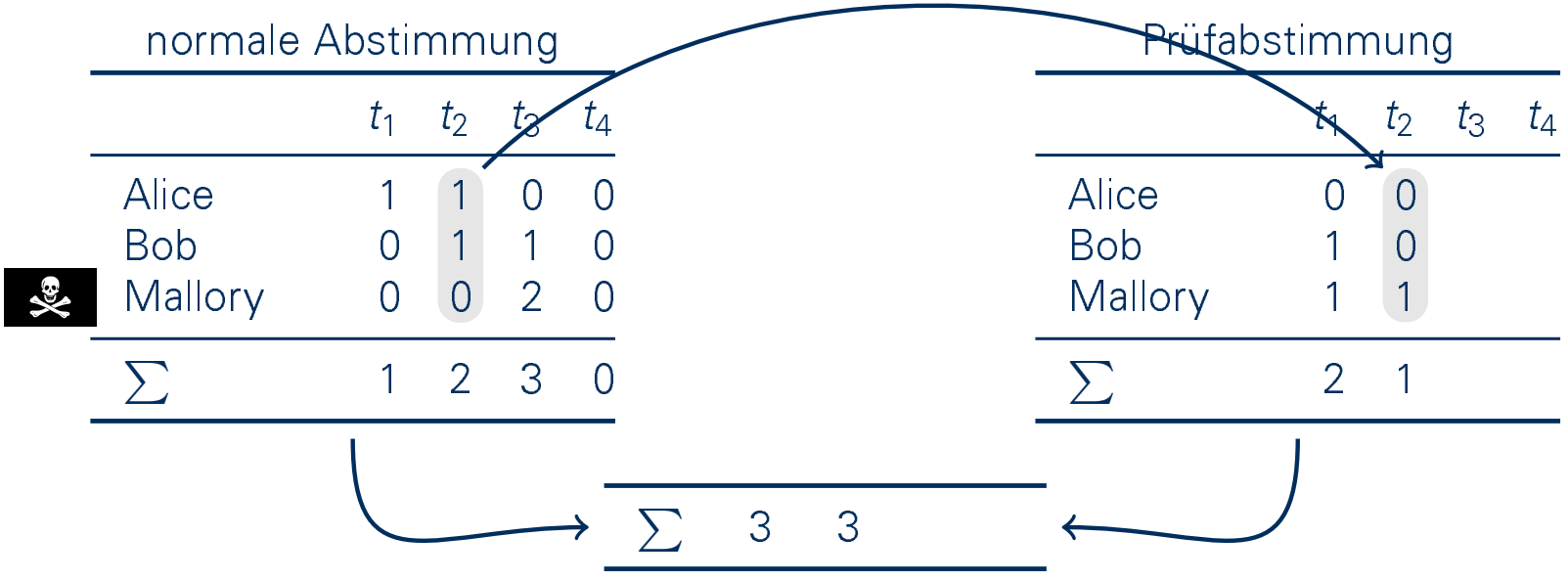
(+2)-Angriffe erkennen [Kellermann, IFIP/SEC 2011]



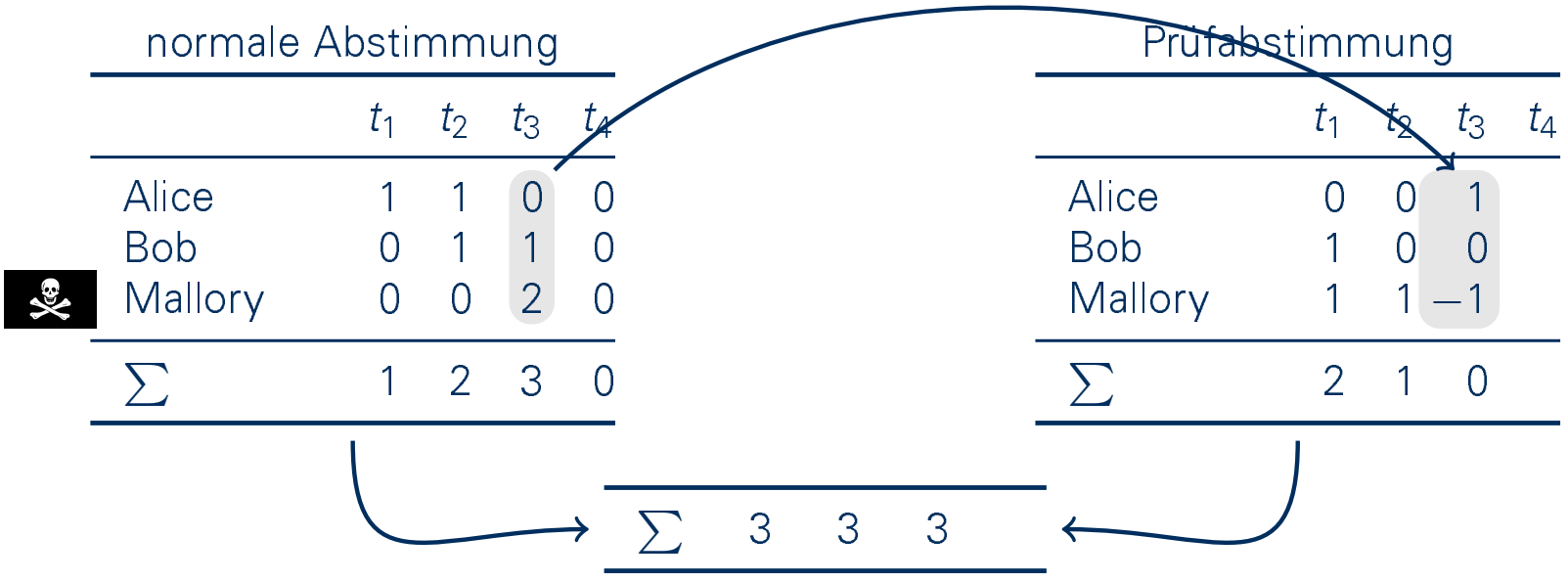
(+2)-Angriffe erkennen [Kellermann, IFIP/SEC 2011]



(+2)-Angriffe erkennen [Kellermann, IFIP/SEC 2011]



(+2)-Angriffe erkennen [Kellermann, IFIP/SEC 2011]



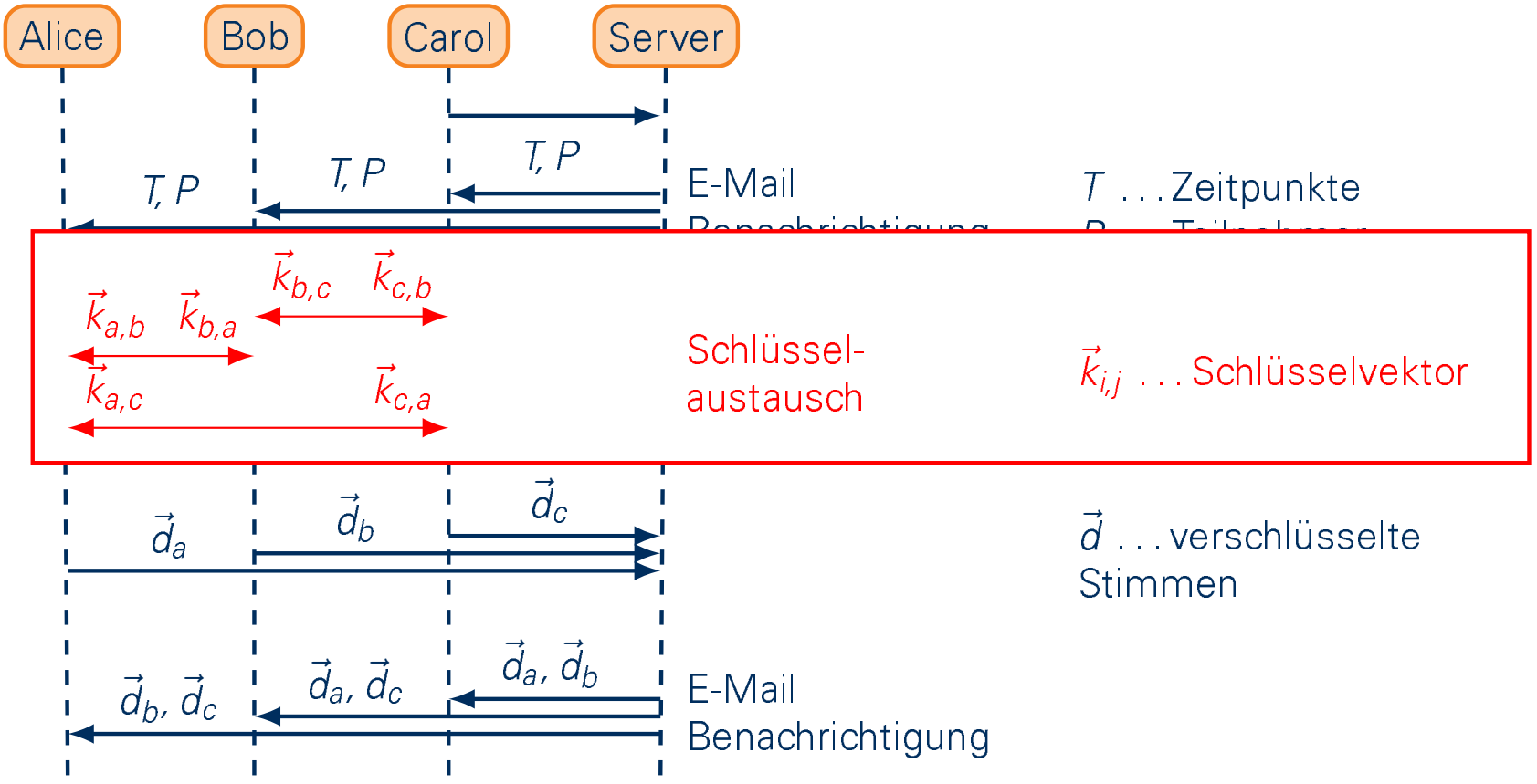
Verfügbarkeitsangriff

- Angriff erkannt?
  - ➥ Identifikationsphase (Schlüssel aufdecken)
    - ➥ Reputationsverlust in kleinen Gruppen

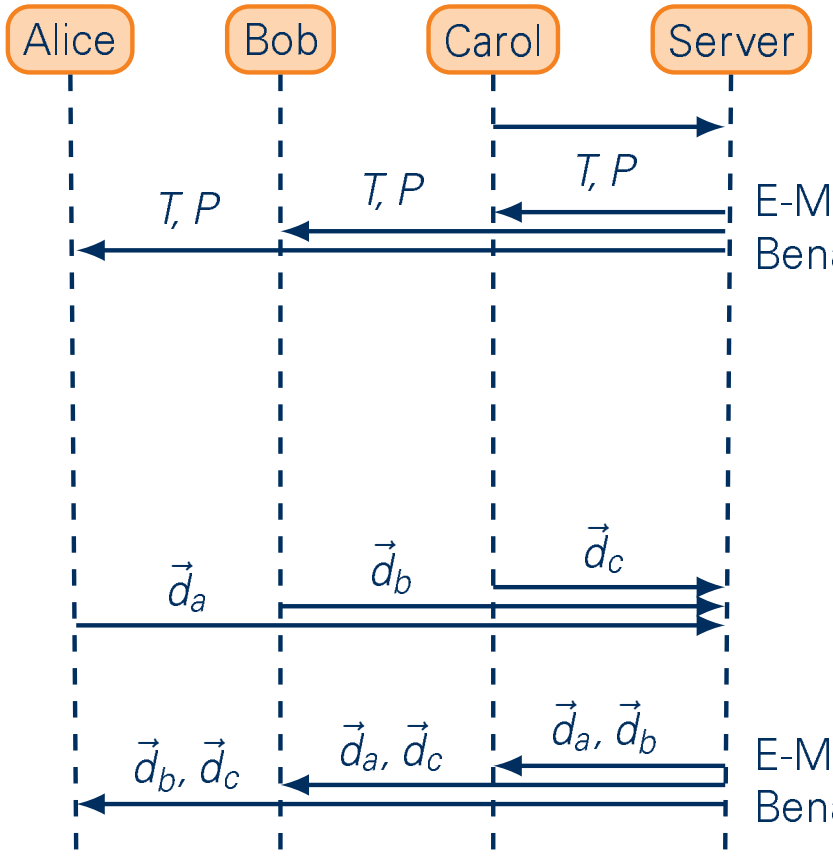
Verfügbarkeitsangriff

- Angriff erkannt?
  - ➥ Identifikationsphase (Schlüssel aufdecken)
    - ➥ Reputationsverlust in kleinen Gruppen
- Richtiger Schlüssel?
  - ➥ Commitmentschema in Abstimmungsphase

Vereinfachung des Schlüsselaustauschs



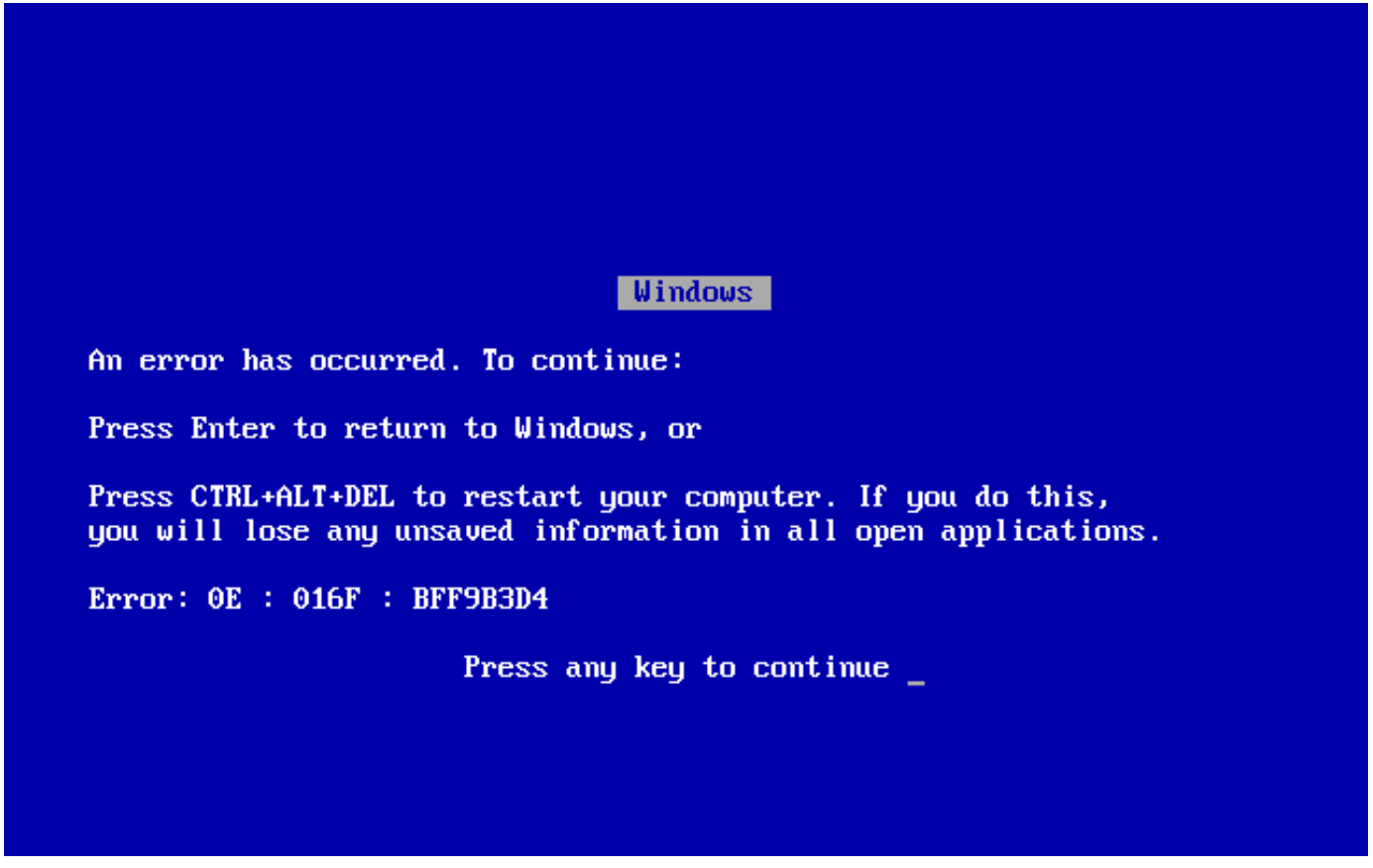
Vereinfachung des Schlüsselaustauschs



T . . . Zeitpunkte
P . . . Teilnehmer

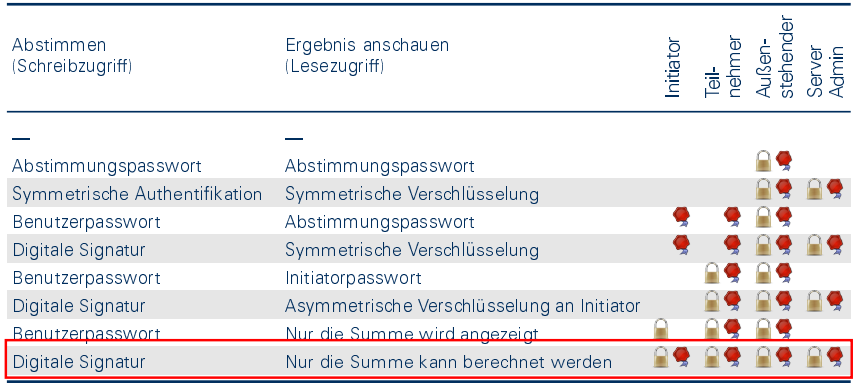
$\vec{d}$ . . . verschlüsselte Stimmen

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 _

Inhalt

- Anforderungen
- → Neues Protokoll
  - ➥ geringe Vertrauensannahmen
  - ➥ 1 asym. Operation pro Teilnehmer
  - ➥ 1 Interaktion pro Teilnehmer
- Implementierung
  - ➥ Schlüsselspeicherung
  - ➥ JavaScript Watchdog
  - ➥ Evaluation / Praktischer Einfluss
- Zusammenfassung / Ausblick

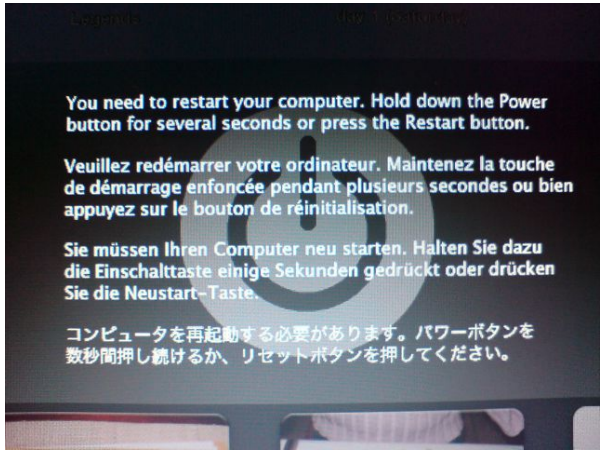


Abstimmen (Schreibzugriff)	Ergebnis anschauen (Lesezugriff)	Initiator	Teil-nehmer	Außen-stehender	Server Admin
–	–				
Abstimmungspasswort	Abstimmungspasswort			●	
Symmetrische Authentifikation	Symmetrische Verschlüsselung			●	●
Benutzerpasswort	Abstimmungspasswort	●	●	●	
Digitale Signatur	Symmetrische Verschlüsselung	●	●	●	●
Benutzerpasswort	Initiatorpasswort		●	●	
Digitale Signatur	Asymmetrische Verschlüsselung an Initiator		●	●	●
Benutzerpasswort	Nur die Summe wird angezeigt	○	●	●	
Digitale Signatur	Nur die Summe kann berechnet werden	●	●	●	●

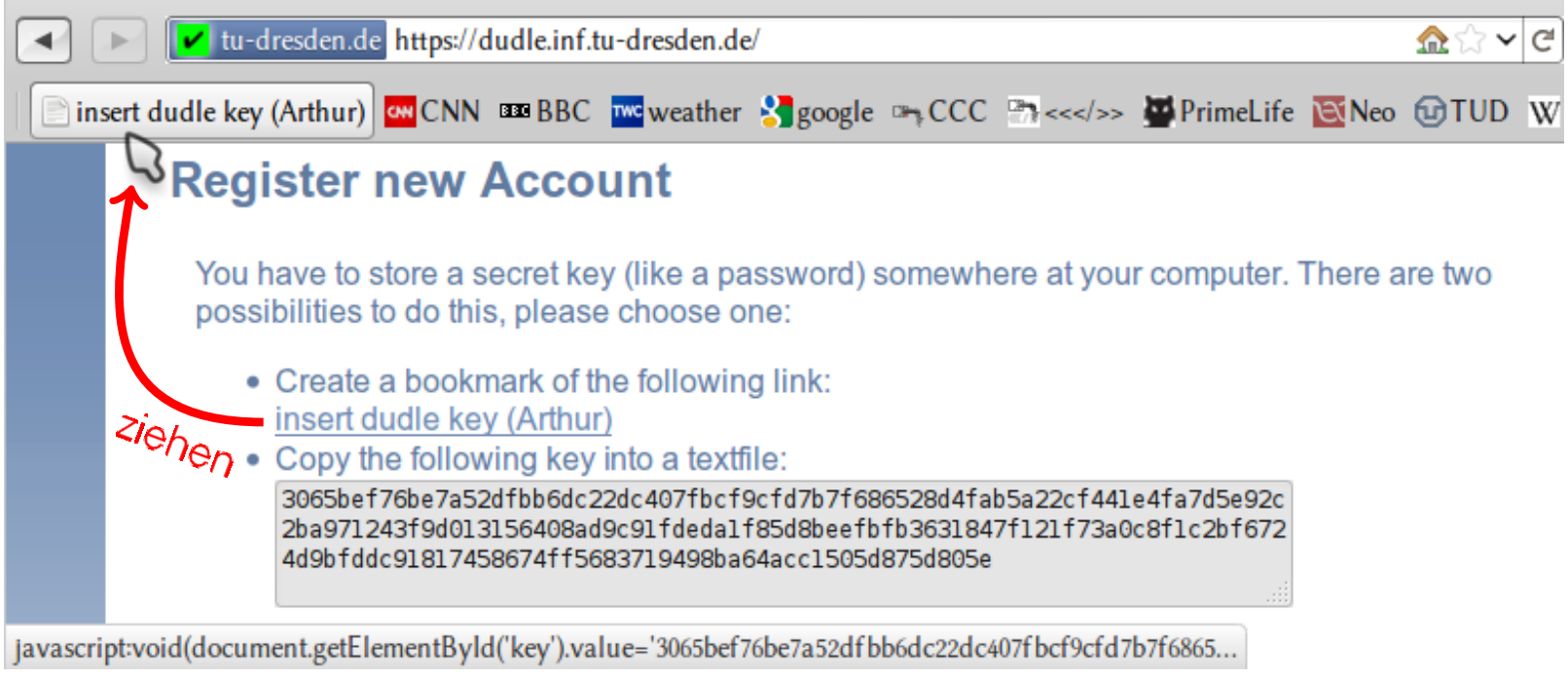
Inhalt

- Anforderungen
- Neues Protokoll
  - ➥ geringe Vertrauensannahmen
  - ➥ 1 asym. Operation pro Teilnehmer
  - ➥ 1 Interaktion pro Teilnehmer
- ➙ Implementierung
  - ➥ Schlüsselspeicherung
  - ➥ JavaScript Watchdog
  - ➥ Evaluation / Praktischer Einfluss
- Zusammenfassung / Ausblick

Abstimmen (Schreibzugriff)	Ergebnis anschauen (Lesezugriff)	Initiator	Teil-nehmer	Außen-stehender	Server Admin
–	–				
Abstimmungspasswort	Abstimmungspasswort			🔒🌹	
Symmetrische Authentifikation	Symmetrische Verschlüsselung			🔒🌹	🔒🌹
Benutzerpasswort	Abstimmungspasswort	🌹	🌹	🔒🌹	
Digitale Signatur	Symmetrische Verschlüsselung	🌹	🌹	🔒🌹	🔒🌹
Benutzerpasswort	Initiatorpasswort		🔒🌹	🔒🌹	
Digitale Signatur	Asymmetrische Verschlüsselung an Initiator		🔒🌹	🔒🌹	🔒🌹
Benutzerpasswort	Nur die Summe wird angezeigt	🔒	🔒🌹	🔒🌹	
Digitale Signatur	Nur die Summe kann berechnet werden	🔒🌹	🔒🌹	🔒🌹	🔒🌹

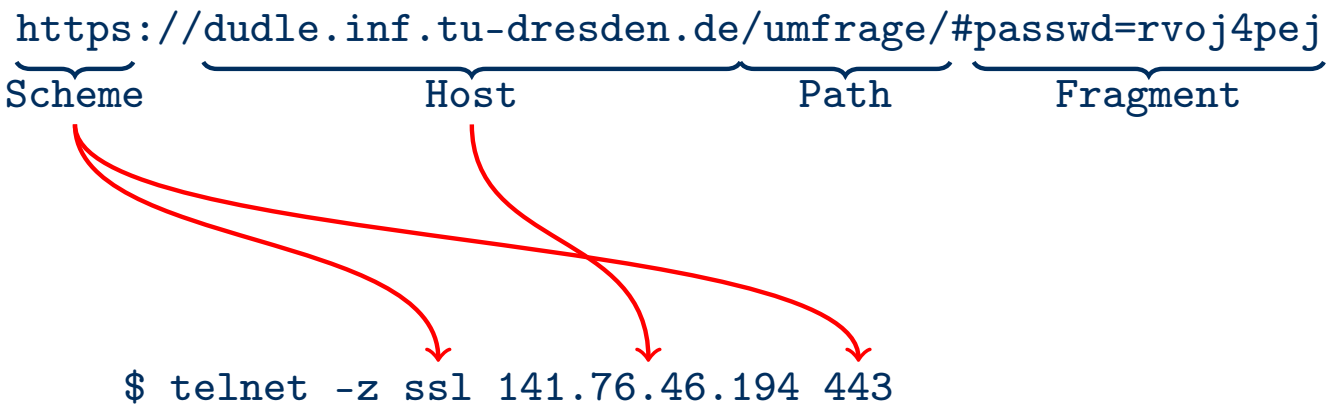


Speichern privater Schlüssel

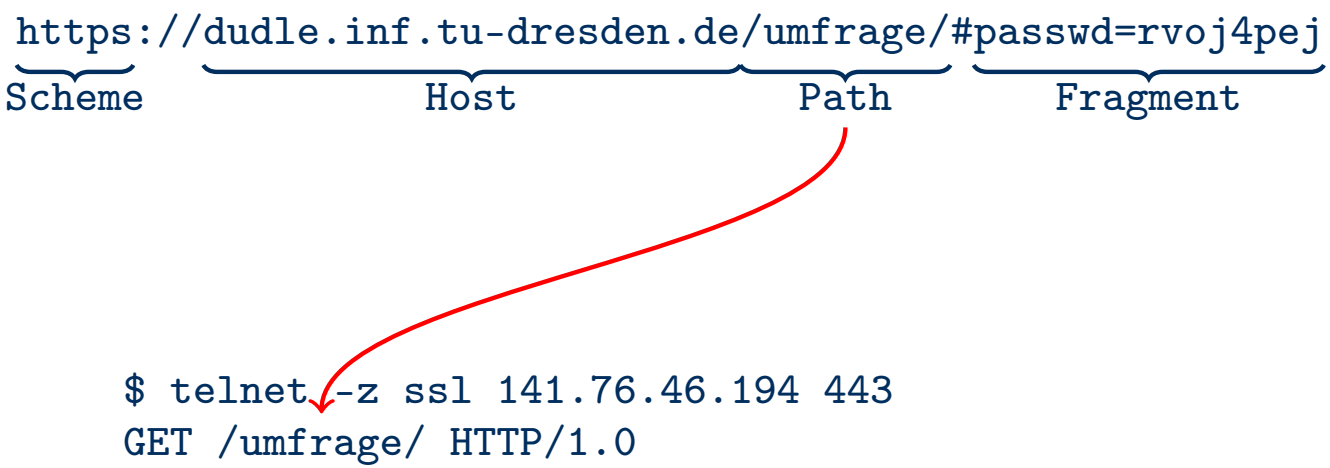


Symmetrische Schlüssel

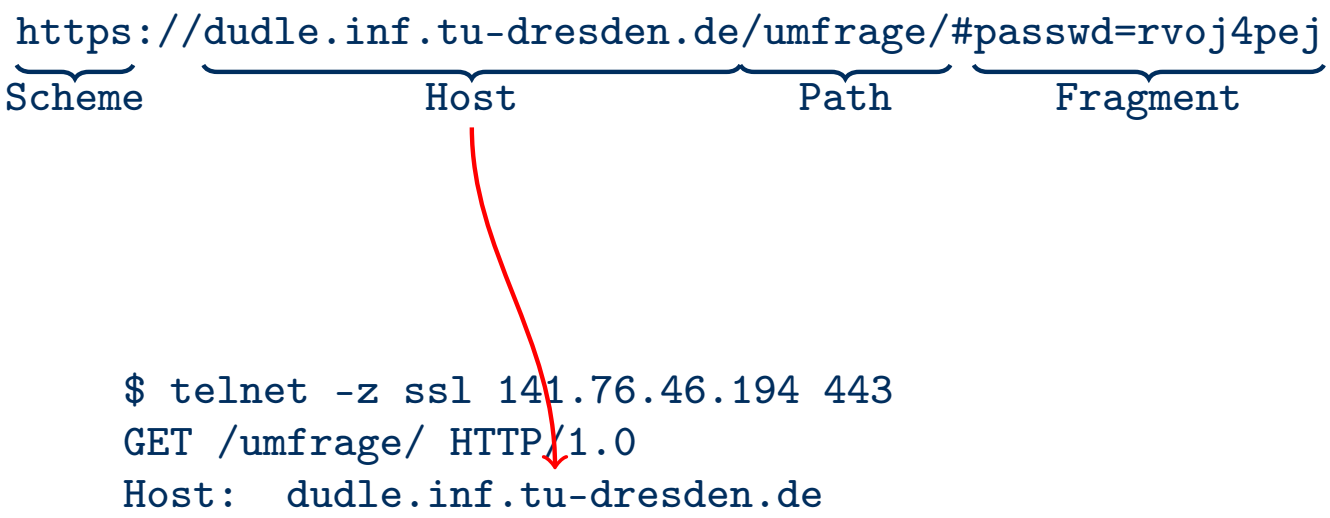
Symmetrische Schlüssel



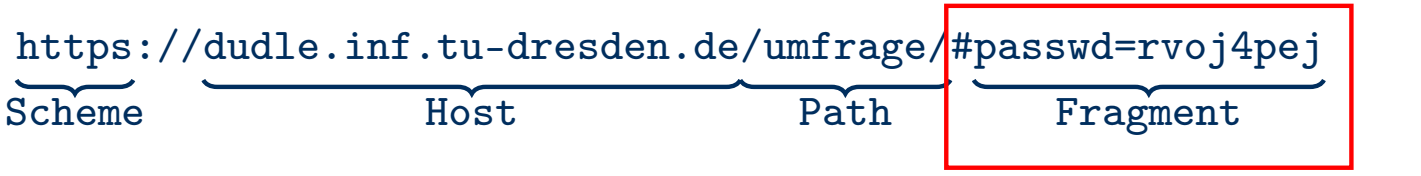
Symmetrische Schlüssel



Symmetrische Schlüssel



Symmetrische Schlüssel




```
$ telnet -z ssl 141.76.46.194 443
GET /umfrage/ HTTP/1.0
Host:  dudle.inf.tu-dresden.de
```

JavaScript Watchdog

```
function extensiveCalculation(x, y) {


  while(reallyReallyOften) {
    shortCalculation();

  }
  return foo;



}
var bar = extensiveCalculation(a, b);
sendToServer(bar);
```

JavaScript Watchdog

```
function extensiveCalculation(x, y) {


  while(reallyReallyOften) {
    shortCalculation();

  }
  return foo;



}
var bar = extensiveCalculation(a, b);
sendToServer(bar);
```

```
function extensiveCalculation(x, y, callbackfunc) {

   function oneRound() {
    if (reallyReallyOften) {
      shortCalculation();
      window.setTimeout(oneRound, 1);
    } else {
    callbackfunc(foo);
    }
  }
  oneRound();
}
extensiveCalculation(a, b, function(bar) {
  sendToServer(bar);
});
```

- lange synchrone Funktion ➠ asynchrone tail-rekursive Funktion

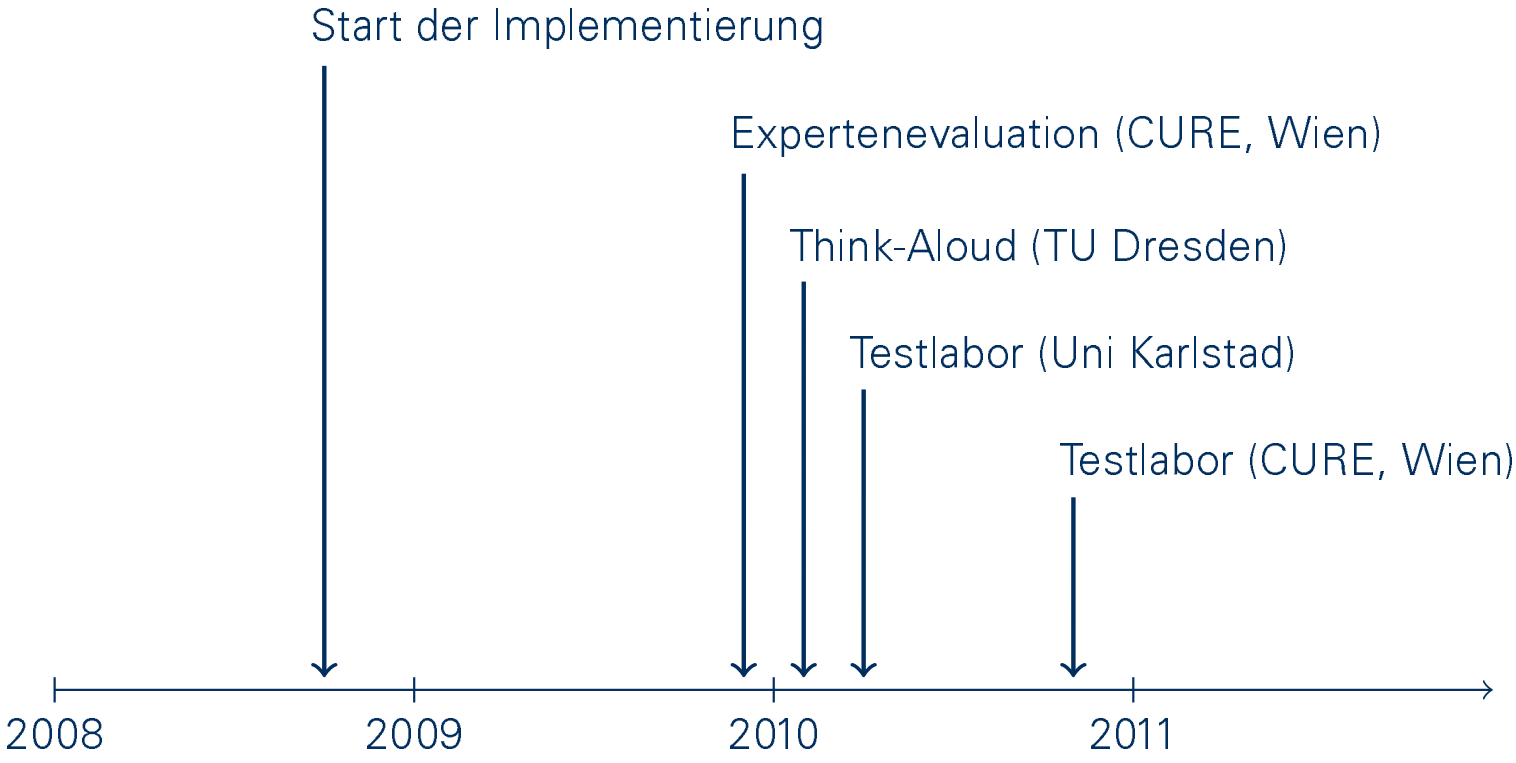
JavaScript Watchdog

```
function extensiveCalculation(x, y) {
  /* lokale Variablen */

  while(reallyReallyOften) {
    shortCalculation();

  }
  return foo;



}
var bar = extensiveCalculation(a, b);
sendToServer(bar);
```

```
function extensiveCalculation(x, y, callbackfunc) {
  /* lokale Variablen */
   function oneRound() {
    if (reallyReallyOften) {
      shortCalculation();
      window.setTimeout(oneRound, 1);
    } else {
    callbackfunc(foo);
    }
  }
  oneRound();
}
extensiveCalculation(a, b, function(bar) {
  sendToServer(bar);
});
```

- lange synchrone Funktion ➠ asynchrone tail-rekursive Funktion
- universell einsetzbar durch inline-Definition

Evaluation

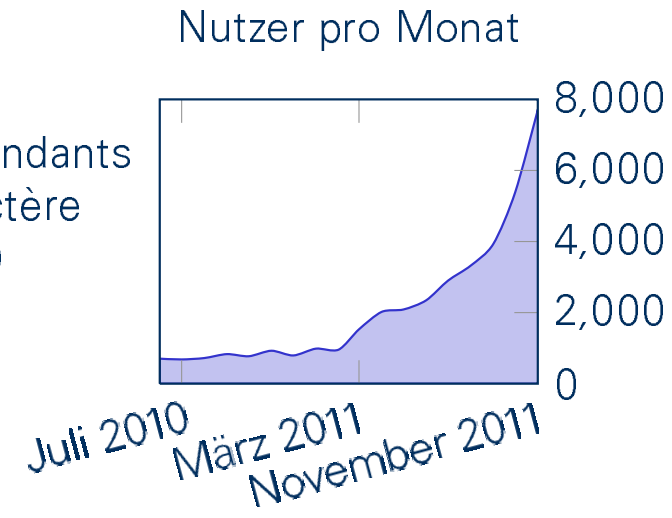

Start der Implementierung
Expertenevaluation (CURE, Wien)
Think-Aloud (TU Dresden)
Testlabor (Uni Karlstad)
Testlabor (CURE, Wien)
2008
2009
2010
2011

Praktischer Einfluss

- Server
  - **https://dudle.mafiasi.de** (Informatik Fachschaft Hamburg)
  - **https://dudle.piratenbrandenburg.de** (Piratenpartei Brandenburg)
  - **http://piratenumfragen.de** (Piratenpartei Thüringen)
  - **http://dudle.mister-muffin.de**
  - **http://poll.faui2k9.de**
  - **https://0j3.de/t**
- Anfragen
  - Association Française des Correspondants à la protection des Données à caractère Personnel (**http://www.afcdp.net**)
  - Landesportal Nordrhein-Westfalen (**http://nrw.de**)
  - edacentrum GmbH

Praktischer Einfluss

- Server
  - **https://dudle.mafiasi.de** (Informatik Fachschaft Hamburg)
  - **https://dudle.piratenbrandenburg.de** (Piratenpartei Brandenburg)
  - **http://piratenumfragen.de** (Piratenpartei Thüringen)
  - **http://dudle.mister-muffin.de**
  - **http://poll.faui2k9.de**
  - **https://0j3.de/t**
- Anfragen
  - Association Française des Correspondants à la protection des Données à caractère Personnel (**http://www.afcdp.net**)
  - Landesportal Nordrhein-Westfalen (**http://nrw.de**)
  - edacentrum GmbH



Zusammenfassung

- ☑ Applikation zur mehrseitig sicheren Terminabstimmung
  - ➠ Vertrauensmodell nach Bedarf wählbar
  - ➠ Gute Akzeptanz in Praxis

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

Zusammenfassung / Ausblick

- ☑ Applikation zur mehrseitig sicheren Terminabstimmung
  - ➠ Vertrauensmodell nach Bedarf wählbar
  - ➠ Gute Akzeptanz in Praxis

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

- ☐ Vertrauenswürdiges JavaScript
- ☐ Mehr Usability
  - ➠ Problem: „Was ist ein Schlüssel?“
- ☐ meet.me@Doodle, appointment-slot@google, tungle.me

TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik Institut für Systemarchitektur, Lehrstuhl für Datenschutz und Datensicherheit

Diskussion

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

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

Dresden, 16. Dezember 2011

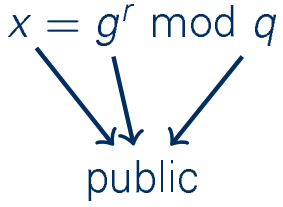
Diffie–Hellman Key Agreement

Discrete Logarithm assumption

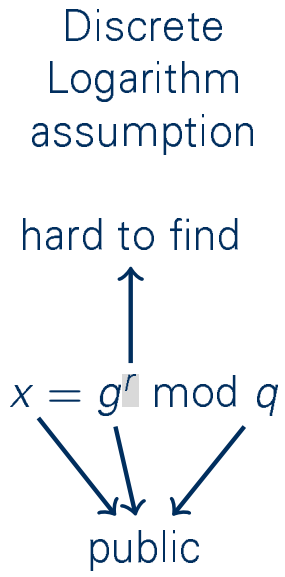
$x = g^r \bmod q$

Diffie–Hellman Key Agreement

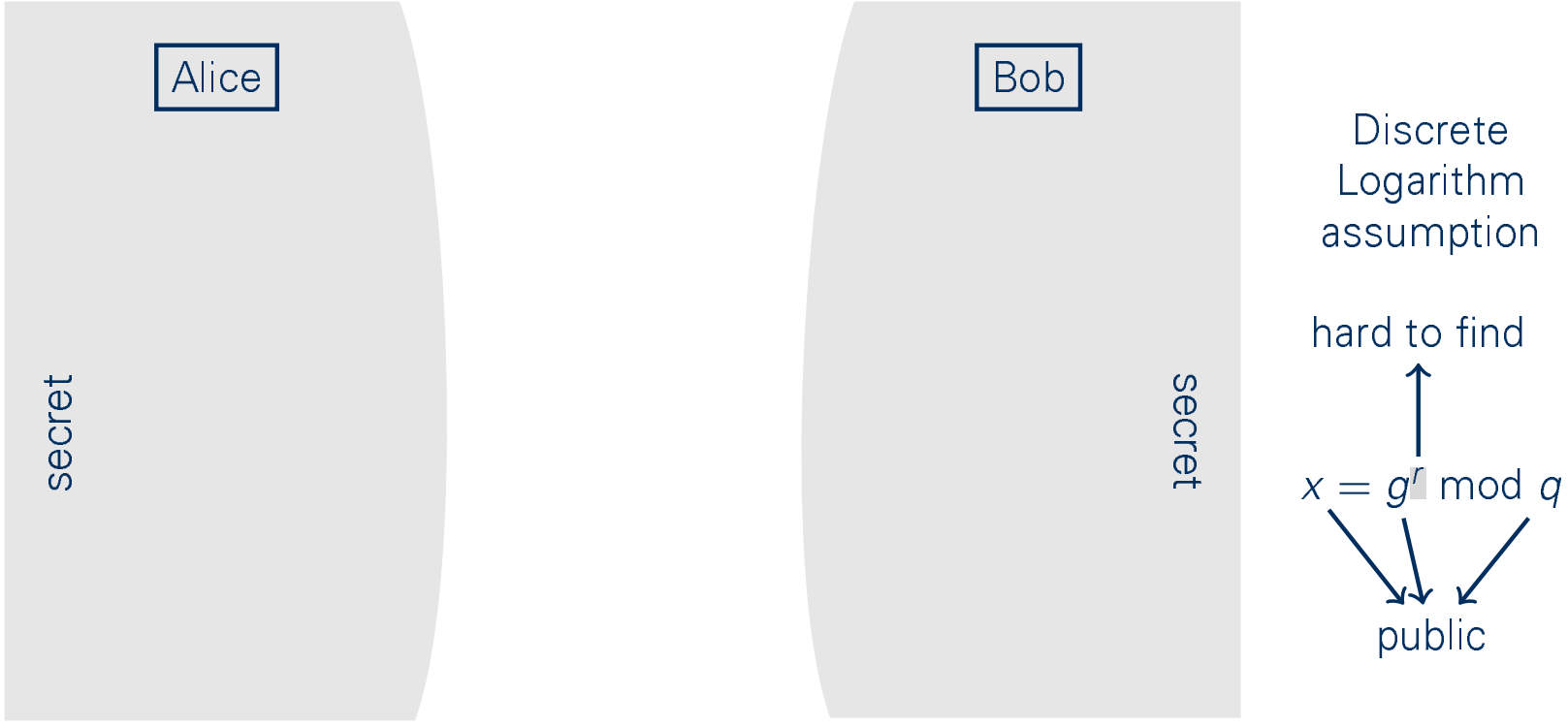
Discrete Logarithm assumption



Diffie–Hellman Key Agreement

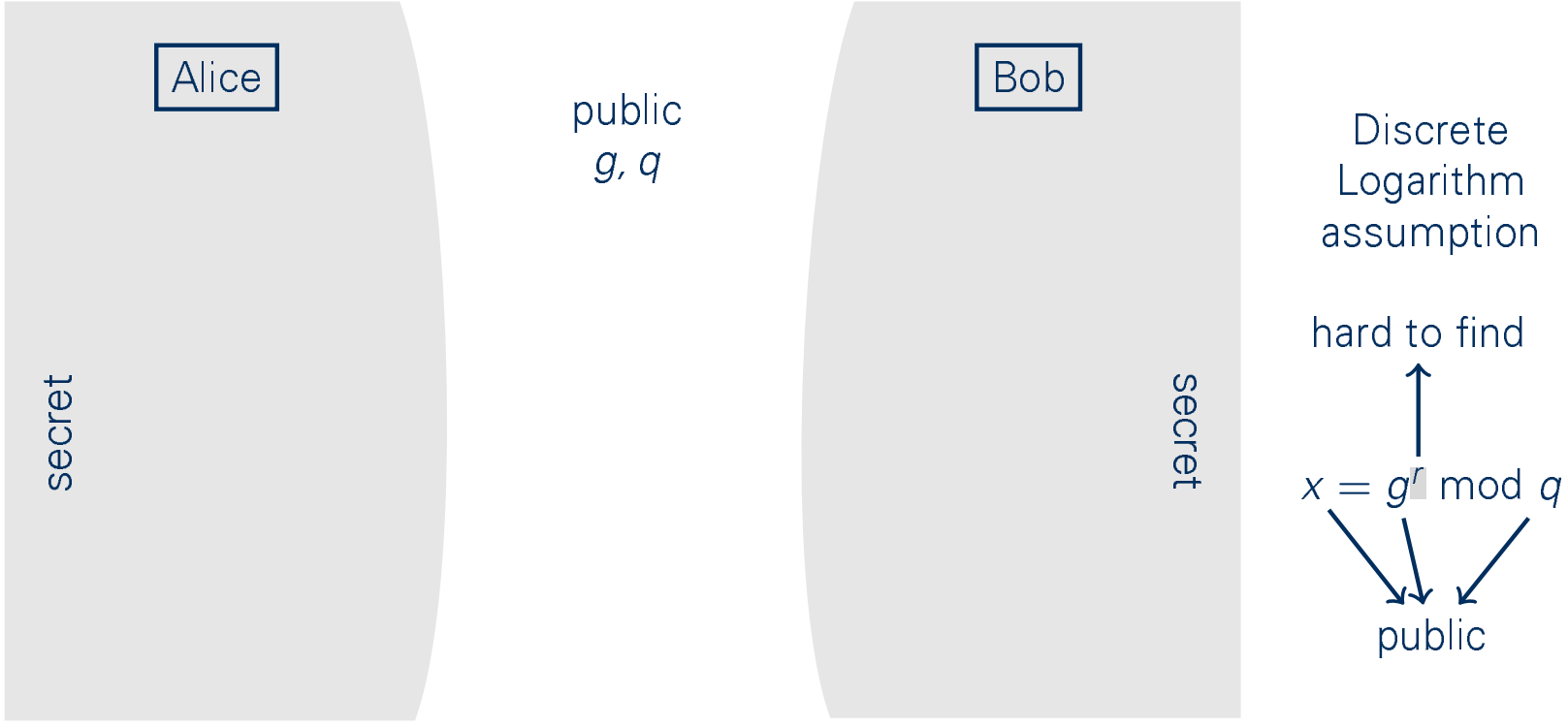


Diffie–Hellman Key Agreement



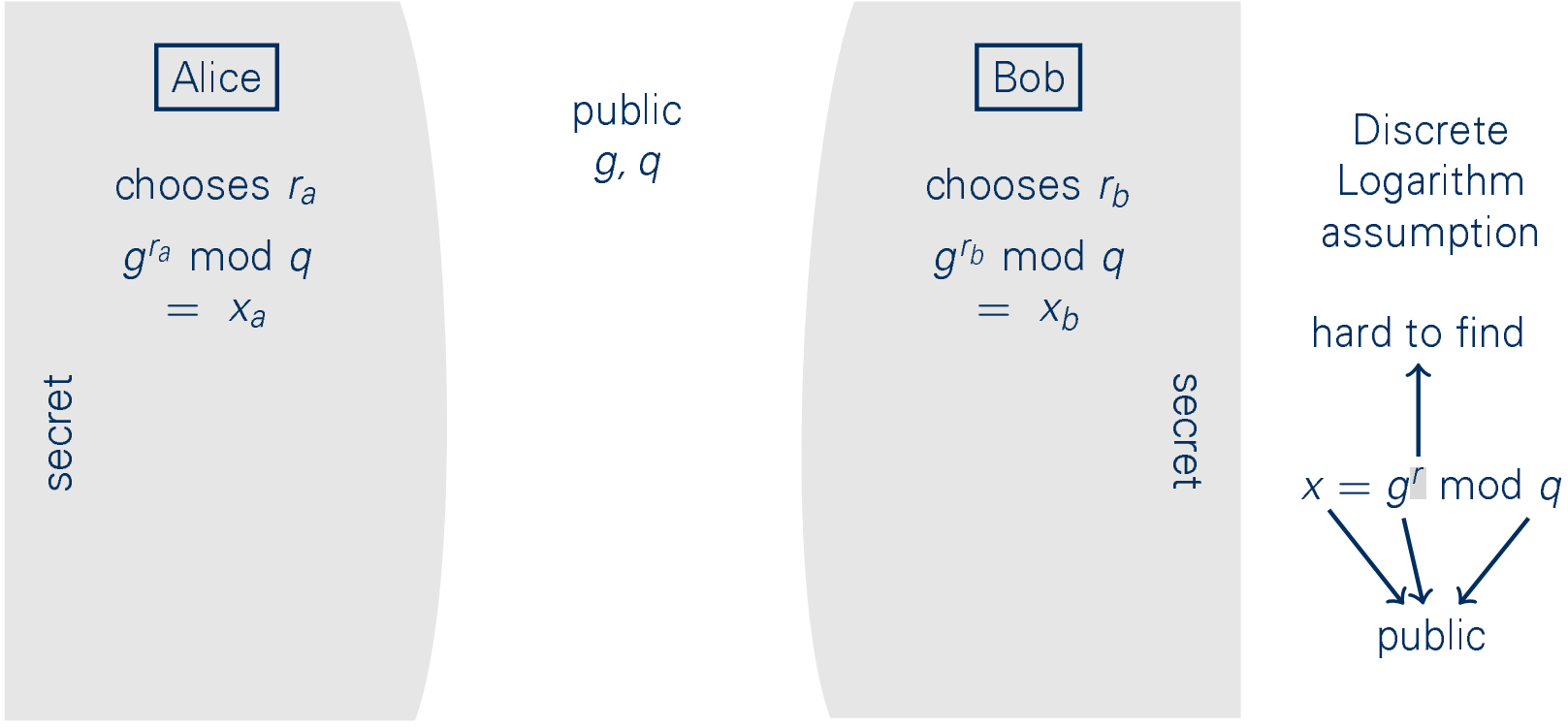
W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

Diffie–Hellman Key Agreement



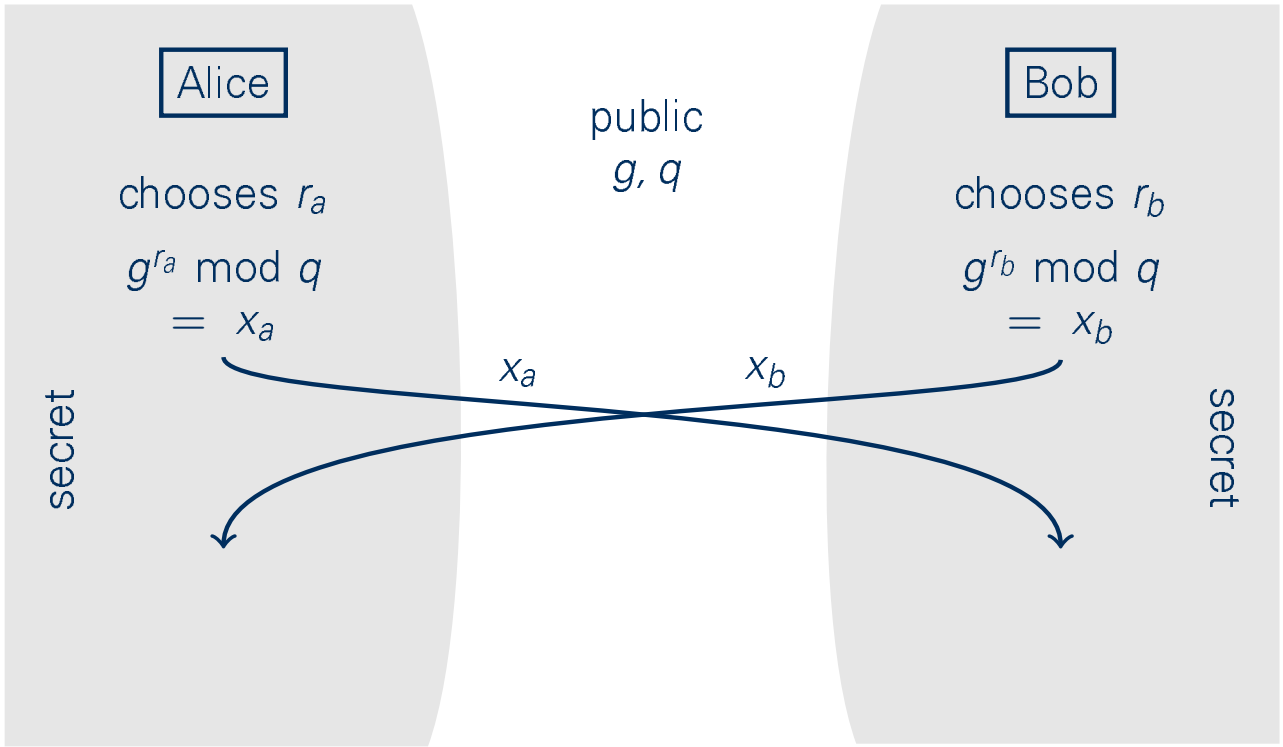
W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

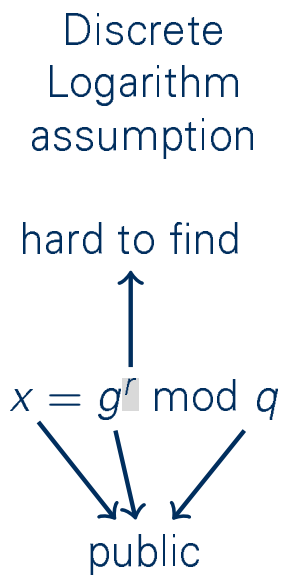
Diffie–Hellman Key Agreement



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

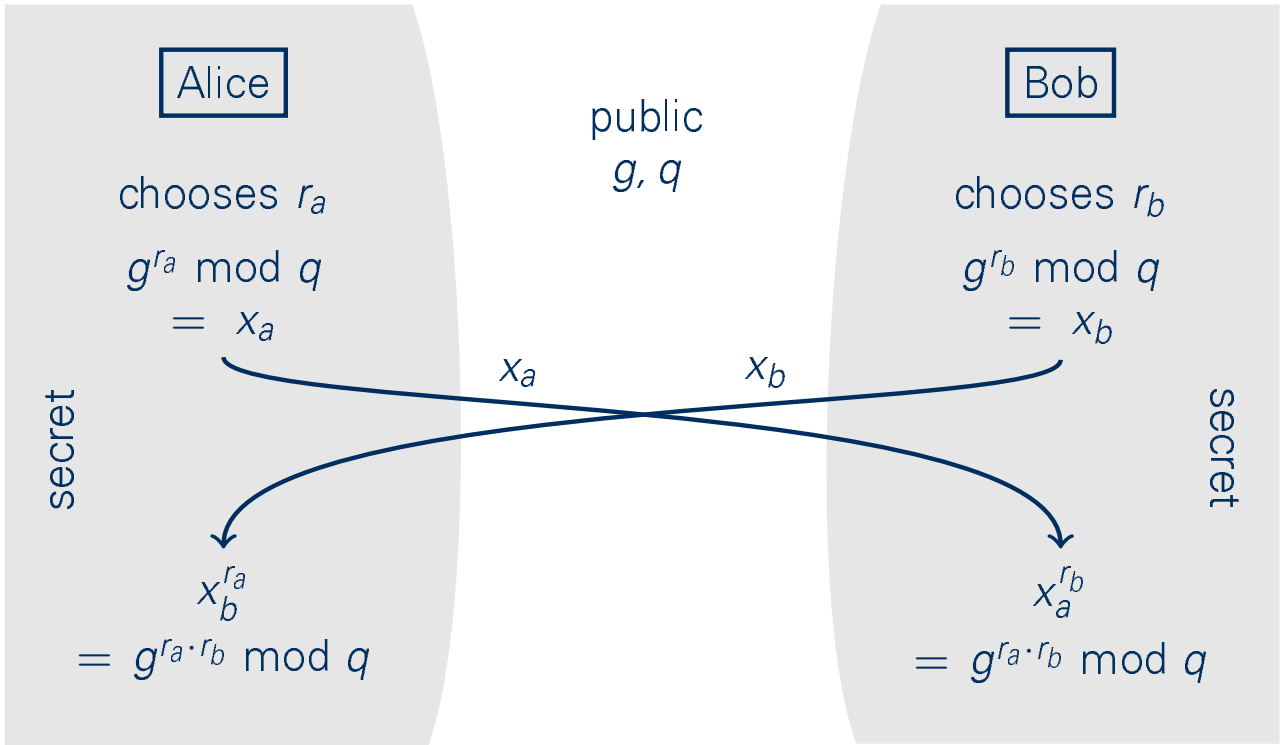
Diffie–Hellman Key Agreement

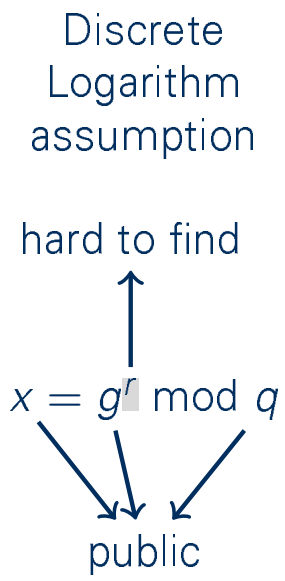




W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

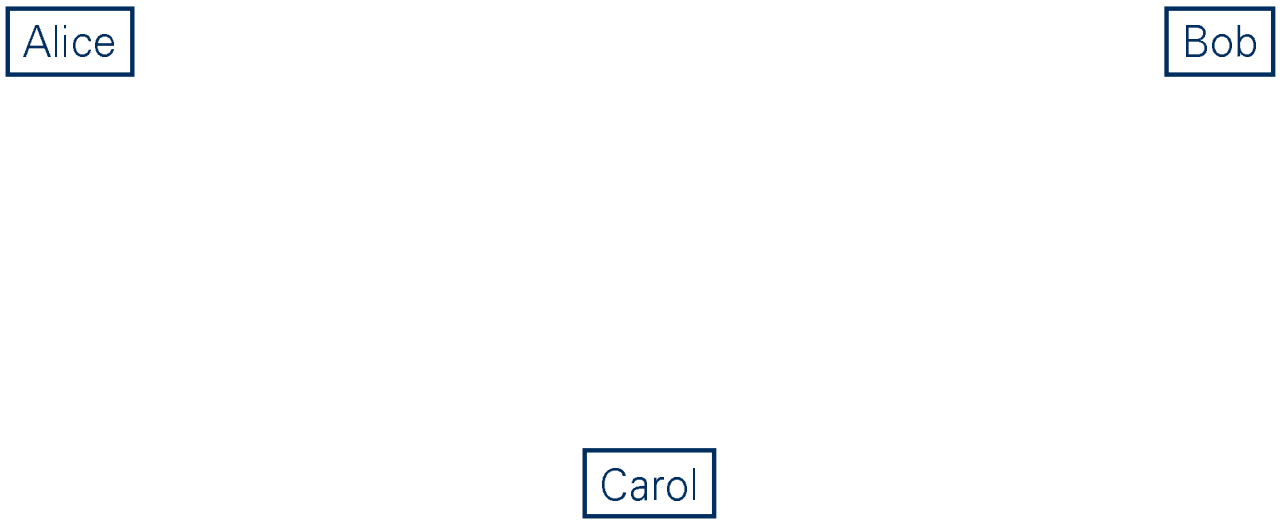
Diffie–Hellman Key Agreement





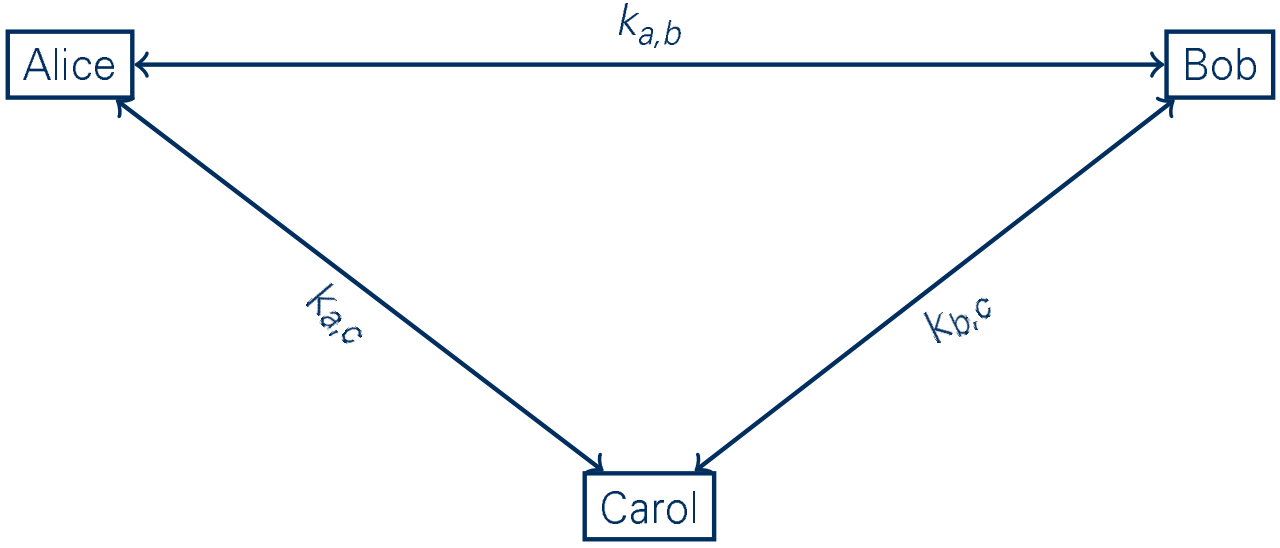
W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

Superposed Sending



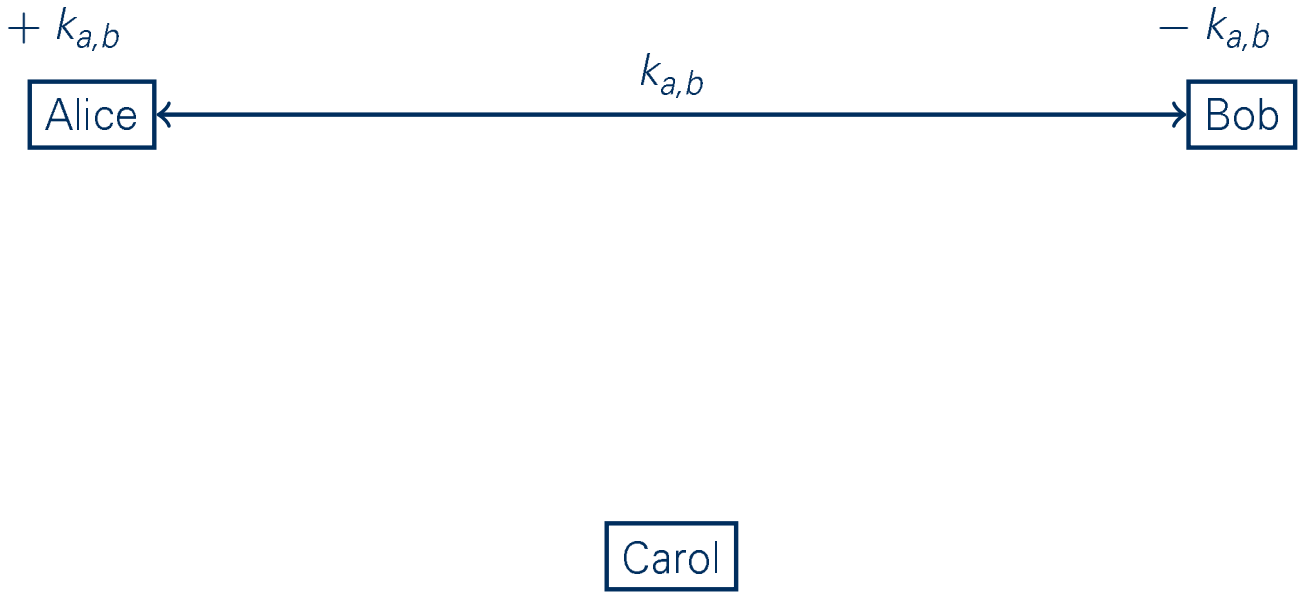
D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

Superposed Sending



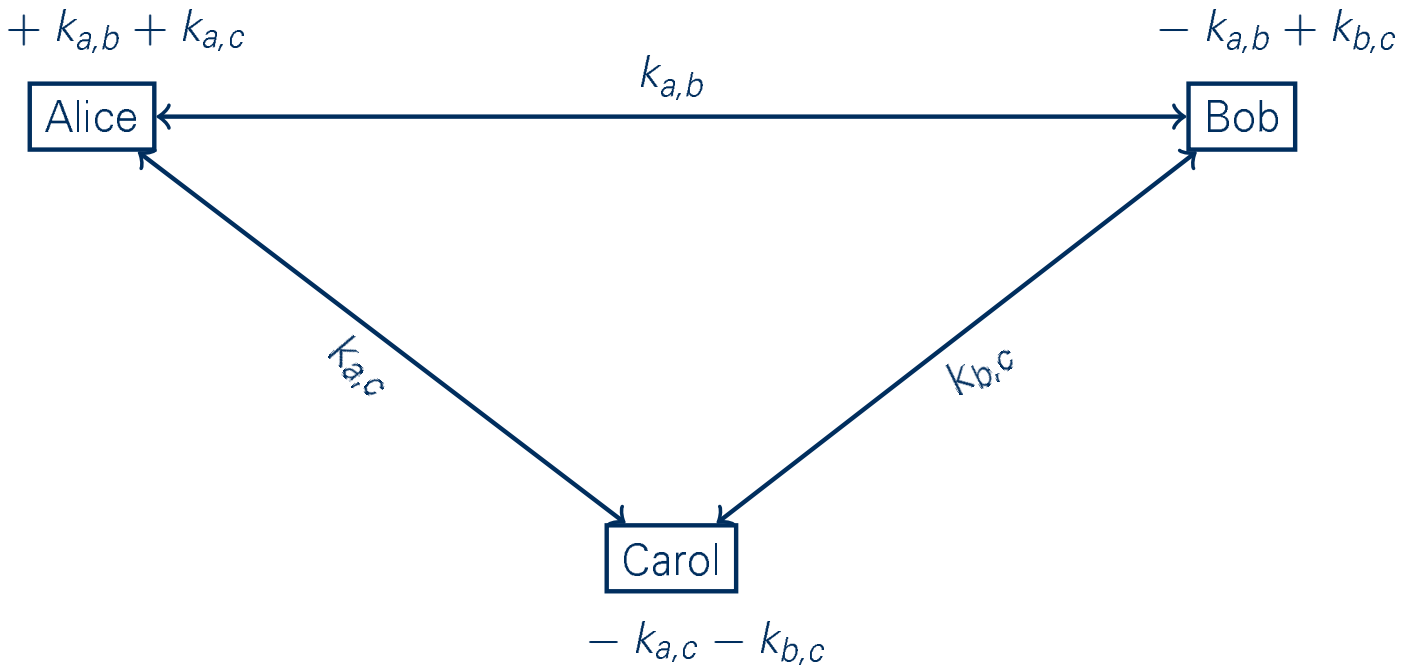
D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

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

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

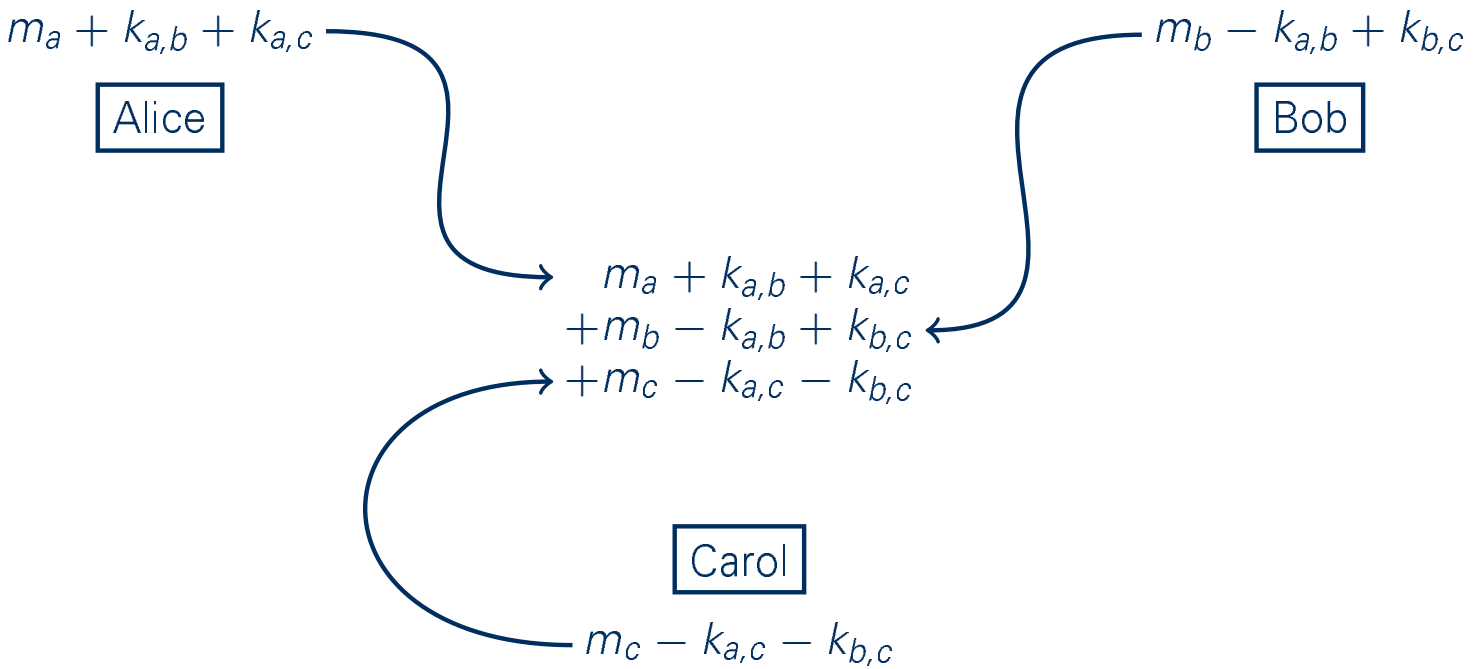
Bob

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

Alice

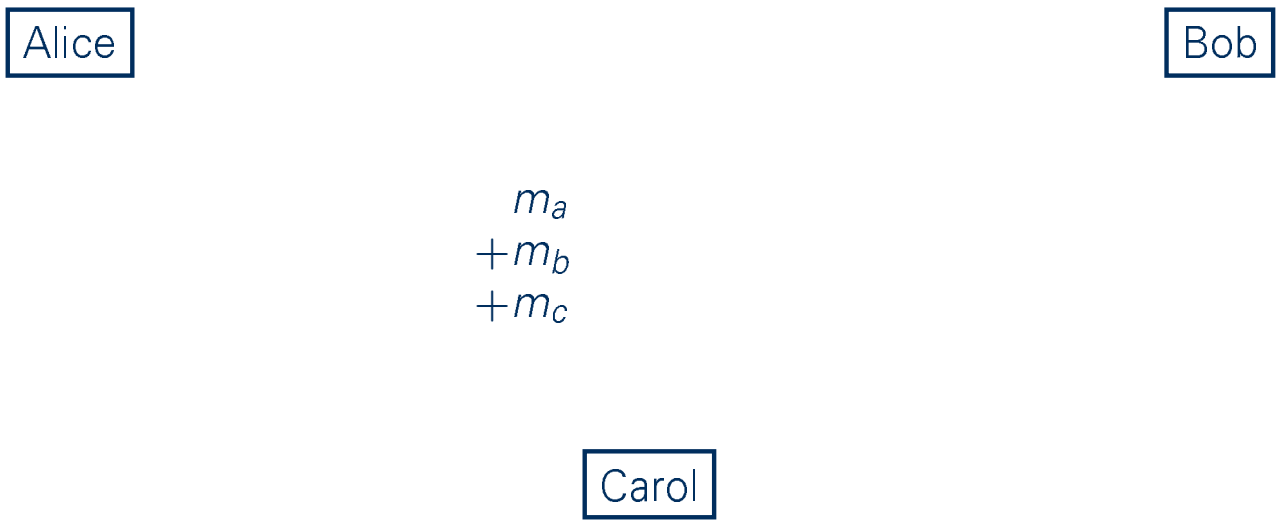
Bob

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

Carol

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

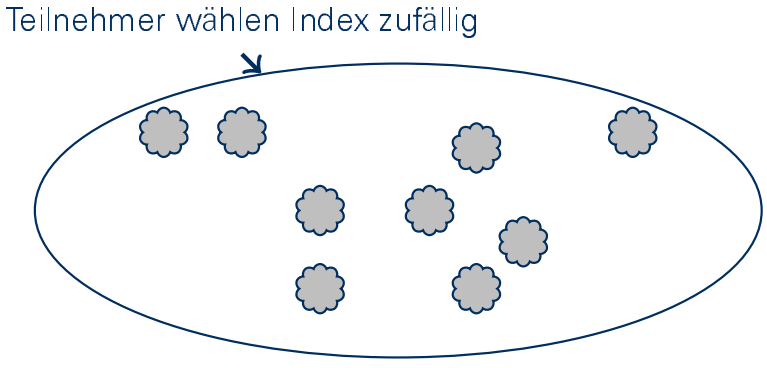
Superposed Sending



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

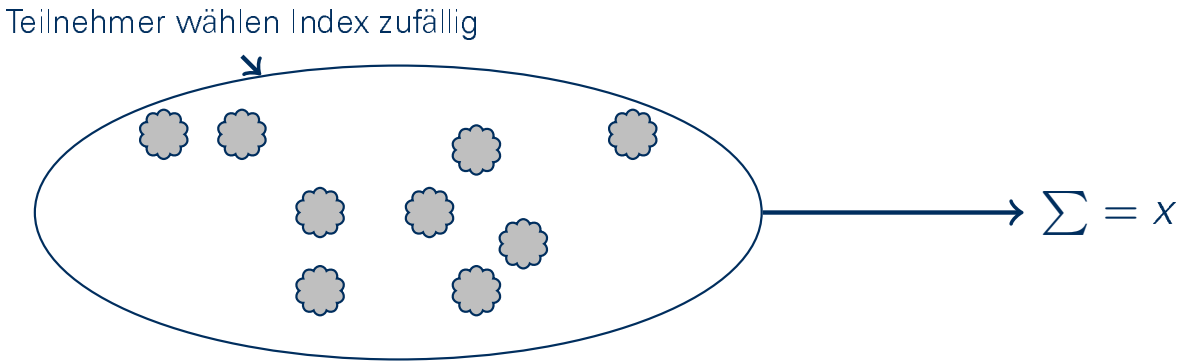
Vertraulichkeit

Induktion über simultane DC-Netz Runden (ℓ)



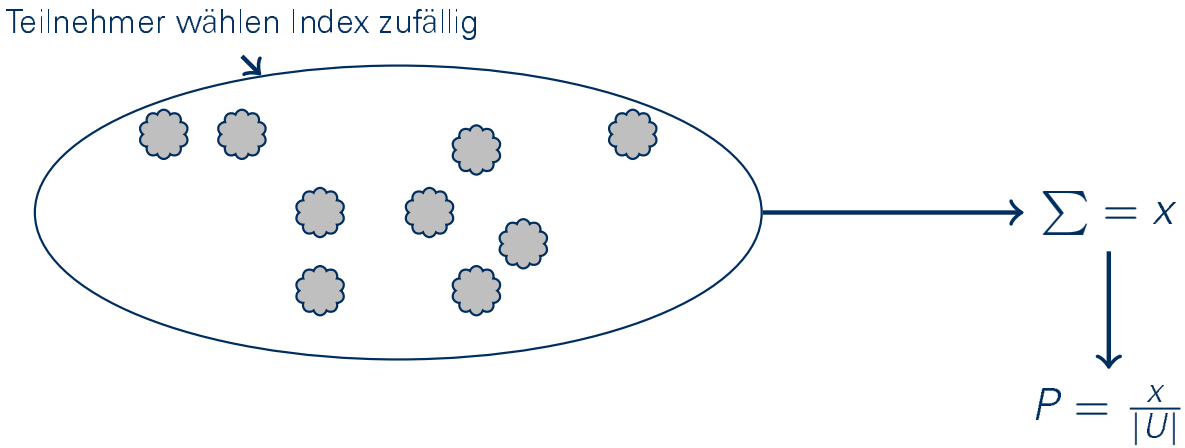
Vertraulichkeit

Induktion über simultane DC-Netz Runden (ℓ)



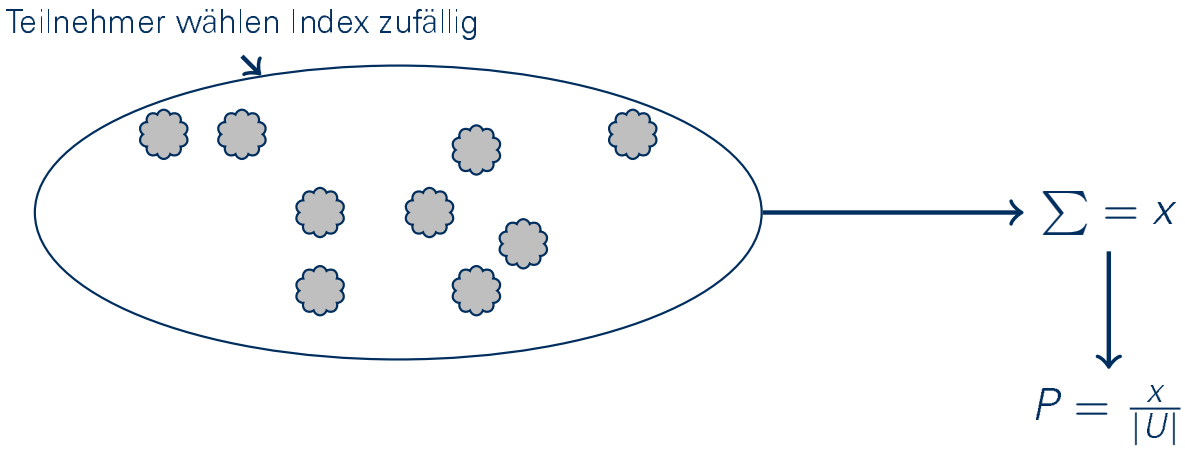
Vertraulichkeit

Induktion über simultane DC-Netz Runden (ℓ)



Vertraulichkeit

Induktion über simultane DC-Netz Runden (ℓ)

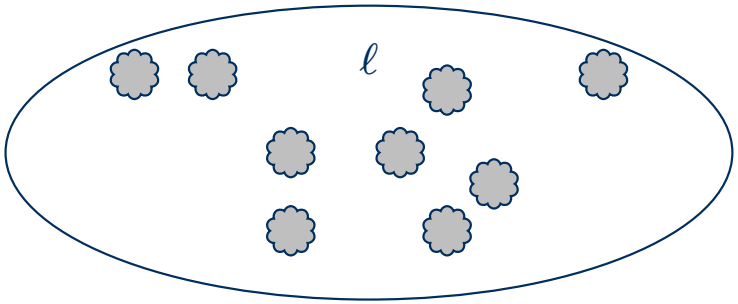


Induktionsanfang

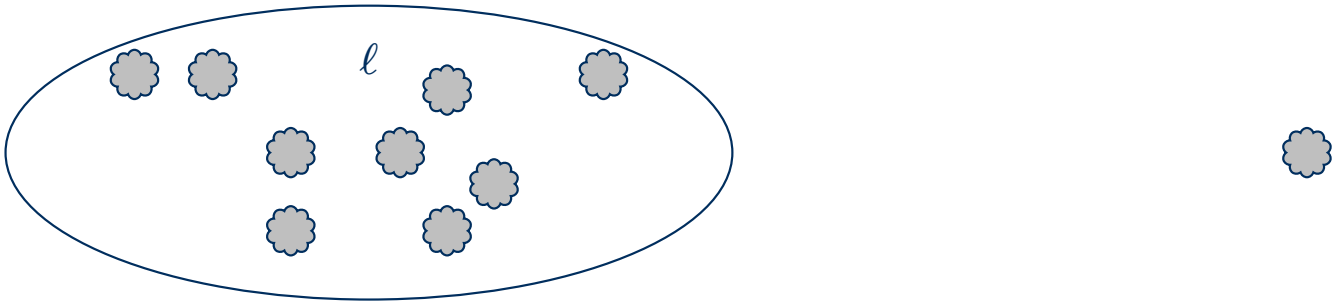
$\ell = 1 \rightarrow$ analog zu DC-Netz

Induktionsschritt ($\ell \rightarrow \ell + 1$)

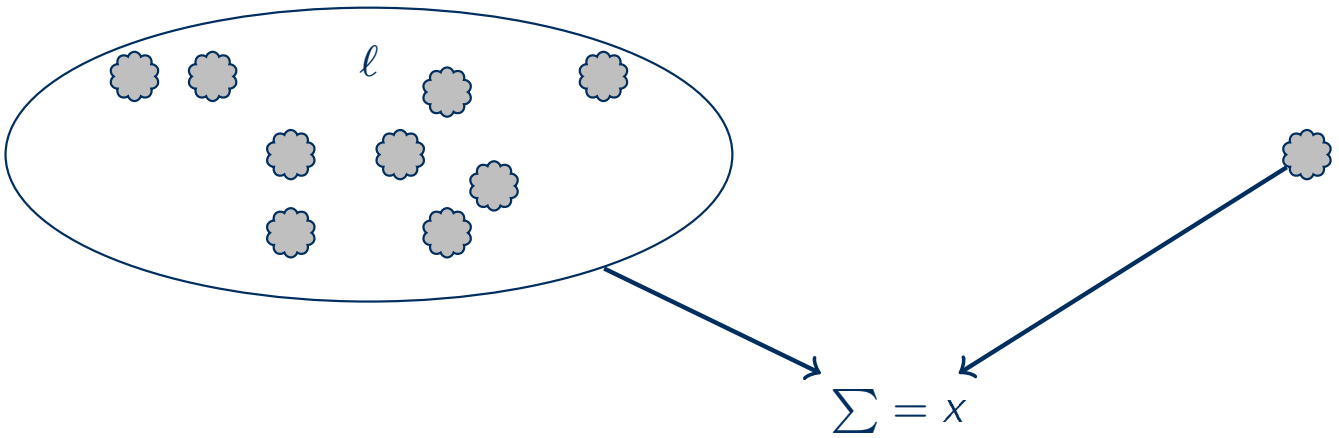
Induktionsschritt ($\ell \rightarrow \ell + 1$)



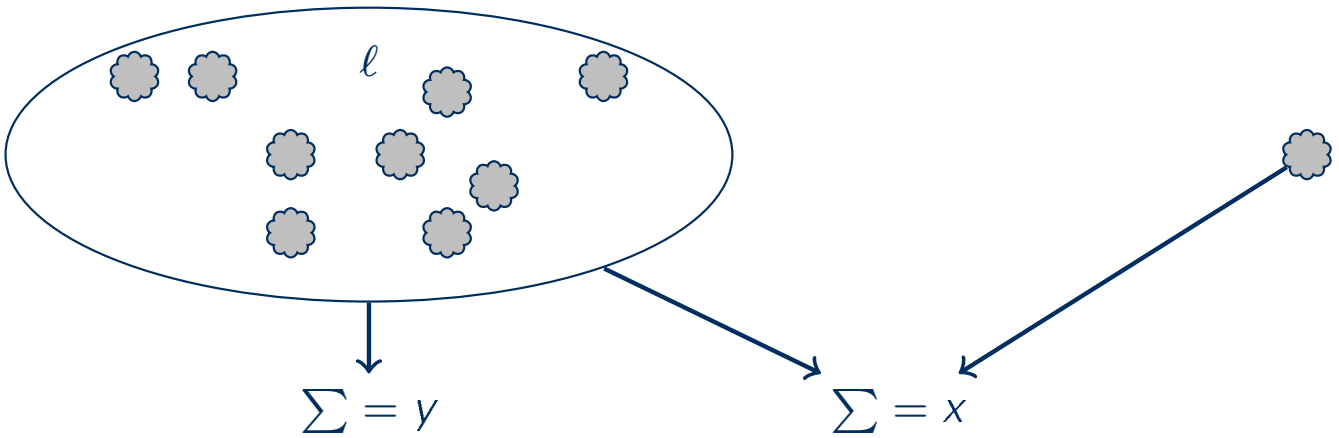
Induktionsschritt ($\ell \to \ell + 1$)



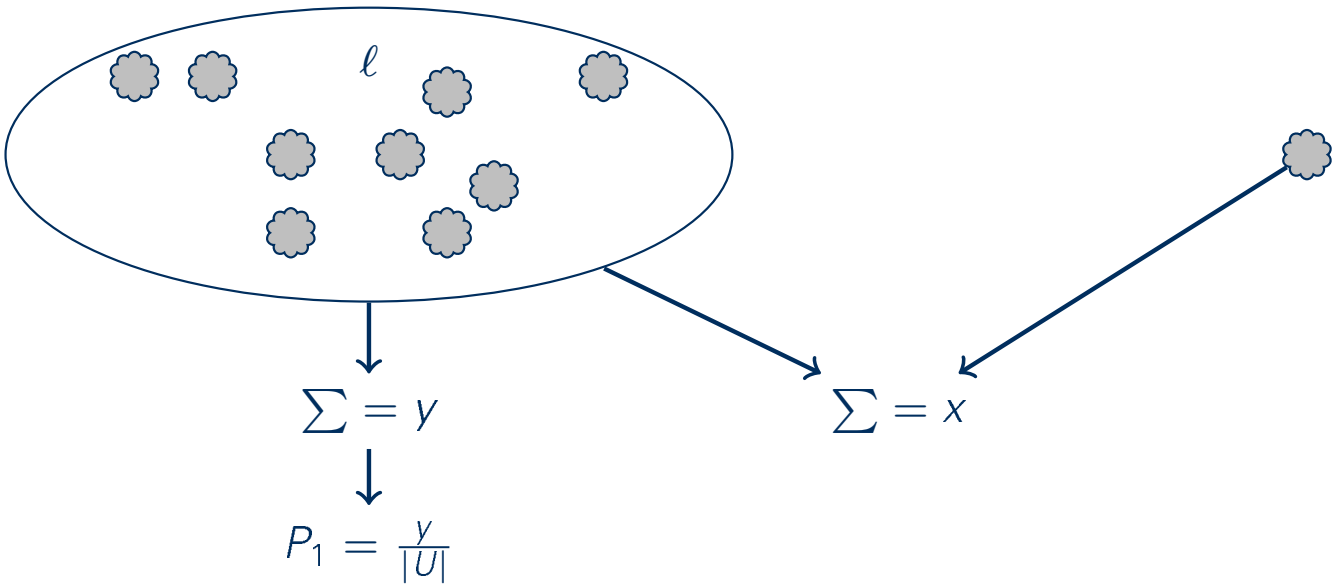
Induktionsschritt ($\ell \rightarrow \ell + 1$)



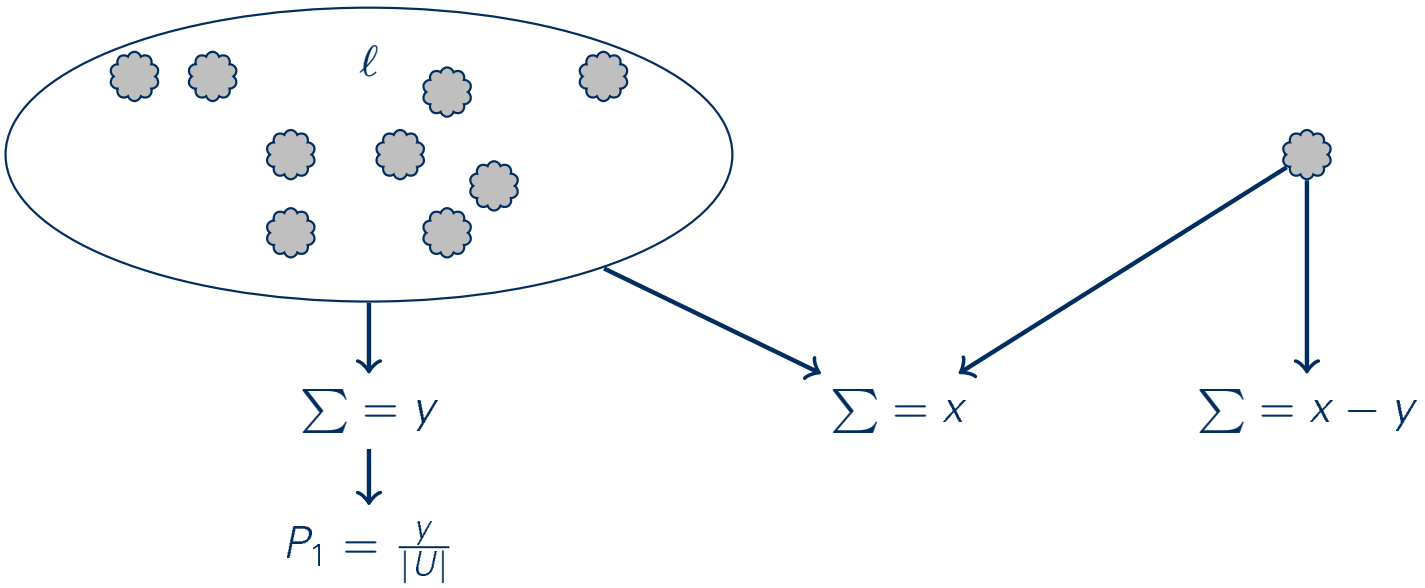
Induktionsschritt ($\ell \rightarrow \ell + 1$)



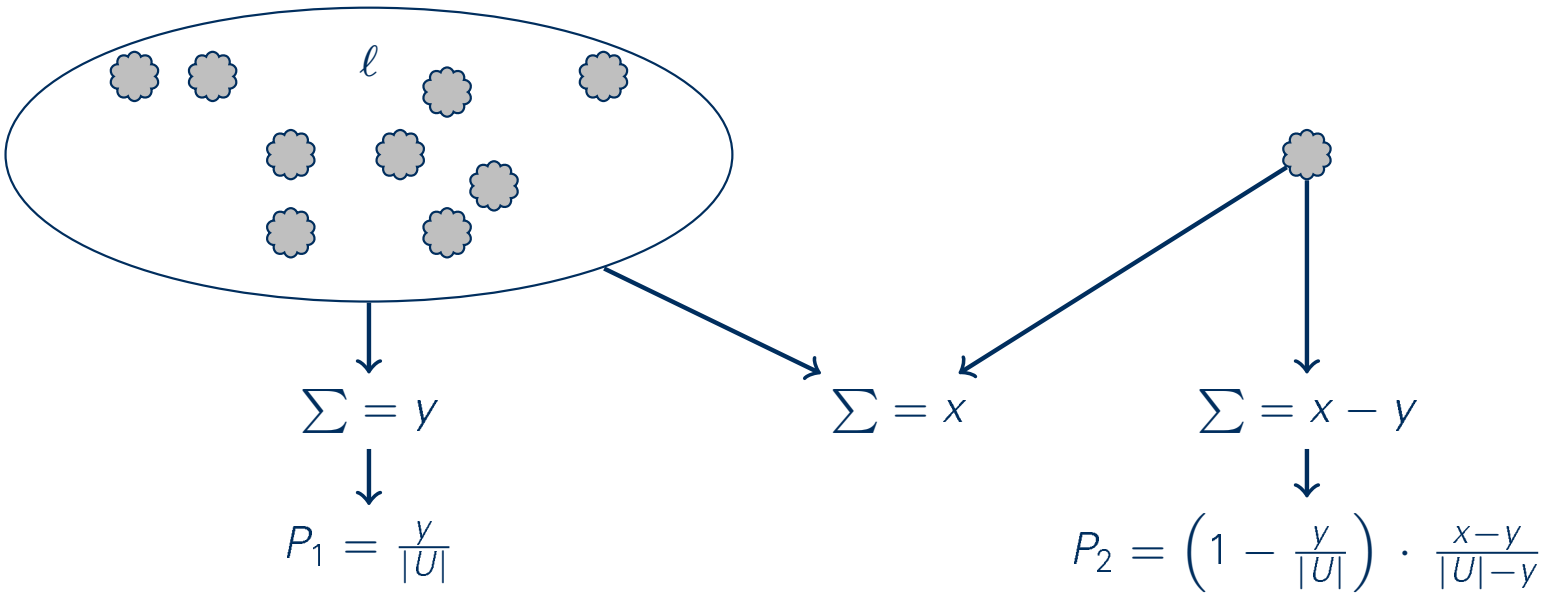
Induktionsschritt ($\ell \rightarrow \ell + 1$)



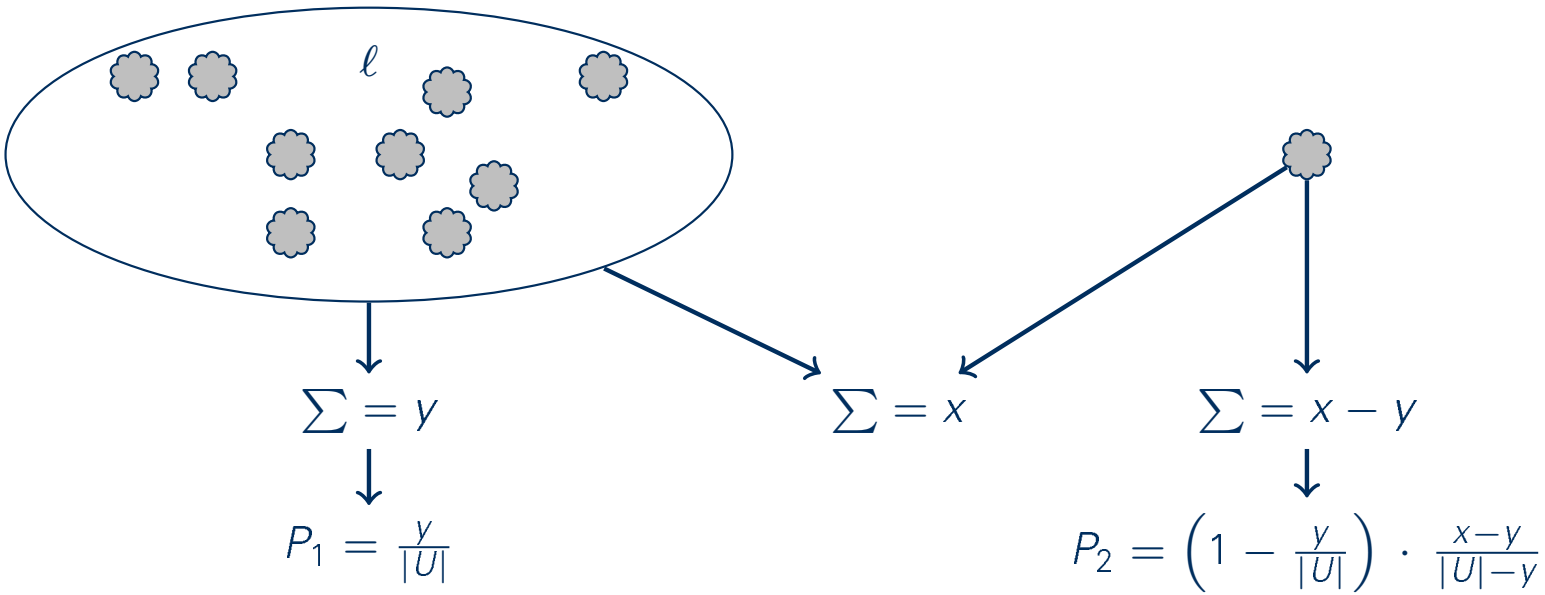
Induktionsschritt ($\ell \rightarrow \ell + 1$)



Induktionsschritt ($\ell \to \ell + 1$)

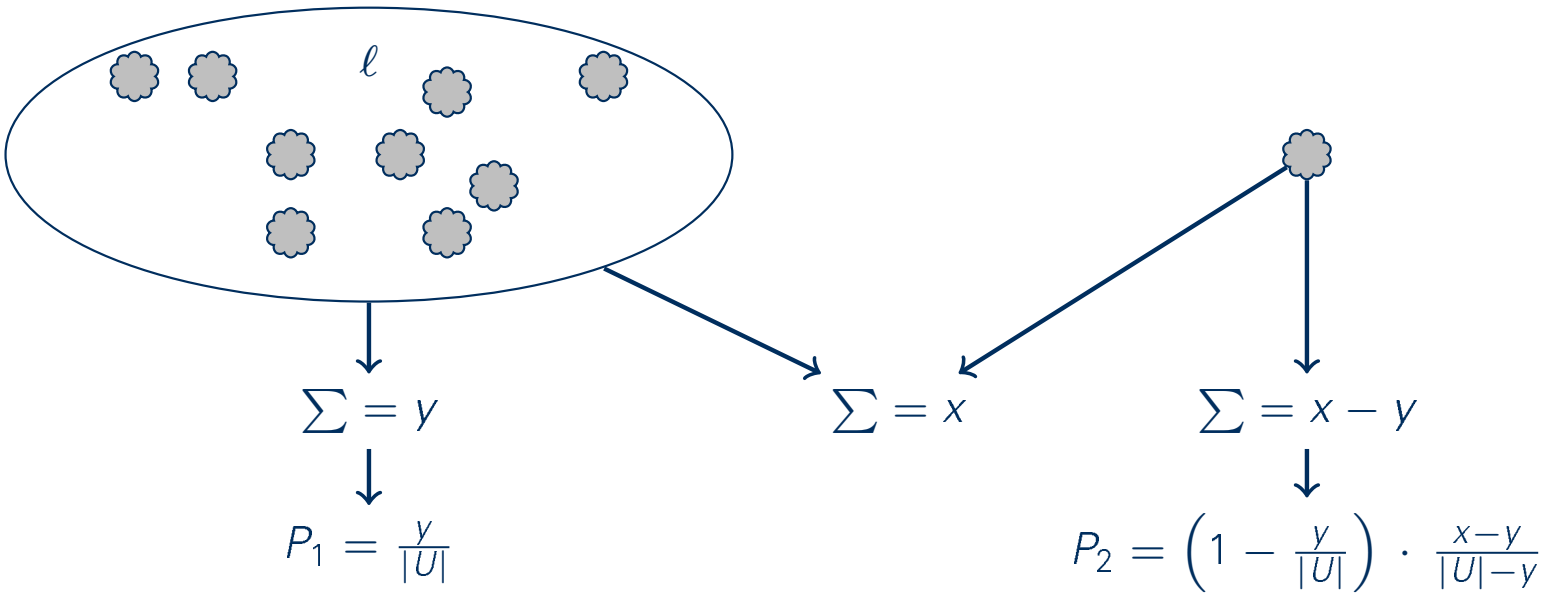


Induktionsschritt ($\ell \to \ell + 1$)



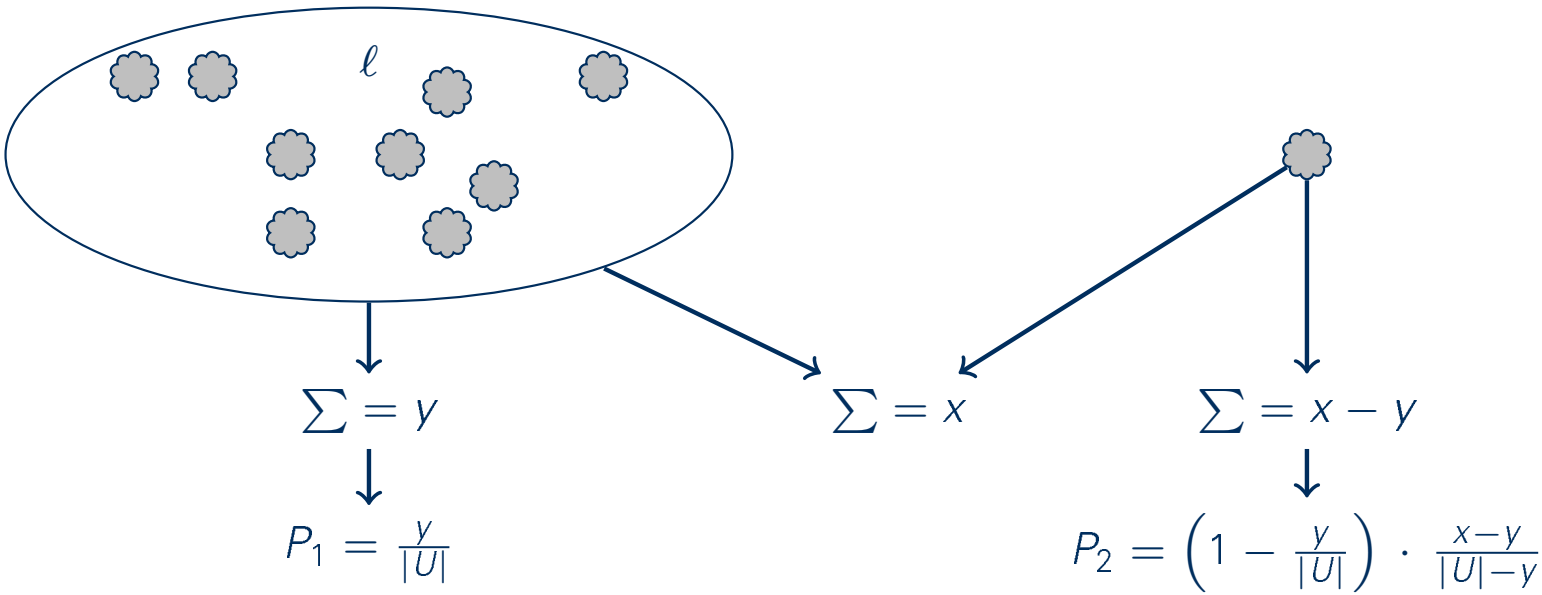
$$P_1 + P_2 \stackrel{?}{=} \frac{x}{|U|}$$

Induktionsschritt ($\ell \to \ell + 1$)



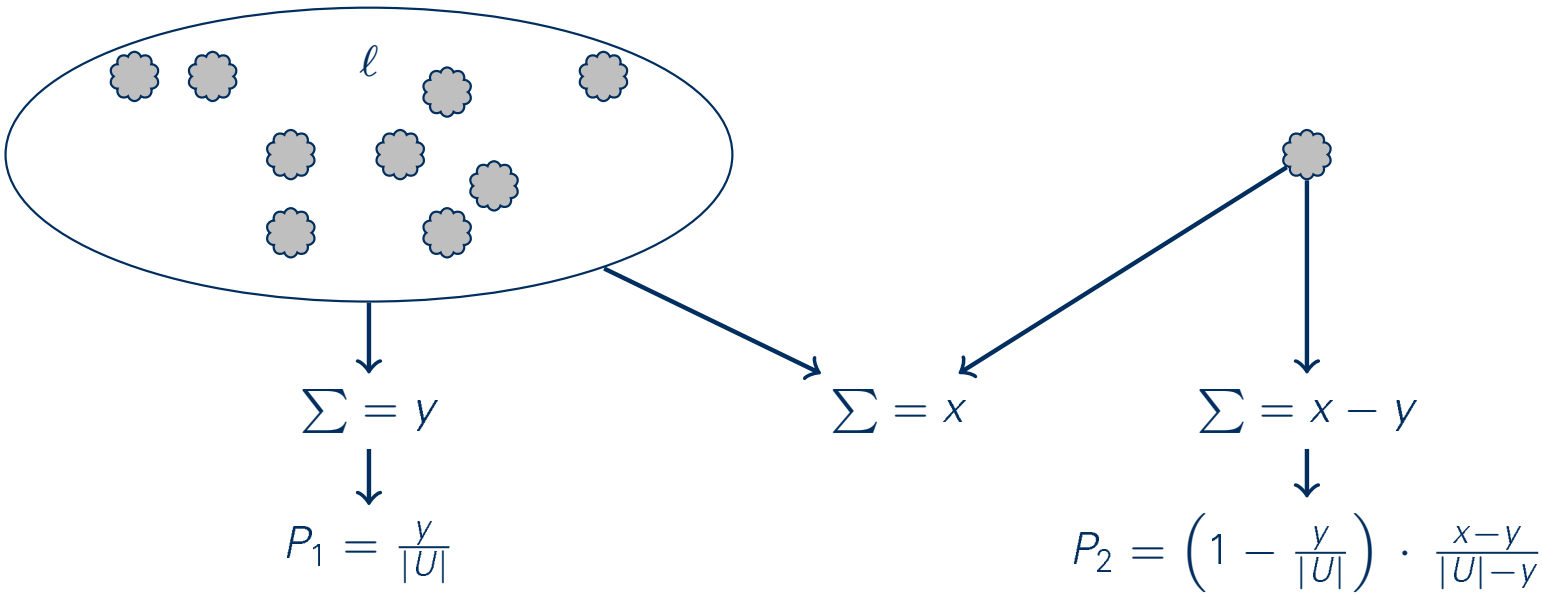
$$P_1 + P_2 = \frac{y}{|U|} + \left(1 - \frac{y}{|U|}\right) \cdot \frac{x-y}{|U|-y} = \frac{x}{|U|}$$

Induktionsschritt ($\ell \to \ell + 1$)



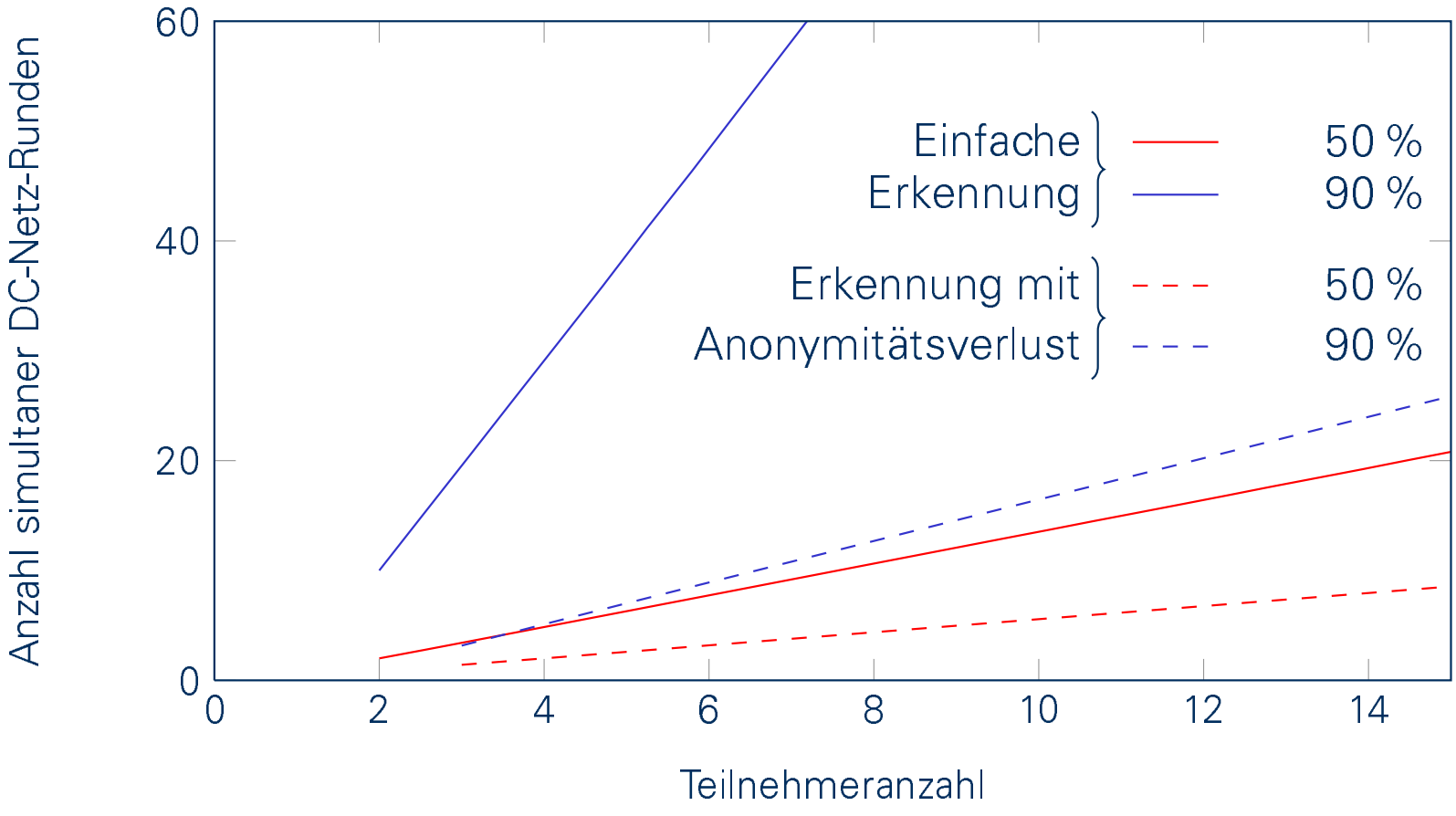
$$P_1 + P_2 = \frac{y}{|U|} + \left(1 - \frac{y}{|U|}\right) \cdot \frac{x-y}{|U|-y} = \frac{y}{|U|} + \frac{(|U|-y)\cdot(x-y)}{|U|\cdot(|U|-y)} = \frac{x}{|U|}$$

Induktionsschritt ($\ell \to \ell + 1$)

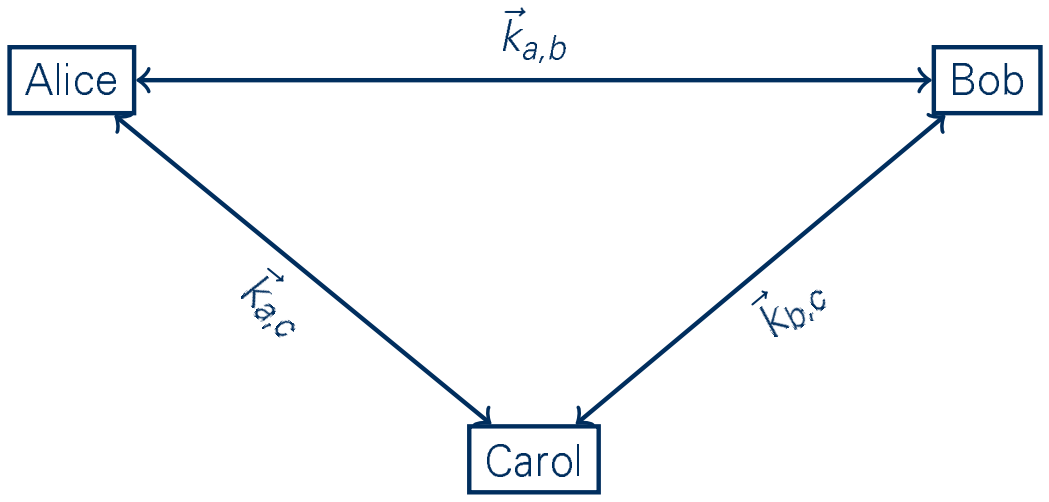


$$P_1 + P_2 = \frac{y}{|U|} + \left(1 - \frac{y}{|U|}\right) \cdot \frac{x-y}{|U|-y} = \frac{y}{|U|} + \frac{(|U|-y)\cdot(x-y)}{|U|\cdot(|U|-y)} = \frac{y}{|U|} + \frac{x-y}{|U|} = \frac{x}{|U|}$$

Sicherheitsparameter



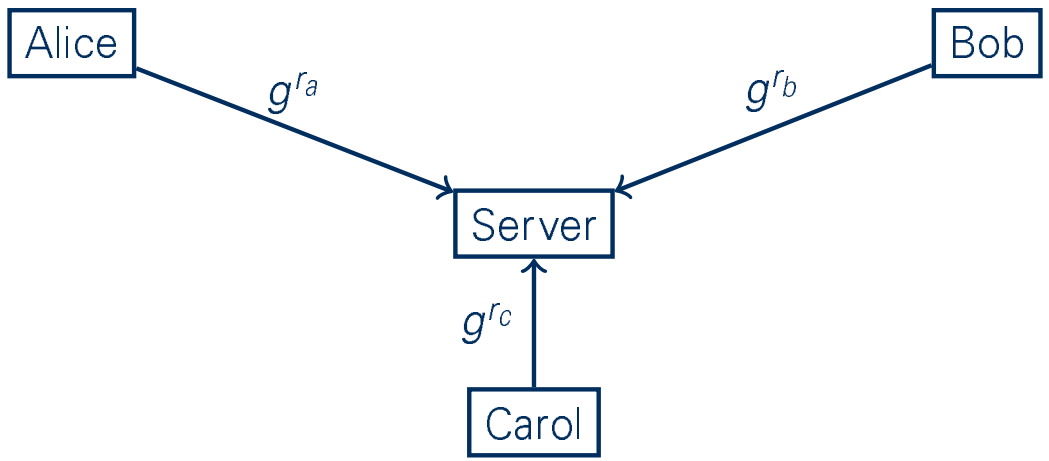
Vereinfachung des Schlüsselaustauschs



Schlüsselaustausch

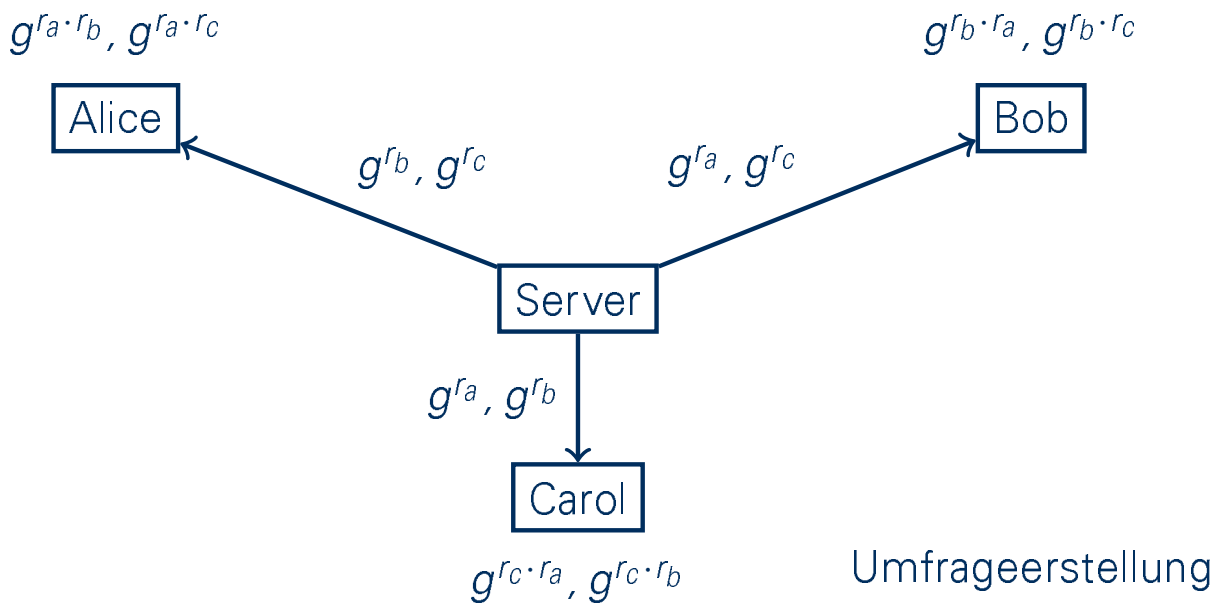
Vereinfachung des Schlüsselaustauschs

Diffie–Hellman



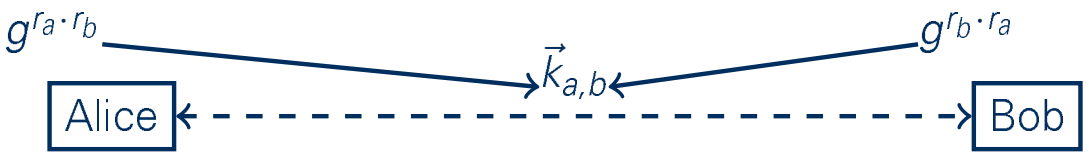
Vereinfachung des Schlüsselaustauschs

Diffie–Hellman



Vereinfachung des Schlüsselaustauschs

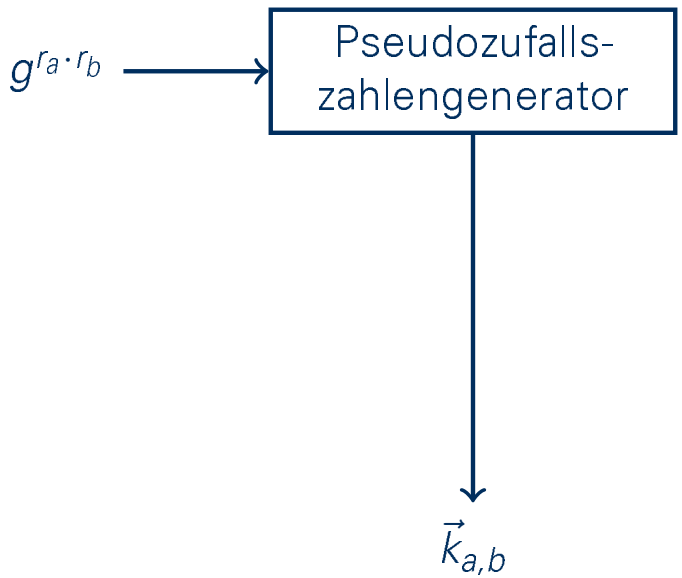
Diffie–Hellman



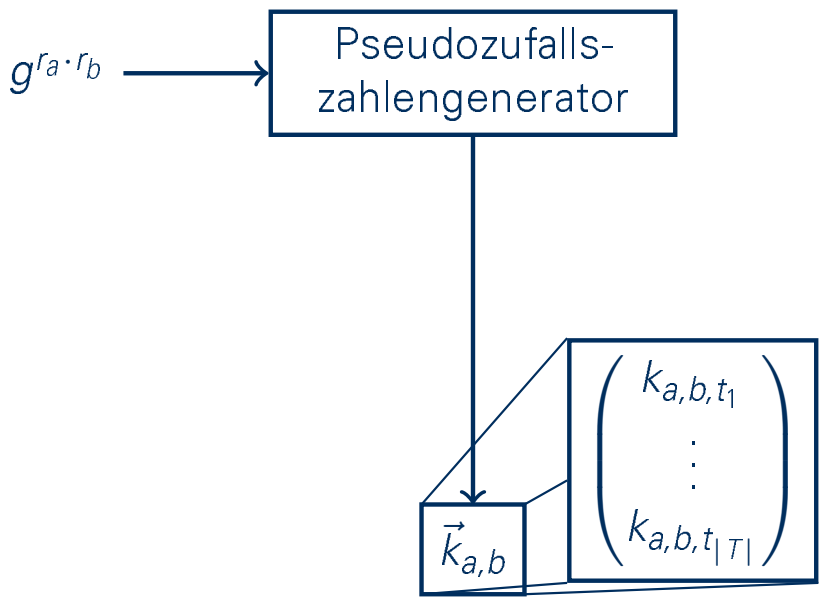
Carol

Umfrageerstellung

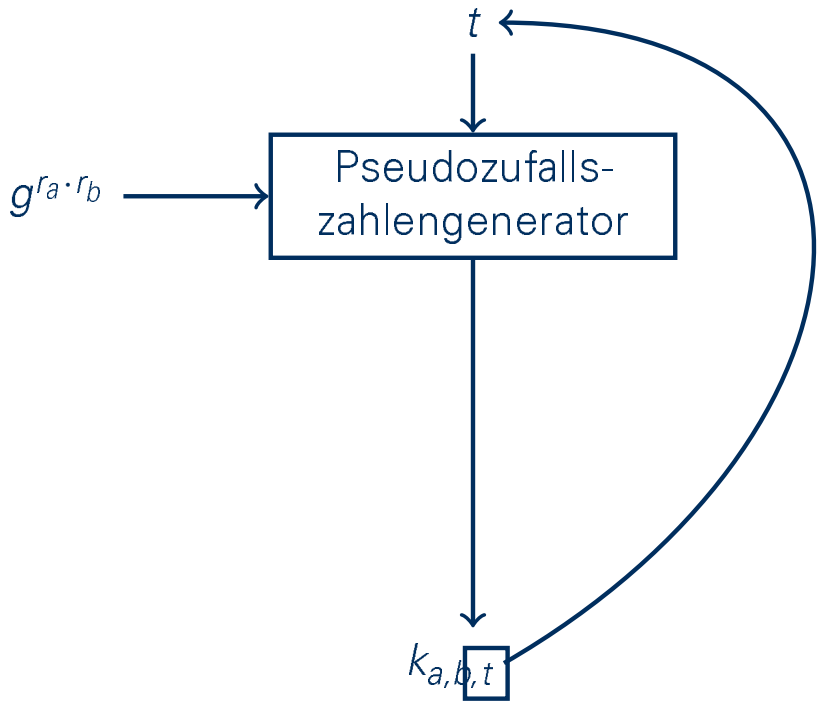
Vereinfachung des Schlüsselaustauschs



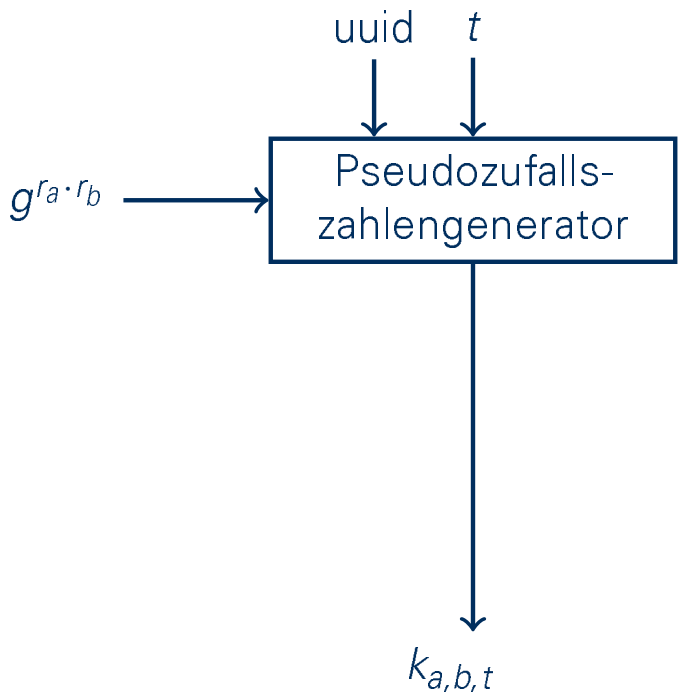
Vereinfachung des Schlüsselaustauschs



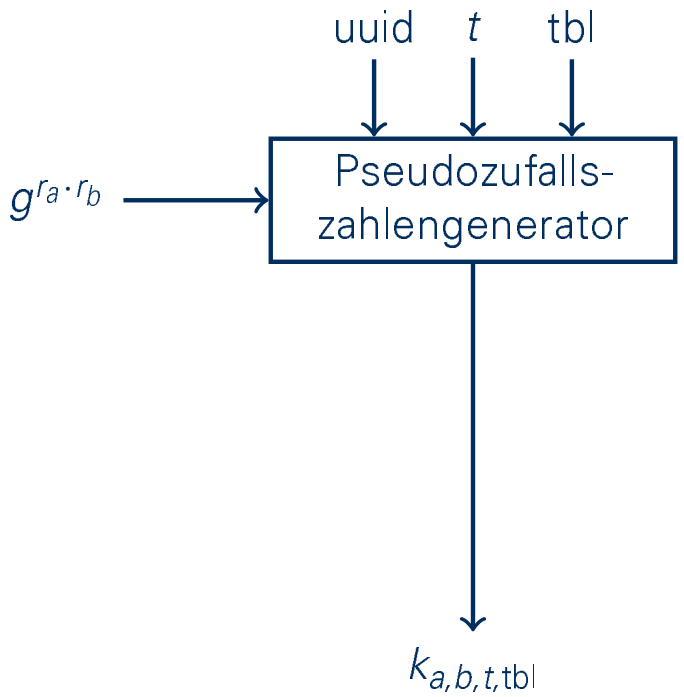
Vereinfachung des Schlüsselaustauschs



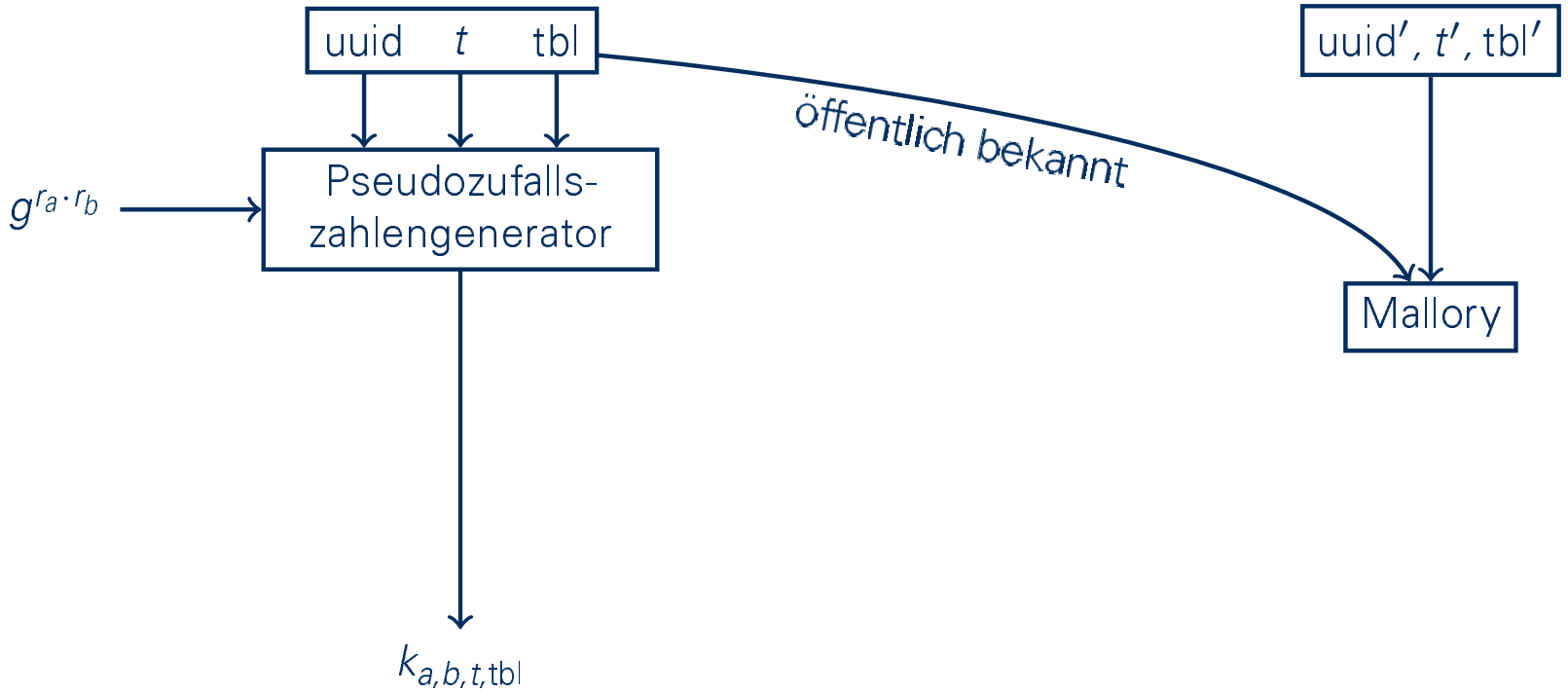
Vereinfachung des Schlüsselaustauschs



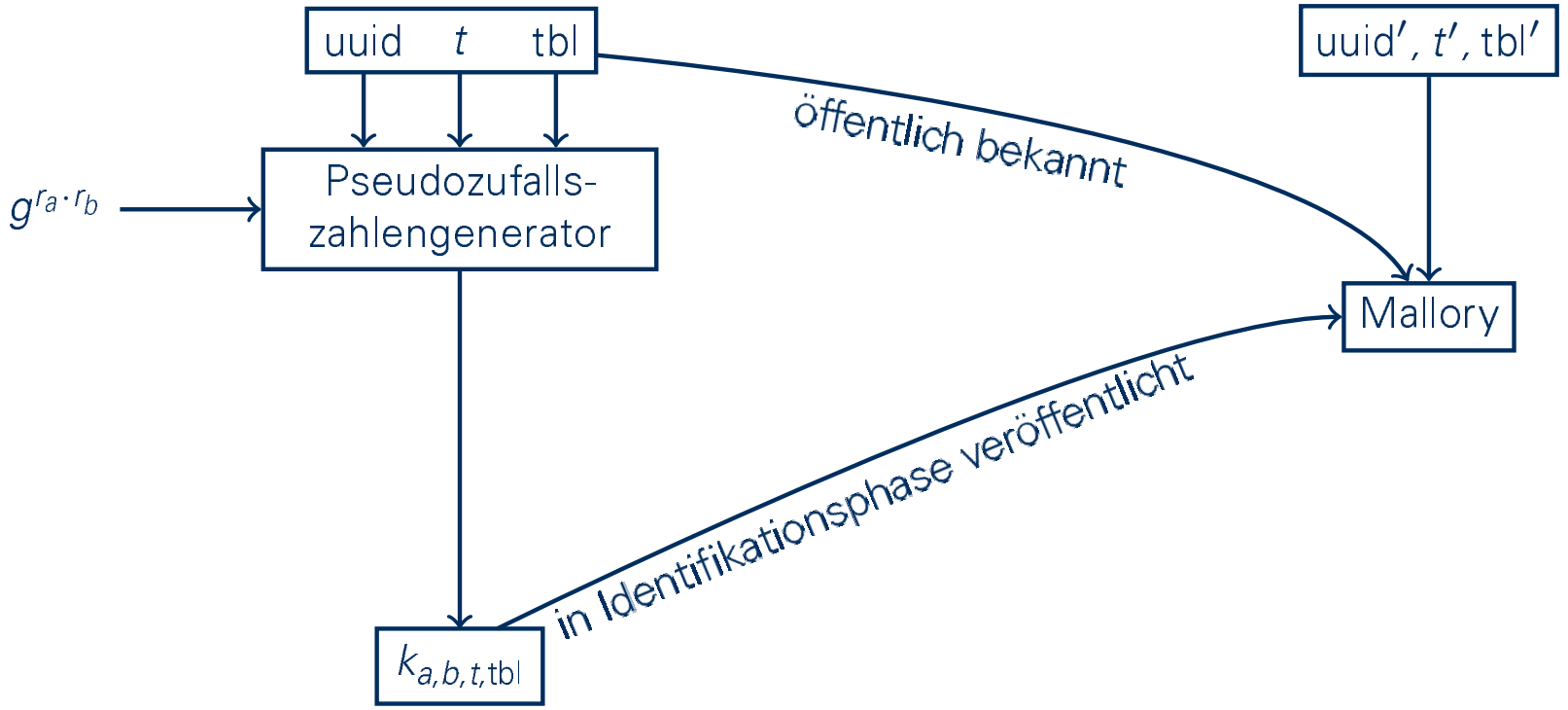
Vereinfachung des Schlüsselaustauschs



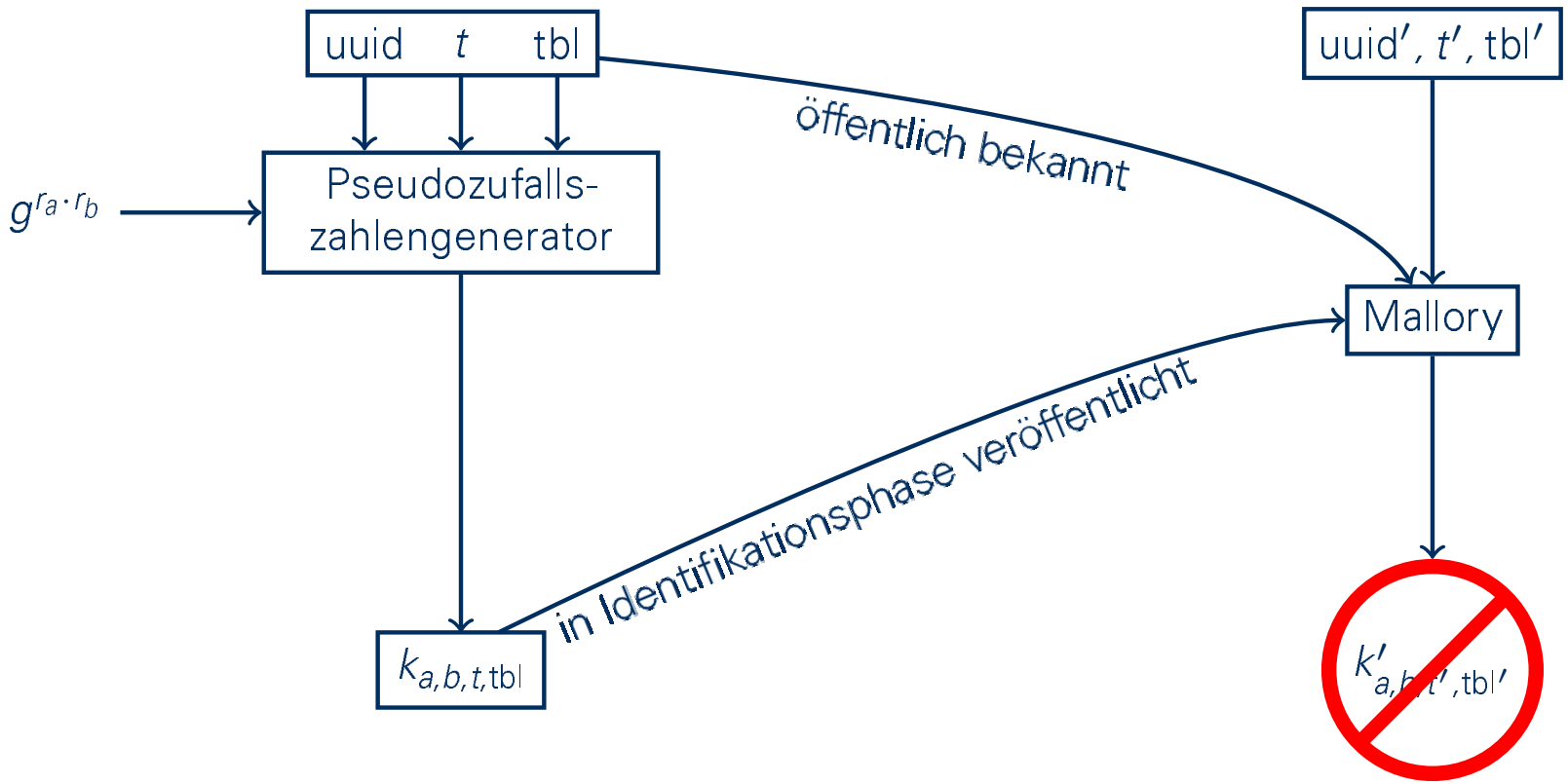
Vereinfachung des Schlüsselaustauschs



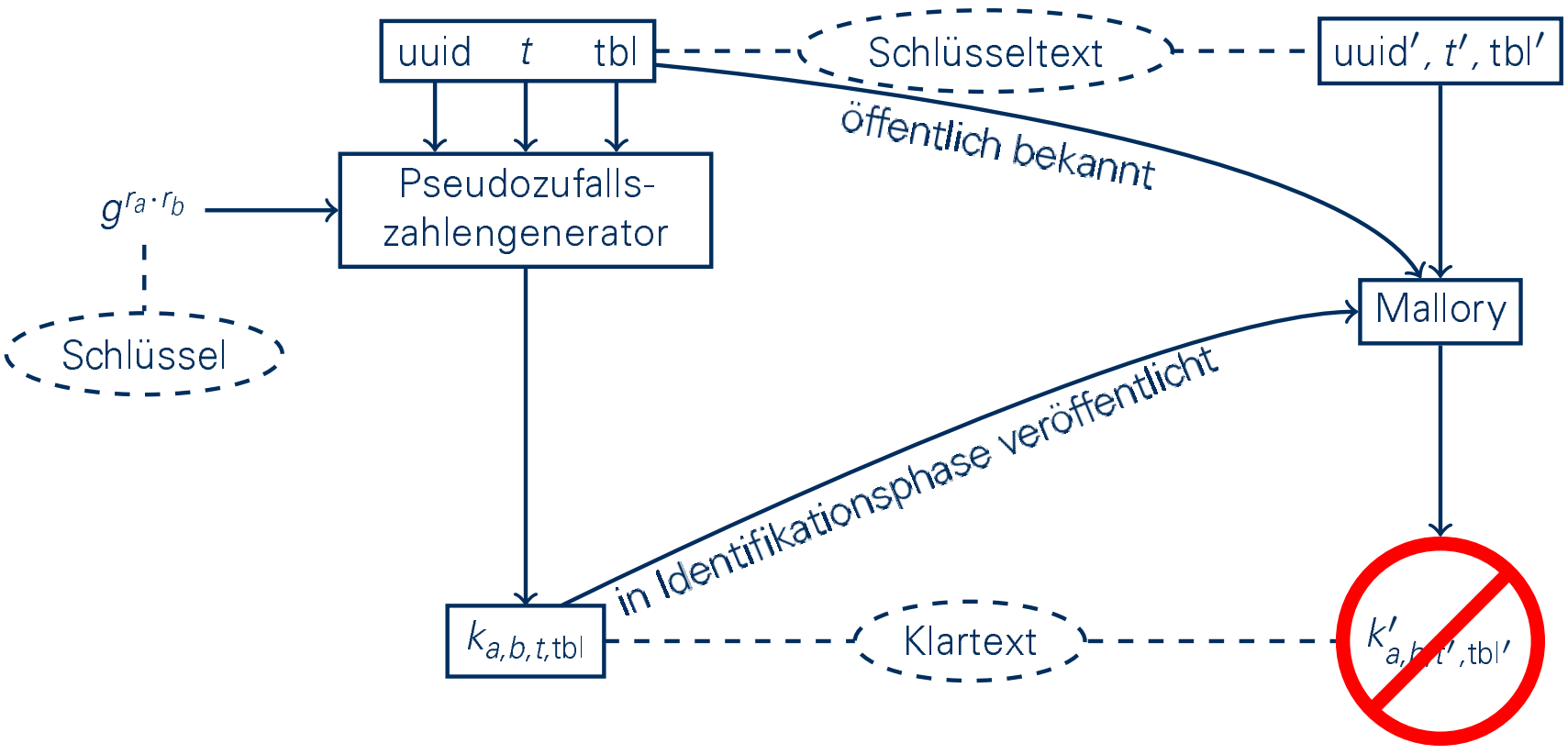
Vereinfachung des Schlüsselaustauschs



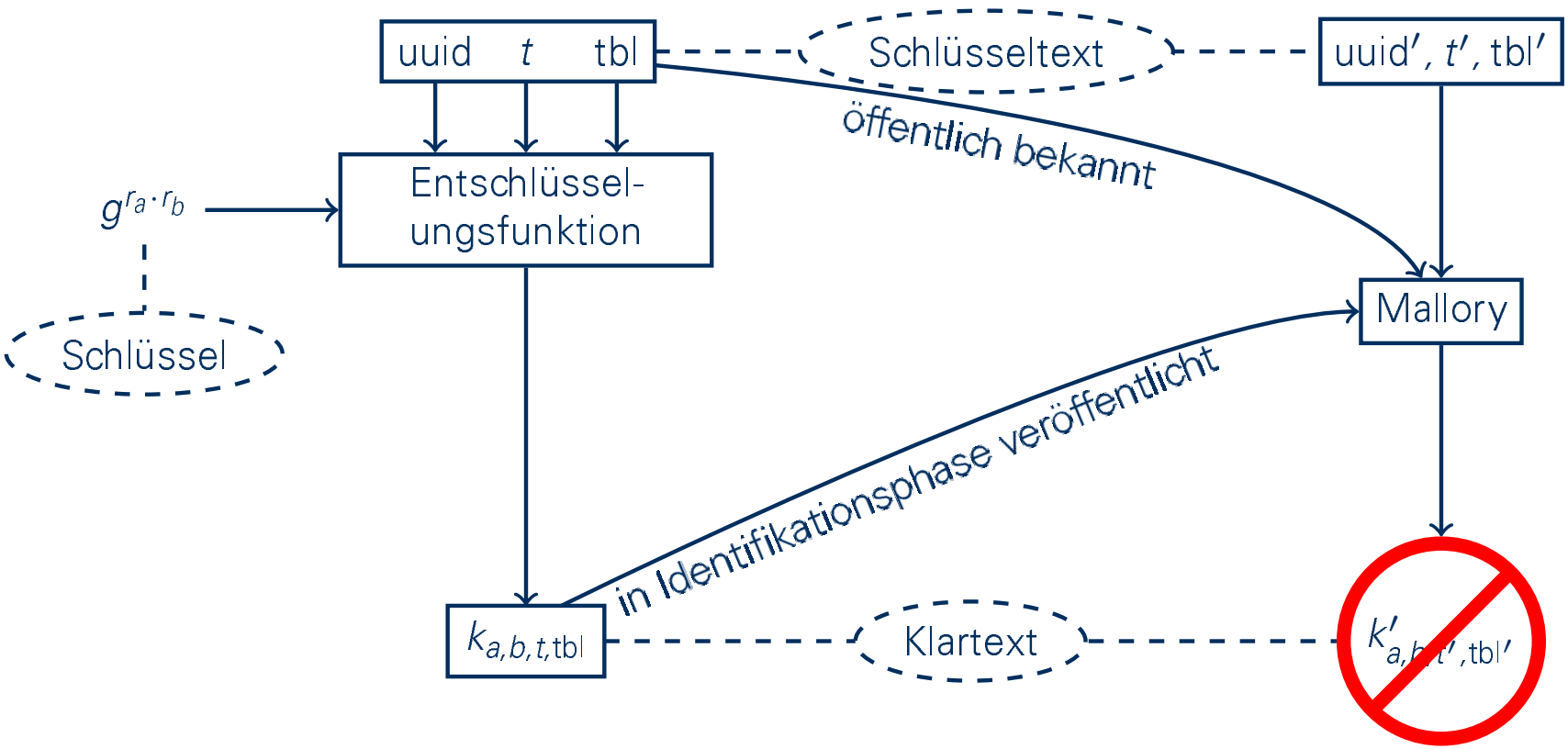
Vereinfachung des Schlüsselaustauschs



Vereinfachung des Schlüsselaustauschs



Vereinfachung des Schlüsselaustauschs



Bookmarklet als Schlüsselspeicherung

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

Bookmarklet als Schlüsselspeicherung

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

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

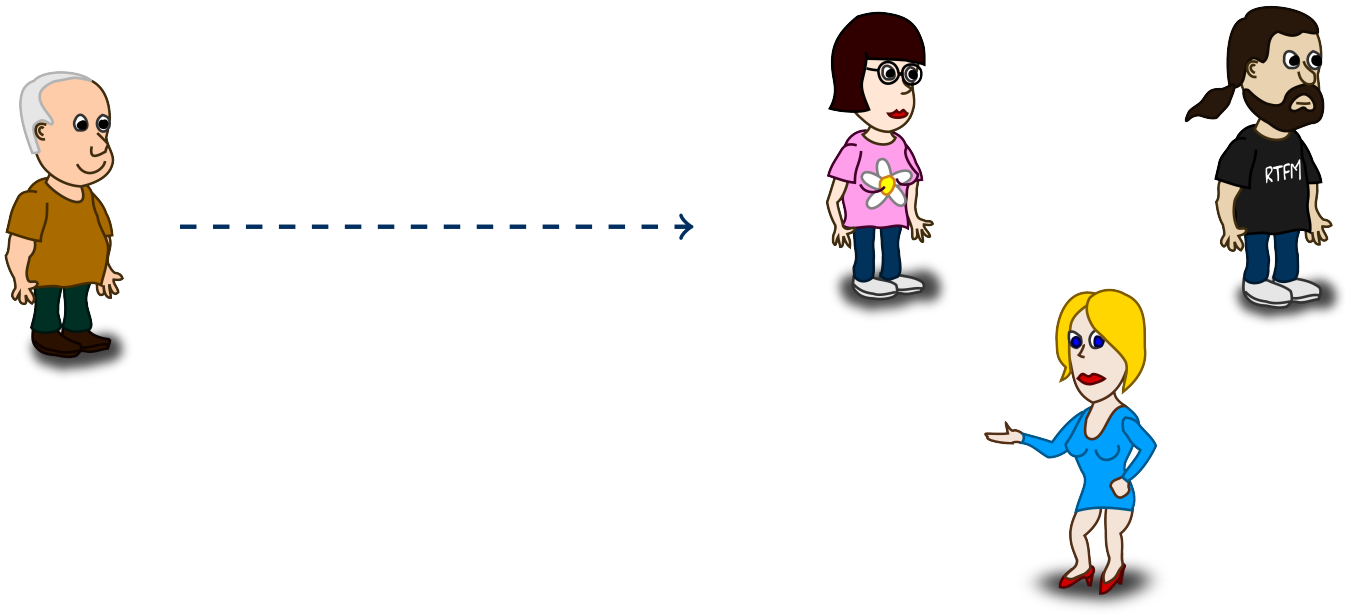
Bookmarklet als Schlüsselspeicherung

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

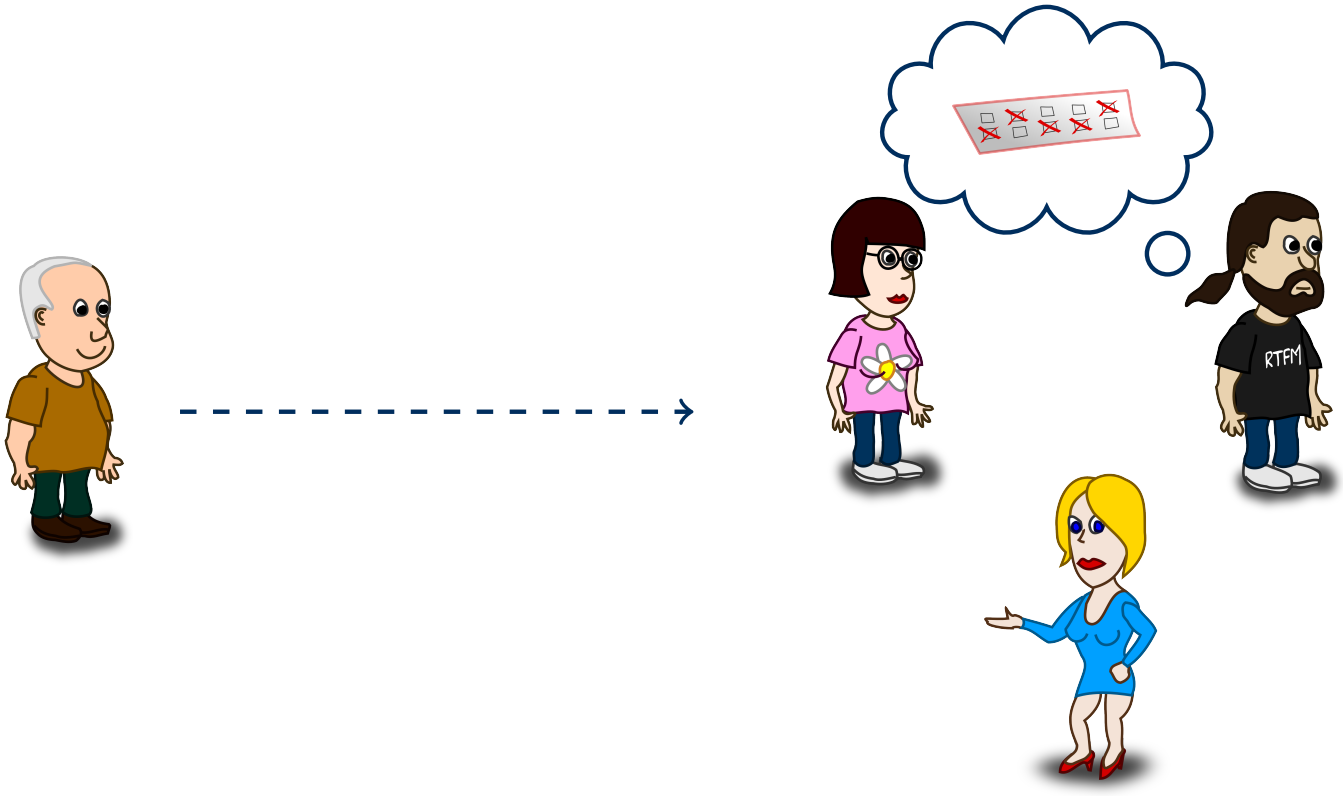
```
<a href="javascript:void(document.getElementById('key')
.value='0xDEADBEEF')">insert key</a>
```

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

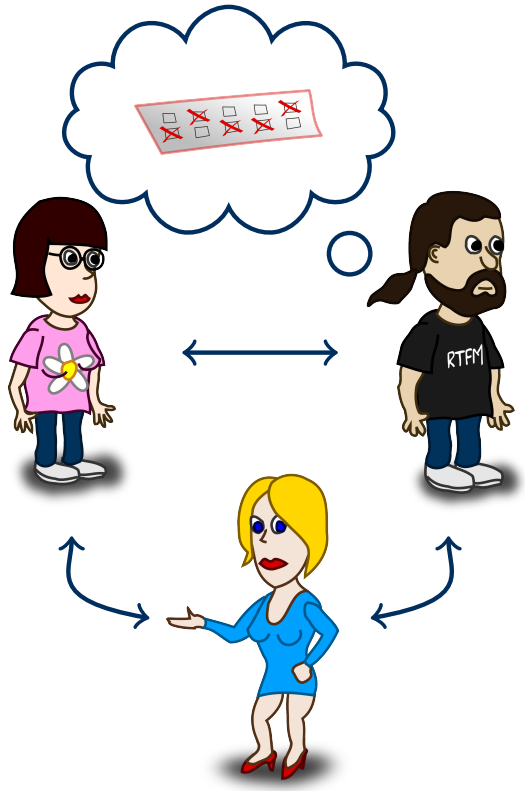
Dynamic Joining



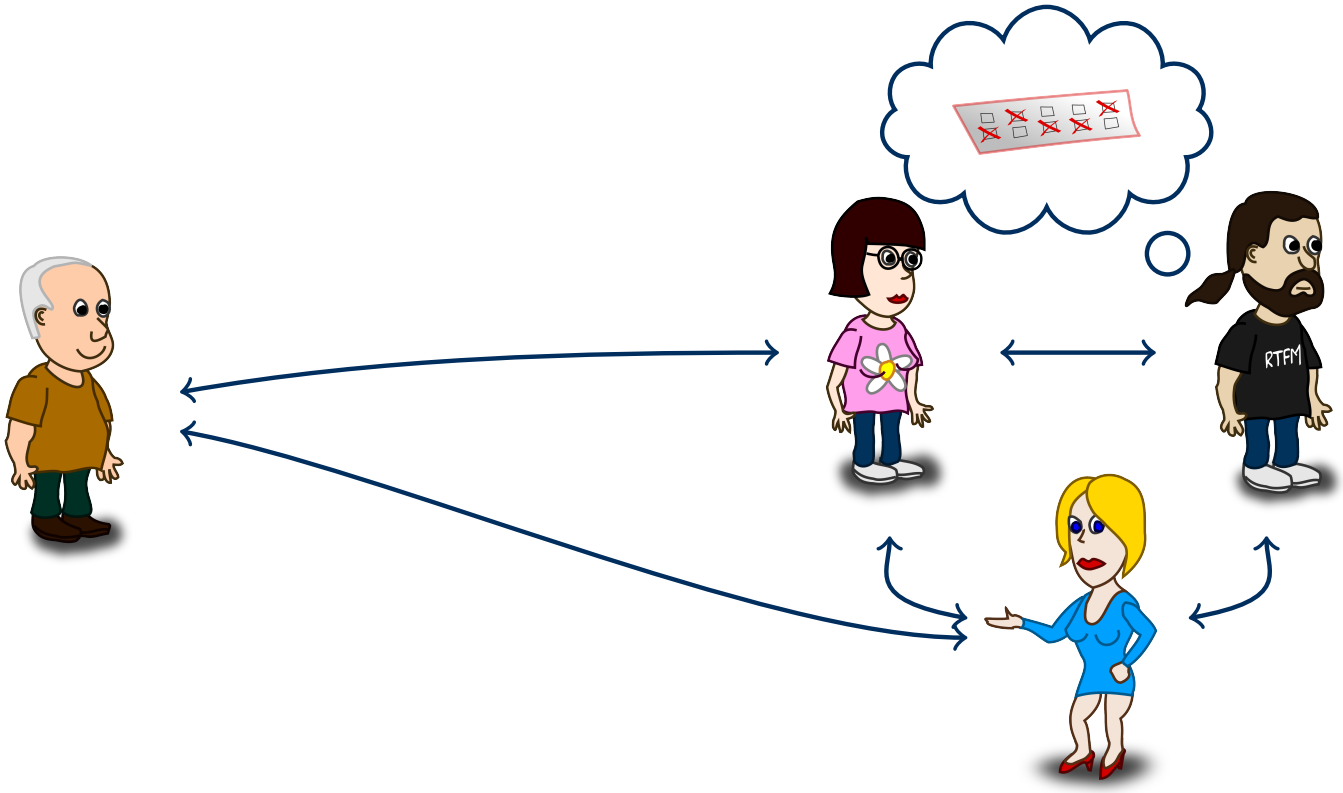
Dynamic Joining



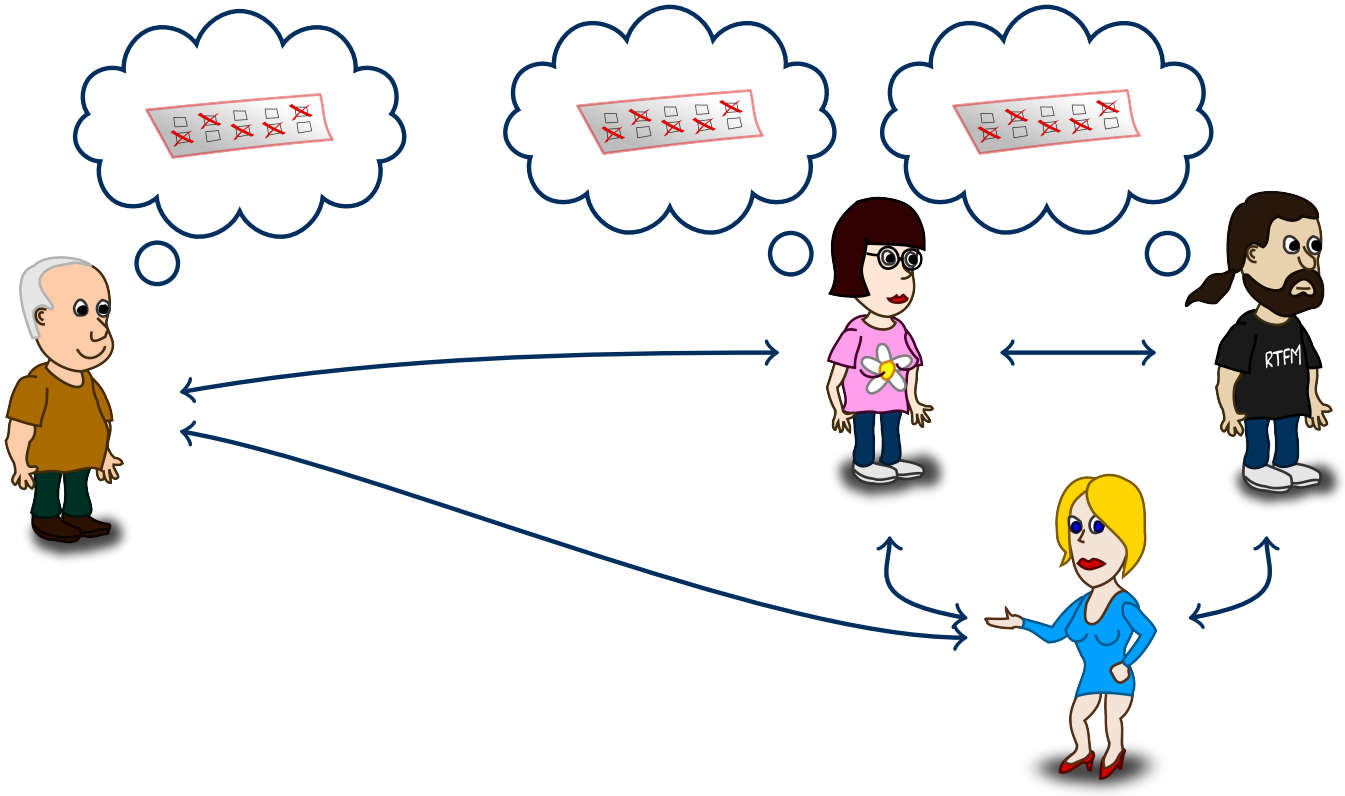
Dynamic Joining



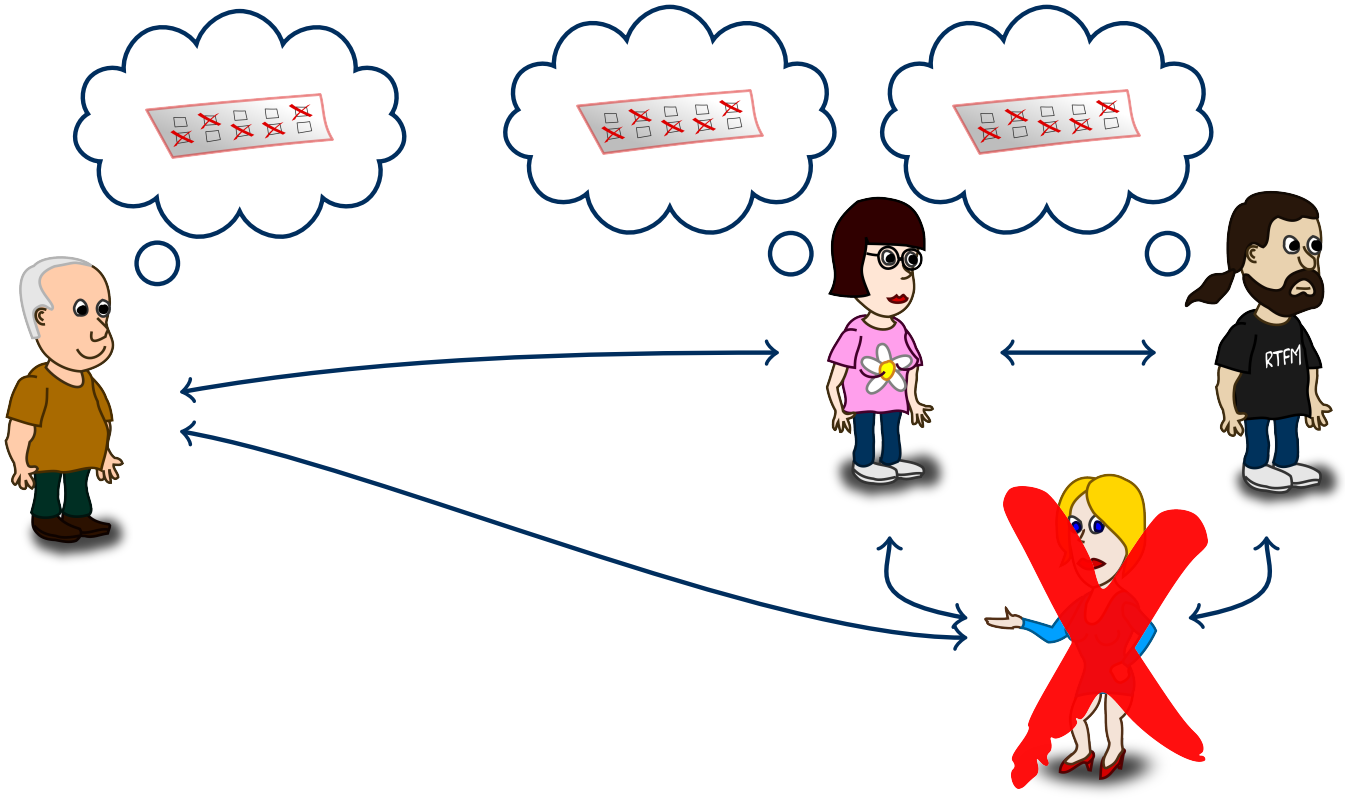
Dynamic Joining



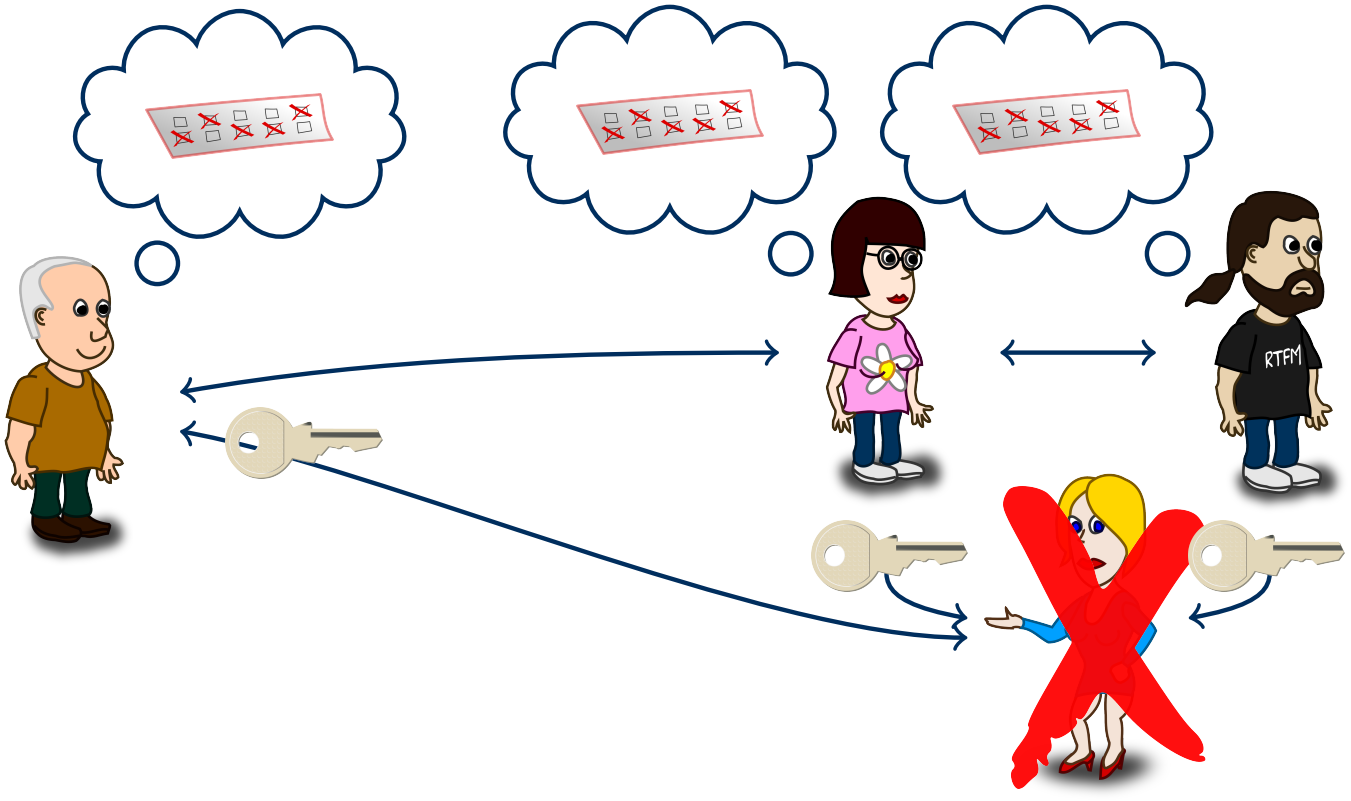
Dynamic Leaving



Dynamic Leaving



Dynamic Leaving



Computational Complexity

server

no expensive computation needed

client

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

Publikationen


„Privacy-Enhanced Web-Based Event Scheduling with Majority Agreement“, in Proc. of SEC 2011, IFIP AICT 354


„Privacy-Enhanced Event Scheduling“, mit R. Böhme, in Proc. of IEEE PASSAT 2009


„Open Research Questions of Privacy-Enhanced Event Scheduling“, in Proc. of iNetSec 2010, Springer/LNCS 6555


„Datenschutzfreundliche Terminplanung“, in Proc. of 26th CCC 2009


„Dudle – Privacy-enhanced Web 2.0 Event Scheduling“, in Privacy and Identity Management for Life, Kap. 24.3, Springer 2011


„Mechanisms supporting users' privacy and trust“, Tech. rep. D2.4.1, PrimeLife 2011


„Anonymous Credentials in Web Applications“, mit I. Scholz, Privacy and Identity Management for Life 2009, IFIP/AICT 320


„Privacy-respecting reputation for wiki users“, mit S. Pötzsch und S. Steinbrecher, in Proc. Trust Magement 2011, IFIP/AICT 358


„Trustworthiness of Online Content“, mit J. Camenisch, S. Steinbrecher, R. Leenes, S. Pötzsch, L. Klaming, in Privacy and Identity Management for Life, Kap. 3, Springer 2011