



# Privacy-Enhanced Single Event Scheduling

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

**Benjamin.Kellermann@tu-dresden.de**

D19E 04A8 8895 020A 8DF6

0092 3501 1A32 491A 3D9C



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

Bertinoro, Italy, September 2, 2010

# Single Event Scheduling

**Doodle®** Poll: Business D

**TelCo - 2009-10**

Voller Name	5. 08:00	6. 11:00	7. 10:00	7. 13:00	8. 10:00	8. 13:00
Joe	✓	✓		✓	✓	
Alice	✓		✓	✓		
Gustav	✓	✓			✓	
Beatrice		✓	✓		✓	✓
	3	3	2	2	3	1

Abschicken

**Free/Busy**

3/04/2006 Tue 09/05/2006 Wed 09/06/2006

12:00pm 3:00pm 9:00am 12:00pm 3:00pm 9:00am 12:00pm

Attendee

Sankar P

Hobbitts

Options

Tentative Busy Out of Office No Information

Start time: 09/02/2006 09:00 AM

End time: 09/02/2006 09:30 AM

Close

**Zeitfinder**

Herzlich Willkommen! Zeitfinder

Monatsansicht

JUNI 2009


KW MO DI MI DO FR SA SO

23 24 25 26 27 28 29 30

Anstehende Termine

# Single Event Scheduling

☐ Home  
☒ private  
☒ work  
☒ John  
☒ Peter  
☒ Julie  
☒ Tom



## 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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Count	2	3	2	4	3

3:00 8. 10:00 8. 13:00

	3	1
	<input type="checkbox"/>	<input type="checkbox"/>

Wed 09/06

3:00pm 9:00am 12

No Information

M v

M v

X Close

## E-Voting vs. Event Scheduling

	Vote
Candidate #1	
Candidate #2	✗
⋮	
Candidate #10	

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

one vote per column

# E-Voting vs. Event Scheduling

scales  
↓

	Vote
Candidate #1	
Candidate #2	✗
⋮	
Candidate #10	

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

one vote per column

# E-Voting vs. Event Scheduling

scales  
↓

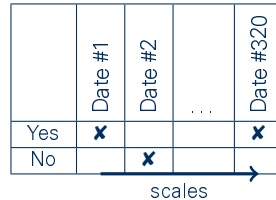
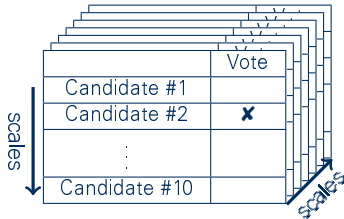
	Vote
Candidate #1	
Candidate #2	✗
⋮	
Candidate #10	

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

→ scales

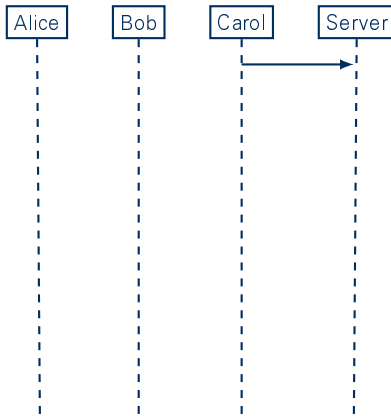
one vote per column

# E-Voting vs. Event Scheduling

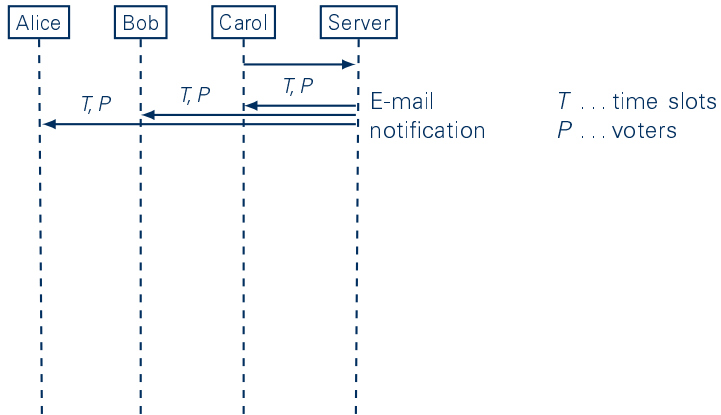


one vote per column

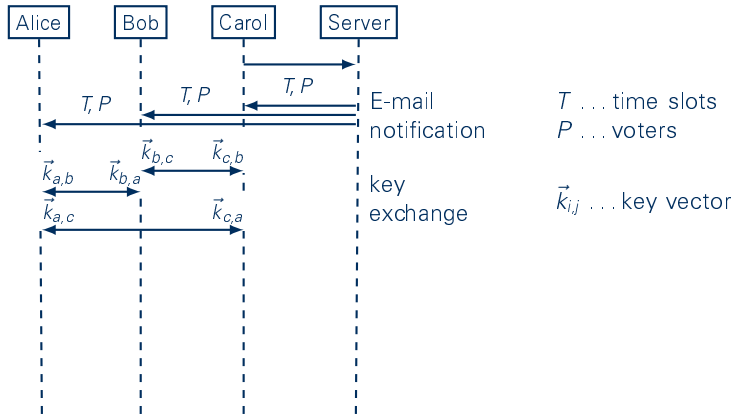
## Poll Initialization



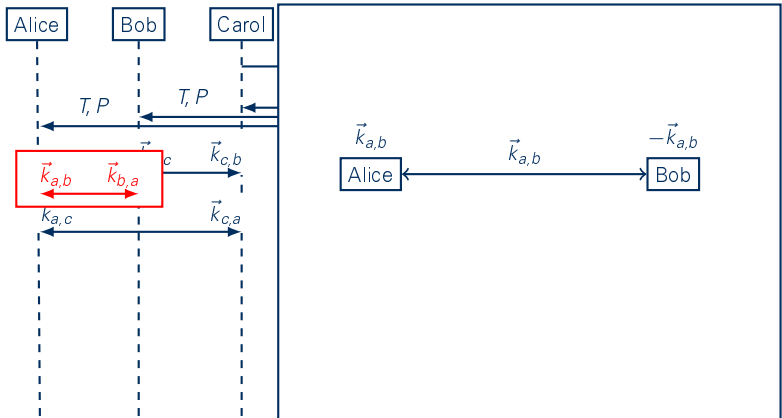
## Poll Initialization



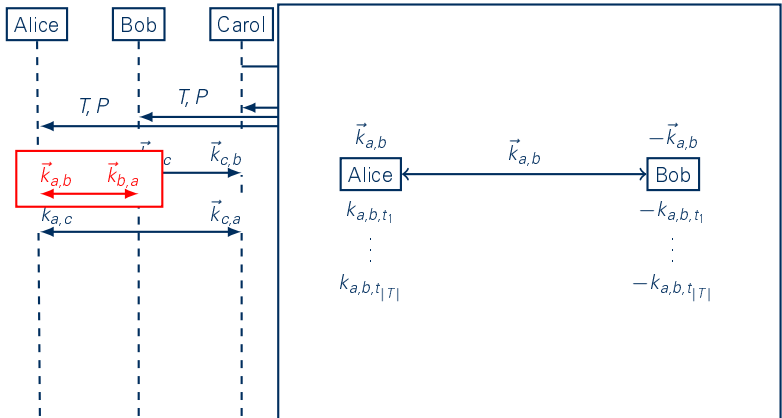
## Poll Initialization



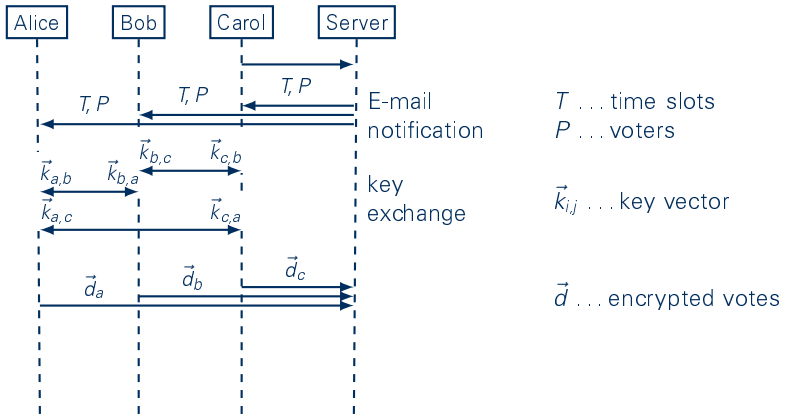
## Poll Initialization



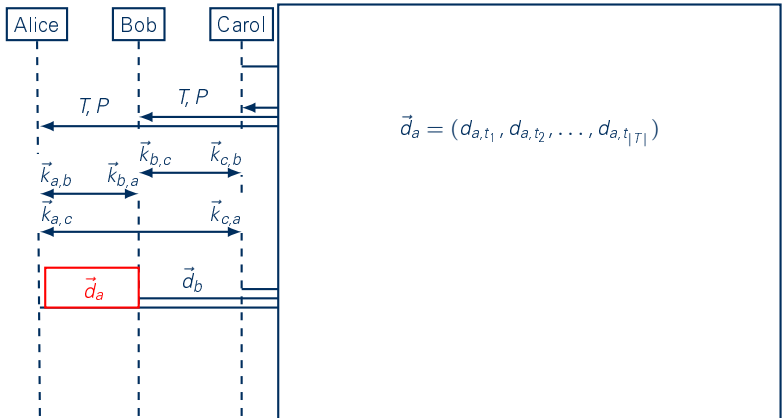
## Poll Initialization



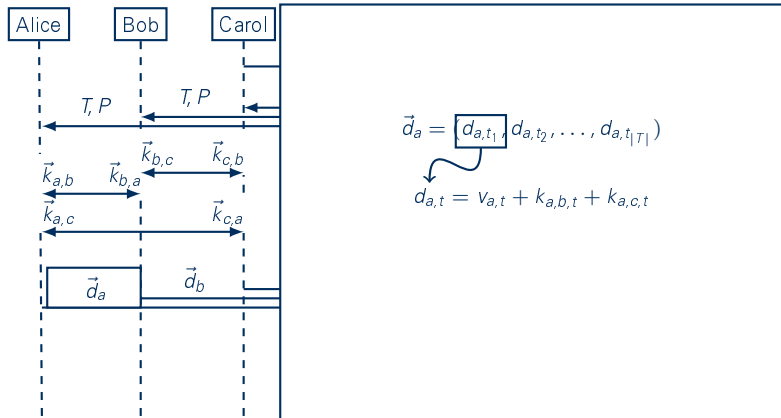
## Casting of Votes



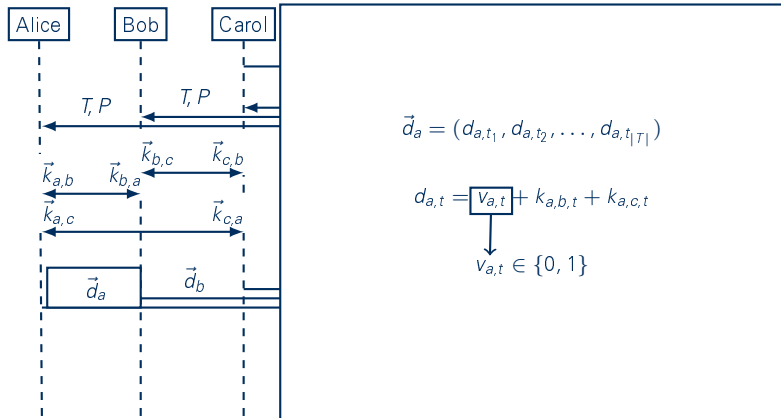
## Casting of Votes



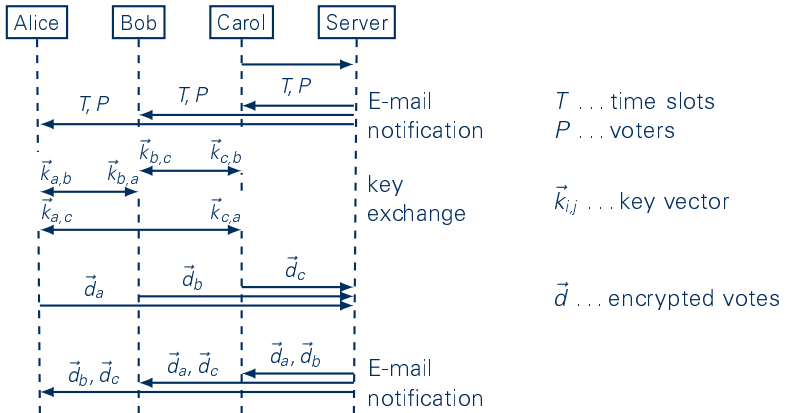
# Casting of Votes



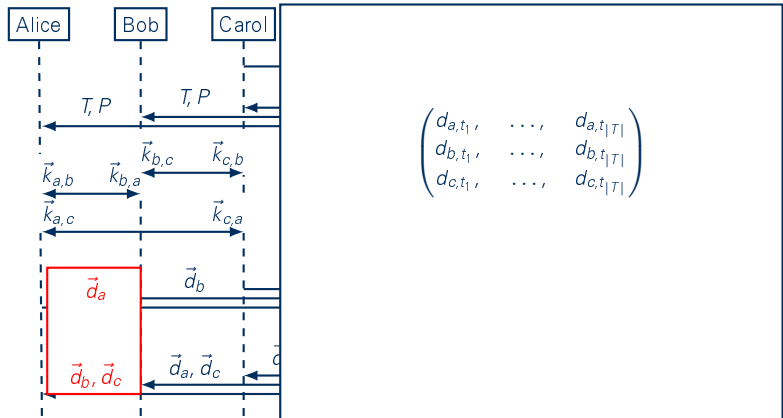
# Casting of Votes



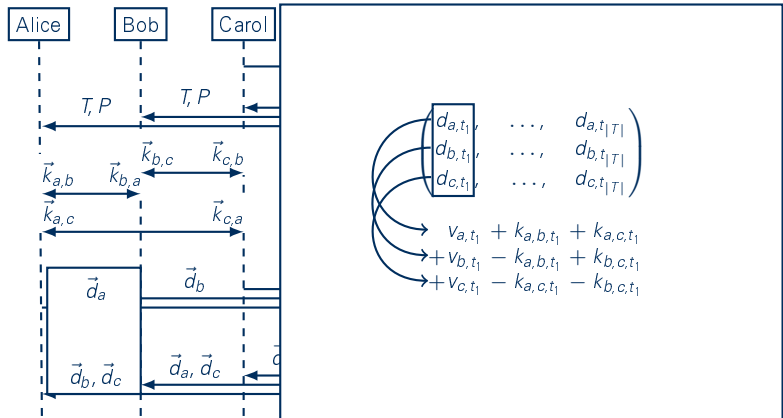
## Result Publication



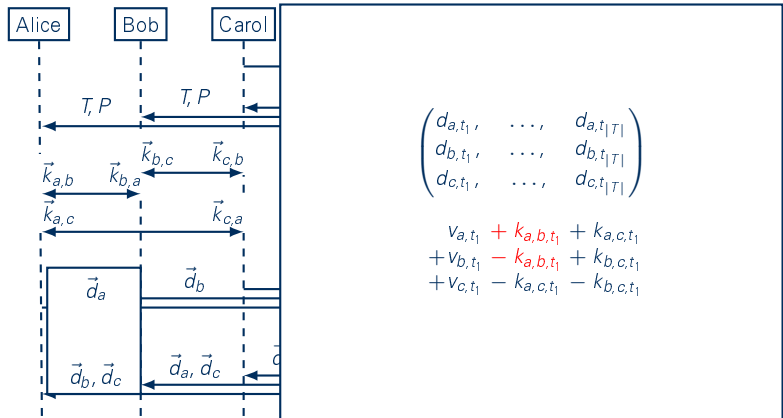
## Result Publication



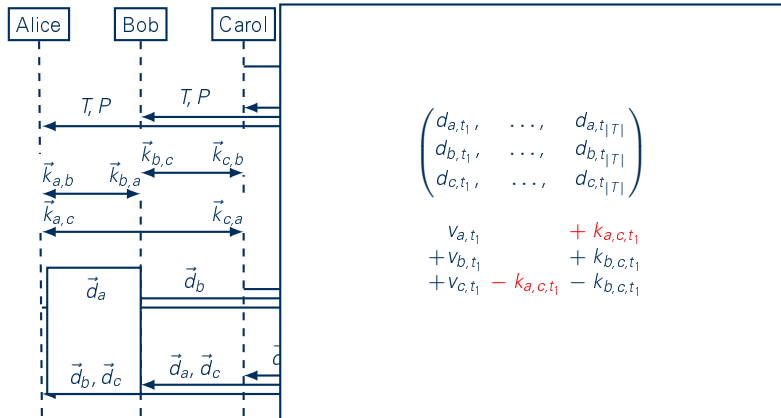
## Result Publication



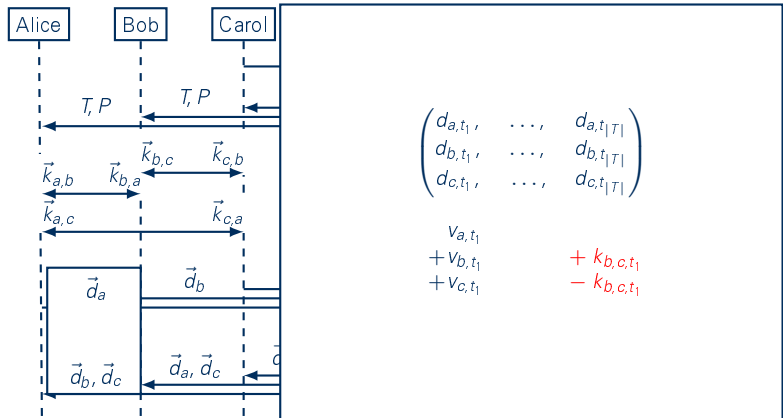
## Result Publication



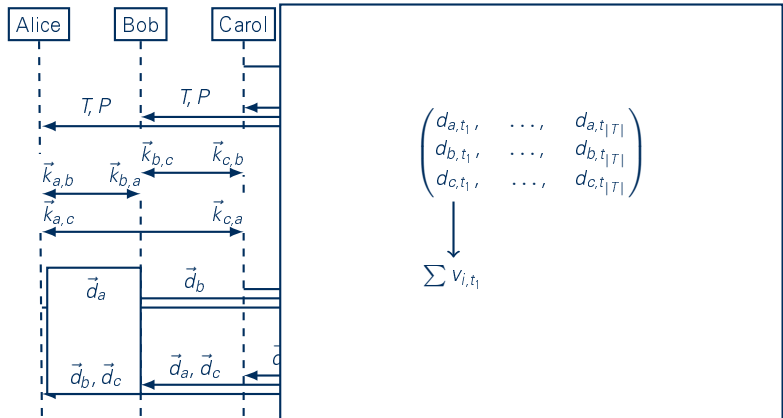
# Result Publication



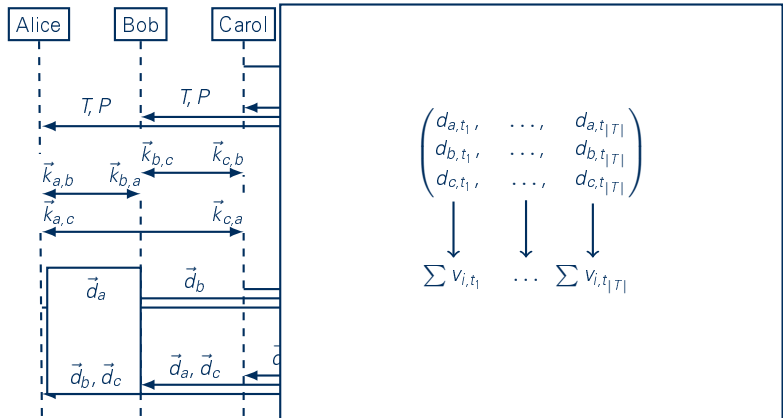
## Result Publication



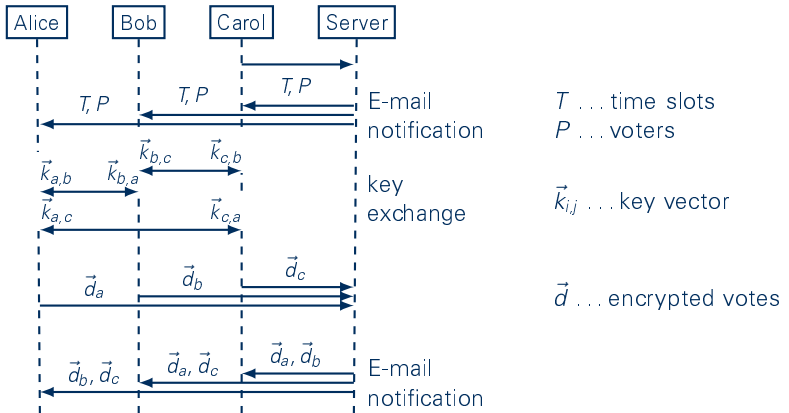
## Result Publication



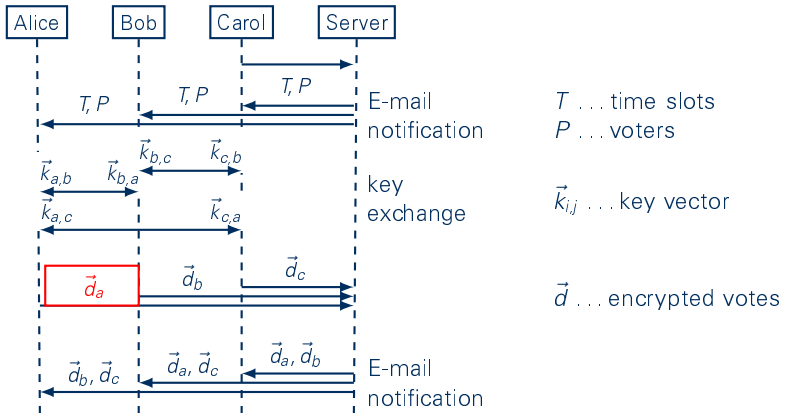
## Result Publication



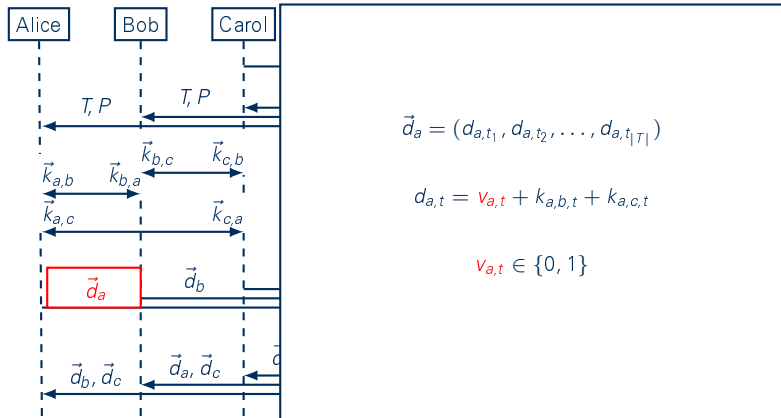
## Trying to Cheat



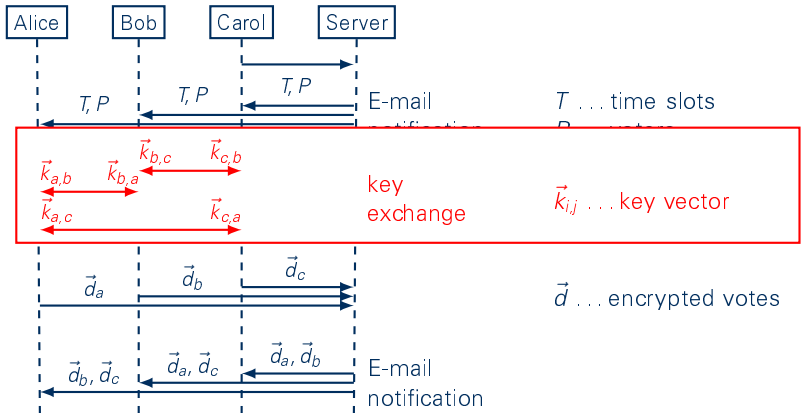
## Trying to Cheat



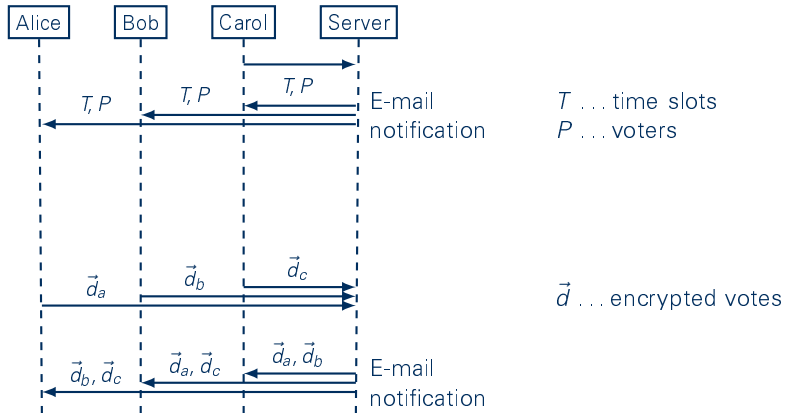
## Trying to Cheat



## Simplifying the Key Exchange



## Simplifying the Key Exchange



# 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

## Conclusion and Outlook

- ✓ novel scheme for privacy-enhanced single event scheduling
  - ▢ scales in number of time slots
  - ▢ no central trust entity
- ✓ main functionality implemented as Web 2.0 application
- Formal Definition / Proof
- Complex Decision Rules
- Updating / Revoking Votes
- Existing PKI usage





TECHNISCHE  
UNIVERSITÄT  
DRESDEN



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

# Thank you for your attention!

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

**Benjamin.Kellermann@tu-dresden.de**

D19E 04A8 8895 020A 8DF6

0092 3501 1A32 491A 3D9C



PrimeLife is a research project  
funded by the European Commis-  
sion's 7<sup>th</sup> Framework Programme

Bertinoro, Italy, September 2, 2010

# Privacy Problems

## Direct Inference

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

**Doodle®**

**Poll: Business Dinner**

		October 2009				
		Mon 19	Tue 20	Wed 21	Thu 22	Fri 23
		8:00 PM	8:00 PM	8:00 PM	8:00 PM	8:00 PM
John		OK		OK	OK	OK
Peter			OK		OK	OK
Julie		OK	OK		OK	
Tom			OK	OK	OK	OK
Your name	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Count		2	3	2	4	3

# Privacy Problems

## Direct Inference

**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	OK	
Julie	OK	OK	OK	OK	
Tom	OK	OK	OK	OK	
Your name	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Count	2	3	2	4	3

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

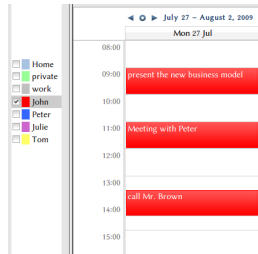
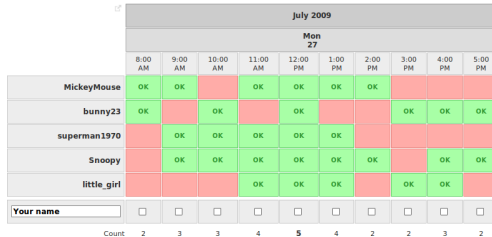
# Privacy Problems

## Indirect Inference

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

**Doodle®**

Poll: Chat



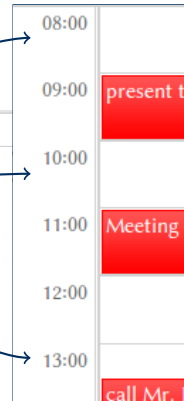
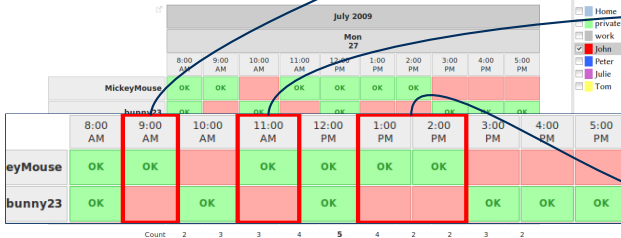
# Privacy Problems

## Indirect Inference

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

Doodle®

Poll: Chat



# Requirements

- Untrusted Server



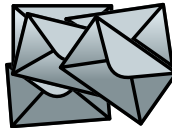
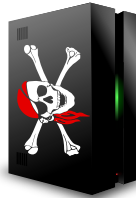
# Requirements

- Untrusted Server
- Privacy
- Verifiability



# Requirements

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



# Low Communication Complexity



config

## Schedule event: Select dates (Step 2 of 4)

Select days by clicking them (click as many date options as you wish to provide).

Tip: On average, 5 options are sufficient to successfully find a common date and time.

4

March 2010

5

Mon	Tue	Wed	Thu	Fri	Sat	Sun
		3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Selected dates:

Mar 15, 2010 ✗

Mar 16, 2010 ✗

Mar 17, 2010 ✗

Mar 18, 2010 ✗

Mar 19, 2010 ✗

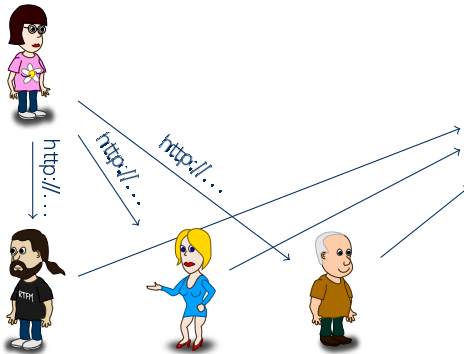
Back

Next

Options

Finish

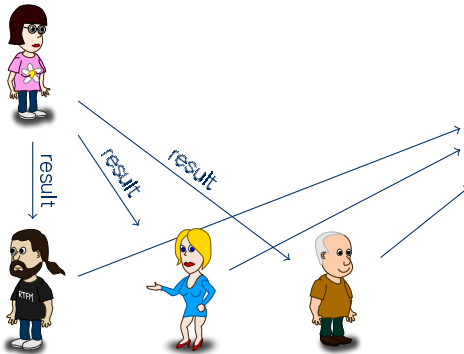
# Low Communication Complexity



**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		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Count		2	3	2	4	3

# Low Communication Complexity



**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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Count		2	3	2	4	3

# Superposed Sending

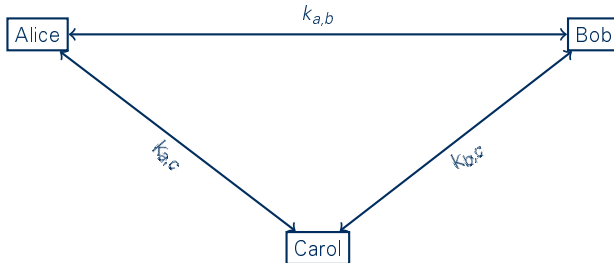
Alice

Bob

Carol

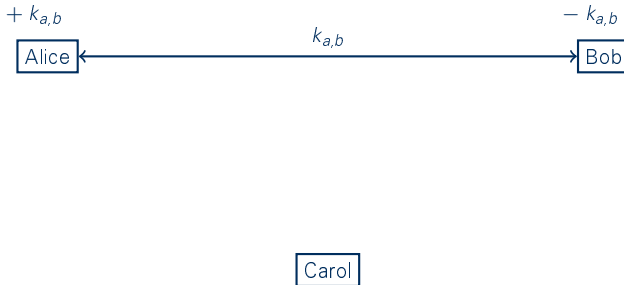
D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

# Superposed Sending



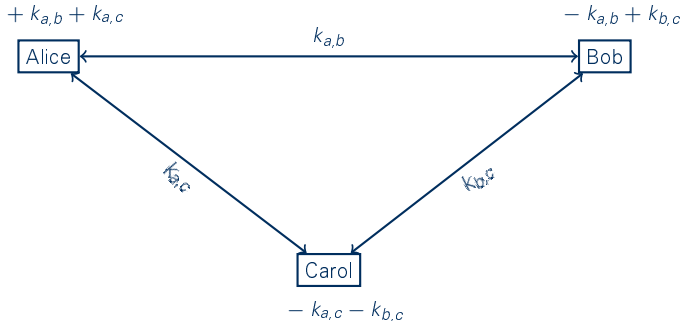
D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988

# Superposed Sending



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

# Superposed Sending



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

# Superposed Sending

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

Alice

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

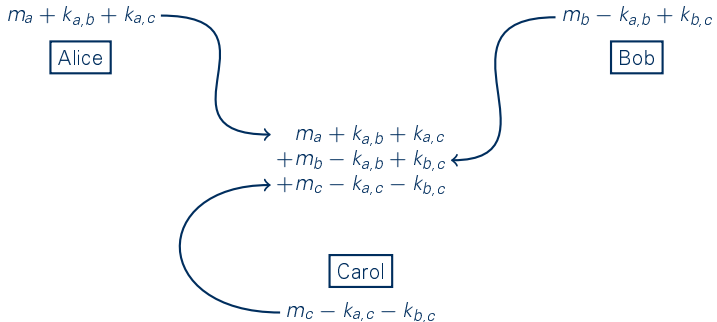
Bob

Carol

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

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

# Superposed Sending



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

# Superposed Sending

Alice

Bob

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

Carol

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

# Superposed Sending

Alice

Bob

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

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

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

Carol

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

# Superposed Sending

Alice

Bob

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

Carol

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


# Diffie–Hellman Key Agreement

Discrete  
Logarithm  
assumption

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

# Diffie–Hellman Key Agreement

Discrete  
Logarithm  
assumption

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


public

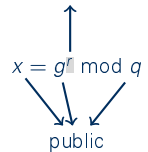
# Diffie–Hellman Key Agreement

Discrete  
Logarithm  
assumption

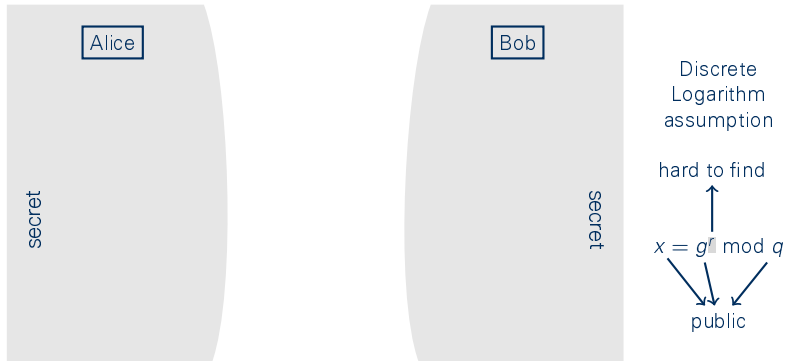
hard to find

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

public

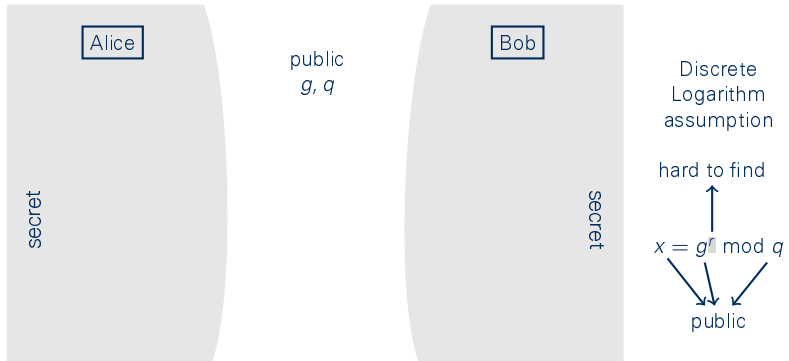


# Diffie–Hellman Key Agreement



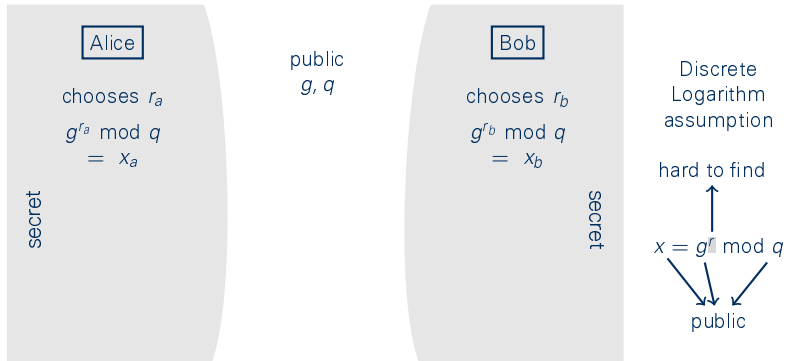
W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

# Diffie–Hellman Key Agreement



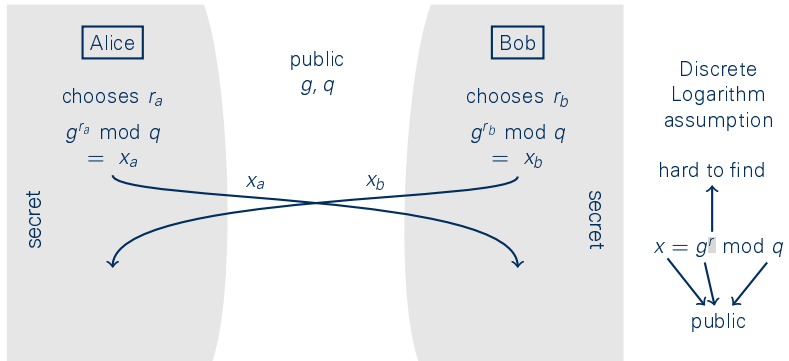
W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

# Diffie–Hellman Key Agreement



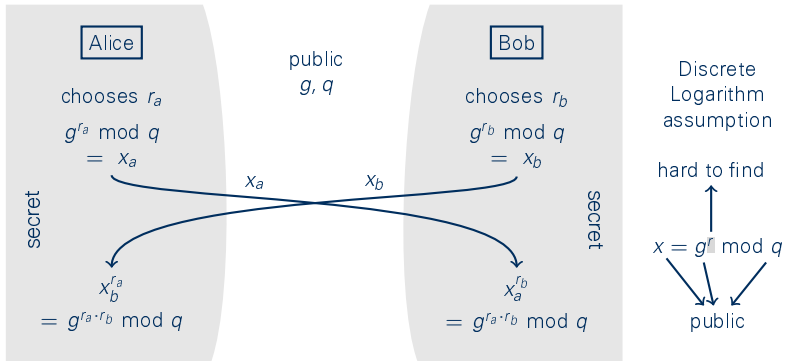
W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

# 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.

## Avoid –1 Cheaters

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

## Avoid –1 Cheaters

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

## Avoid –1 Cheaters

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

## Avoid -1 Cheaters

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

## Avoid –1 Cheaters

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

## Avoid –1 Cheaters

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

→ Alice	0	0	0	0
---------	---	---	---	---

→ Alice	0	1	0	0
---------	---	---	---	---

→ Alice	1	0	0	0
---------	---	---	---	---

$\Sigma$	1	1	0	0
----------	---	---	---	---

## Avoid –1 Cheaters

	T1	T2	T3	T4
Alice	1	1	0	0
Bob	0	1	1	0
Mallory	0	-1	1	0
$\Sigma$	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

$\Sigma$	1	2	1	0
----------	---	---	---	---

## Avoid –1 Cheaters

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

Alice	0	0	0	0
Bob	0	1	0	0

$$\Sigma \geq 0?$$

Alice	0	1	0	0
Bob	0	0	0	0

$$\Sigma \geq 0?$$

Alice	1	0	0	0
Bob	0	0	1	0

$$\Sigma \geq 0?$$

$\Sigma$	1	2	1	0
----------	---	---	---	---

## Avoid –1 Cheaters

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

Alice	0	0	0	0
Bob	0	1	0	0
Mallory	0	?	0	0
$\Sigma$		$\geq 0?$		
Alice	0	1	0	0
Bob	0	0	0	0
Mallory	0	?	0	0
$\Sigma$		$\geq 0?$		
Alice	1	0	0	0
Bob	0	0	1	0
Mallory	0	?	1	0
$\Sigma$		$\geq 0?$		
$\Sigma$	1	2	2	0

## Avoid +2 Cheaters

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

## Avoid +2 Cheaters

normal poll					check poll				
	T1	T2	T3	T4		T1	T2	T3	T4
Alice	1	1	0	0	Alice	0			
Bob	0	1	1	0	Bob	1			
Mallory	0	0	2	0	Mallory	1			
$\Sigma$	1	2	3	0	$\Sigma$	2			

## Avoid +2 Cheaters

normal poll					check poll				
	T1	T2	T3	T4		T1	T2	T3	T4
Alice	1	1	0	0	Alice		0		
Bob	0	1	1	0	Bob		1		
Mallory	0	0	2	0	Mallory		1		
$\Sigma$	1	2	3	0	$\Sigma$		2		

	$\Sigma$	3
--	----------	---

## Avoid +2 Cheaters

normal poll					check poll				
	T1	T2	T3	T4		T1	T2	T3	T4
Alice	1	1	0	0	Alice	0	0		
Bob	0	1	1	0	Bob	1	0		
Mallory	0	0	2	0	Mallory	1	1		
$\Sigma$	1	2	3	0	$\Sigma$	2	1		

$\Sigma$	3	3
----------	---	---

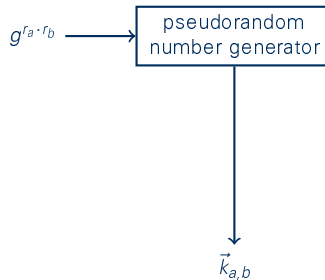
## Avoid +2 Cheaters

normal poll					check poll				
	T1	T2	T3	T4		T1	T2	T3	T4
Alice	1	1	0	0	Alice	0	0	1	
Bob	0	1	1	0	Bob	1	0	0	
Mallory	0	0	2	0	Mallory	1	1	-1	
$\Sigma$	1	2	3	0	$\Sigma$	2	1	0	

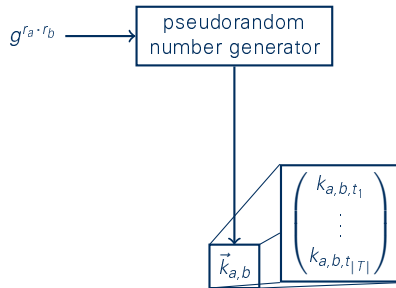
  

$\Sigma$	3	3	3
----------	---	---	---

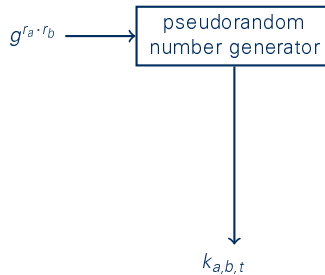
# Simplifying the Key Exchange



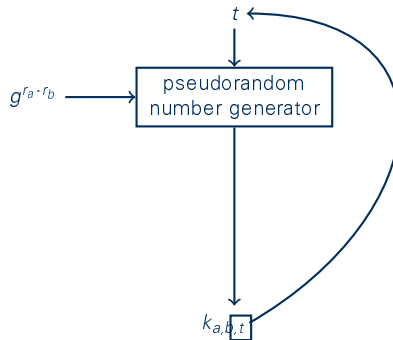
# Simplifying the Key Exchange



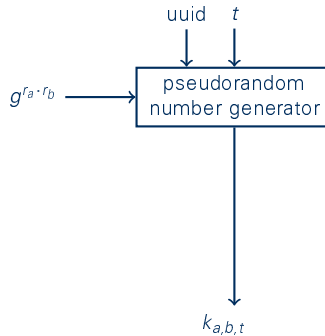
# Simplifying the Key Exchange



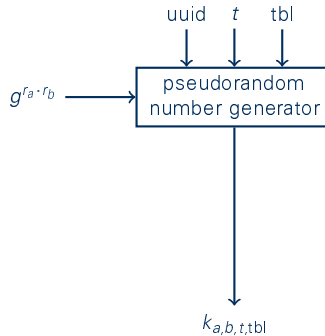
# Simplifying the Key Exchange



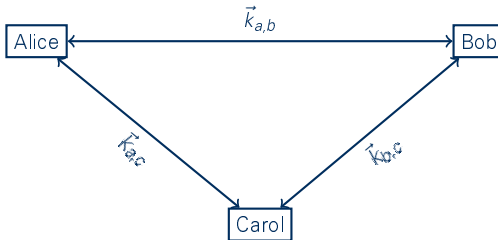
# Simplifying the Key Exchange



# Simplifying the Key Exchange



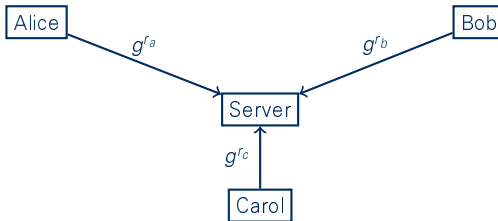
# Simplifying the Key Exchange



key exchange

# Simplifying the Key Exchange

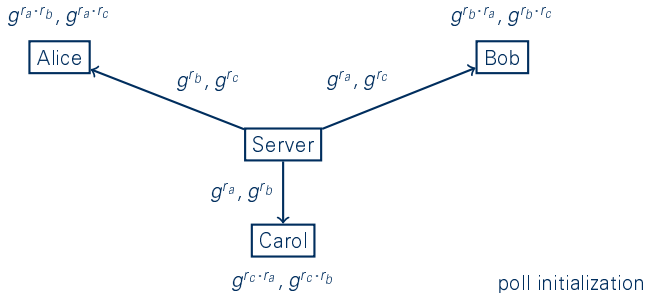
## Diffie–Hellman



registration

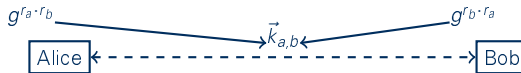
# Simplifying the Key Exchange

## Diffie-Hellman



# Simplifying the Key Exchange

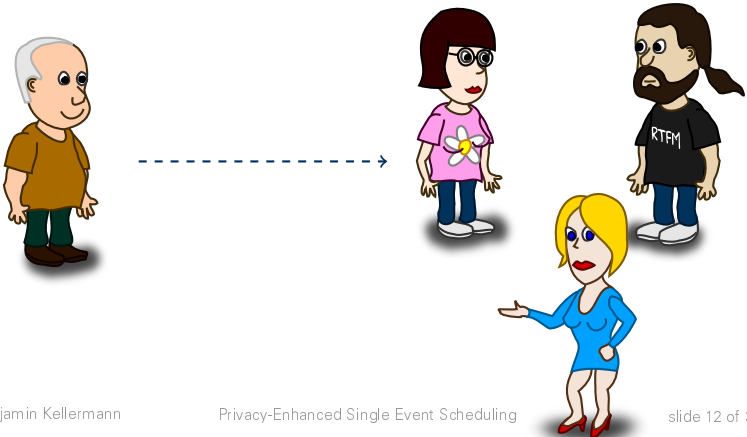
## Diffie-Hellman



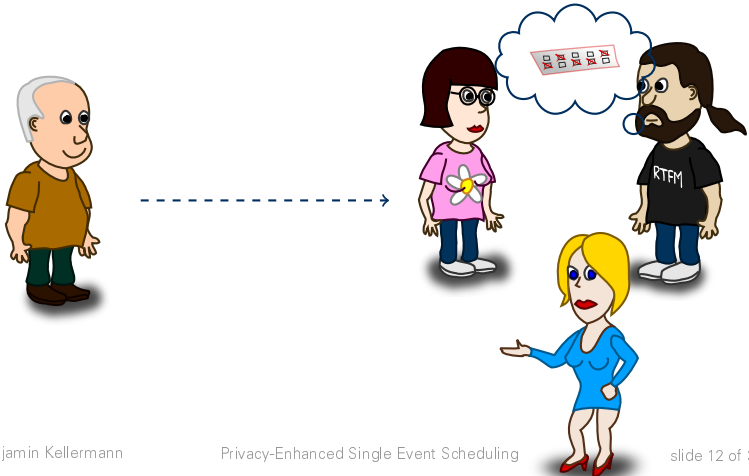
Carol

poll initialization

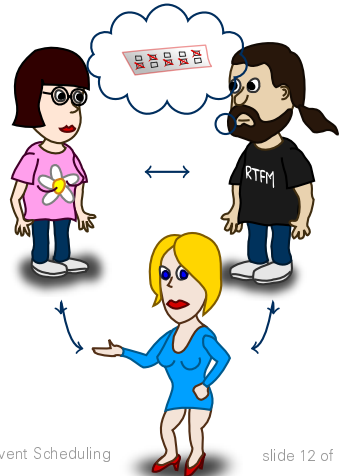
## Dynamic Joining



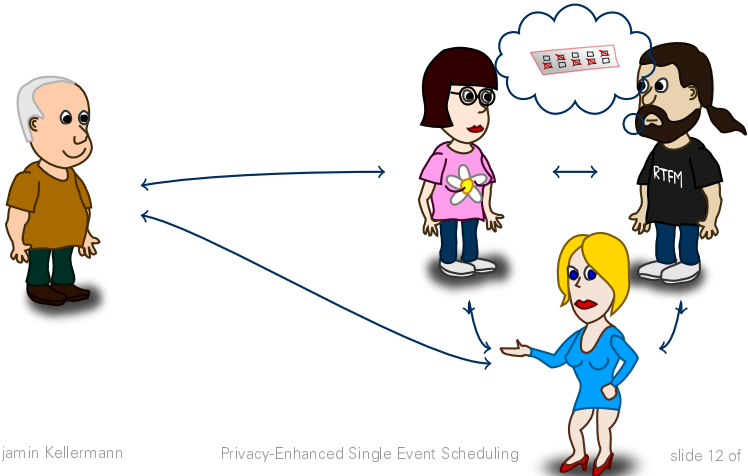
## Dynamic Joining



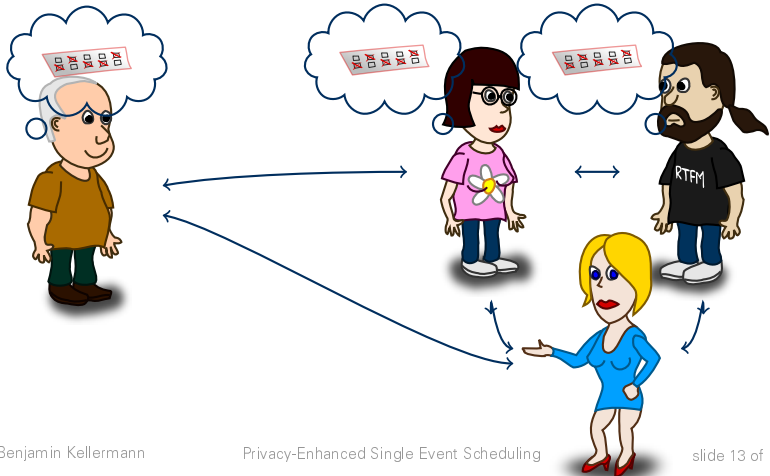
# Dynamic Joining



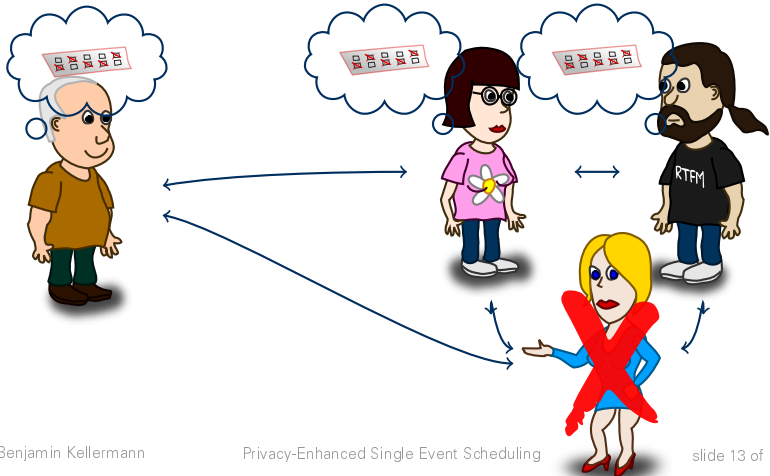
## Dynamic Joining



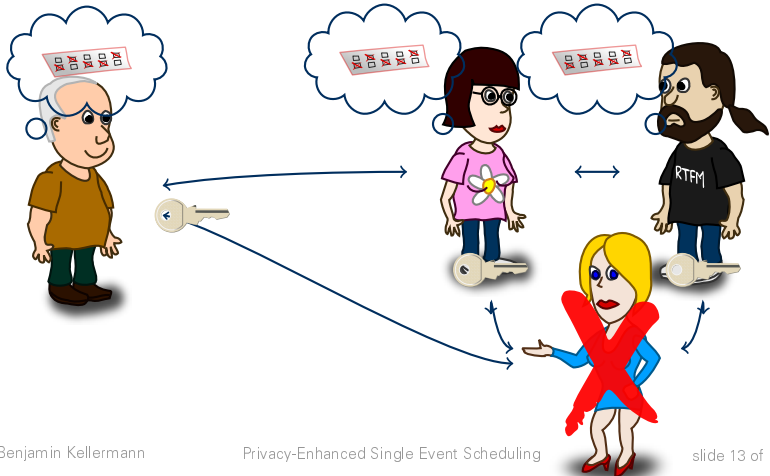
## Dynamic Leaving



## Dynamic Leaving



## Dynamic Leaving



# Phases

1. Poll Initialization
2. Casting of Votes
3. Result Publication
4. Result Verification

## Registration/Login

Name:

Password:

email:

Name:

Password:

# Poll Initialization

invite/delete participant

Alice

Alice  
Bob  
Carol  
Mallory

ve column

Oct 2009							→	→→
Mon	Tue	Wed	Thu	Fri	Sat	Sun		
			1	2	3	4		
5	6	7	8	9	10	11		
12	13	14	15	16	17	18		
19	20	21	22	23	24	25		
26	27	28	29	30	31			

Oct 2009				
Mon, 19	Tue, 20	Wed, 21	Thu, 22	Fri, 23
18:00	18:00	18:00	18:00	18:00
18:30	18:30	18:30	18:30	18:30
19:00	19:00	19:00	19:00	19:00
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Add	Add	Add	Add	Add

# Vote Casting

## Business Dinner

Oct 2009									
	Mon, 19	Tue, 20	Wed, 21		Thu, 22			Fri, 23	
Name	18:00	19:00	18:00	18:30	18:00	18:30	19:00	18:00	Last Edit
Alice	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="submit"/>
Bob	Participant has voted.								08.10, 10:30
Carol	Participant has voted.								08.10, 10:29
Mallory	Participant has not voted yet. <a href="#">kickout</a>								08.10, 10:21

# Vote Casting

## Business Dinner

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

# Dynamic Leaving

## Business Dinner

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

# Result Publication

## Business Dinner

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

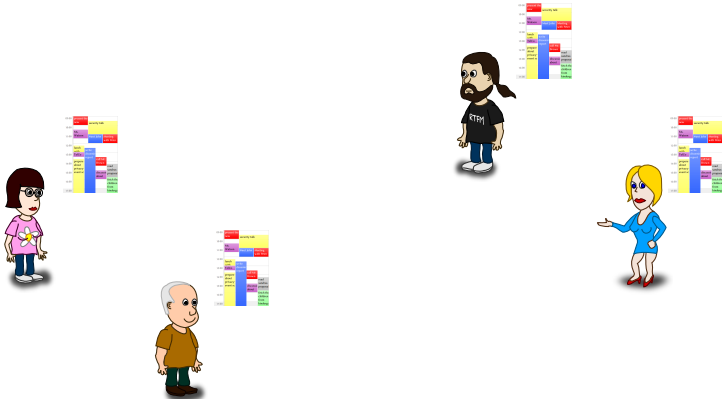
## Related Literature

- Distributed Constraint Satisfaction/Optimization Problem (DCSP/DCOP)
- E-Voting
  - ▢ Mix based
  - ▢ Blind Signature based
  - ▢ Homomorphic Encryption based
- Specific Literature
  - ▢ Herlea et al., "On Securely Scheduling a Meeting" (2001)
  - ▢ Kellermann and Böhme, "Privacy-Enhanced Event Scheduling" (2009)

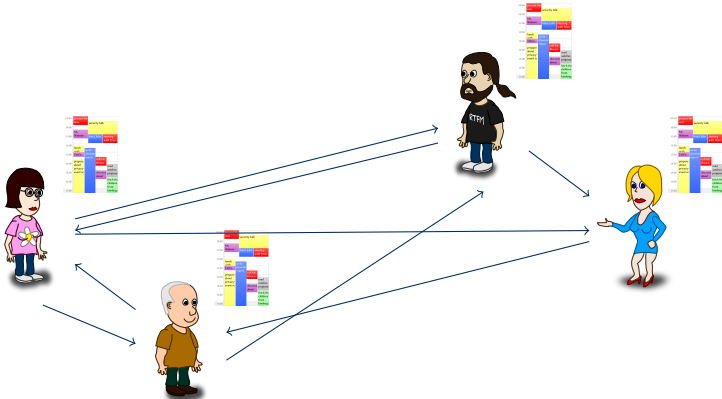
# Distributed Constraint Optimization Problem



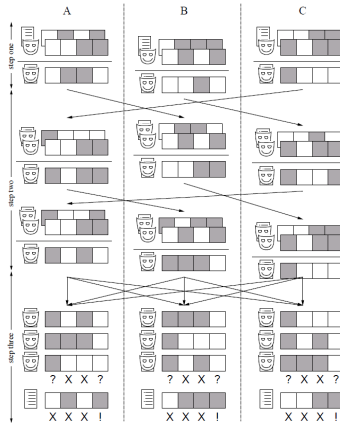
# Distributed Constraint Optimization Problem



# Distributed Constraint Optimization Problem



# Herlea et al. (2001)



# Security Definition / Proof of Correctness

- E-Voting traditionally well defined
- DCOP/DSCP by Franzin and Greenstadt
- ➡ Adoption to Privacy-Enhanced Event Scheduling needed

# Guaranteed Poll Termination

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

# Guaranteed Poll Termination

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

# Complex Decision Rules

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

## Preferences instead of Binary Choice

**Your name**





1  
2  
3  
4  
5

12:00 PM - 2:00 PM Thursday, March 11, 2010

# Updating / Revoking Votes

**Doodle®**

**Poll: Business Dinner**


		October 2009				
		Mon 19	Tue 20	Wed 21	Thu 22	Fri 23
		8:00 PM	8:00 PM	8:00 PM	8:00 PM	8:00 PM
	Alice	OK		OK	OK	OK
	Bob		OK		OK	OK
	Carol	OK	OK		OK	
	Dave		OK	OK	OK	OK
Your name <input type="text"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Count		2	3	2	4	3

## Dynamic Insertion of Time Slots

**Doodle®**

**Poll: Business Dinner**

October 2009					
	Mon 19	Tue 20	Wed 21	Thu 22	Fri 23
	8:00 PM	8:00 PM	8:00 PM	8:00 PM	8:00 PM
Alice	OK		OK	OK	OK
Bob		OK		OK	OK
Carol	OK	OK		OK	
Dave		OK	OK	OK	OK
<input type="text" value="Your name"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Count	2	3	2	4	3



**Mon 26**

## Existing PKI usage



## More Features

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

