



TECHNISCHE
UNIVERSITÄT
DRESDEN



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

Open Research Questions in Privacy-Enhanced Event Scheduling

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 7th Framework Programme

Sofia, Bulgaria, March 05, 2010

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! Mein Kalender

Monatsansicht

JUNI 2009

KW MO DI MI DO FR SA SO

23 24 25 26 27 28 29 30

Anstehende Termine

Home

private

work

John

Peter

Julie

Tom

Watson

Meet John

Meeting with Peter

lunch with TelCo

write

prepare about privacy-event sc

Privacy Problems

Direct Inference

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

Doodle®

Poll: Business Dinner

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

Privacy Problems

Direct Inference

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	☐	☐	☐	☐	☐
Count	2	3	2	4	3

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

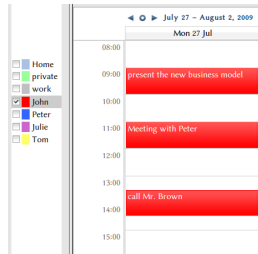
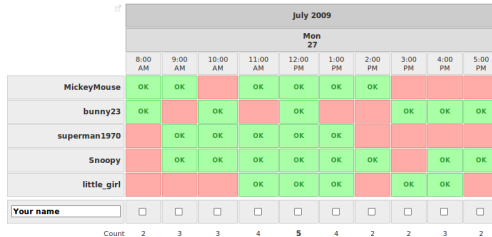
Privacy Problems

Indirect Inference

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

Doodle®

Poll: Chat



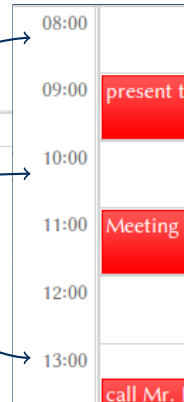
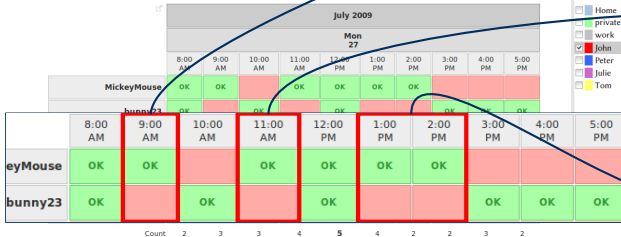
Privacy Problems

Indirect Inference

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

Doodle®

Poll: Chat



Requirements

- Untrusted Server



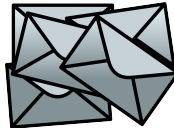
Requirements

- Untrusted Server
- Privacy
- Verifiability



Requirements

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

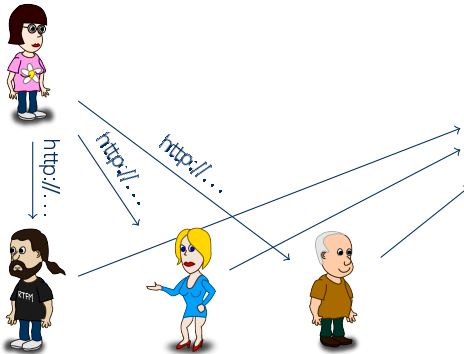


Related Literature

- 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)

« Back Next » Options Finish

Low Communication Complexity



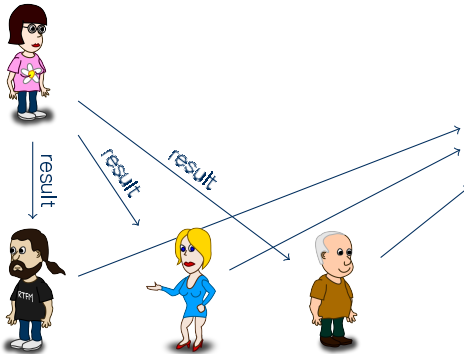
Doodle

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	☐	☐	☐	☐	☐

Count 2 3 2 4 3

Low Communication Complexity



Doodle

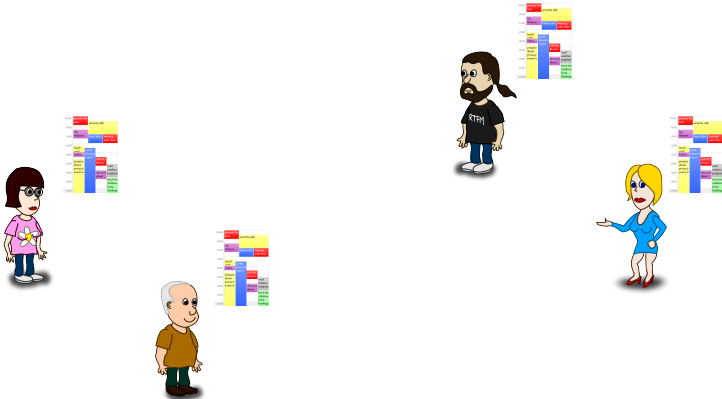
Poll: Business Dinner

		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		☐	☐	☐	☐	☐
Count		2	3	2	4	3

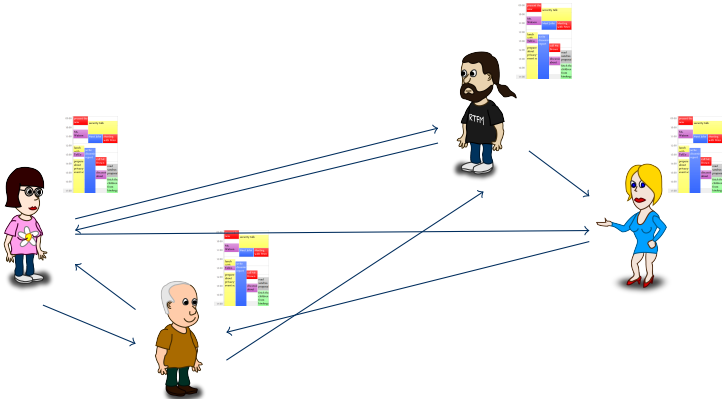
Distributed Constraint Optimization Problem



Distributed Constraint Optimization Problem



Distributed Constraint Optimization Problem



E-Voting vs. Event Scheduling

	Vote
Candidate #1	
Candidate #2	x
⋮	
Candidate #10	

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

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
↓

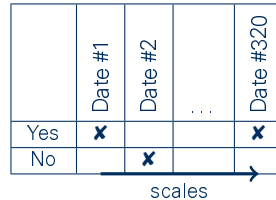
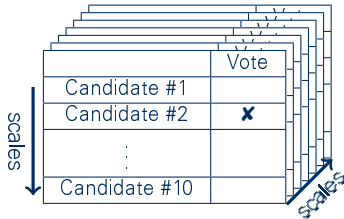
	Vote
Candidate #1	
Candidate #2	✗
⋮	
Candidate #10	

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

→ scales

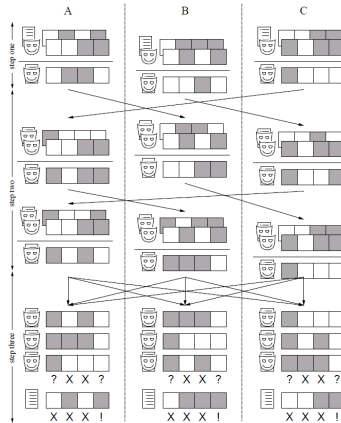
one vote per column

E-Voting vs. Event Scheduling

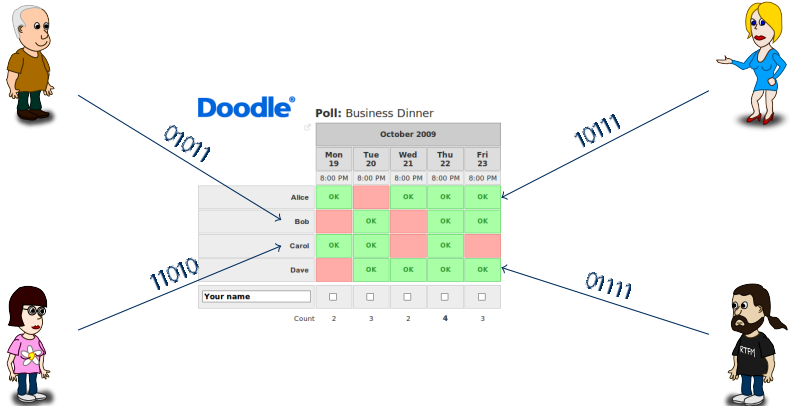


one vote per column

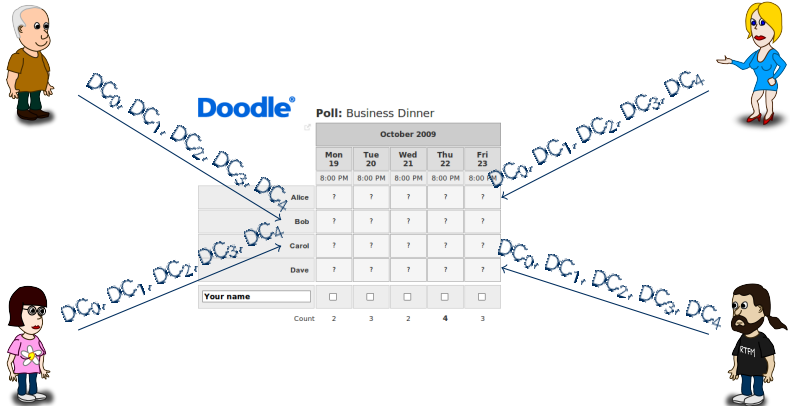
Herlea et al. (2001)



Kellermann and Böhme (2009)



Kellermann and Böhme (2009)



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

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		☐	☐	☐	☐	☐
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
Your name	☐	☐	☐	☐	☐
Count	2	3	2	4	3



Mon 26

Existing PKI usage



Conclusion

- some Literature on Privacy-Enhanced Single Event Scheduling
 - ▢ Lots of DCSP/DCOP Literature
 - ▢ Lots of E-Voting Literature
 - ▢ Few Specific Literature
- Open Problems
 - ▢ Formal Definition / Proof
 - ▢ Complex Decision Rules
 - ▢ Preferences instead of Binary Choice
 - ▢ Updating / Revoking Votes
 - ▢ Existing PKI usage



Thank you for your attention!

Discussion

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 7th Framework Programme

Sofia, Bulgaria, March 05, 2010