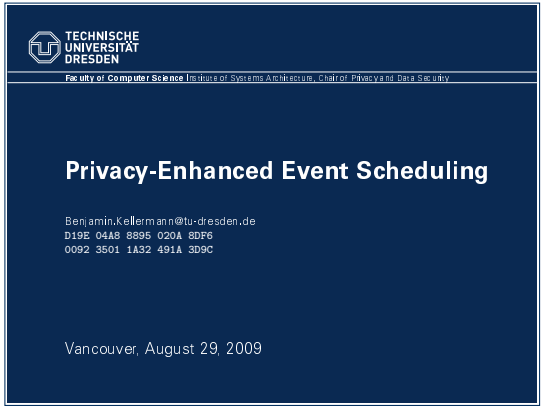
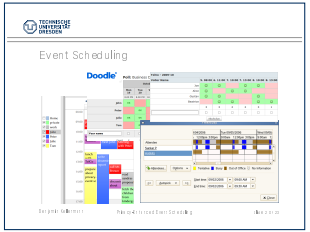


1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

General:

- **have** voted
- can participate → is available

This slide:

- first explain the term "Privacy-Enhanced Event Scheduling"

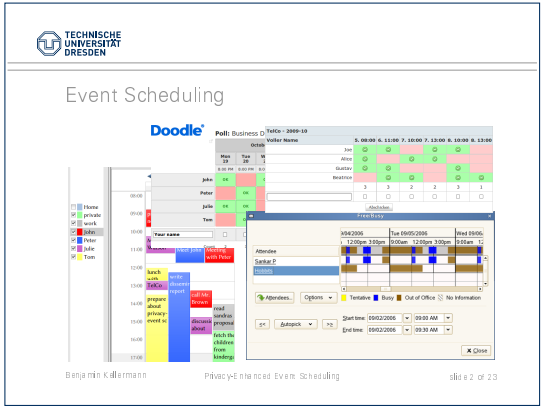
TECHNISCHE UNIVERSITÄT DRESDEN

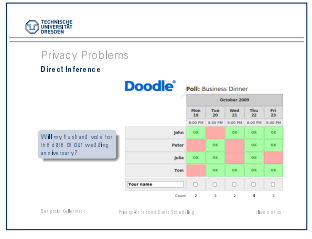
Faculty of Computer Science Institute of Systems Architecture, Chair of Privacy and Data Security

Privacy-Enhanced Event Scheduling

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

Vancouver, August 29, 2009





1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

Problem Statement
- Event Scheduling
  - Direct Inference
  - Indirect Inference
  - Requirements
  - E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

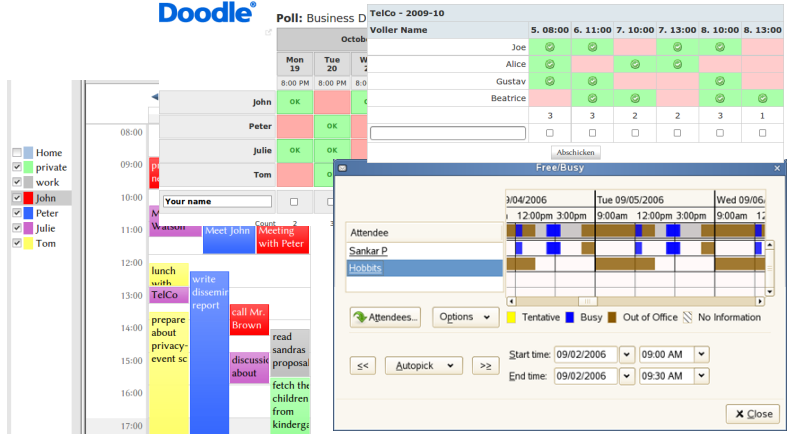
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

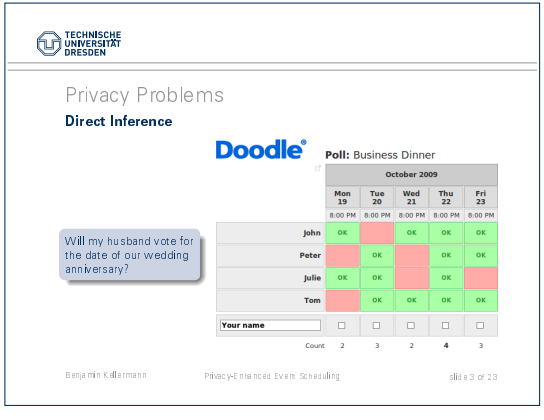
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

- Meeting, TelCo
- MS exchange, Outlook, Thunderbird, doodle
- common in all solutions: publish availability pattern
- next: define "**Privacy-Enhanced** Event Scheduling"
- 2 different privacy problems occur

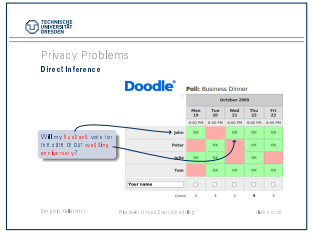
Event Scheduling





- business dinner
- john's wife asks herself

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Privacy Problems

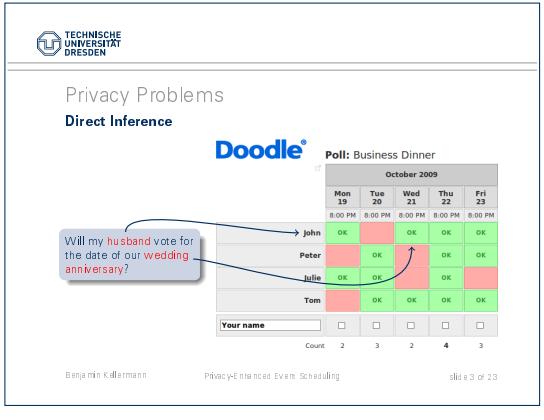
Direct Inference

Doodle

Poll: Business Dinner

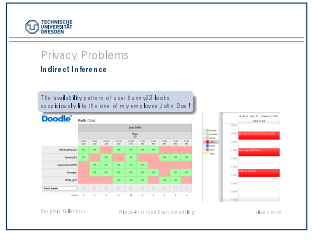
	October 2009				
	Mon 19	Tue 20	Wed 21	Thu 22	Fri 23
	8:00 PM	8:00 PM	8:00 PM	8:00 PM	8:00 PM
John	OK		OK	OK	OK
Peter		OK		OK	OK
Julie	OK	OK		OK	
Tom		OK	OK	OK	OK
Your name	☐	☐	☐	☐	☐
Count	2	3	2	4	3

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



- business dinner
- john's wife asks herself

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Privacy Problems

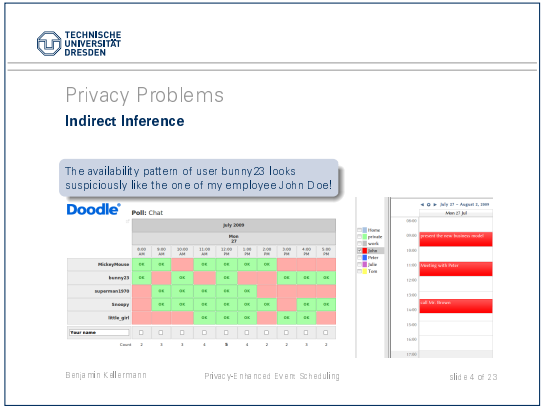
Direct Inference

Doodle®

Poll: Business Dinner

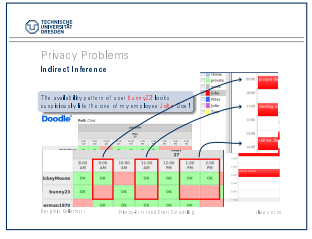
	October 2009				
	Mon 19	Tue 20	Wed 21	Thu 22	Fri 23
	8:00 PM	8:00 PM	8:00 PM	8:00 PM	8:00 PM
John	OK		OK	OK	OK
Peter		OK		OK	OK
Julie	OK	OK		OK	
Tom		OK	OK	OK	OK
Your name	☐	☐	☐	☐	☐
Count	2	3	2	4	3

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



- matching 2 information sources
- next: TOC!

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

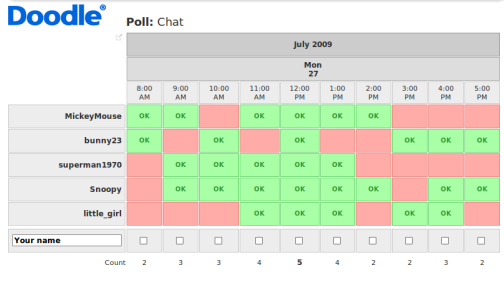
Conclusion and Outlook
- Conclusion and Outlook

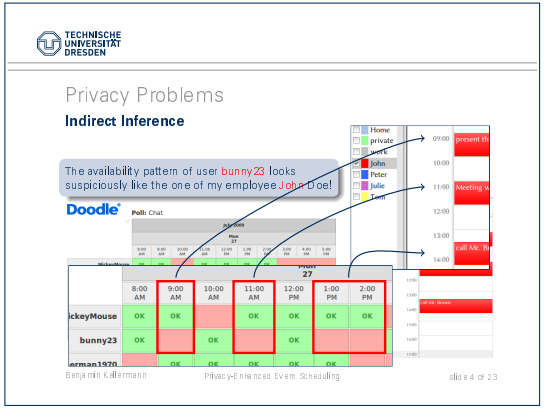
TECHNISCHE UNIVERSITÄT DRESDEN

Privacy Problems

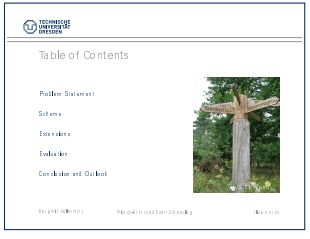
Indirect Inference

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





- matching 2 information sources
- discussing the paper at lunch
- wife of my colleague:
- boss unavailable, MS Exchange, appointment same size
- next: TOC!

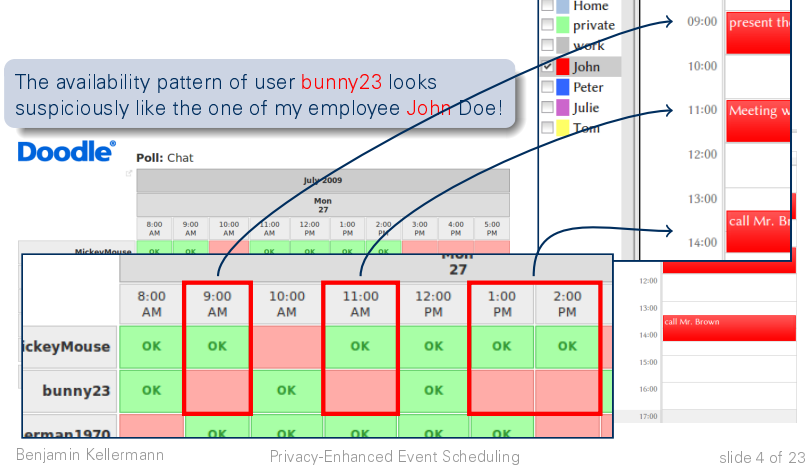


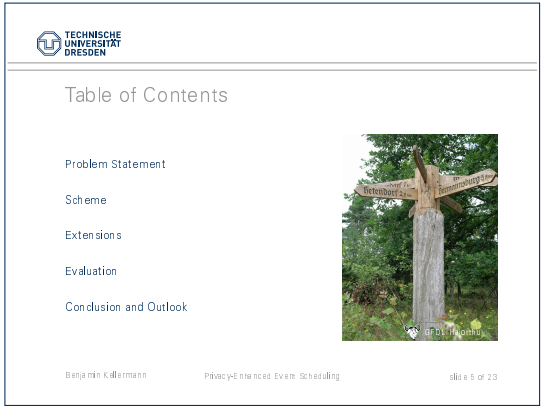
Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

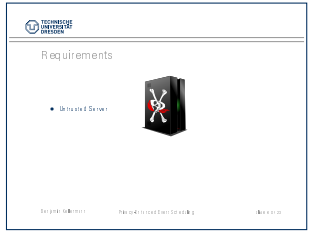
Privacy Problems

Indirect Inference





1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

- already defined the term
- next: requirements + distinguish from E-Voting
- present basic scheme
- extend → make more practical
- evaluate requirements

TECHNISCHE UNIVERSITÄT DRESDEN

Table of Contents

Problem Statement

Scheme

Extensions

Evaluation

Conclusion and Outlook

Requirements

- Untrusted Server

- no trusted entity

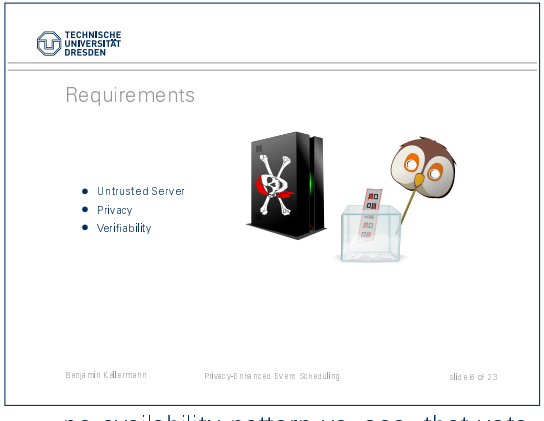
1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

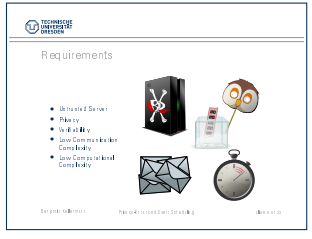
Requirements

- Untrusted Server



- no availability pattern vs. see, that vote counted

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

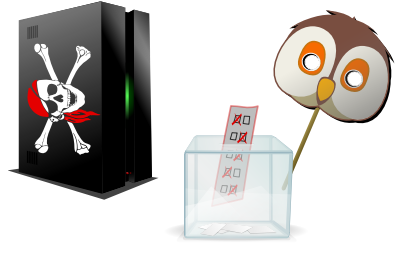
Evaluation
- Evaluation

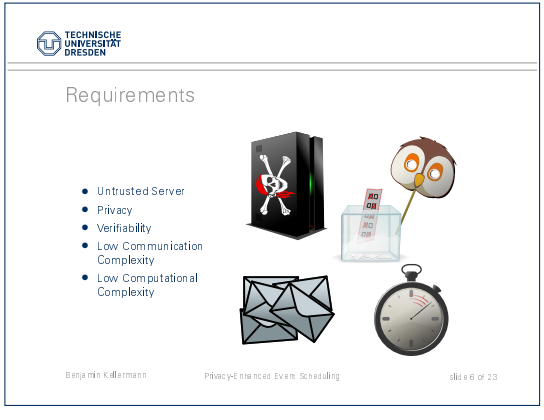
Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Requirements

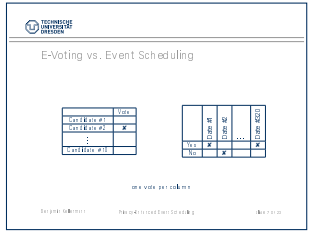
- Untrusted Server
- Privacy
- Verifiability





- few messages: necessary for usability
- similar to E-Voting (next: comparison)

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Requirements

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

E-Voting vs. Event Scheduling

	Vote
Candidate #1	
Candidate #2	✘
⋮	
Candidate #10	

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

one vote per column

- nicht dates sagen → time slots
- $40 \cdot 4 \cdot 2 = 320$

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

E-Voting vs. Event Scheduling

one vote per column

Benjamin Kellermann Privacy-Enhanced Event Scheduling slide 7 of 23

TECHNISCHE UNIVERSITÄT DRESDEN

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

- nicht dates sagen → time slots
- $40 \cdot 4 \cdot 2 = 320$

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

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

Benjamin Kellermann Privacy-Enhanced Event Scheduling slide 7 of 23

TECHNISCHE UNIVERSITÄT DRESDEN

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

Benjamin Kellermann Privacy-Enhanced Event Scheduling slide 7 of 23

E-Voting vs. Event Scheduling

	Vote
Candidate #1	
Candidate #2	✘
⋮	
Candidate #10	

scales ↓

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

scales →

one vote per column

- nicht dates sagen → time slots
- $40 \cdot 4 \cdot 2 = 320$

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

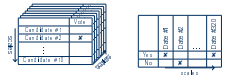
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

E-Voting vs. Event Scheduling



one vote per column

Benjamin Kellermann Privacy-Enhanced Event Scheduling slide 7 of 23

TECHNISCHE UNIVERSITÄT DRESDEN

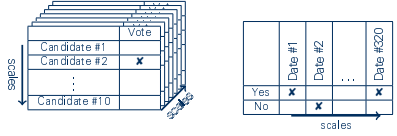
E-Voting vs. Event Scheduling

scales ↓

scales →

one vote per column

E-Voting vs. Event Scheduling



one vote per column

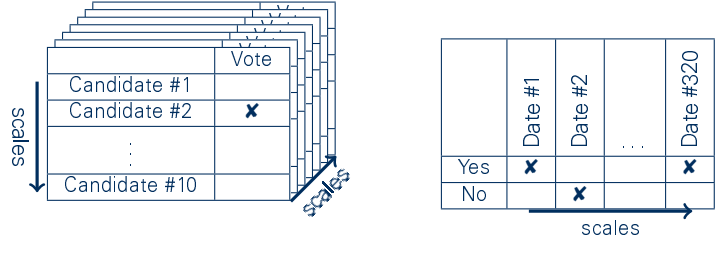
- nicht dates sagen → time slots
- $40 \cdot 4 \cdot 2 = 320$

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

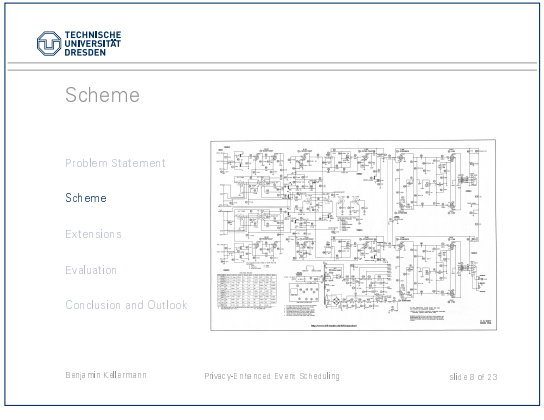
Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

E-Voting vs. Event Scheduling

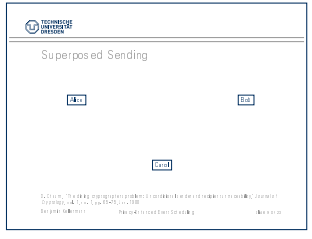


one vote per column



- no worry, its not so complicated
- recall superposed sending!

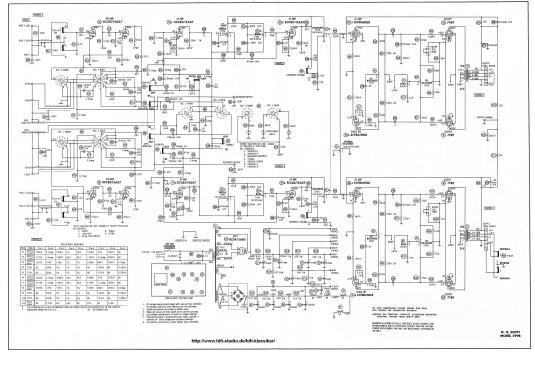
1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

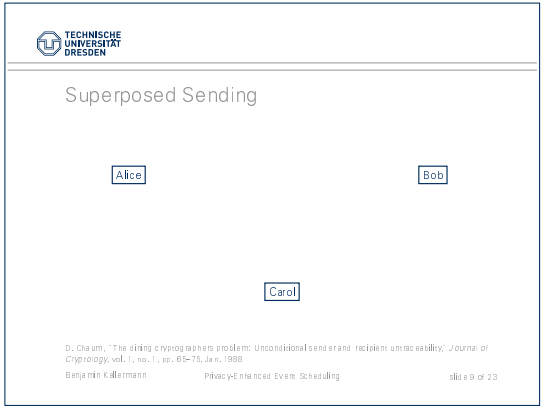


Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

Scheme

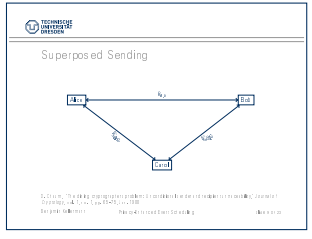
Problem Statement
Scheme
Extensions
Evaluation
Conclusion and Outlook





- also known as

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

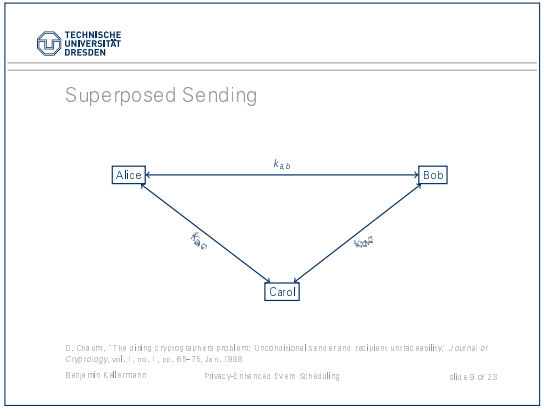
Superposed Sending

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



- also known as
- inverse

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

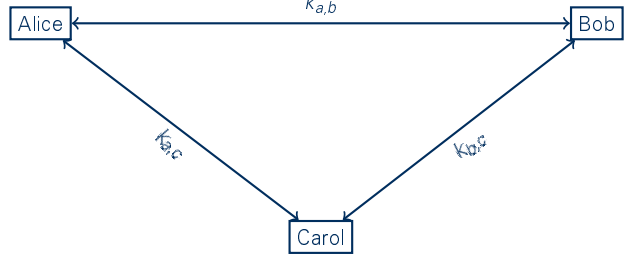
Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

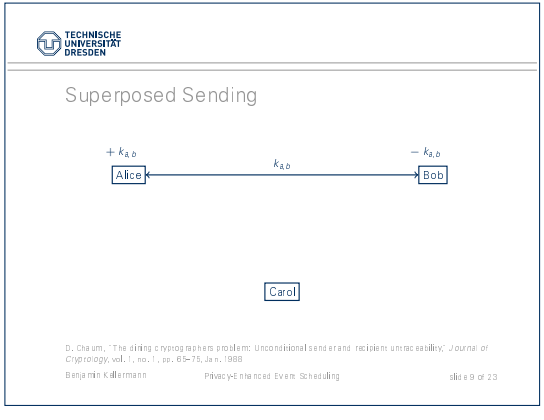
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

Superposed Sending

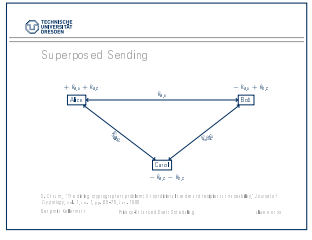


D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988



- inverse

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

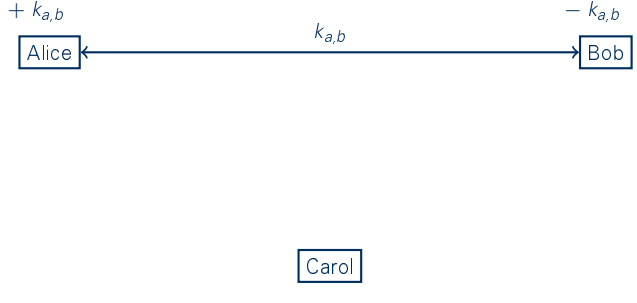
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

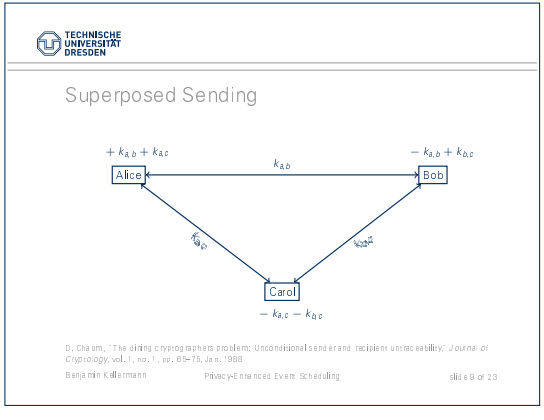
Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Superposed Sending

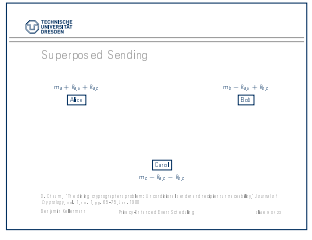


D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988



- inverse

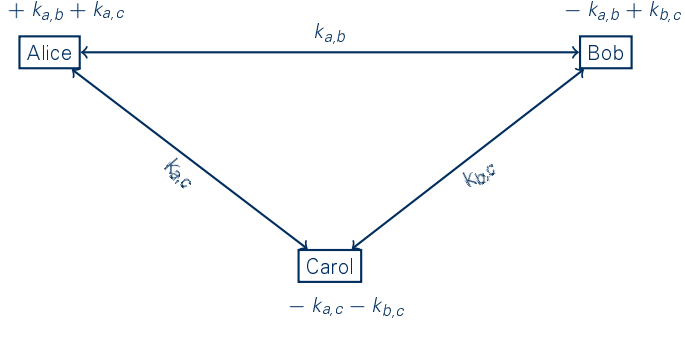
1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



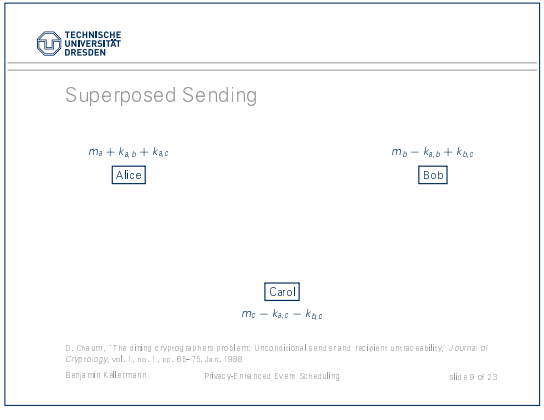
Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

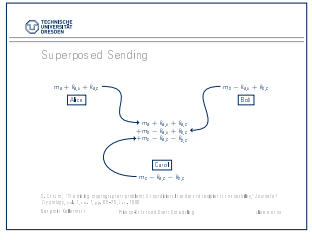
Superposed Sending



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



- inverse



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Superposed Sending

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

Alice

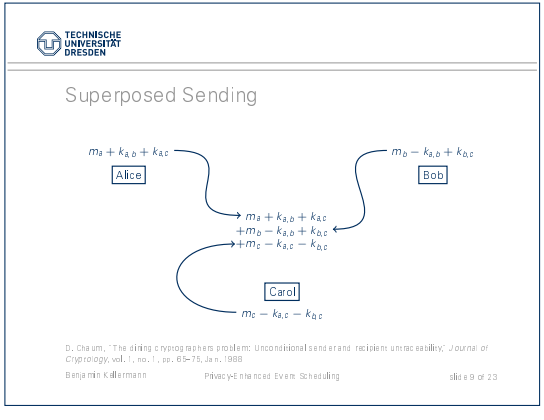
$m_b - k_{a,b} + k_{b,c}$

Bob

Carol

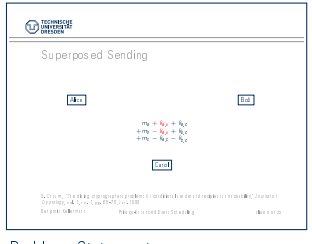
$m_c - k_{a,c} - k_{b,c}$

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



- inverse
- remark, that not infer
- neutral element

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

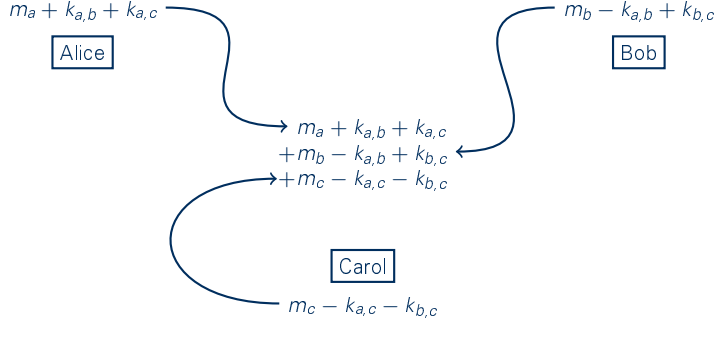
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

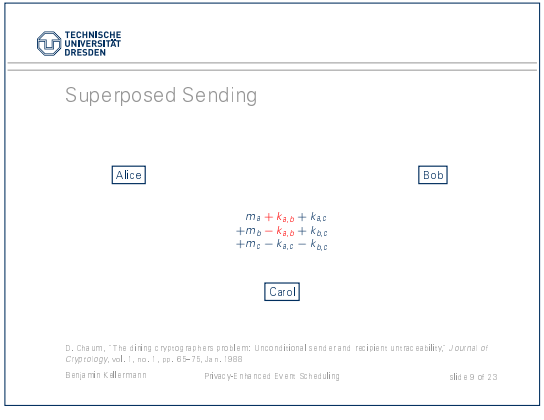
Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Superposed Sending

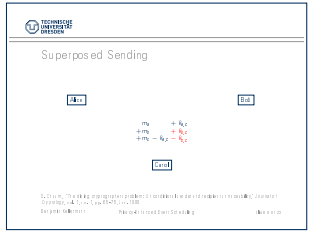


D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988



- inverse
- remark, that not infer
- neutral element

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Superposed Sending

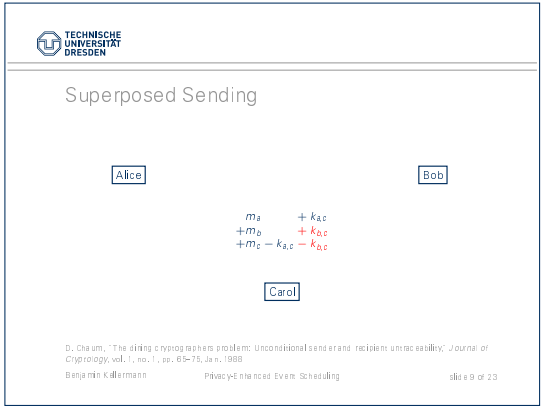
Alice

Bob

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

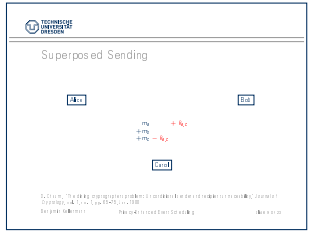
Carol

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



- inverse
- neutral element

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Superposed Sending

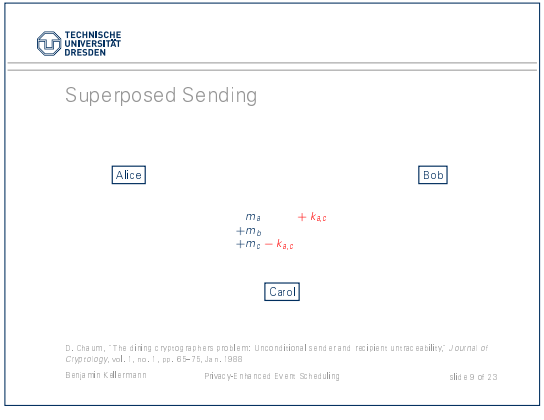
Alice

Bob

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

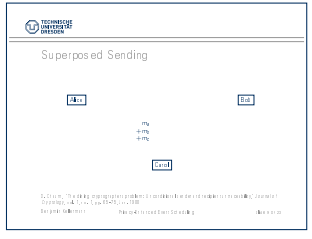
Carol

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



- inverse
- neutral element

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Superposed Sending

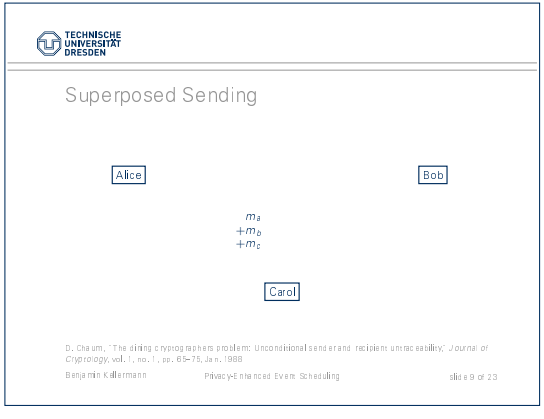
Alice

Bob

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

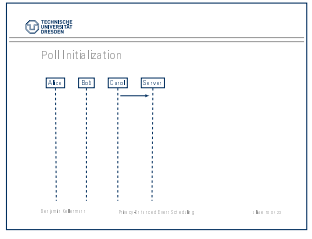
Carol

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



- inverse
- neutral element

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Superposed Sending

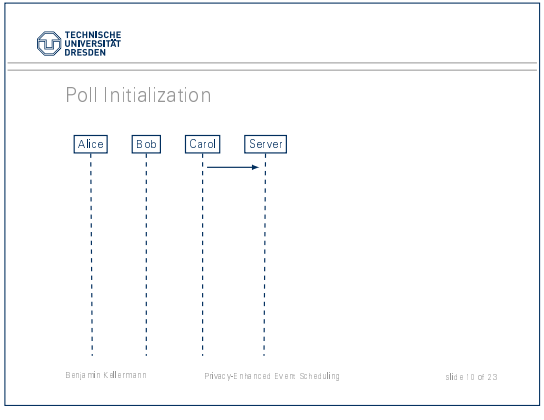
Alice

Bob

m_a
$+m_b$
$+m_c$

Carol

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



1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

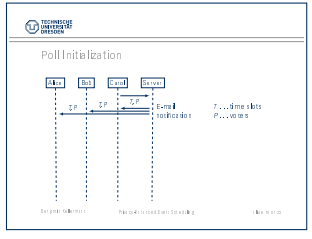
Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

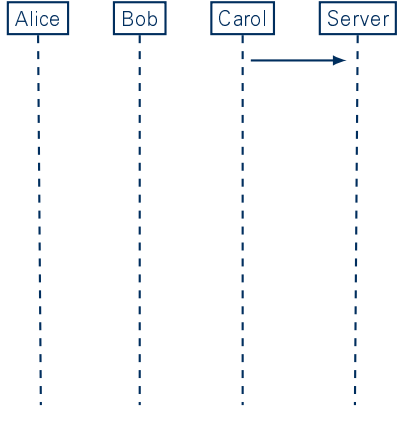
Evaluation
- Evaluation

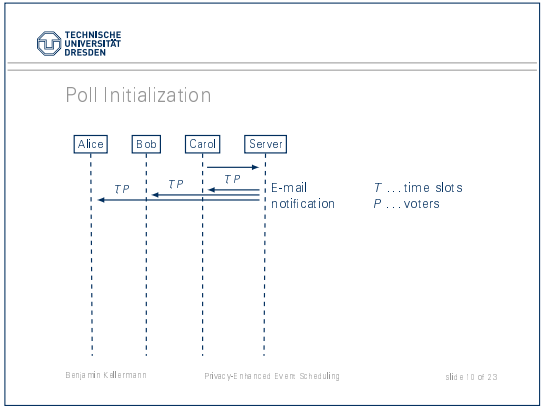
Conclusion and Outlook
- Conclusion and Outlook



TECHNISCHE UNIVERSITÄT DRESDEN

Poll Initialization





1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

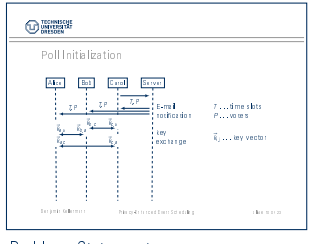
Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

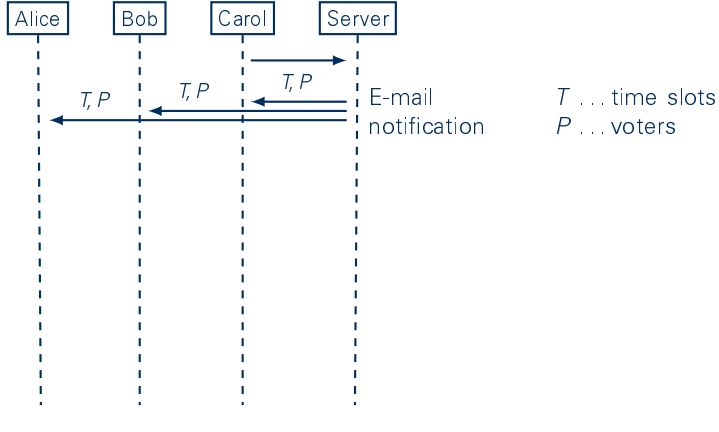
Evaluation
- Evaluation

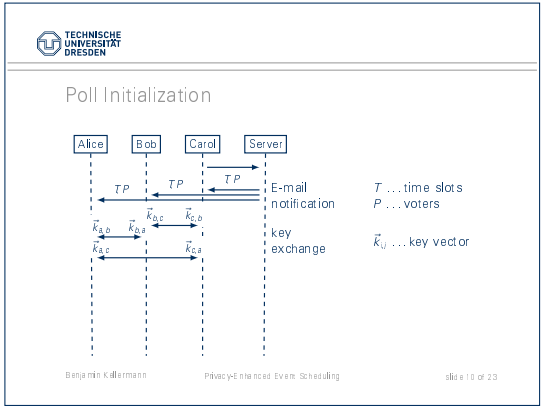
Conclusion and Outlook
- Conclusion and Outlook



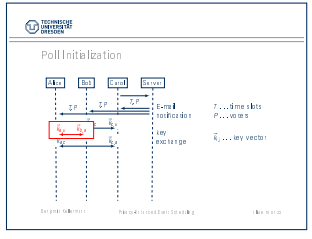
TECHNISCHE UNIVERSITÄT DRESDEN

Poll Initialization





1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

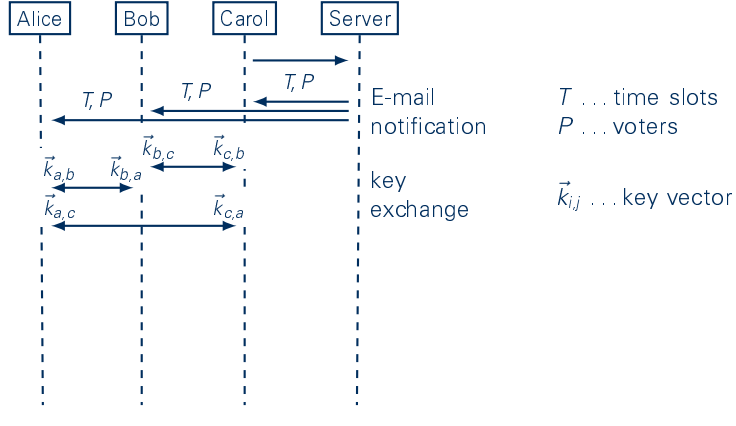
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

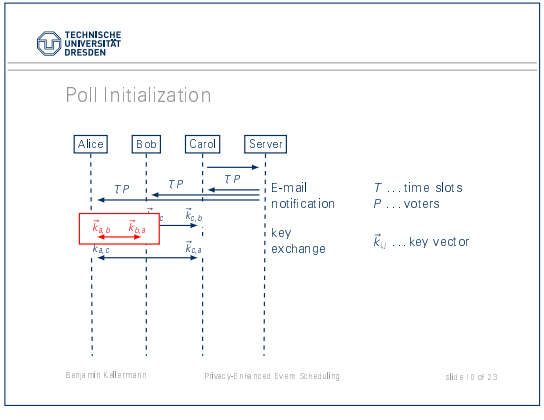
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

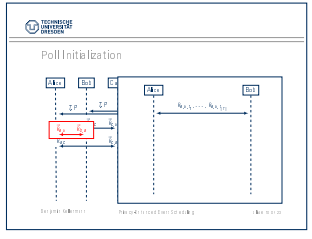
TECHNISCHE UNIVERSITÄT DRESDEN

Poll Initialization





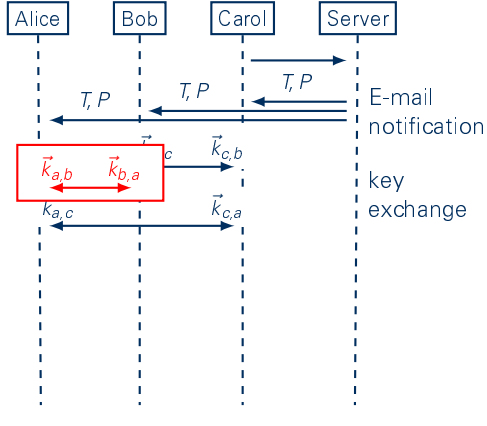
1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

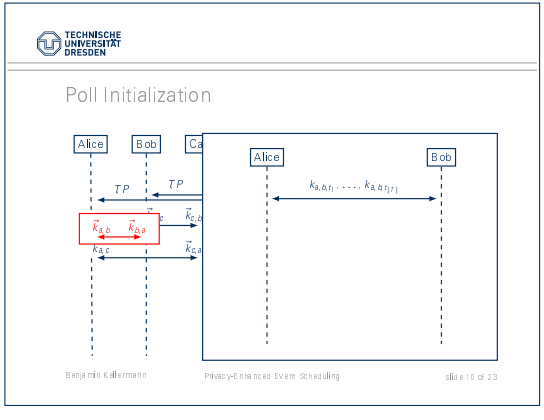
TECHNISCHE UNIVERSITÄT DRESDEN

Poll Initialization



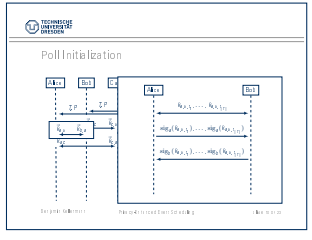
T . . . time slots
P . . . voters

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



- Doppelpfeil erklären

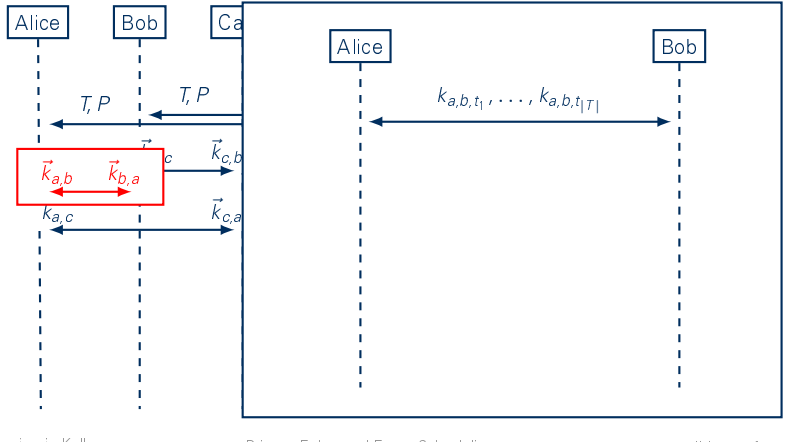
1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

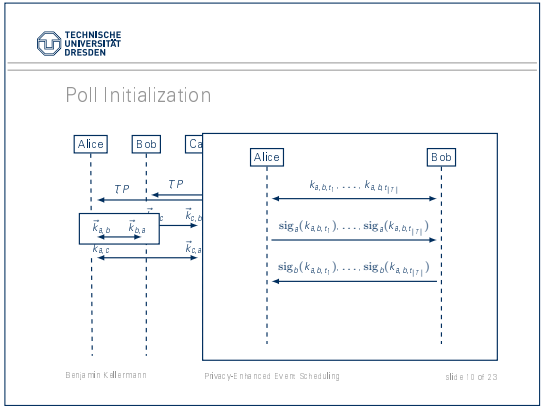


Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

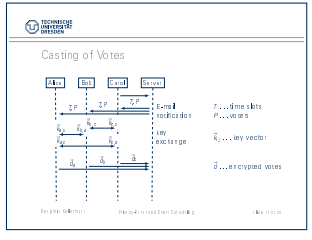
Poll Initialization





- Doppelpfeil erklären

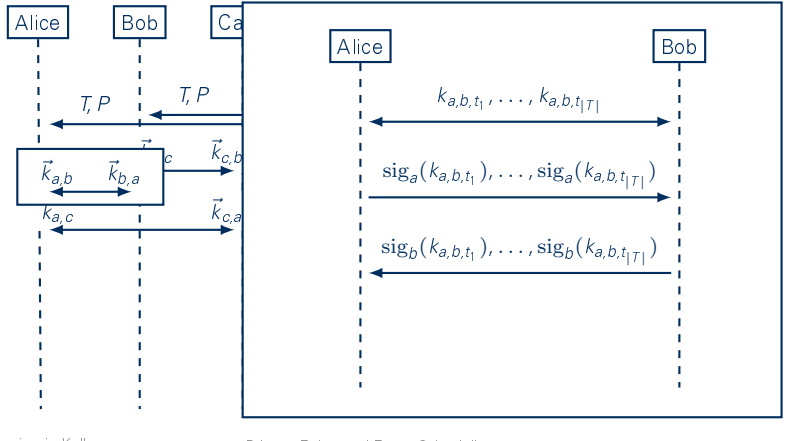
1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

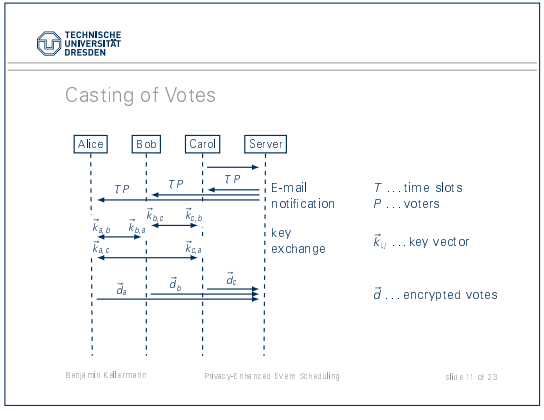


Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

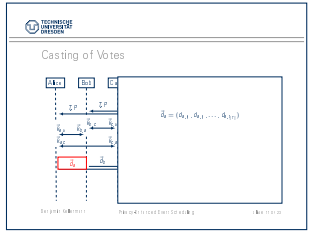
TECHNISCHE UNIVERSITÄT DRESDEN

Poll Initialization





1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

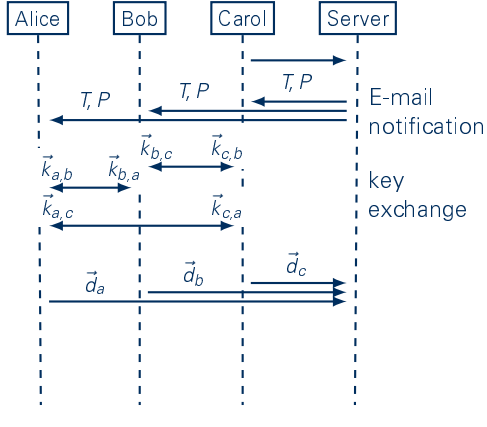
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Casting of Votes

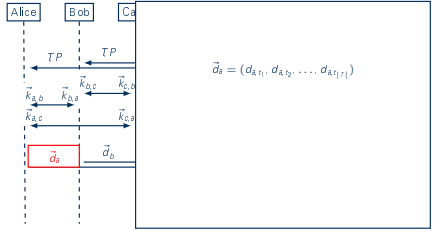


T . . . time slots
P . . . voters

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

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

Casting of Votes



1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

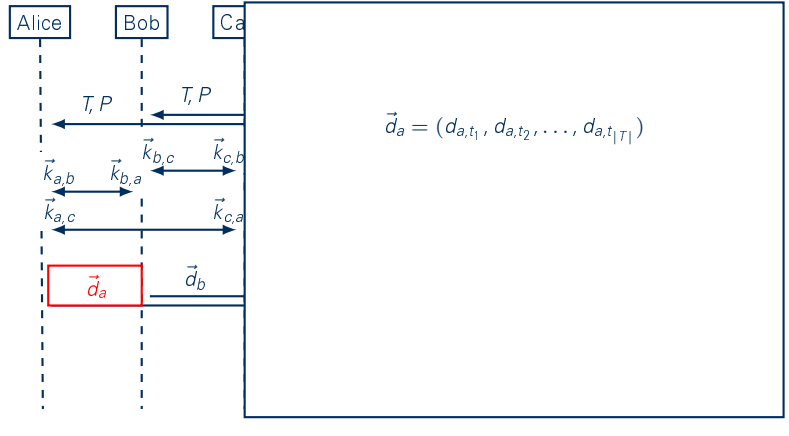
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

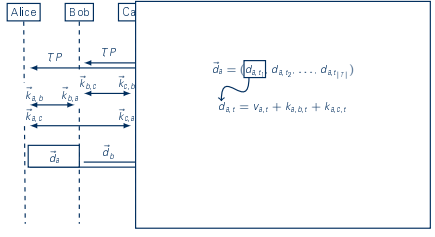
TECHNISCHE UNIVERSITÄT DRESDEN

Casting of Votes



Benjamin Kellermann Privacy-Enhanced Event Scheduling slide 11 of 23

Casting of Votes



1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

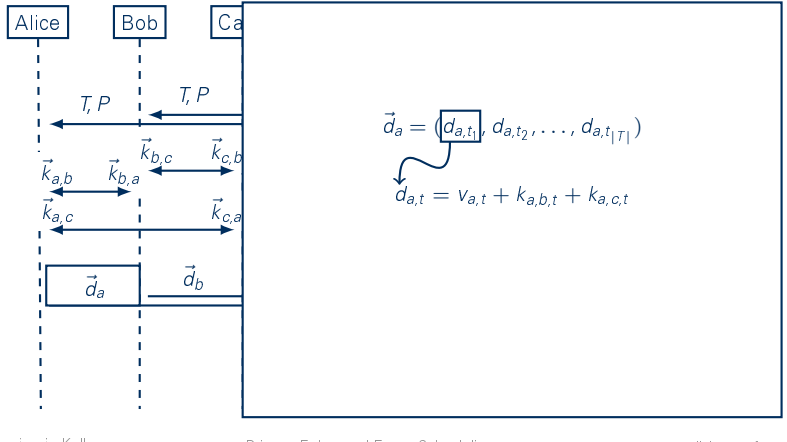
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

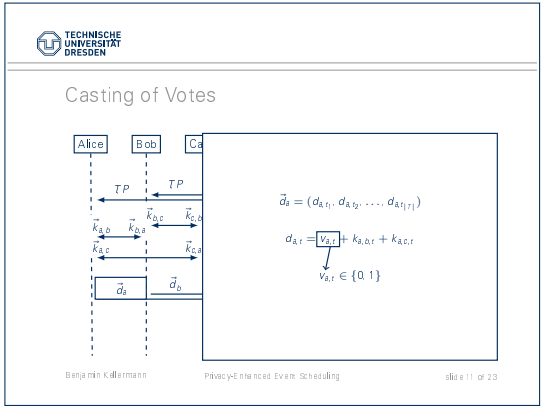
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

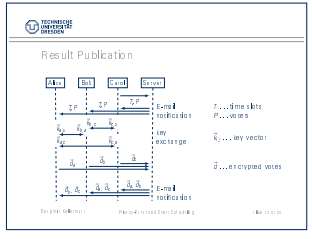
TECHNISCHE UNIVERSITÄT DRESDEN

Casting of Votes





- group



1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

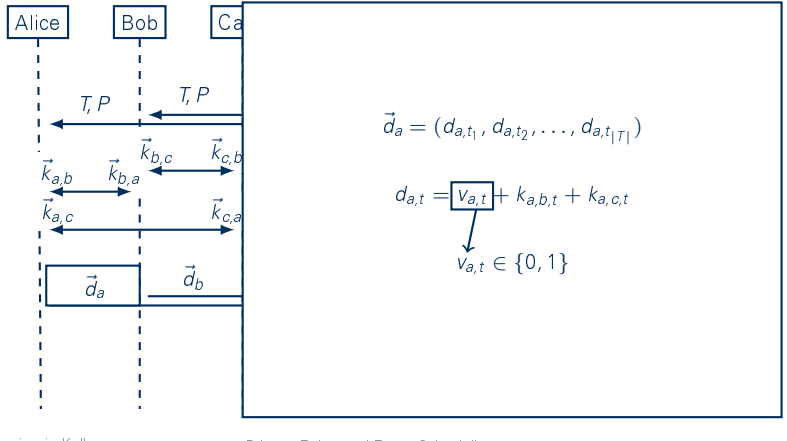
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

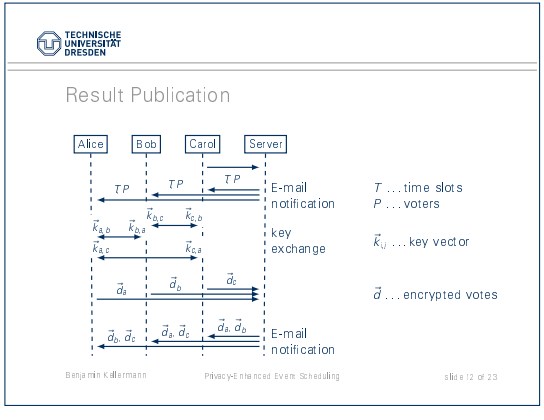
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

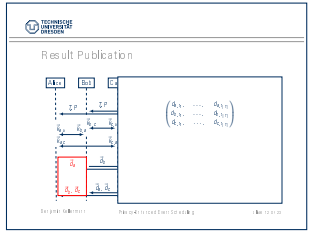
TECHNISCHE UNIVERSITÄT DRESDEN

Casting of Votes





1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

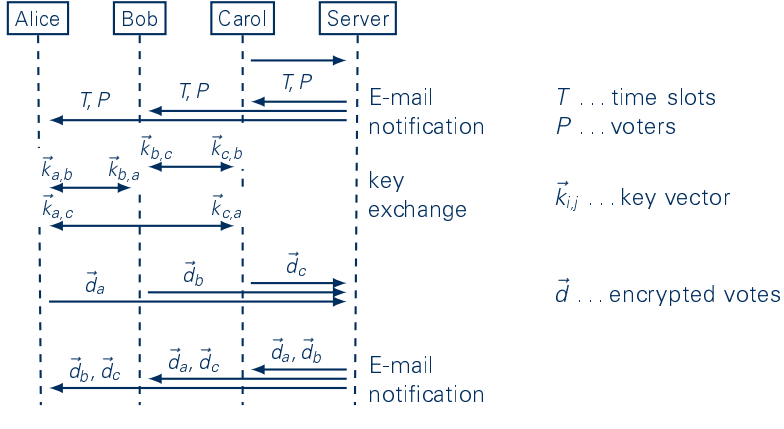
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

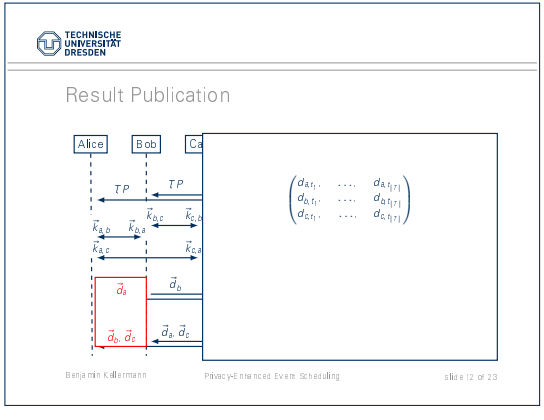
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

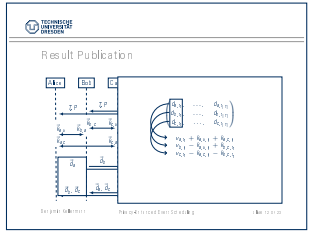
TECHNISCHE UNIVERSITÄT DRESDEN

Result Publication





1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

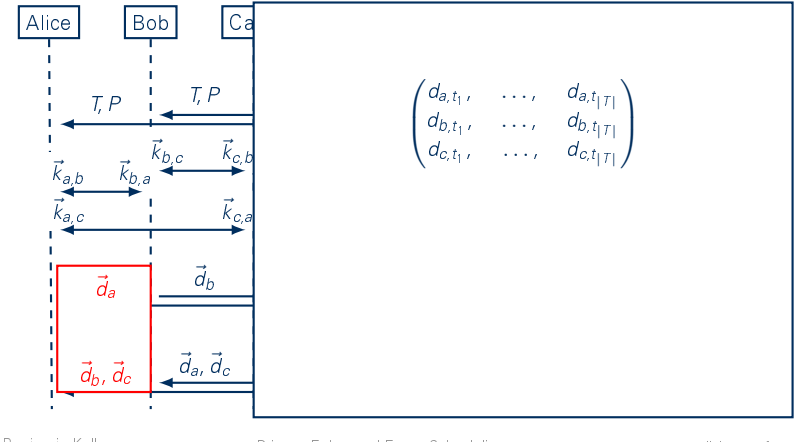
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

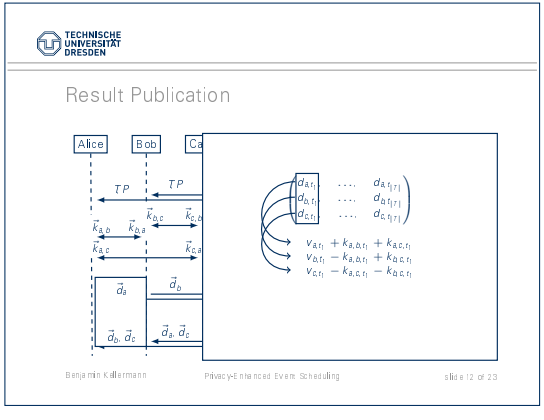
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

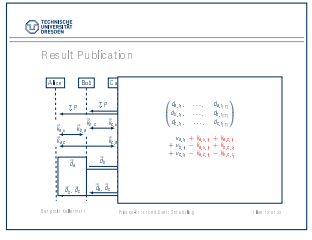
TECHNISCHE UNIVERSITÄT DRESDEN

Result Publication





1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

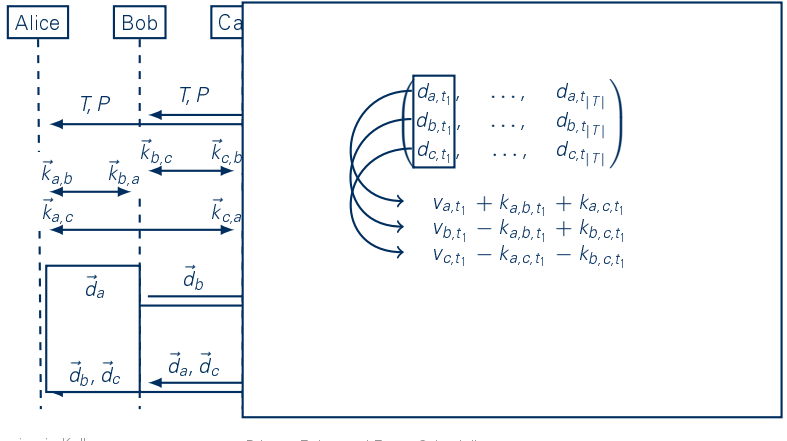
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

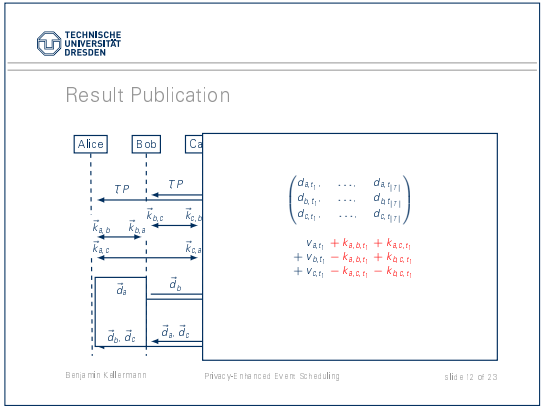
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

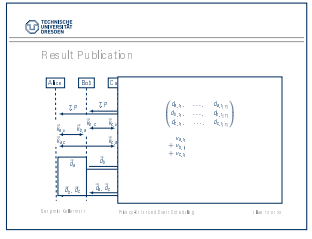
TECHNISCHE UNIVERSITÄT DRESDEN

Result Publication





1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

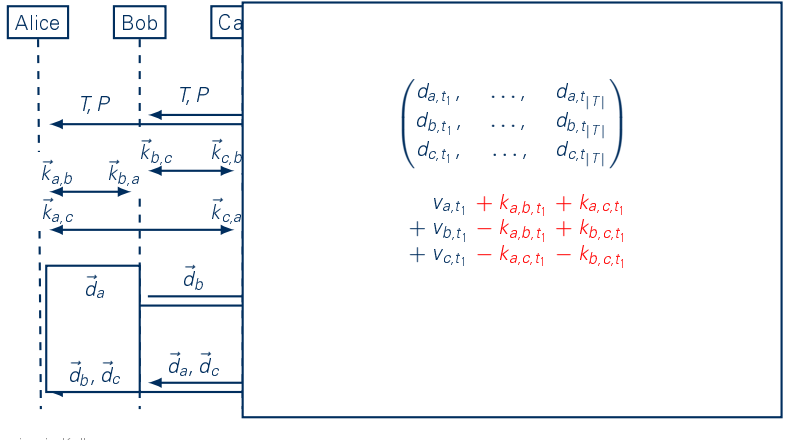
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

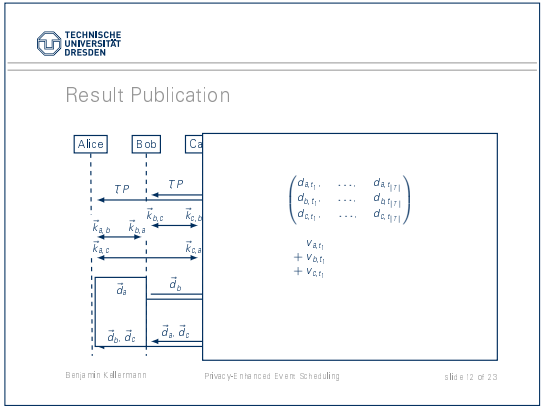
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

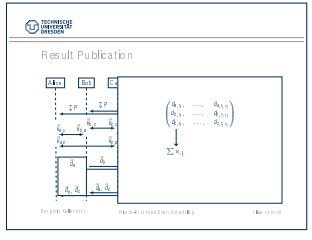
TECHNISCHE UNIVERSITÄT DRESDEN

Result Publication





1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

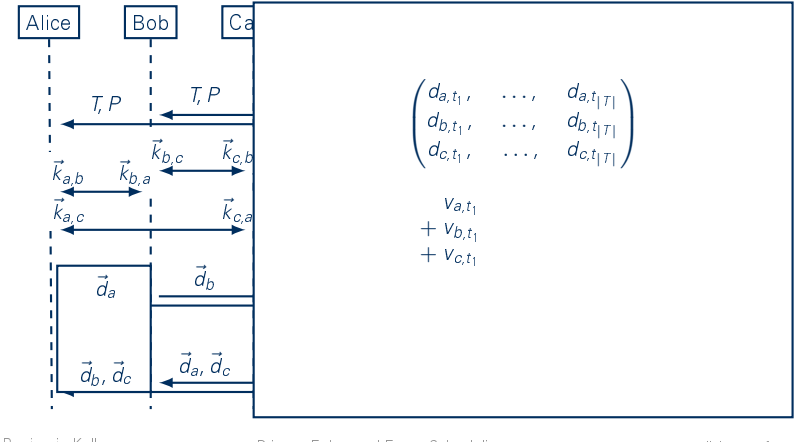
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

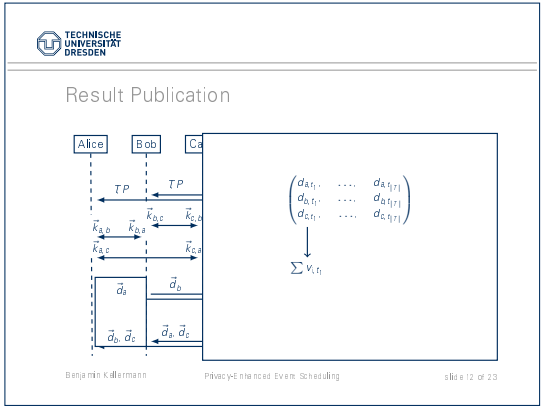
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

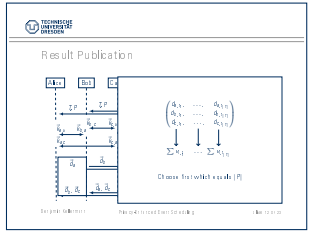
TECHNISCHE UNIVERSITÄT DRESDEN

Result Publication





1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

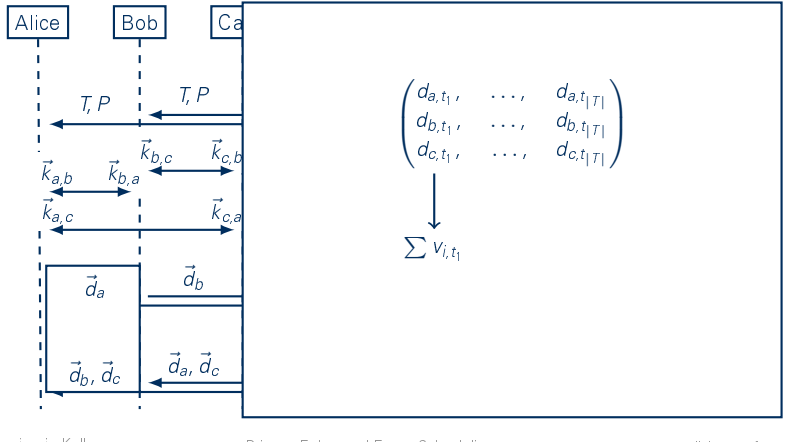
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

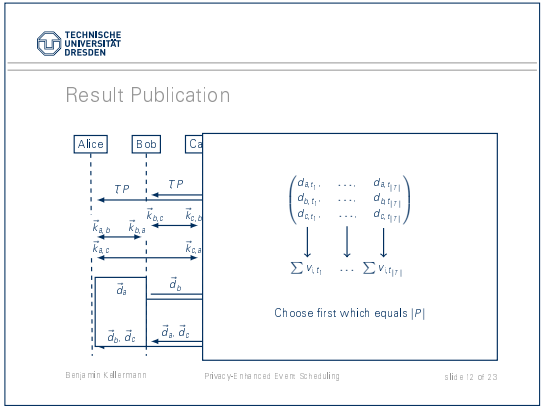
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

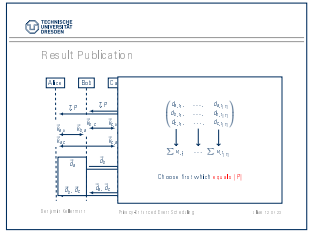
Result Publication





- limitation

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

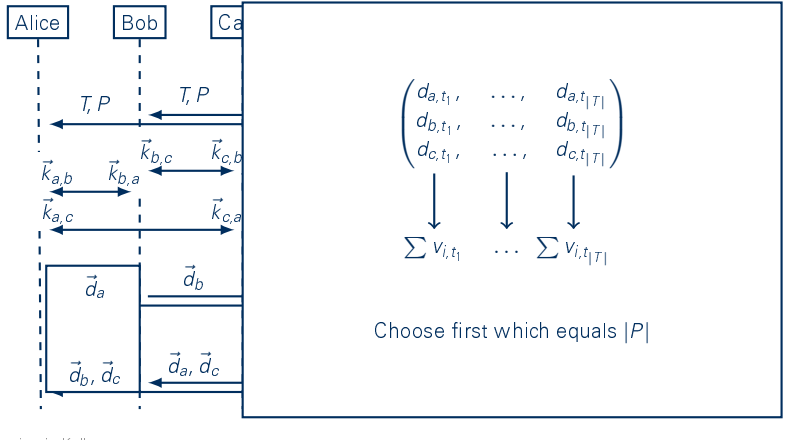
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

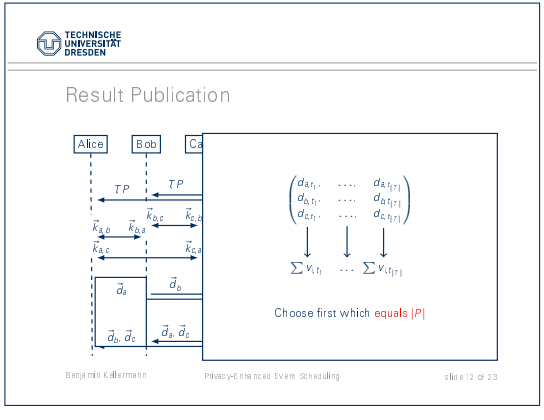
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

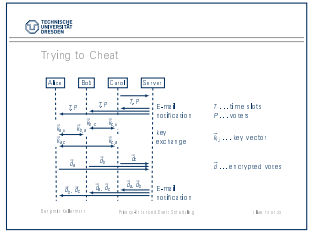
Result Publication





- limitation

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

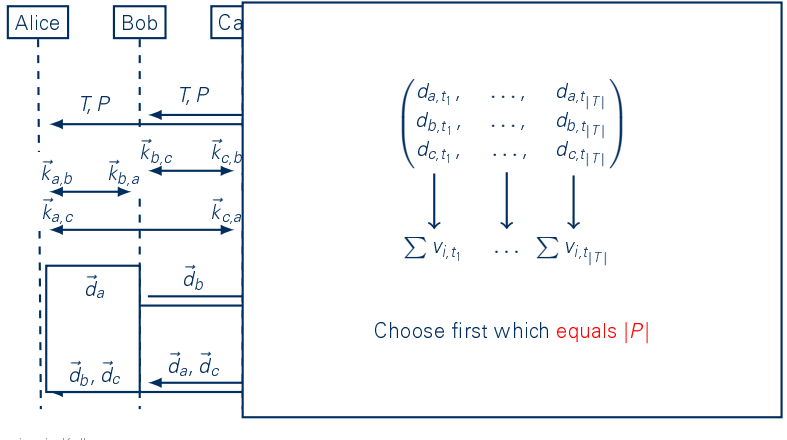
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

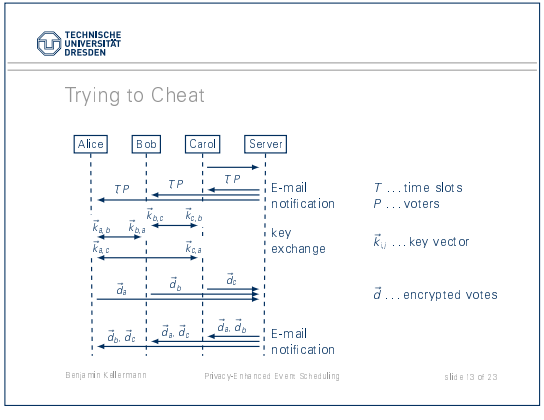
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

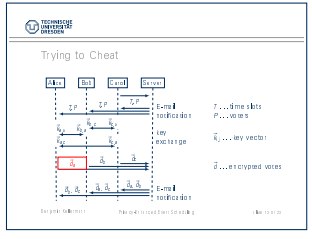
TECHNISCHE UNIVERSITÄT DRESDEN

Result Publication





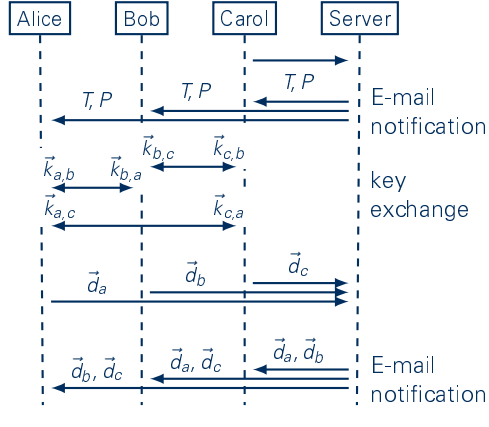
1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

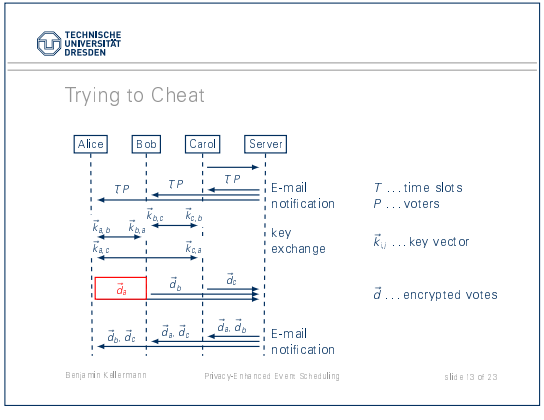
Trying to Cheat



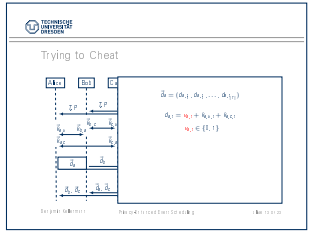
T . . . time slots
P . . . voters

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

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



1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

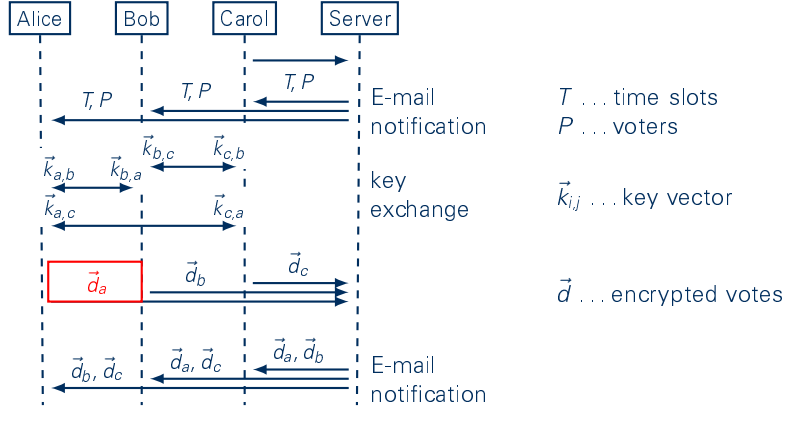
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

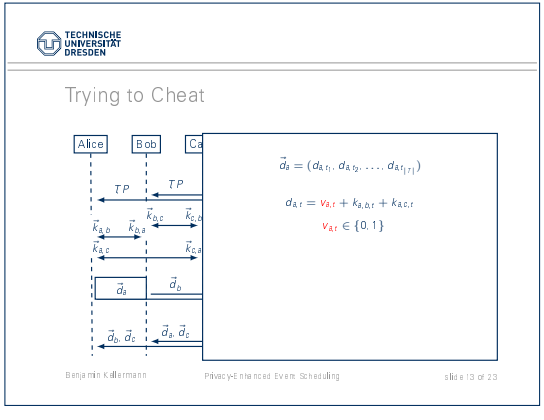
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

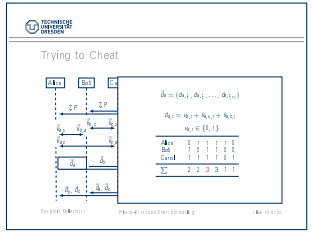
TECHNISCHE UNIVERSITÄT DRESDEN

Trying to Cheat





1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

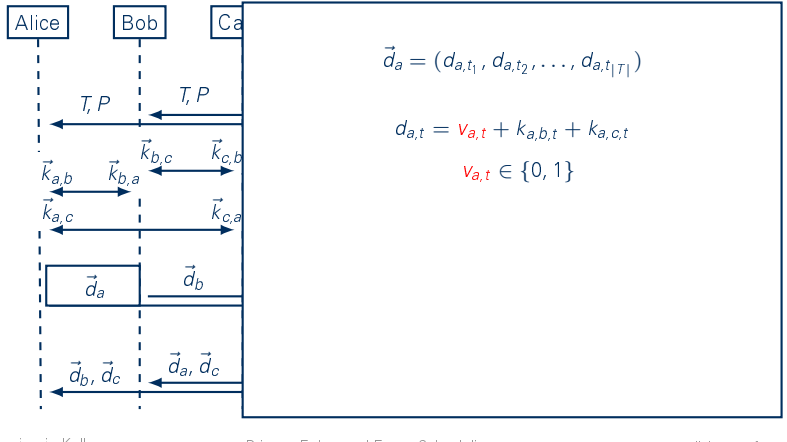
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

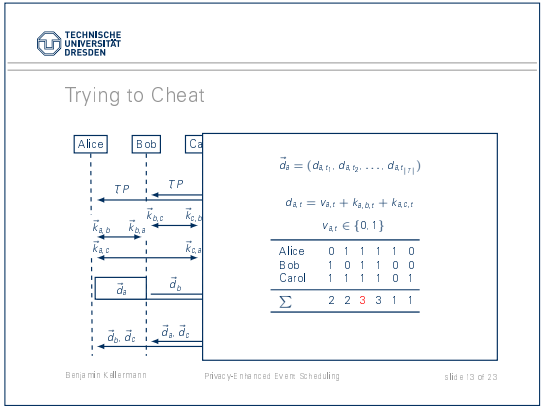
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

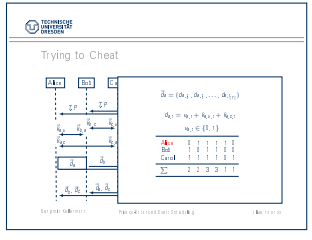
TECHNISCHE UNIVERSITÄT DRESDEN

Trying to Cheat





1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

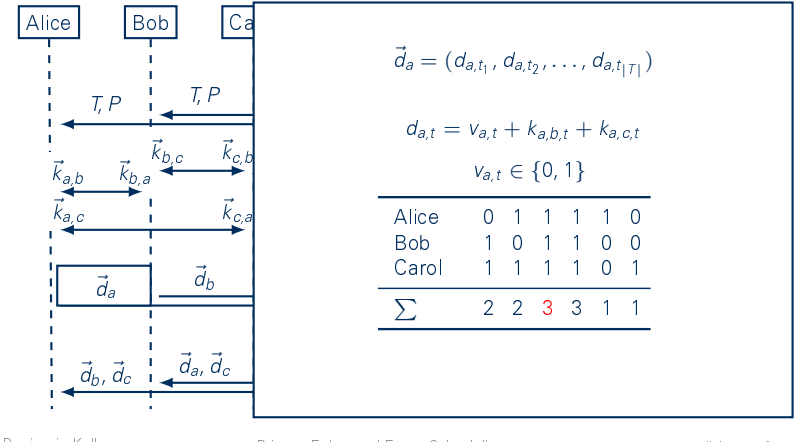
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

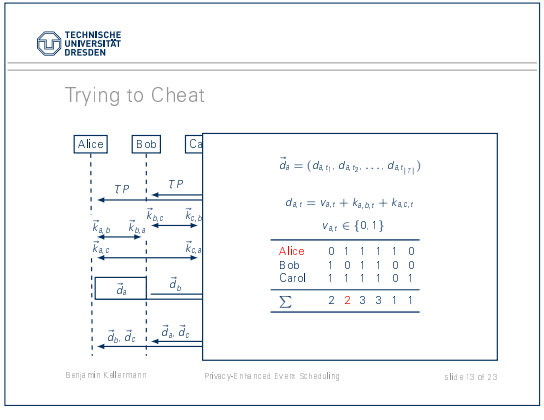
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

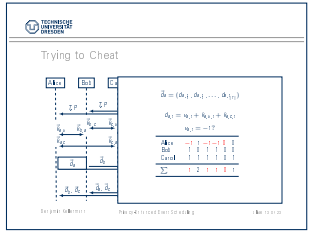
TECHNISCHE UNIVERSITÄT DRESDEN

Trying to Cheat





1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

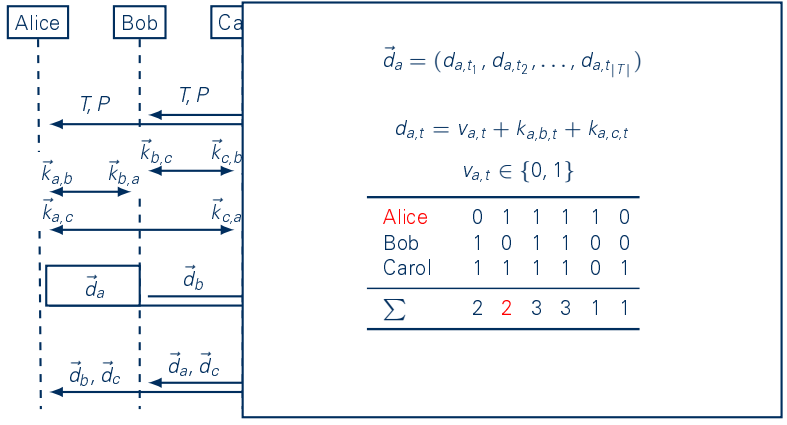
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

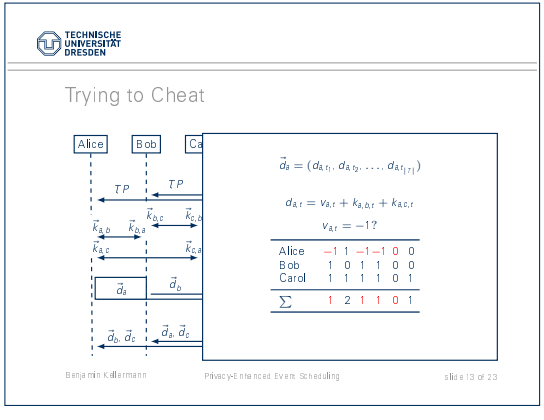
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Trying to Cheat





1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

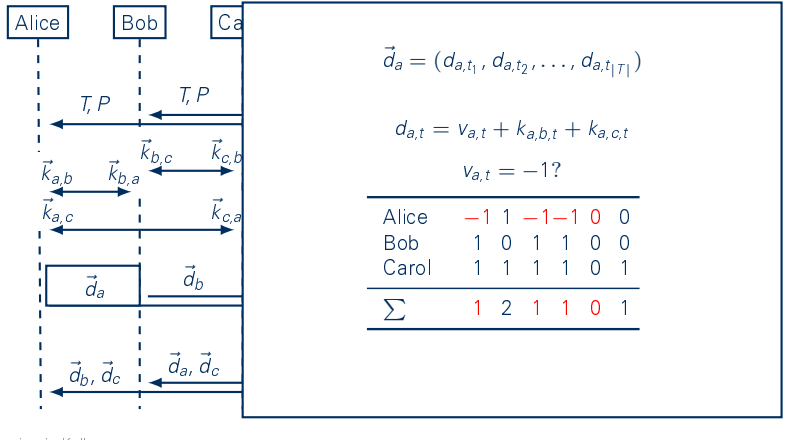
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

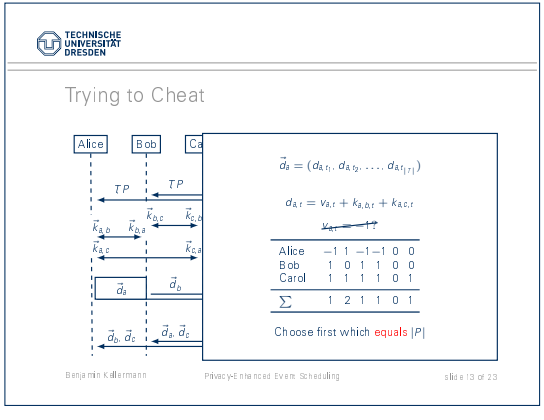
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

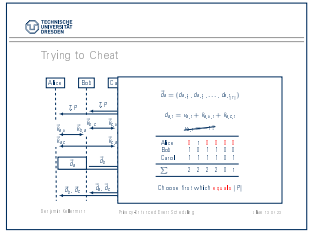
TECHNISCHE UNIVERSITÄT DRESDEN

Trying to Cheat





1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

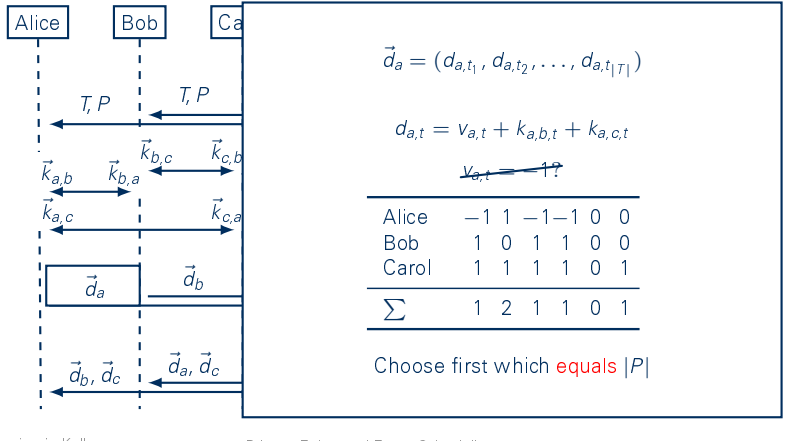
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

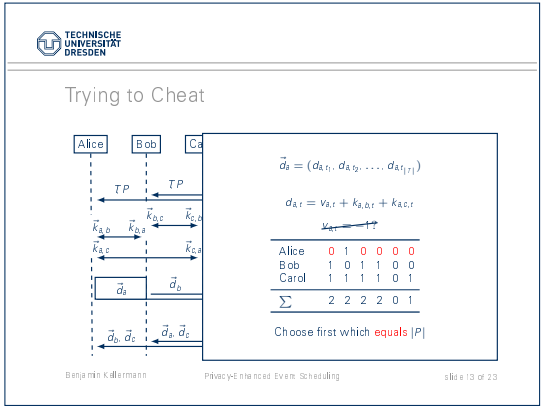
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

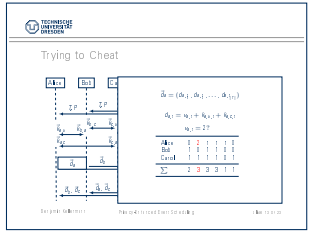
Trying to Cheat





- "legal-but-selfish" vote

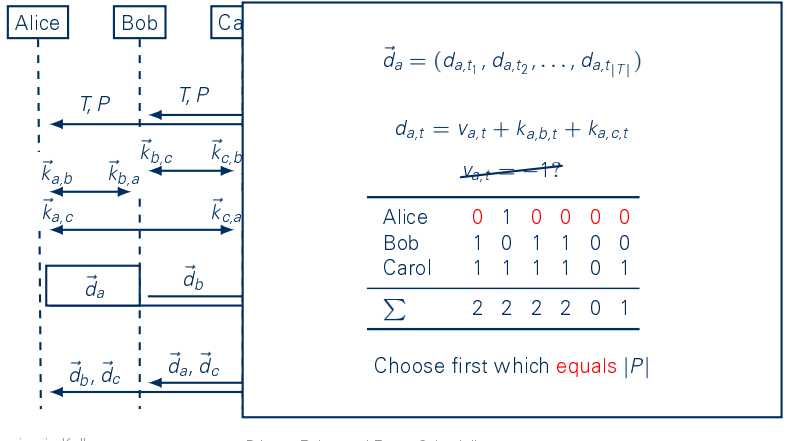
1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

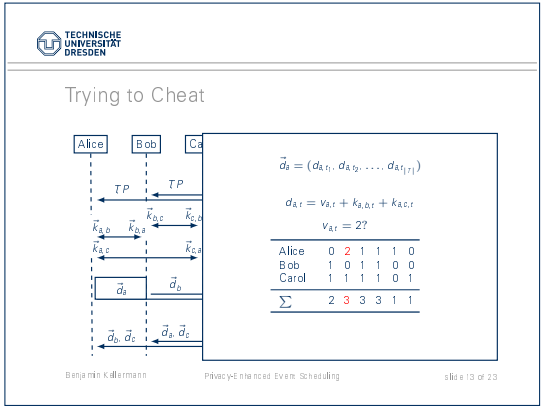


Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

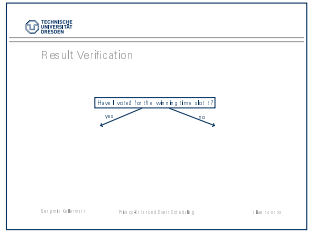
TECHNISCHE UNIVERSITÄT DRESDEN

Trying to Cheat





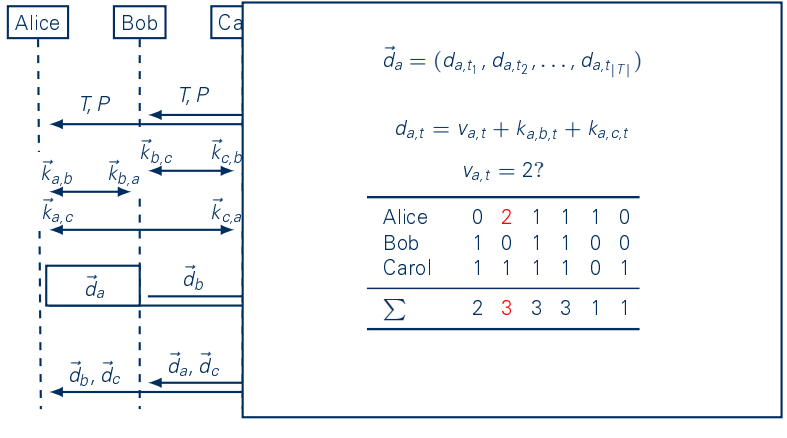
1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



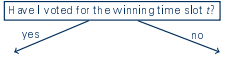
Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Trying to Cheat



Result Verification



1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

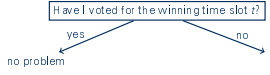
Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN
Result Verification
Have I voted for the winning time slot t?
yes
no
no problem
Benjamin Kellermann Privacy-Enhanced Event Scheduling slide 14 of 23

TECHNISCHE UNIVERSITÄT DRESDEN

Result Verification

Result Verification



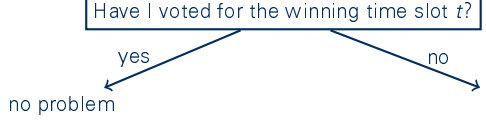
- Entlarven: unmask

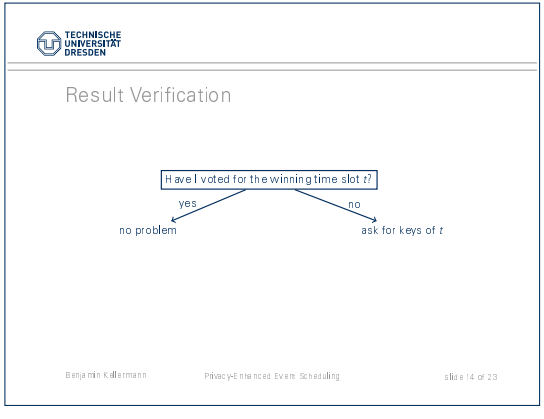
1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Result Verification





- Entlarven: unmask

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

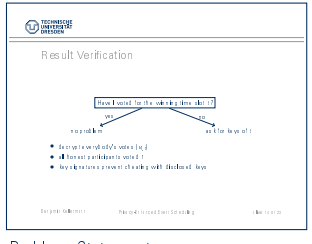
Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

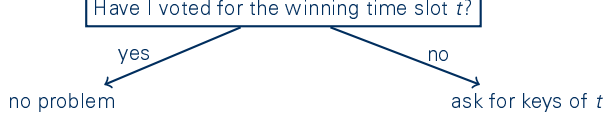
Evaluation
- Evaluation

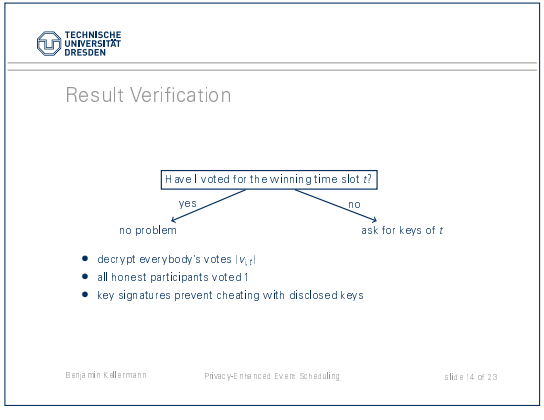
Conclusion and Outlook
- Conclusion and Outlook



TECHNISCHE UNIVERSITÄT DRESDEN

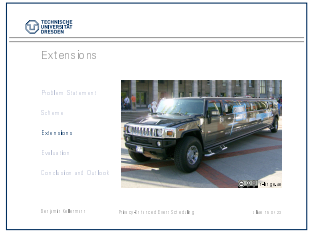
Result Verification





- Entlarven: unmask

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Result Verification

Have I voted for the winning time slot t?

yes → no problem

no → ask for keys of t

- decrypt everybody's votes ($v_{i,t}$)
- all honest participants voted 1
- key signatures prevent cheating with disclosed keys

Extensions

Problem Statement

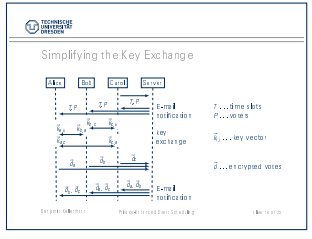
Scheme

Extensions

Evaluation

Conclusion and Outlook

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Extensions

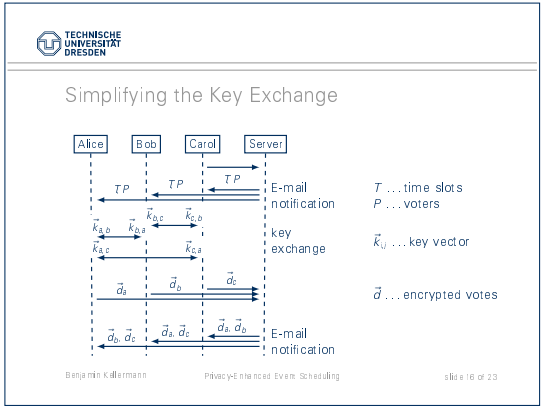
Problem Statement

Scheme

Extensions

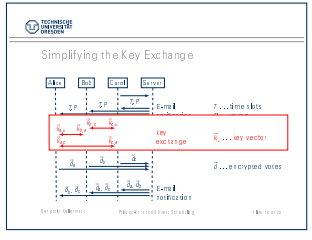
Evaluation

Conclusion and Outlook



- quadratic in number of voters

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

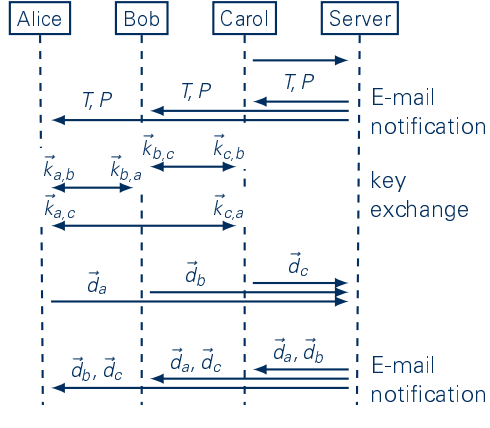
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

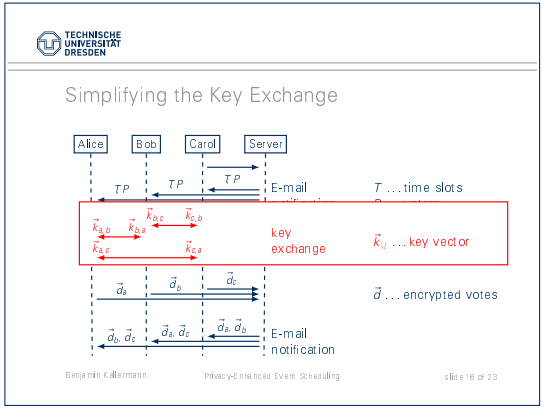
Simplifying the Key Exchange



T . . . time slots
P . . . voters

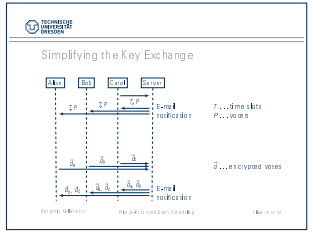
$\vec{k}_{i,j}$ . . . key vector

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



- quadratic in number of voters

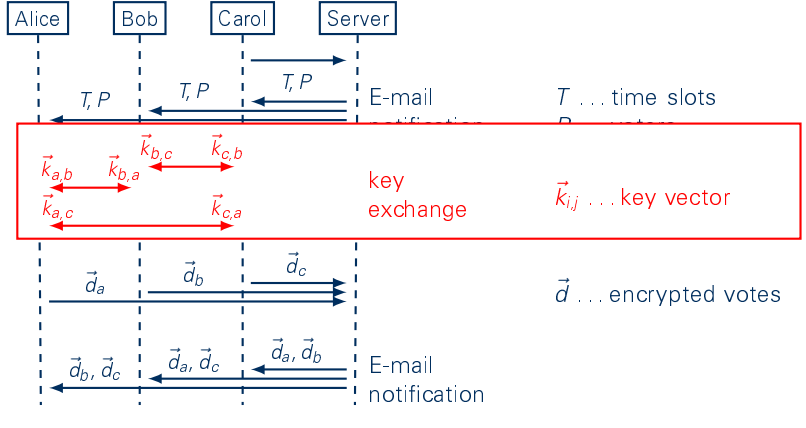
1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

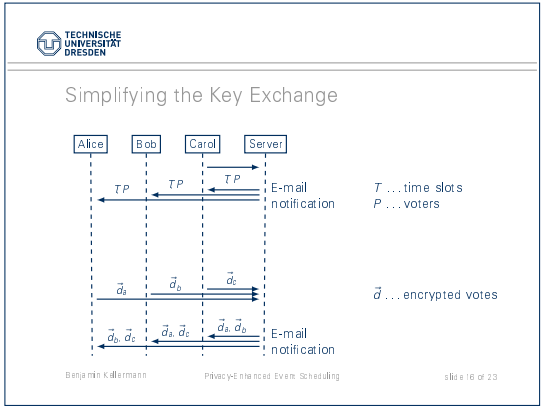


Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

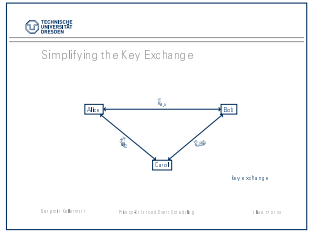
Simplifying the Key Exchange





- quadratic in number of voters

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

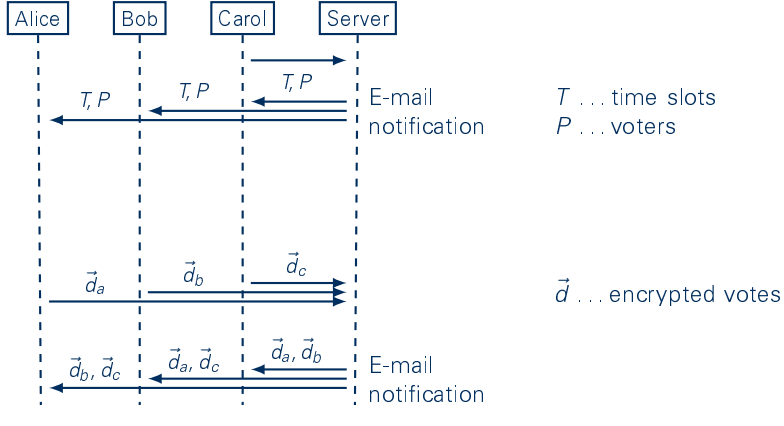
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

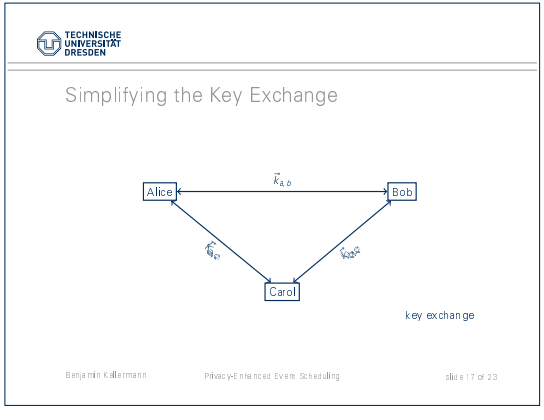
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

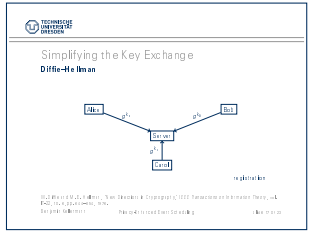
Simplifying the Key Exchange





- quadratic in number of voters

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

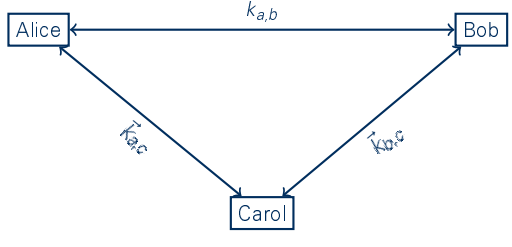
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

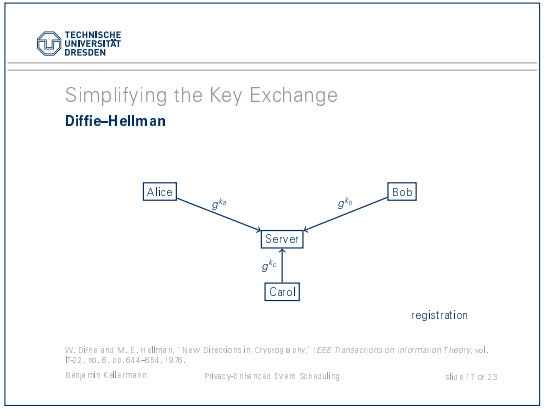
Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Simplifying the Key Exchange

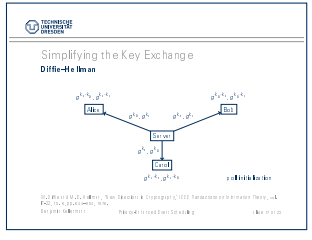


key exchange



- remark: g, p equal for all

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

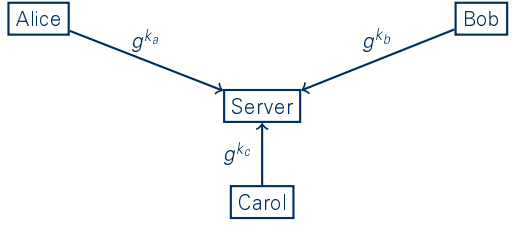
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

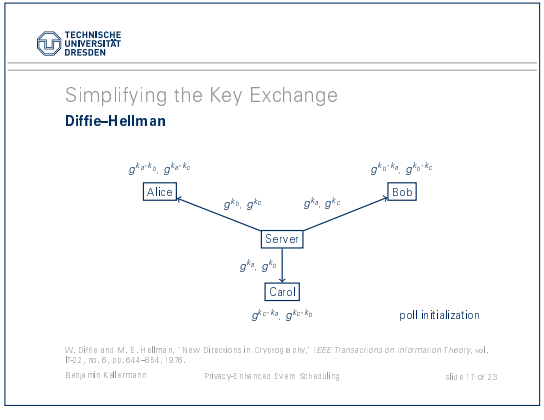
Simplifying the Key Exchange

Diffie–Hellman



registration

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



- remark: g, p equal for all

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

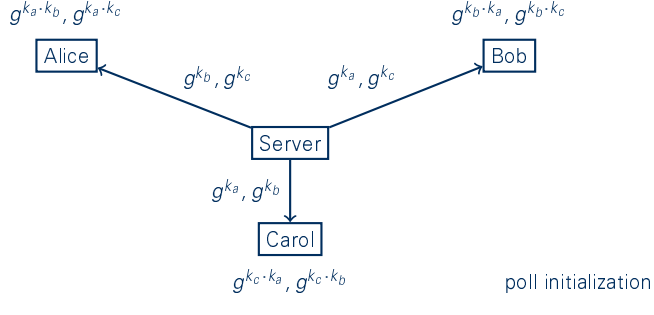
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

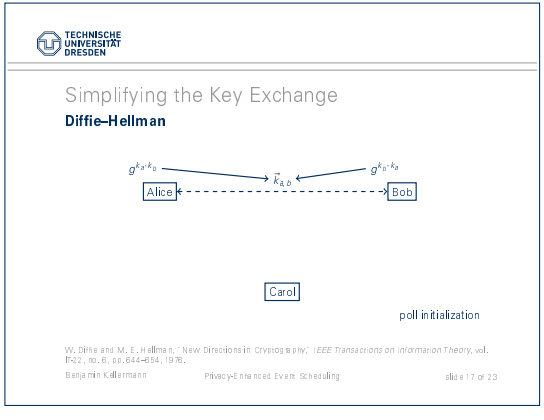
Conclusion and Outlook
- Conclusion and Outlook

Simplifying the Key Exchange

Diffie–Hellman

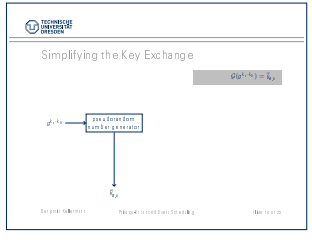


W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.



- remark: g, p equal for all

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

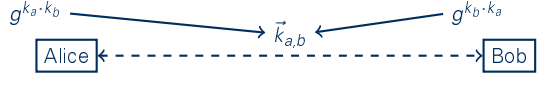
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Simplifying the Key Exchange

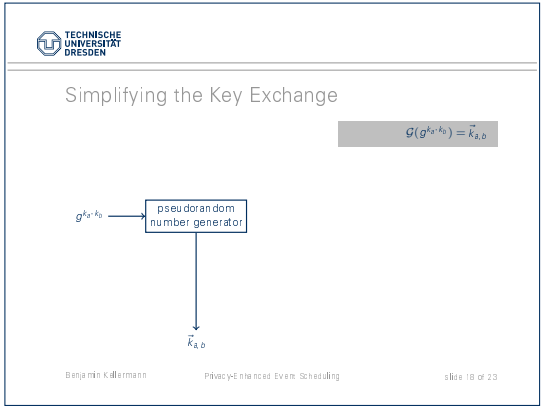
Diffie–Hellman



Carol

poll initialization

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



- formula denotes notation found in the paper

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

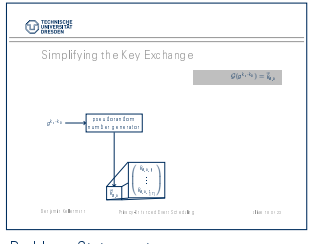
Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

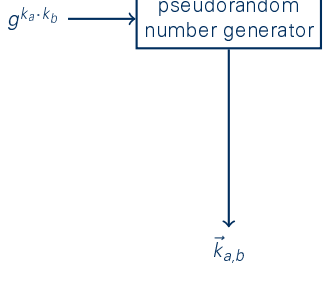
Conclusion and Outlook
- Conclusion and Outlook

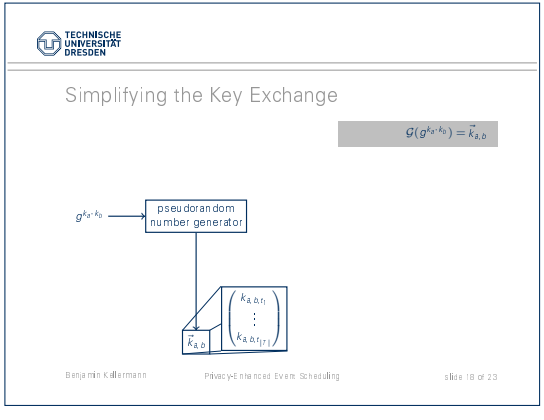


TECHNISCHE UNIVERSITÄT DRESDEN

Simplifying the Key Exchange

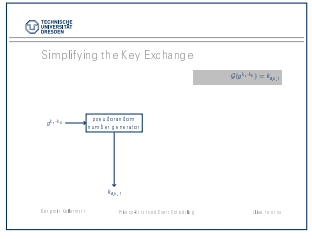
$$\mathcal{G}(g^{k_a \cdot k_b}) = \vec{k}_{a,b}$$





- formula denotes notation found in the paper

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

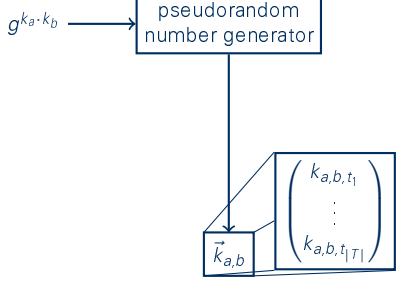


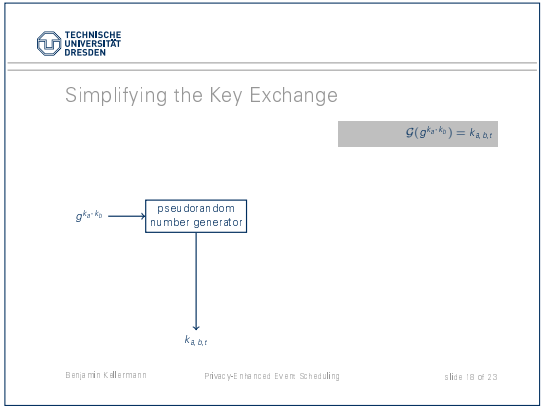
Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Simplifying the Key Exchange

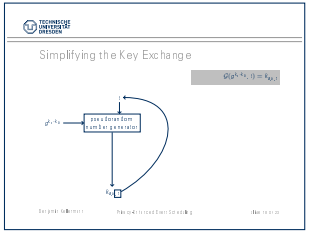
$$\mathcal{G}(g^{k_a \cdot k_b}) = \vec{k}_{a,b}$$





- formula denotes notation found in the paper

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

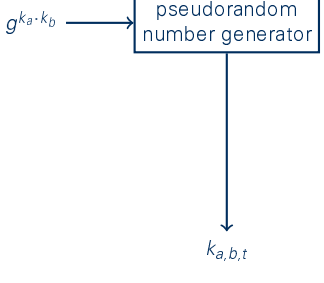


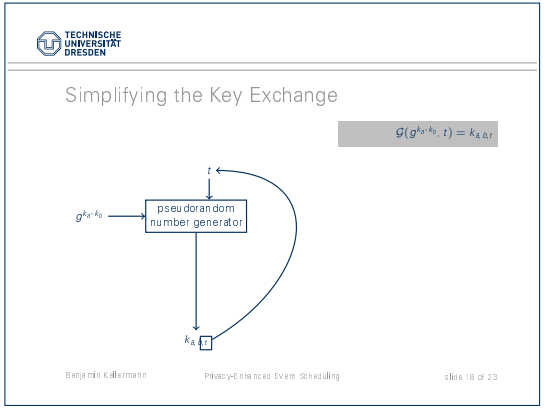
Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Simplifying the Key Exchange

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





- formula denotes notation found in the paper

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

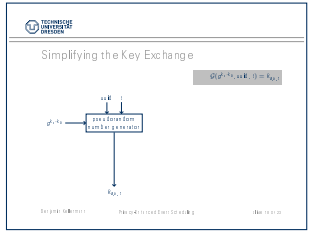
Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

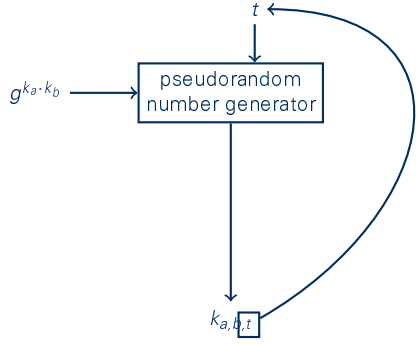
Conclusion and Outlook
- Conclusion and Outlook

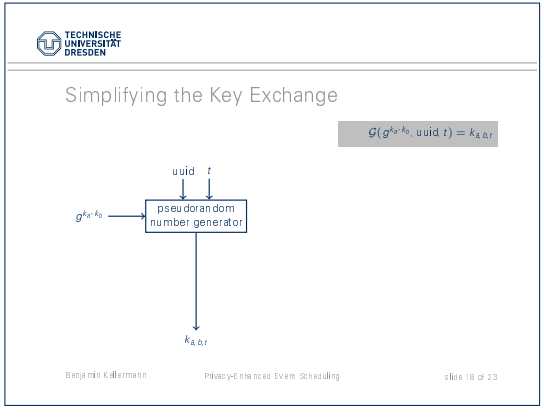


TECHNISCHE UNIVERSITÄT DRESDEN

Simplifying the Key Exchange

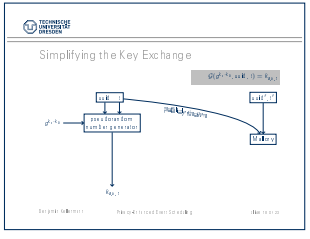
$$\mathcal{G}(g^{k_a \cdot k_b}, t) = k_{a,b,t}$$





- formula denotes notation found in the paper

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

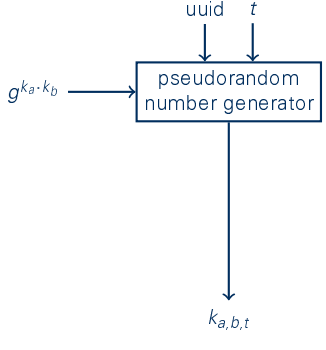


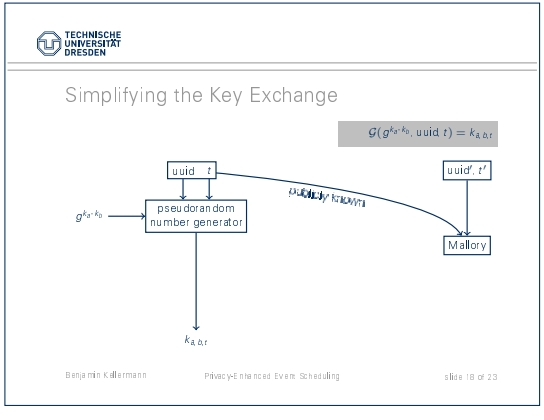
Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Simplifying the Key Exchange

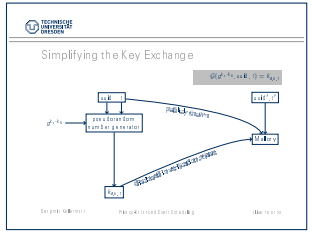
$$\mathcal{G}(g^{k_a \cdot k_b}, \text{uuid}, t) = k_{a,b,t}$$





- formula denotes notation found in the paper

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

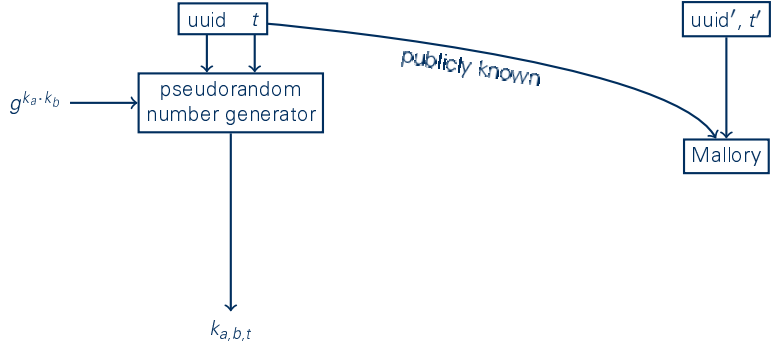


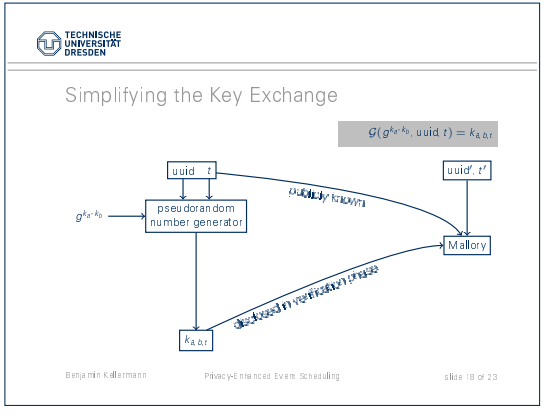
Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Simplifying the Key Exchange

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





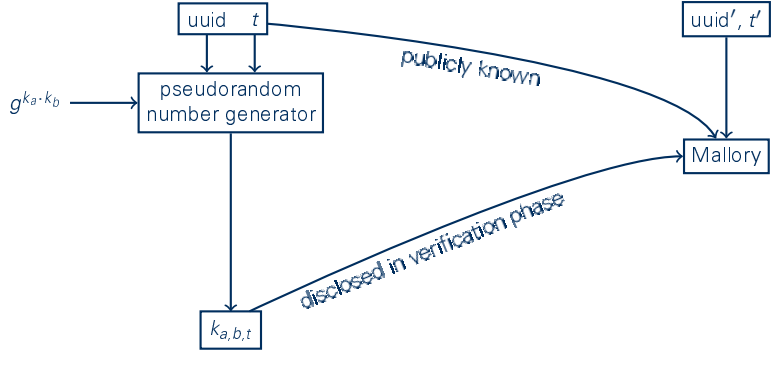
- formula denotes notation found in the paper

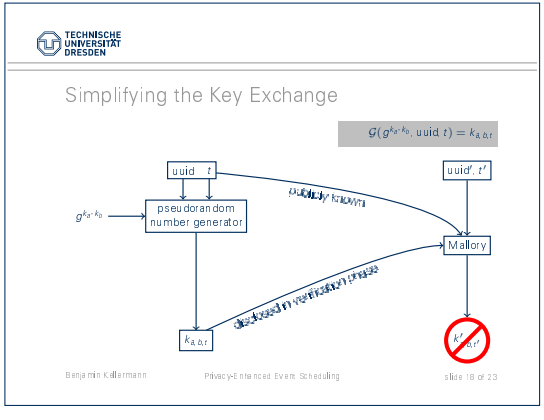
1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

Simplifying the Key Exchange

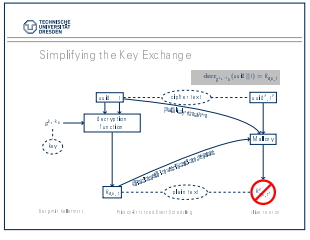
$$\mathcal{G}(g^{k_a \cdot k_b}, \text{uuid}, t) = k_{a,b,t}$$





- formula denotes notation found in the paper

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

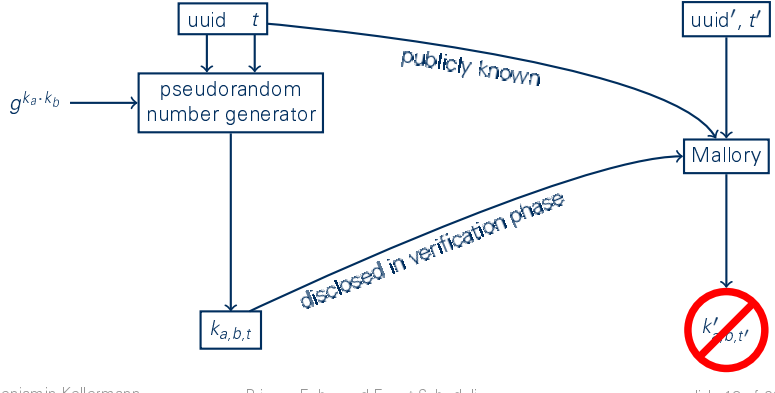


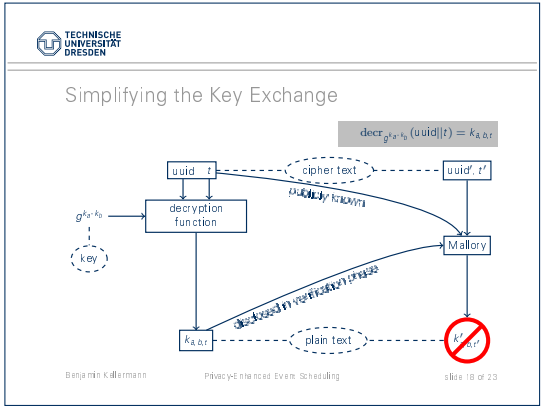
Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Simplifying the Key Exchange

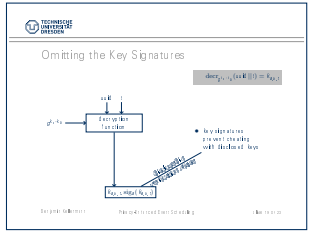
$$\mathcal{G}(g^{k_a \cdot k_b}, \text{uuid}, t) = k_{a,b,t}$$





- formula denotes notation found in the paper
- at least: adaptively chosen plain-cipher-text attack

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

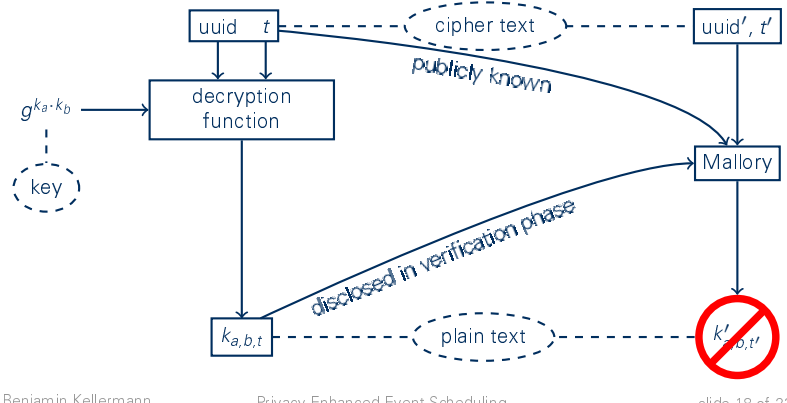


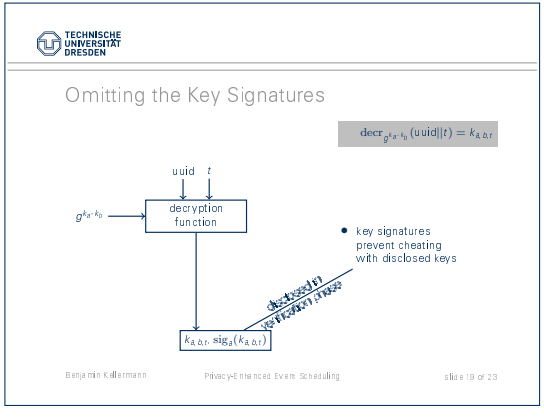
Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

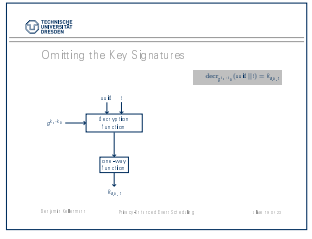
Simplifying the Key Exchange

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





1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

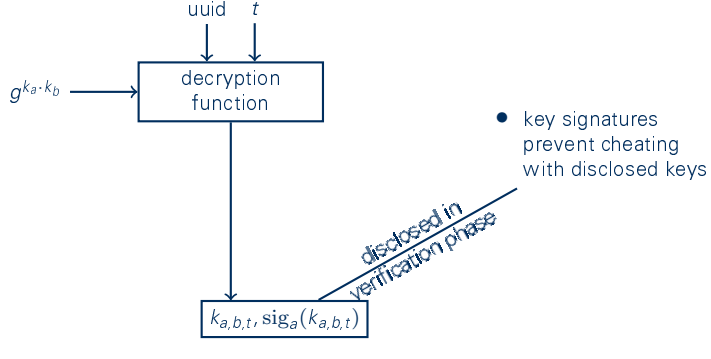


Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

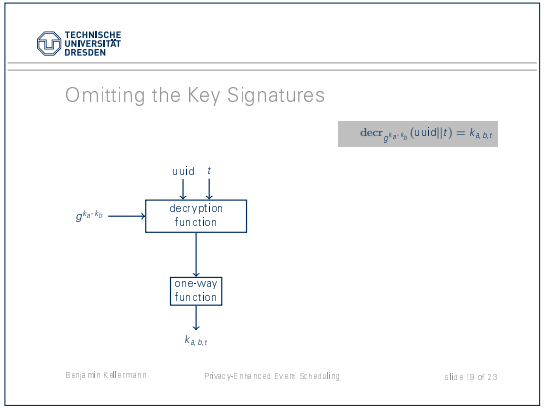
TECHNISCHE UNIVERSITÄT DRESDEN

Omitting the Key Signatures

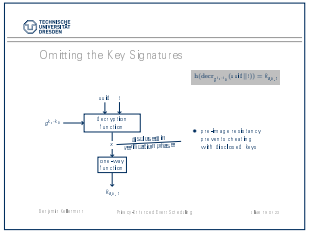
$$\mathrm{decr}_{g^{k_a \cdot k_b}}(\mathrm{uuid}||t) = k_{a,b,t}$$



- key signatures prevent cheating with disclosed keys



1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

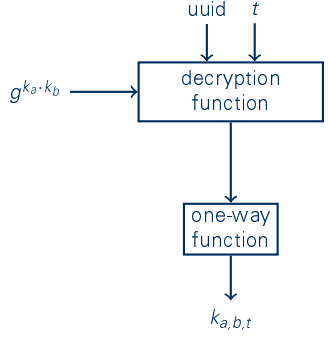
Evaluation
- Evaluation

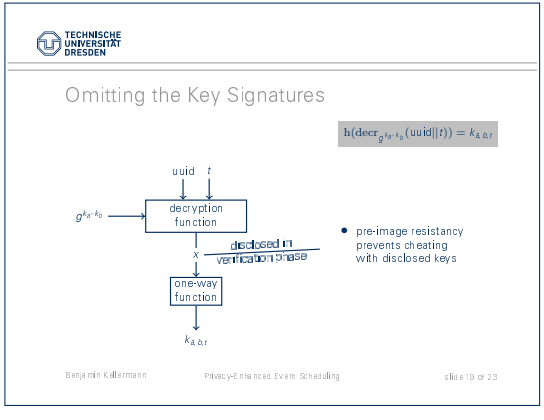
Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

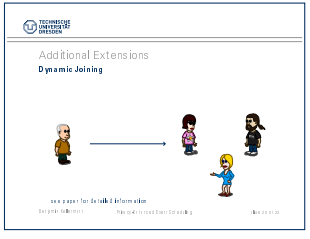
Omitting the Key Signatures

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





1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

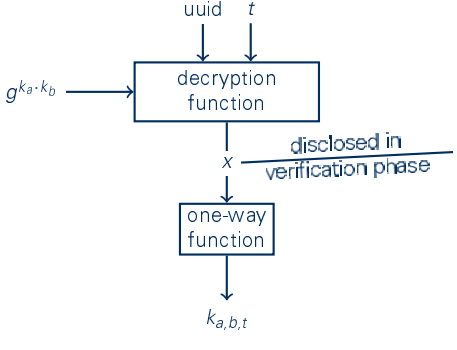


Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

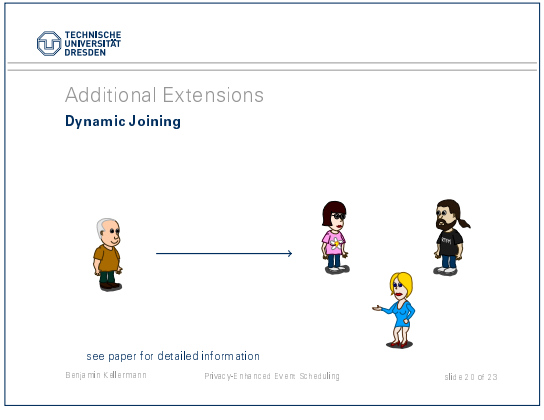
TECHNISCHE UNIVERSITÄT DRESDEN

Omitting the Key Signatures

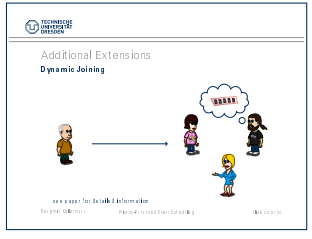
$$\mathrm{h}(\mathrm{decr}_{g^{k_a}\cdot k_b}(\mathrm{uuid}||t)) = k_{a,b,t}$$



- pre-image resistancy prevents cheating with disclosed keys



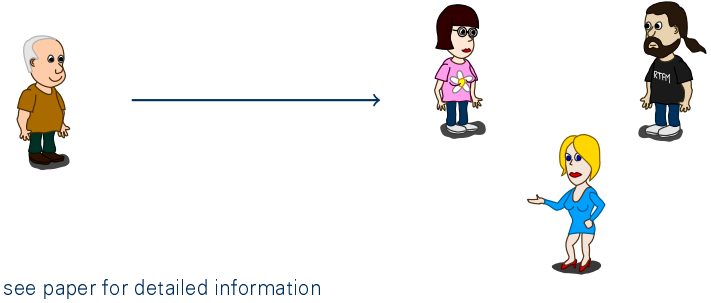
1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



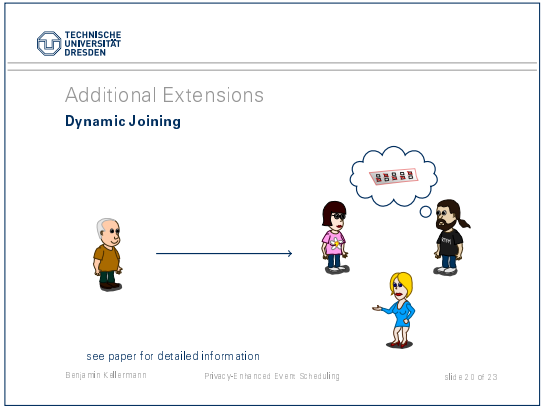
Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

Additional Extensions

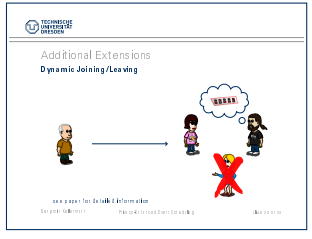
Dynamic Joining



see paper for detailed information



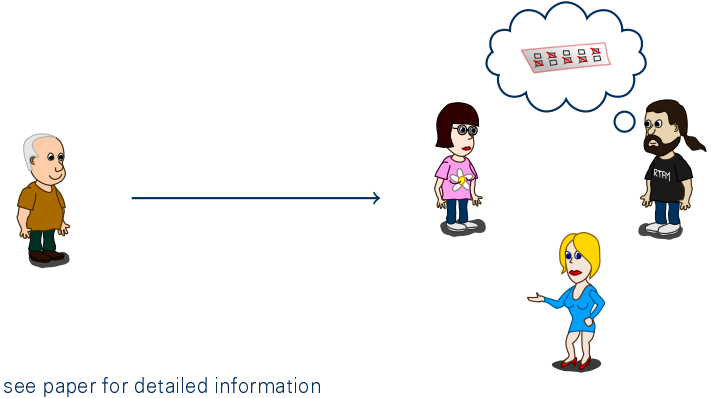
1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



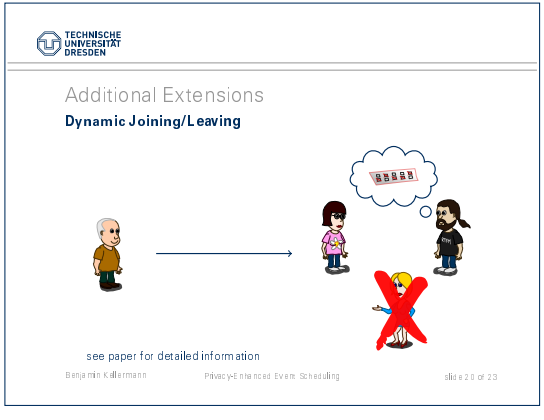
Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

Additional Extensions

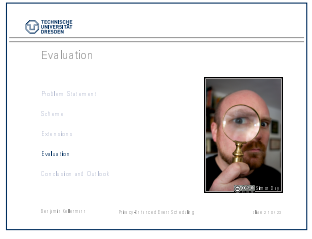
Dynamic Joining



see paper for detailed information



1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

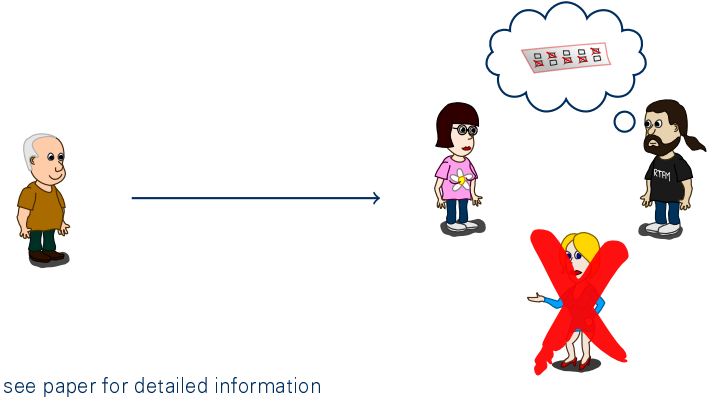


Problem Statement
Event Scheduling
Direct Inference
Indirect Inference
Requirements
E-Voting vs. Event Scheduling
Scheme
Superposed Sending
Poll Initialization
Casting of Votes
Result Publication
Trying to Cheat
Result Verification
Extensions
Simplifying the Key Exchange
Omitting the Key Signatures
Additional Extensions
Evaluation
Evaluation
Conclusion and Outlook
Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Additional Extensions

Dynamic Joining/Leaving



see paper for detailed information

Evaluation

Problem Statement

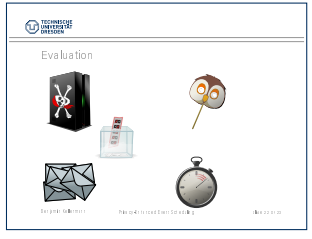
Scheme

Extensions

Evaluation

Conclusion and Outlook

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Evaluation

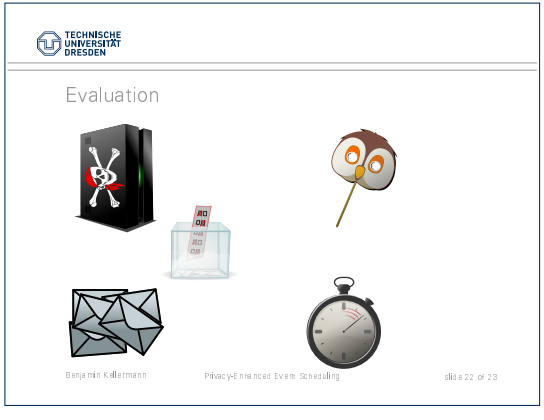
Problem Statement

Scheme

Extensions

Evaluation

Conclusion and Outlook



- no trusted entity

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

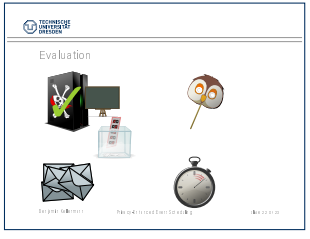
Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

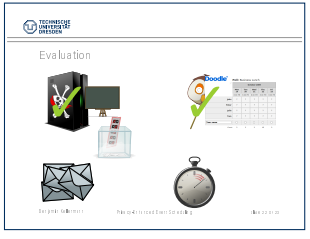
Conclusion and Outlook
- Conclusion and Outlook



Evaluation

- no trusted entity

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

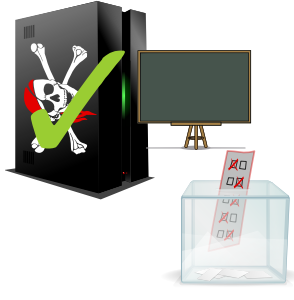
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

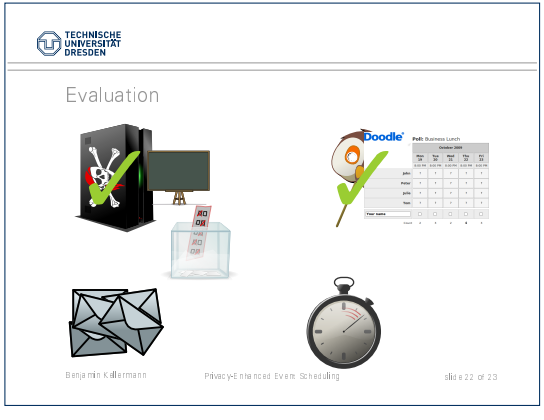
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

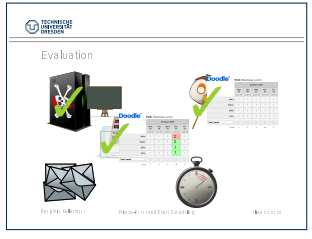
TECHNISCHE UNIVERSITÄT DRESDEN

Evaluation





1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

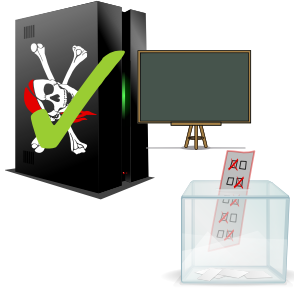
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

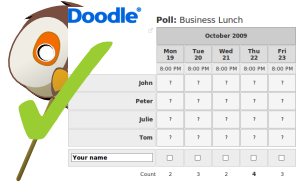
Evaluation
- Evaluation

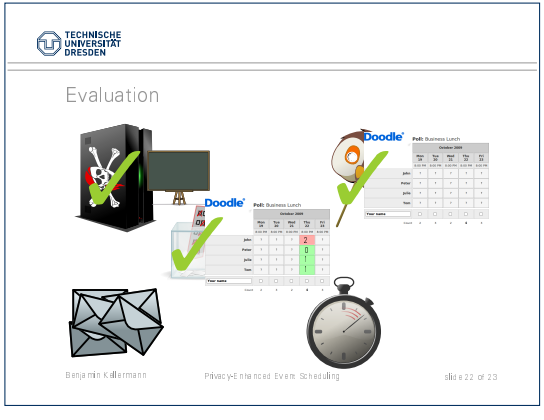
Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

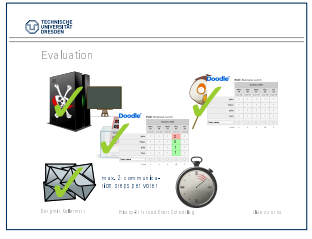
Evaluation







1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

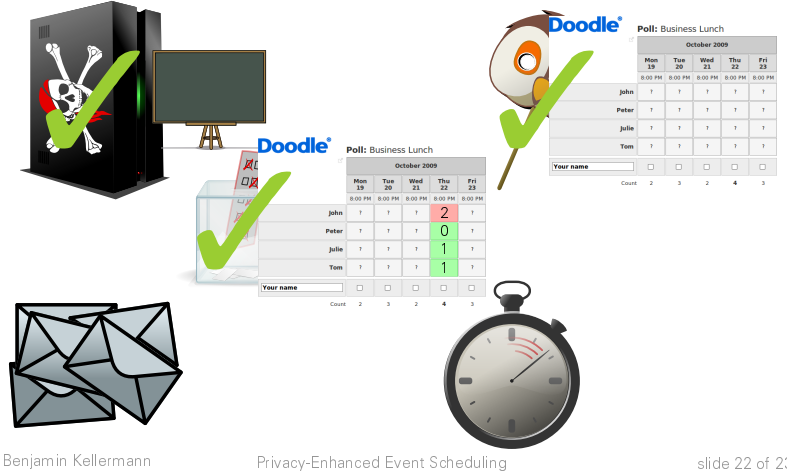
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

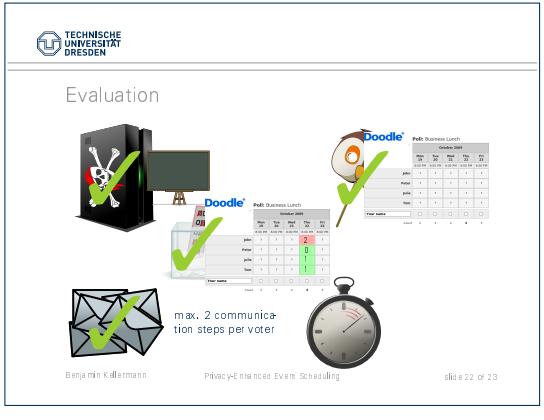
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

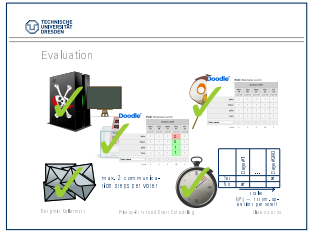
Evaluation





- not more than doodle

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23



Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

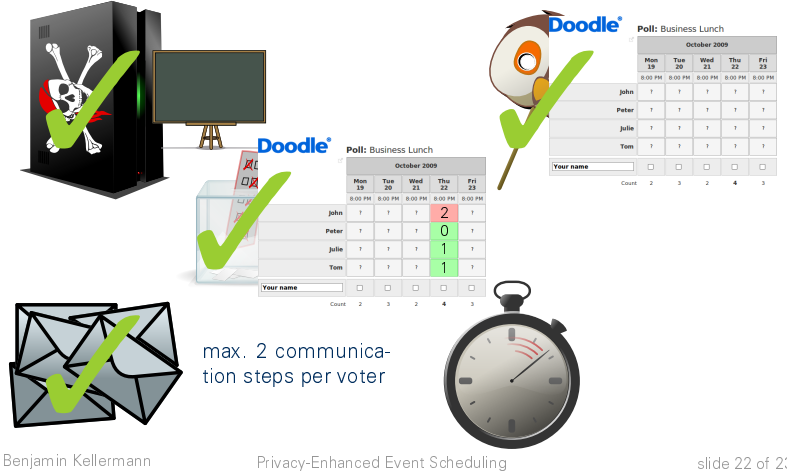
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

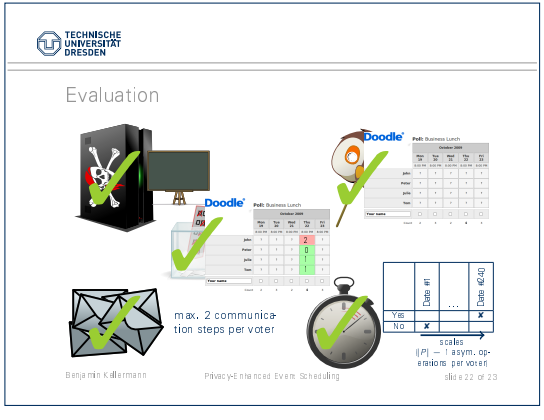
Evaluation
- Evaluation

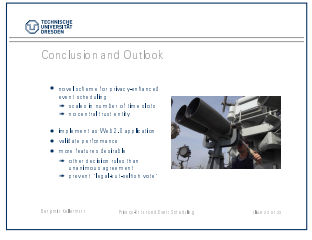
Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Evaluation







1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

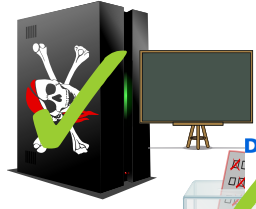
Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

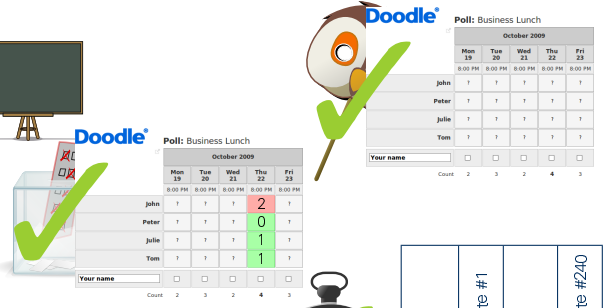
Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Evaluation





max. 2 communication steps per voter

	Date #1	...	Date #240
Yes			✘
No	✘		

scales
(|P| — 1 asym. operations per voter)

Conclusion and Outlook

- novel scheme for privacy-enhanced event scheduling
  - scales in number of time slots
  - no central trust entity
- implement as Web 2.0 application
- validate performance
- more features desirable
  - other decision rules than unanimous agreement
  - prevent "legal-but-selfish vote"

1 2 3
4 5 6
7 8 9
10 11 12
13 14 15
16 17 18
19 20 21
22 23

TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Elektrotechnik und Informationstechnik, Fachgebiet Datenschutz und Datensicherheit

Thank you for your attention!

Discussion

Benjamin.Kellermann@tu-Dresden.de
0352 4463 3505 0258 8575
0092 3501 1832 491A 3D9C

Vancouver, August 29, 2009

Problem Statement
- Event Scheduling
- Direct Inference
- Indirect Inference
- Requirements
- E-Voting vs. Event Scheduling

Scheme
- Superposed Sending
- Poll Initialization
- Casting of Votes
- Result Publication
- Trying to Cheat
- Result Verification

Extensions
- Simplifying the Key Exchange
- Omitting the Key Signatures
- Additional Extensions

Evaluation
- Evaluation

Conclusion and Outlook
- Conclusion and Outlook

TECHNISCHE UNIVERSITÄT DRESDEN

Conclusion and Outlook

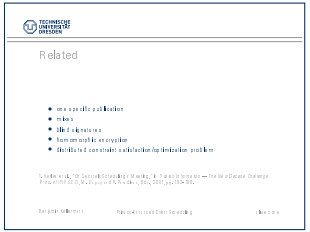
- novel scheme for privacy-enhanced event scheduling
  - scales in number of time slots
  - no central trust entity
- implement as Web 2.0 application
- validate performance
- more features desirable
  - other decision rules than unanimous agreement
  - prevent "legal-but-selfish vote"

Thank you for your attention!

Discussion

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

Vancouver, August 29, 2009



Related
Dynamic Joining
Dynamic Leaving
Computational Complexity
More Features

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

Thank you for your attention!

Discussion

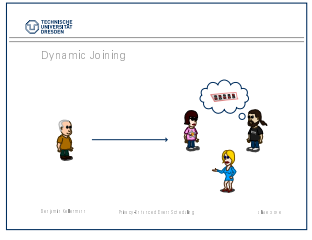
Benjamin.Kellermann@tu-dresden.de
D19E 04A8 8895 020A 8DF6
0092 3501 1A32 491A 3D9C

Vancouver, August 29, 2009

Related

- one specific publication
- mixes
- blind signatures
- homomorphic encryption
- distributed constraint satisfaction/optimization problem

T. Herlea et al., "On Securely Scheduling a Meeting," in *Trusted Information — The New Decade Challenge (Proc. of IFIP SEC)*, M. Dupuy and P. Paradinas, Eds., 2001, pp. 183–198.



Related
Dynamic Joining
Dynamic Leaving
Computational Complexity
More Features

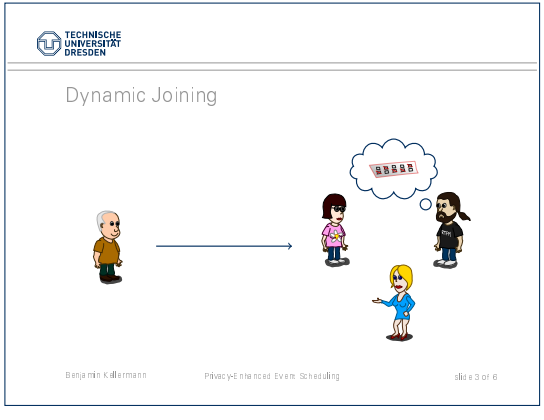
TECHNISCHE UNIVERSITÄT DRESDEN

Related

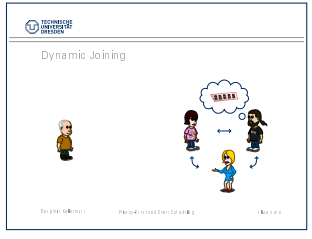
- one specific publication
- mixes
- blind signatures
- homomorphic encryption
- distributed constraint satisfaction/optimization problem

T. Herlea et al., "On Securely Scheduling a Meeting," in *Trusted Information — The New Decade Challenge (Proc. of IFIP SEC)*, M. Dupuy and P. Paradinas, Eds., 2001, pp. 183–198.

Benjamin Kellermann Privacy-Enhanced Event Scheduling slide 2 of 6



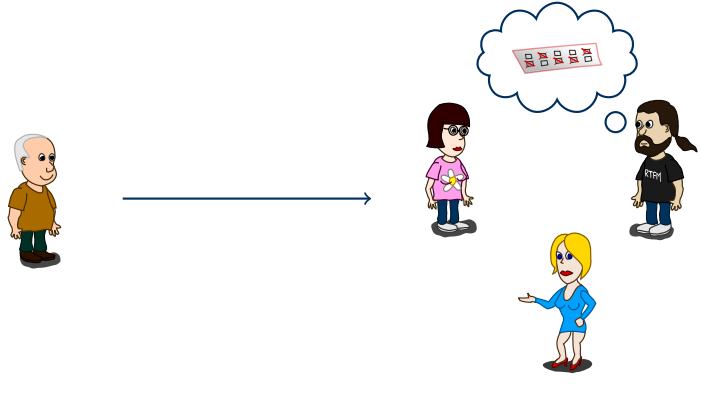
1 2 3
4 5 6



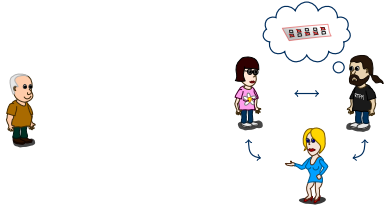
Related
Dynamic Joining
Dynamic Leaving
Computational Complexity
More Features

TECHNISCHE UNIVERSITÄT DRESDEN

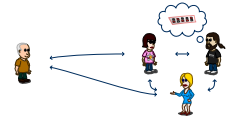
Dynamic Joining



Dynamic Joining



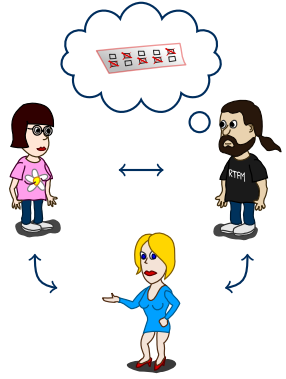
TECHNISCHE UNIVERSITÄT DRESDEN
Dynamic Joining

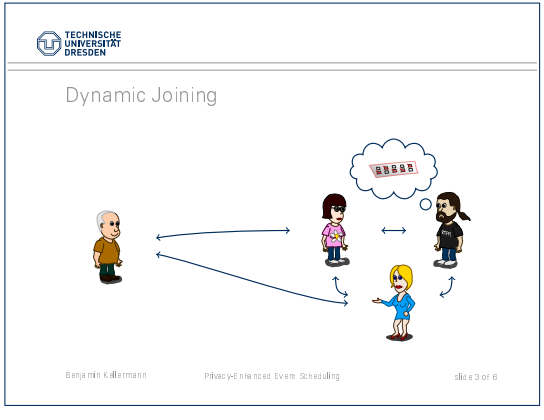


Related
Dynamic Joining
Dynamic Leaving
Computational Complexity
More Features

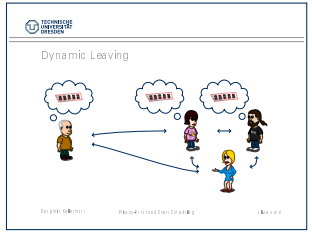
TECHNISCHE UNIVERSITÄT DRESDEN

Dynamic Joining





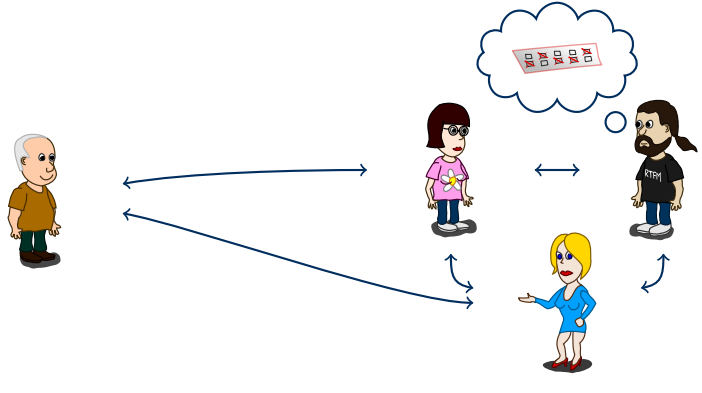
1 2 3
4 5 6



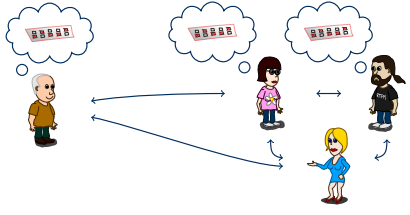
Related
Dynamic Joining
Dynamic Leaving
Computational Complexity
More Features

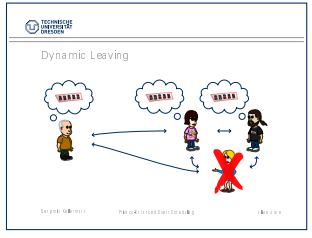
TECHNISCHE UNIVERSITÄT DRESDEN

Dynamic Joining



Dynamic Leaving

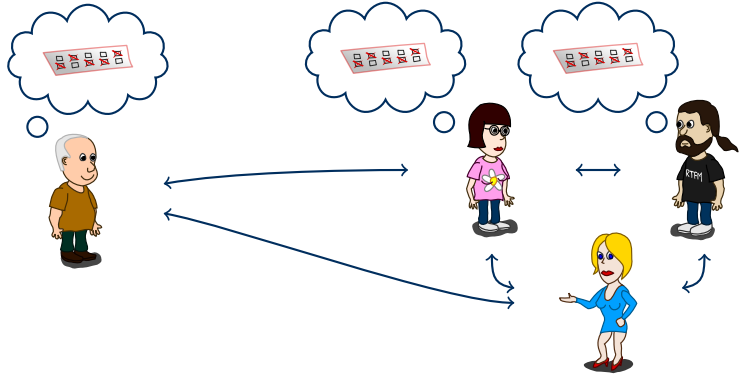


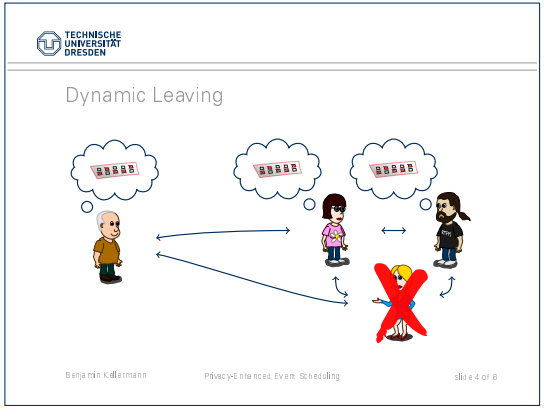


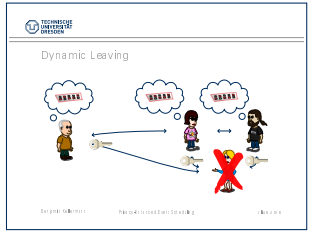
Related
Dynamic Joining
Dynamic Leaving
Computational Complexity
More Features

TECHNISCHE UNIVERSITÄT DRESDEN

Dynamic Leaving



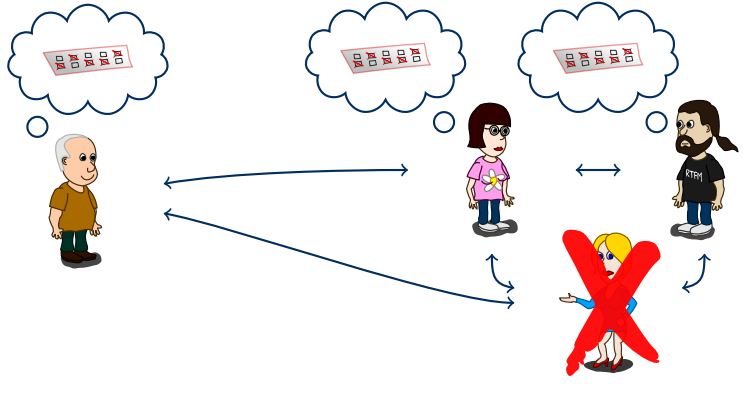




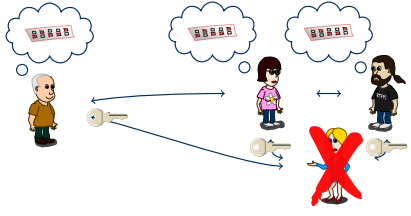
Related
Dynamic Joining
Dynamic Leaving
Computational Complexity
More Features

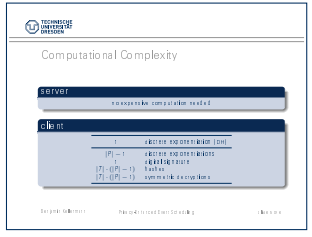
TECHNISCHE UNIVERSITÄT DRESDEN

Dynamic Leaving



Dynamic Leaving

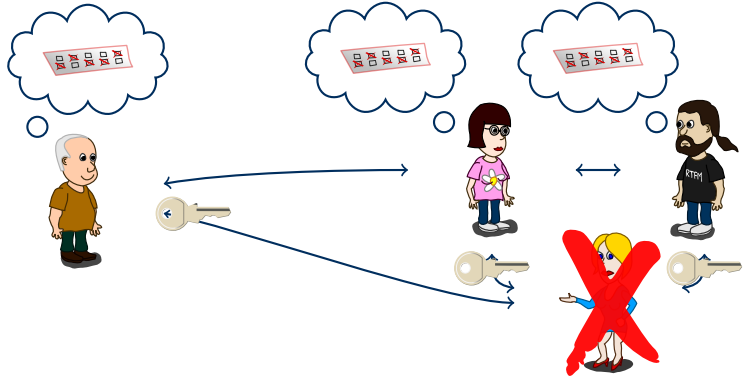




Related
Dynamic Joining
Dynamic Leaving
Computational Complexity
More Features

TECHNISCHE UNIVERSITÄT DRESDEN

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

TECHNISCHE UNIVERSITÄT DRESDEN

More Features

- initiator's scheme
- Randomization/rotation/deletion of time slots
- spoiling/revoking votes
- other decision rules than unanimous agreement
- let voters prove that they signed a valid ballot for more than a certain minimum number of time slots

Related
Dynamic Joining
Dynamic Leaving
Computational Complexity
More Features

TECHNISCHE UNIVERSITÄT DRESDEN

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

Benjamin Kellermann Privacy-Enhanced Event Scheduling slide 5 of 6

More Features

- threshold scheme
- dynamic insertion/deletion of time slots
- updating/revoking votes
- other decision rules than unanimous agreement
- let voters prove that they signaled availability for more than a certain minimum number of time slots

Related
Dynamic Joining
Dynamic Leaving
Computational Complexity
More Features

TECHNISCHE UNIVERSITÄT DRESDEN

More Features

- threshold scheme
- dynamic insertion/deletion of time slots
- updating/revoking votes
- other decision rules than unanimous agreement
- let voters prove that they signaled availability for more than a certain minimum number of time slots