



Privacy-Preserving Applications on Mobile Devices

Prof. Dr. Ulrike Meyer

In cooperation with Prof. Dr. Susanne Wetzel, Stevens Institute of Technology

When shall we meet?

Hope he does not find out...
... that I watch DHW
... that I am attending the lecture on
mobile security FOR FUN



Hope she does not find out...
... that I am working night shifts
... that I have an opera subscription

- Both have something to keep private for now
- Both are honest but curious
 - Will not lie about the time at which they are available
 - Are curious to find out more about the other



...of course I could skip the lecture if this was the only option...

...I am not going to skip opera nights for her!



- Both have preferences
 - Which they also want to keep private
- How can they agree upon a date in a fair but privacy-preserving way?

- Overall set of possible time slots X represented by integers
- Alice and Bob choose subsets A and B of X
 - $A = \{a_1, a_2, \dots, a_k\}$ and $B = \{b_1, b_2, \dots, b_k\}$ of same size k
- Both rank the time slots in their subsets according to their preferences
- Goal: find “the best” time slot that both have in common

	Alice	Bob
K Points	a1	b1
K-1 Points	a2	b2
	.	.
	.	.
	.	.
1 Point	ak	bk

	Alice	Bob
5 Points	a1	b1
4 Points	a2	b2
3 Points	a3	b3
2 Points	a4	b4
1 Points	a5	b5

Maximize sum of points



- Sum of points a1 = b5: 6
- Sum of points a3 = b4: 5
- Sum of points a5 = b2: 5
- **Best: a1 = b5**

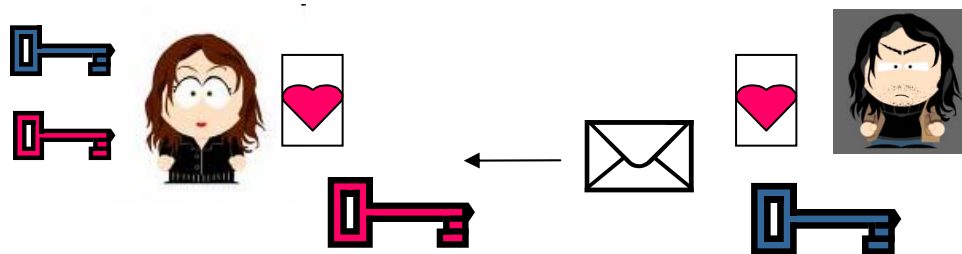
Maximize minimum of points

- Min of points a1, b5 = 1
- Min of points a3, b4 = 2
- Min of points a5, b2 = 1
- **Best: a3 = b4**

- **We developed protocols for both ways of maximizing the joint preferences**
- **Open: are there more interesting ones?**

Public key cryptosystem

- Public key for encryption 
- Private key for decryption 

Semantically secure

- Public key is not sufficient to decide if  contains  or 

Notations:






$$E(\text{heart}) = \text{envelope}$$

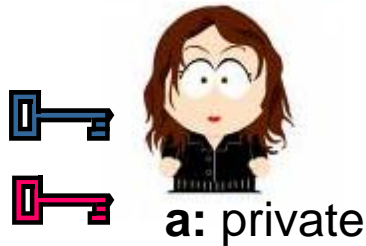
$$E(\text{yellow heart} + \text{purple heart}) = E(\text{green heart}) = \text{green envelope}$$

$$E(\text{yellow heart}) = \text{yellow envelope}$$

$$E(k \cdot \text{purple heart}) = E(\text{blue heart}) = \text{blue envelope}$$

Homomorphic

- From  and  and public key one can compute 
without knowledge of the **private key** or the **plaintexts**
- From  and **k** and public key one can compute 
without knowledge of the **private key** or the **plaintexts**

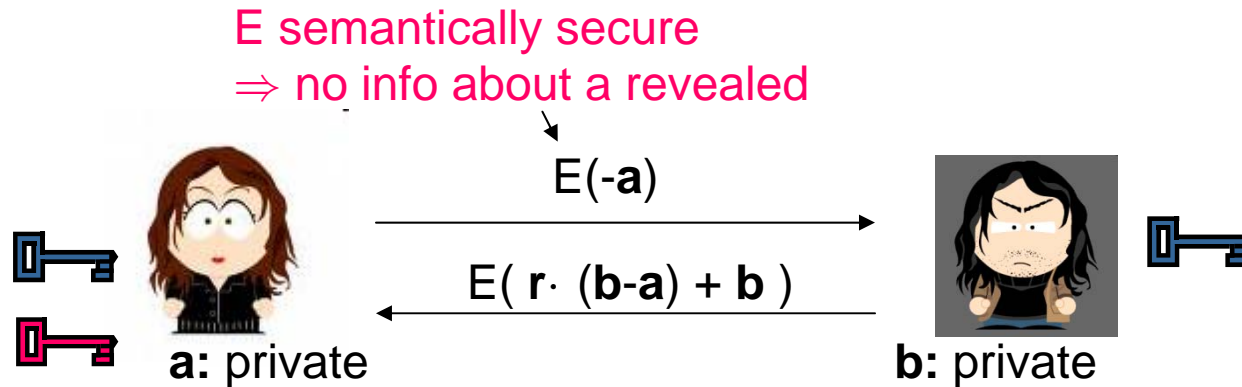


Initial Knowledge

- Alice has private input **a**, public/private key pair
- Bob has private input **b**, public key of Alice

Goal

- Bob and Alice want that Alice can check if **a = b**
 - Alice should not get any info about **b** if **a ≠ b**
 - Bob should not get any info about **a**



Alice

- computes $E(-a)$

Bob

- chooses random r
- computes $E(b)$
- computes $E(b-a)$, $E(r \cdot (b-a))$, $E(r \cdot (b-a) + b)$

E is homomorphic

Alice

- decrypts $E(r \cdot (b-a) + b)$
 - Iff it decrypts to b , then $a=b$
 - Otherwise, it decrypts to random value

Idea:

- Use several rounds of private matching
- Do that in an order such that the common time slot that maximizes the sum of points is found first

1st round

Alice	Bob
a1	b1
a2	b2
a3	b3
a4	b4
a5	b5

2nd round

Alice	Bob
a1	b1
a2	b2
a3	b3
a4	b4
a5	b5

3rd round

Alice	Bob
a1	b1
a2	b2
a3	b3
a4	b4
a5	b5

4th round

Alice	Bob
a1	b1
a2	b2
a3	b3
a4	b4
a5	b5

5th round

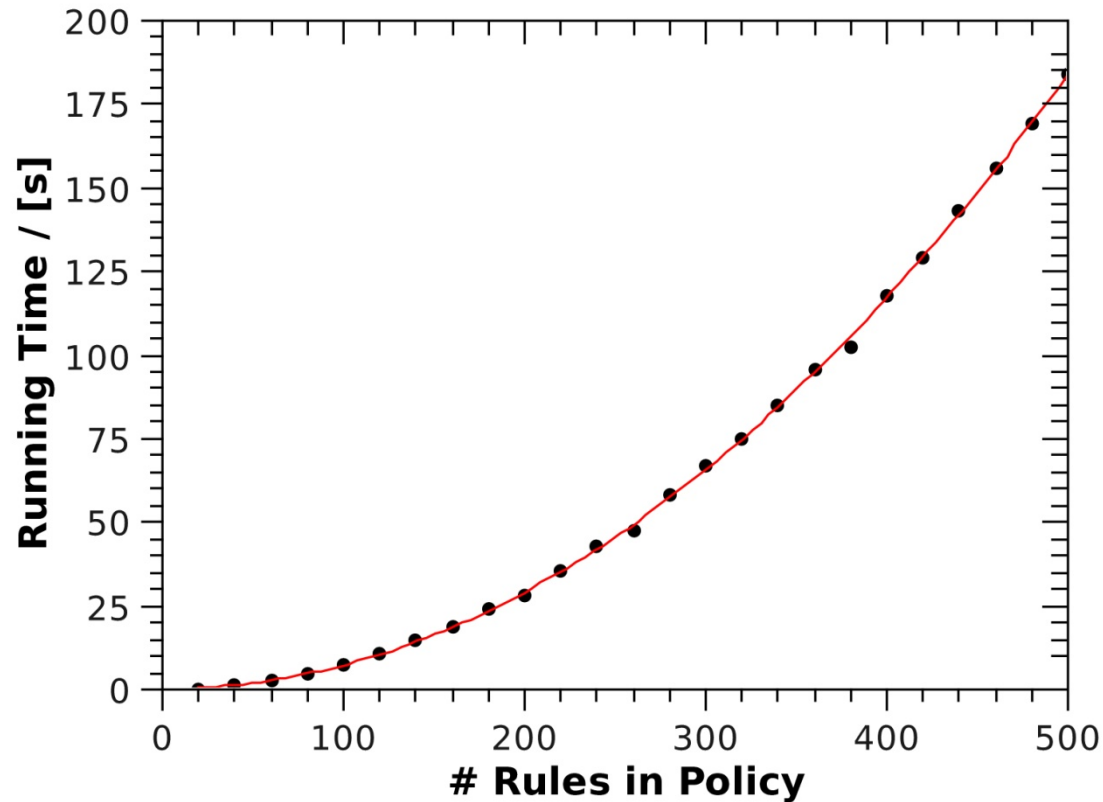
Alice	Bob
a1	b1
a2	b2
a3	b3
a4	b4
a5	b5

Alice	Bob
a1	b1
a2	b2
a3	b3
a4	b4
a5	b5

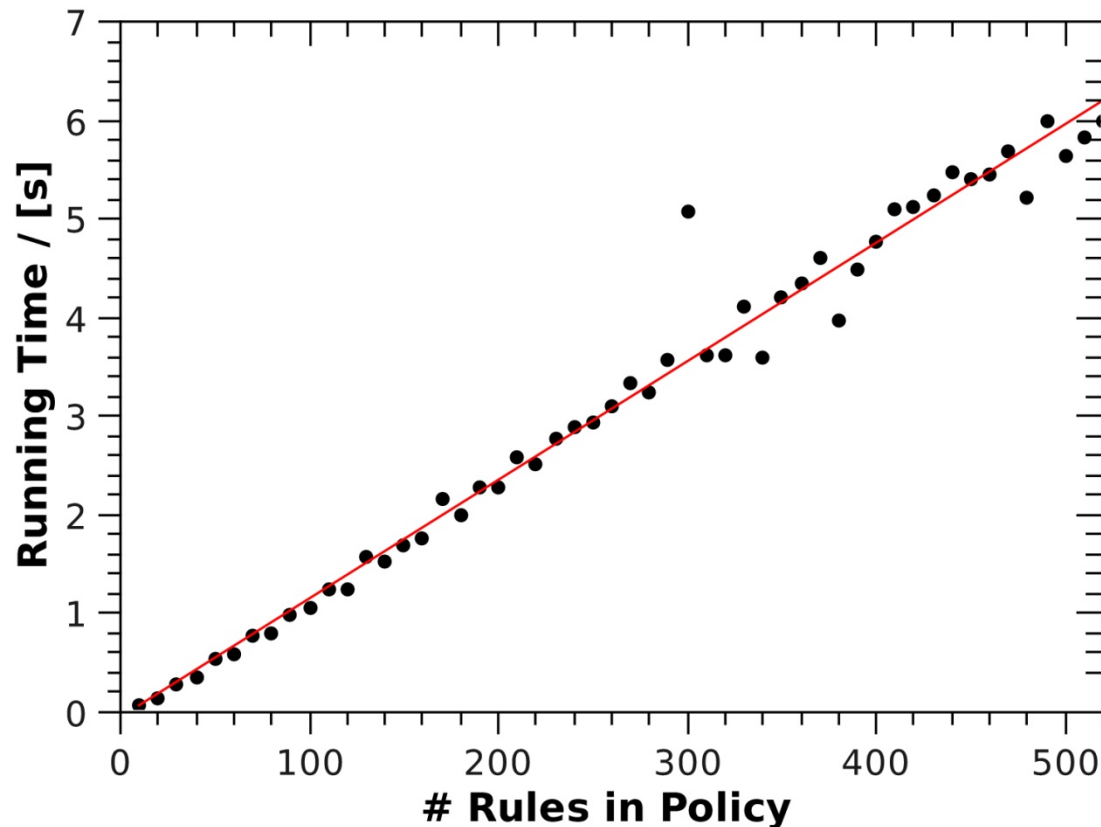
Alice	Bob
a1	b1
a2	b2
a3	b3
a4	b4
a5	b5

Alice	Bob
a1	b1
a2	b2
a3	b3
a4	b4
a5	b5

Alice	Bob
a1	b1
a2	b2
a3	b3
a4	b4
a5	b5



- Dates encoded in bit strings of length 10
- Density of common dates: 5%
- Averaged over 500 runs



- Calendar application for scheduling a meeting
 - Convenient for the user
 - Selection of possible dates and ordering them according to preferences
 - Automatic integration in calendar
 - Finding the correct partner as automated as possible
 - Usable on direct contact as well as remotely





Thanks for your Attention!