Design and analysis methods for privacy technologies

ERCIM WG STM Best Ph.D. Thesis Award

Carmela Troncoso – COSIC (KU Leuven)

Advisors: Prof. Bart Preneel and Prof. Claudia Diaz

Thanks to so many people

- George Danezis
- Claudia Diaz
- Orr Dunkelmann
- Bart Preneel
- Sebastian Faust
- Emilia Kasper
- Eleni Kosta
- Andrei Serjantov
- Benedikt Gierlichs
- Ingrid Verbauwhede
- Danny De Cock
- Steven J. Murdoch
- Ben Laurie
- Prateek Mittal
- Nikita Borisov
- Alfredo Rial
- Reza Shokri
- Julien Freudiger
- Jean-Pierre Hubaux
- Christophe Gueuens
- Josep Balasch
- Stefan Schiffner
- Enrique Costa-Montenegro
- Seda Gürses
- Ian Goldberg
- Femi Olumofin
- Juan Elices
- Fernando Perez-Gonzalez
- Ero Balsa
- George Theodorakopoulos
- Jean-Yves Le Boudec

- Support staff at KUL, friends, family,…

Privacy is a very valuable asset

New technologies make our life easier and more comfortable

facebook Google

and we would like to enjoy technological advances while maintaining similar privacy guarantees as in the offline world

How can we ensure that systems actually protect privacy?

Design and analysis methods for privacy technologies

How can we build systems that integrate privacy protection?

“offline world” vs “online world”

face-to-face conversation

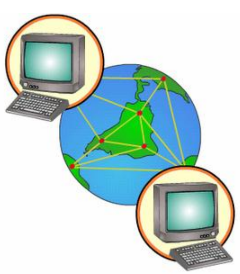
letters in the post

Knowing who your friends are

Paying with cash

Following your movements

Learning your shopping profile



Papers in physical archives

- Easy/cheap to collect, store search, and process
- Easy to copy/disseminate, but hard to destroy
- Easy to aggregate, make profiles and inferences
- Information never forgotten

Privacy-preserving solutions

- Trust organizations to protect data
  - No privacy towards data collector
  - Trust assumptions may not be realistic
    - incentives to misuse information
    - accidental leakages or malicious insiders
    - malicious outsiders exploiting vulnerabilities
  - Weak enforcement, low penalties
  - Once data is out there is no way back

- Design technology to provide assurances where possible
  - Privacy Enhancing Technologies

Privacy Enhancing Technologies

- Anonymous credentials
  - Prove an attribute meets a given condition without revealing its value
- Private Information Retrieval
  - Access to a database without revealing which entry has been queried
- Differential privacy
  - Extract statistical information from a database without revealing data about individual entries
- Anonymous communications, location privacy mechanisms,...

The challenge

- How to design privacy systems
  - Compositionality of privacy technologies
  - Privacy-by-design methods
- How to analyze privacy systems
  - Current analysis techniques ad-hoc
  - General analysis methods

- The lack of general methodologies hinders
  - The validation and comparison of systems
  - The development of robust PETs

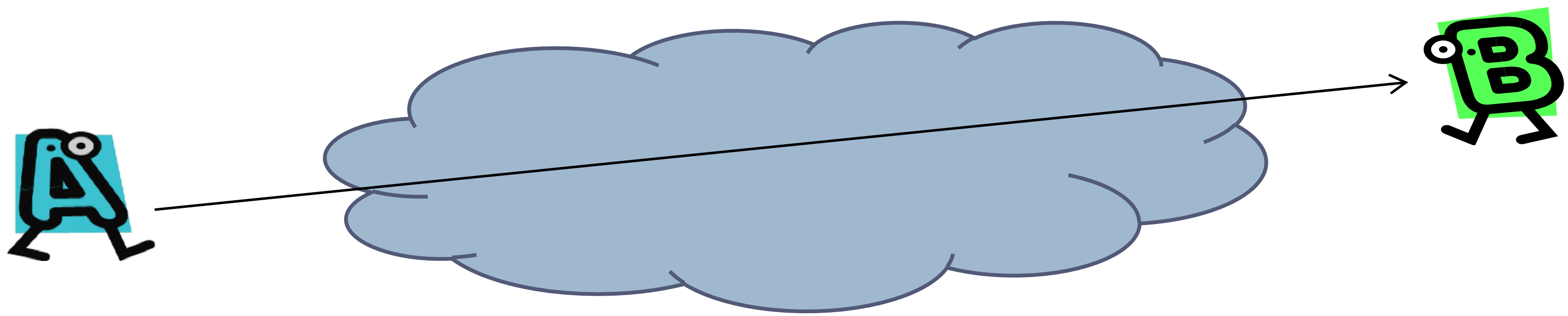
Thesis outline

Goal: *provide tools and guiding principles for the analysis and design of privacy-preserving systems*

- PART I: ANALYSIS OF PRIVACY-PRESERVING SYSTEMS
  - Chapter 2: Traffic analysis in anonymous communications
  - Chapter 3: Perfect matching disclosure attacks
  - Chapter 4: Bayesian inference to de-anonymize persistent communications
  - Chapter 5: A Bayesian framework for the analysis of anonymous communication systems
- PART II: DESIGN OF PRIVACY-PRESERVING SYSTEMS
  - Chapter 6: Location privacy: an overview
  - Chapter 7: Privacy-friendly pay-as-you-drive applications

Part I: Analysis of privacy-preserving systems

Anonymous communications

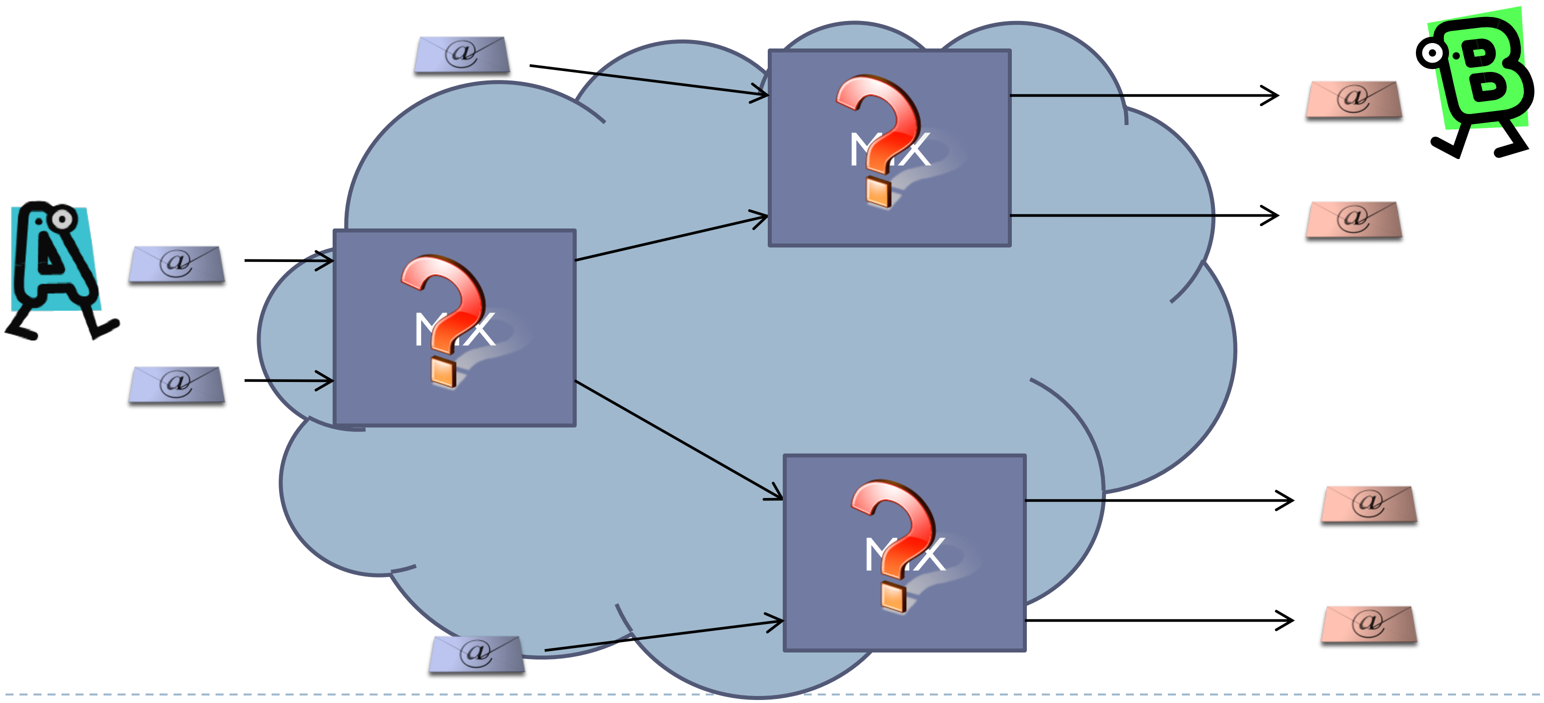


- Content protection is not enough, traffic data encodes information
  - Communication profiles

Anonymous Communications	vs	Traffic Analysis
Conceals who speaks with whom Modifies traffic data		Uncover who speak with whom Exploits traffic data

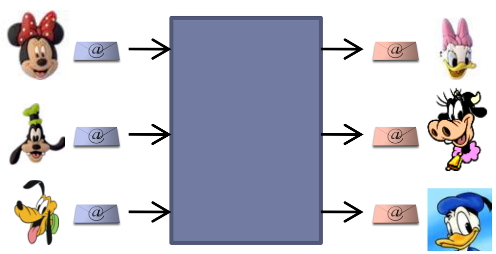
Mix networks

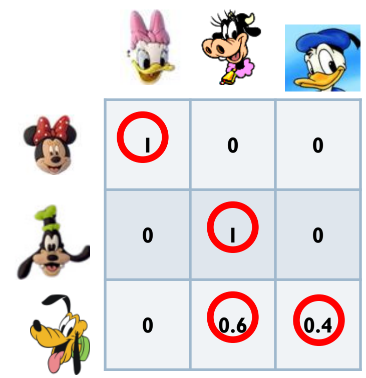
- Mixes hide relations between inputs and outputs
- Mixes are combined in networks in order to
  - Distribute trust (one good mix is enough)
  - Load balancing (no mix is big enough)



Perfect Matching Disclosure Attacks[1]

- Persistent communication partners can be uncovered observing the system long enough (de-anonymization and profiling) [Dan03, DS04,AK03,...]
- Key observation:
  - Considering all senders and receivers simultaneously yields better results





- Contributions
  - PMDA: attack based on finding maximum weighted perfect matchings
  - NSDA: attack based on normalizing matrixes to take into account interdependencies amongst sender profiles
  - Enhanced profiling technique re-using information

[1] Perfect matching disclosure attacks, C. Troncoso, B. Gierlichs, B. Preneel, and I. Verbauwhede. 8th International Symposium on Privacy Enhancing Technologies (PETS 2008)

Bayesian inference to de-anonymize persistent communications[2]

- PMDA: two disadvantages
  - Computationally bounded
  - Straightforward reuse of information biases the result
- Key contributions
  - Vida model: General model to abstract any anonymity system
  - Bayesian techniques to co-estimate profiles and de-anonymize messages
    - Optimal reuse of information
    - Sampling to reduce computation requirements
- Redefining the traffic analysis problem: given an observation find "hidden state" of an anonymity system

We know how to compute this

$$\Pr(HS \mid O, C) = \frac{\Pr(O \mid HS, C) \cdot \Pr(HS \mid C)}{\sum_{HS} \Pr(HS, O \mid C)}$$

Too large to enumerate!!

$$HS_1, HS_2, HS_3, \ldots \sim \Pr(HS \mid O, C)$$

Markov Chain Monte Carlo Methods – Gibbs sampler

 [2] Vida: How to use bayesian inference to de-anonymize persistent communications, G. Danezis and C. Troncoso, 9th International Symposium on Privacy Enhancing Technologies (PETS 2009)

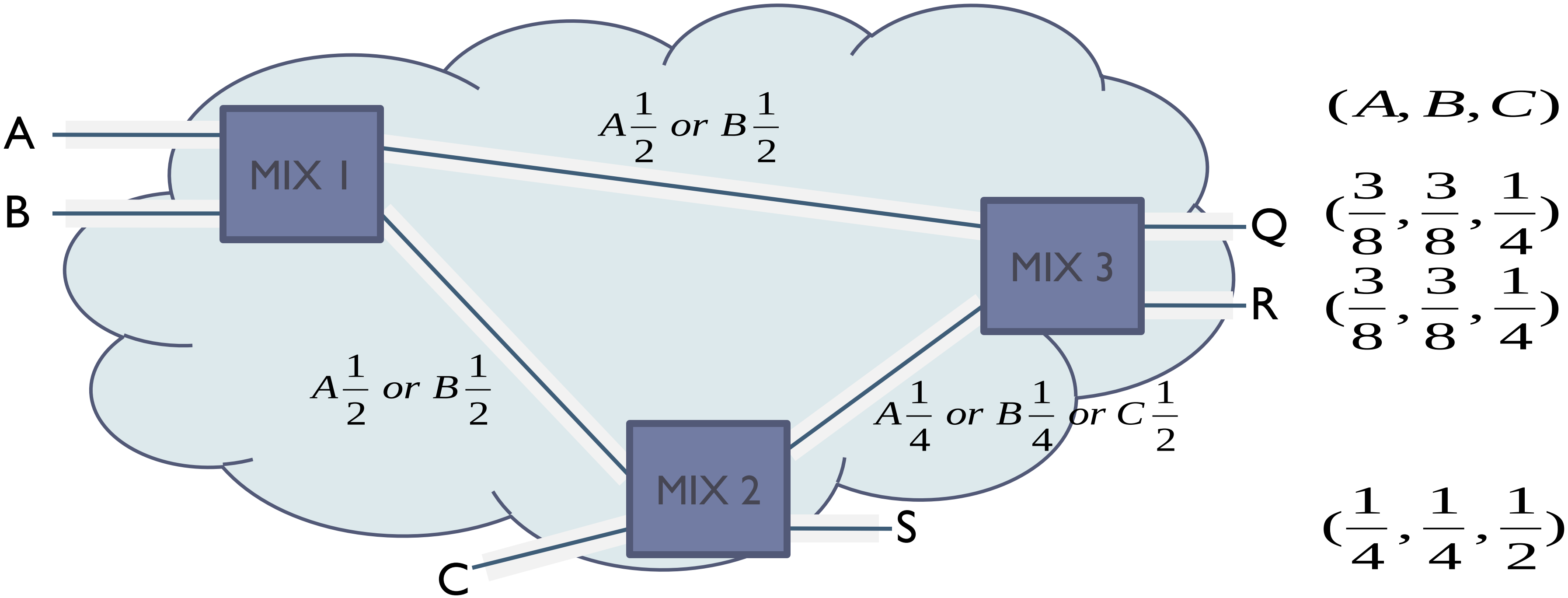
A Bayesian framework for the analysis of anonymous communication systems [3]

- In the past the analysis of anonymous communication systems
  - Based on heuristics and specific models, not generic
  - Systems are evaluated against one attack at a time
    - Network constraints [Dan03]
    - Users knowledge [DanSyv08]
    - Persistent communications [Dan03, DS04,AK03,...]
    - …
  - Simplified models
    - Exact calculation of probability distributions in complex systems was considered as an intractable problem [Serjantov02]

[3] The bayesian traffic analysis of mix networks, C. Troncoso and G. Danezis, 16th on Computer and Communications Security (CCS 2009)

Mix networks and traffic analysis

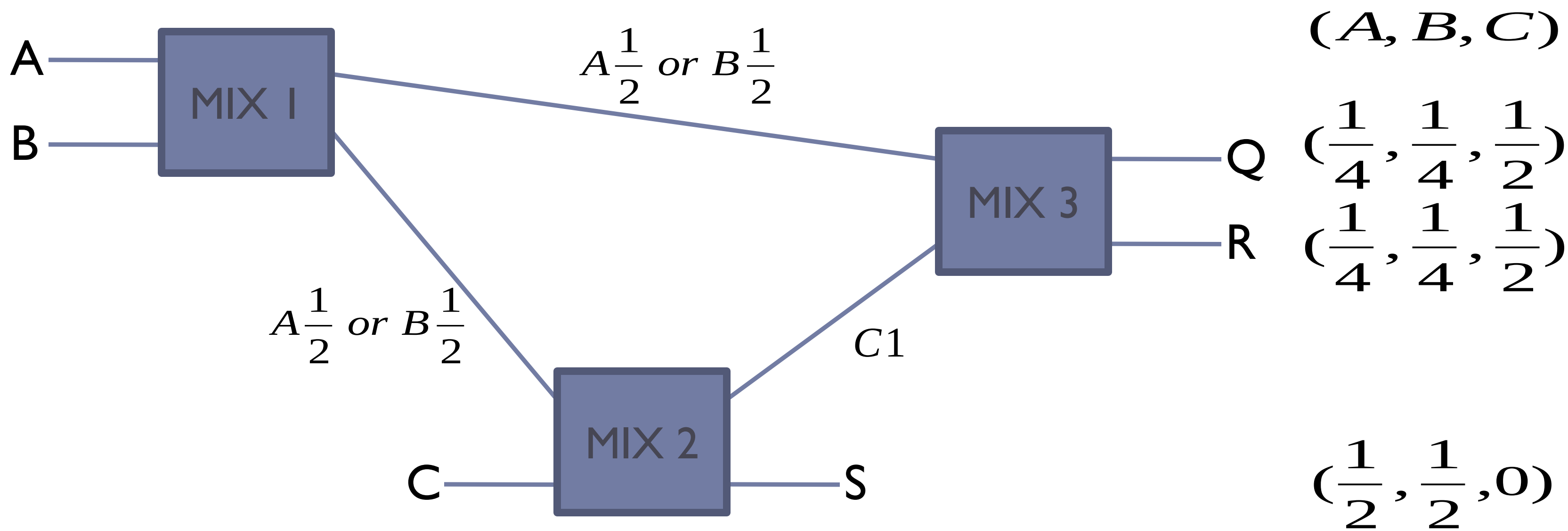
- Determine probability distributions input-output



- Threshold mix: collect t messages, and outputs them changing their appearance and in a random order

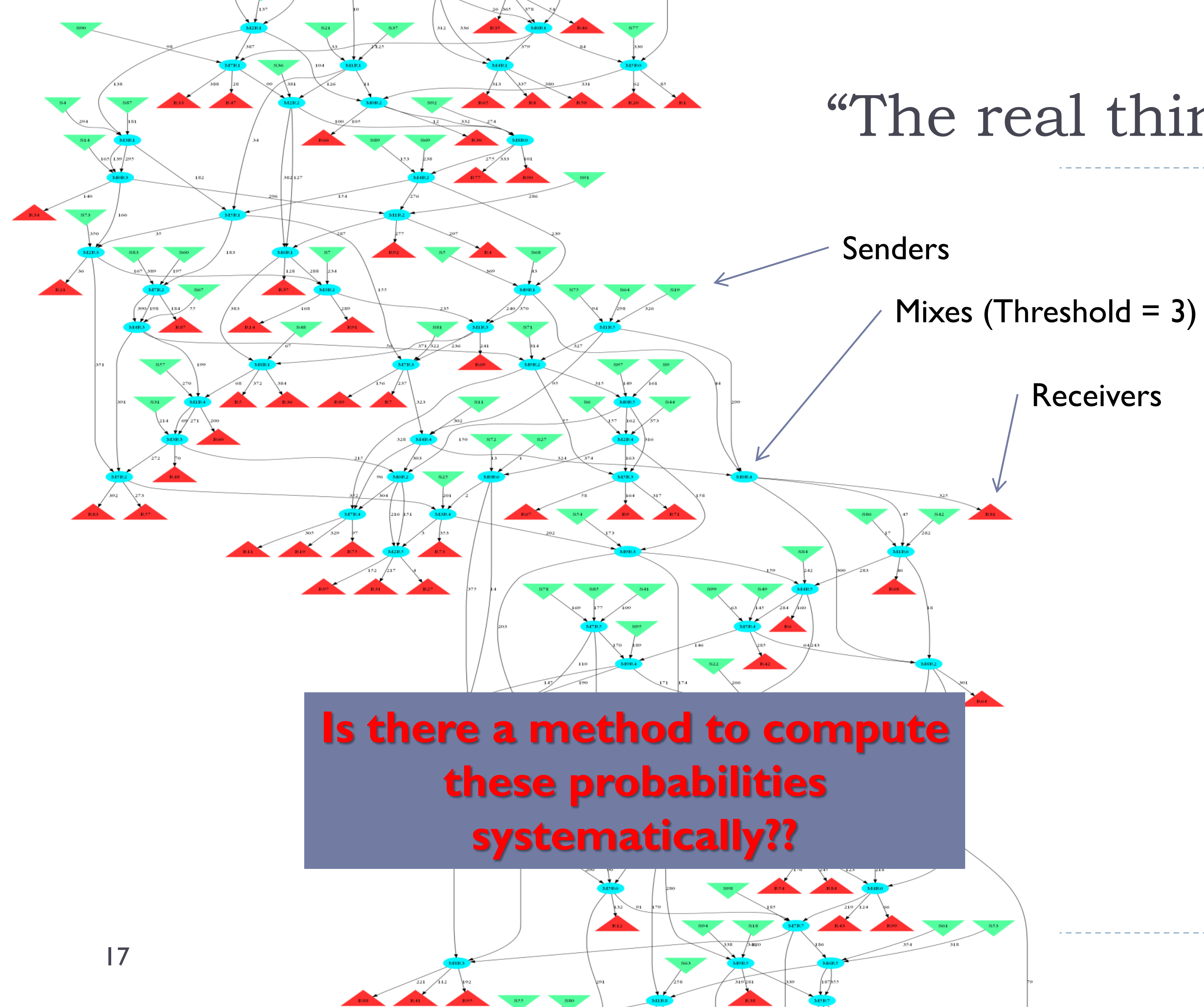
Mix networks and traffic analysis

- Constraints, e.g. length=2



Non trivial given observation!!

“The real thing”



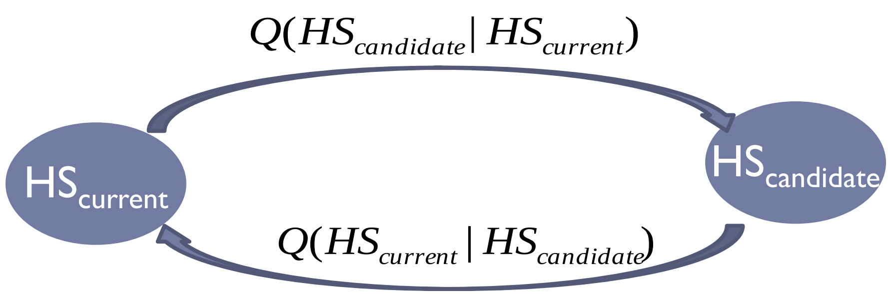
Is there a method to compute these probabilities systematically??

Sampling to estimate probabilities

- Recall: we reduce the traffic analysis problem to computing
$$\Pr(HS \mid O, C)$$
  - infeasible to compute analytically because there are too many HS
- … but we only care about marginal distributions
  - Is Alice speaking to Bob? $\Pr(A \to B \mid O, C)$
- We can calculate those if we have many samples of HS according to $\Pr(HS \mid O, C)$
  - We can simply count how many times Alice speaks to Bob
- Markov Chain Monte Carlo methods
  - Sample from a distribution difficult to sample from directly

Metropolis Hastings Algorithm

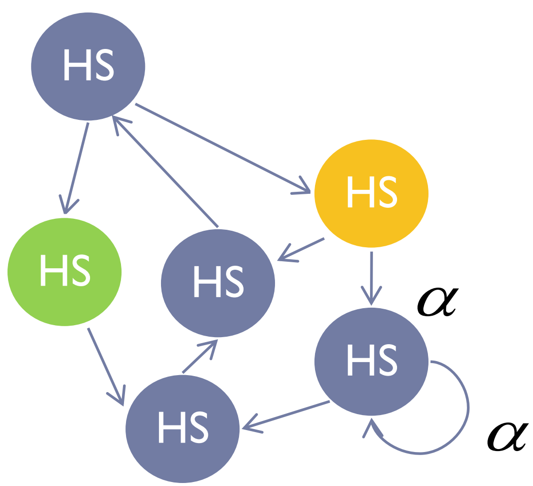
- Constructs a Markov Chain with stationary distribution $\Pr(HS \mid O, C)$



$$\alpha = \frac{\Pr(HS_{candidate})Q(HS_{candidate} \mid HS_{current})}{\Pr(HS_{current})Q(HS_{current} \mid HS_{candidate})}$$

$\alpha \geq 1$ **Go!**

$\alpha < 1$ **Go with probability α**



- Our transition results in dependant states
- Repeat this basic step to get independent samples of HS

Applications

- Evaluation information theoretic metrics for anonymity

$$H = -\sum_{R_i} P(A \rightarrow R_i \mid O, C) \cdot \log P(A \rightarrow R_i \mid O, C)$$

  - e.g., comparison of network topologies [3]
- Estimating probability of arbitrary events
  - Input message to output message?
  - Alice speaking to Bob ever?
  - Two messages having the same sender?
- Accommodate new constraints
  - Key to evaluate new mix network proposals

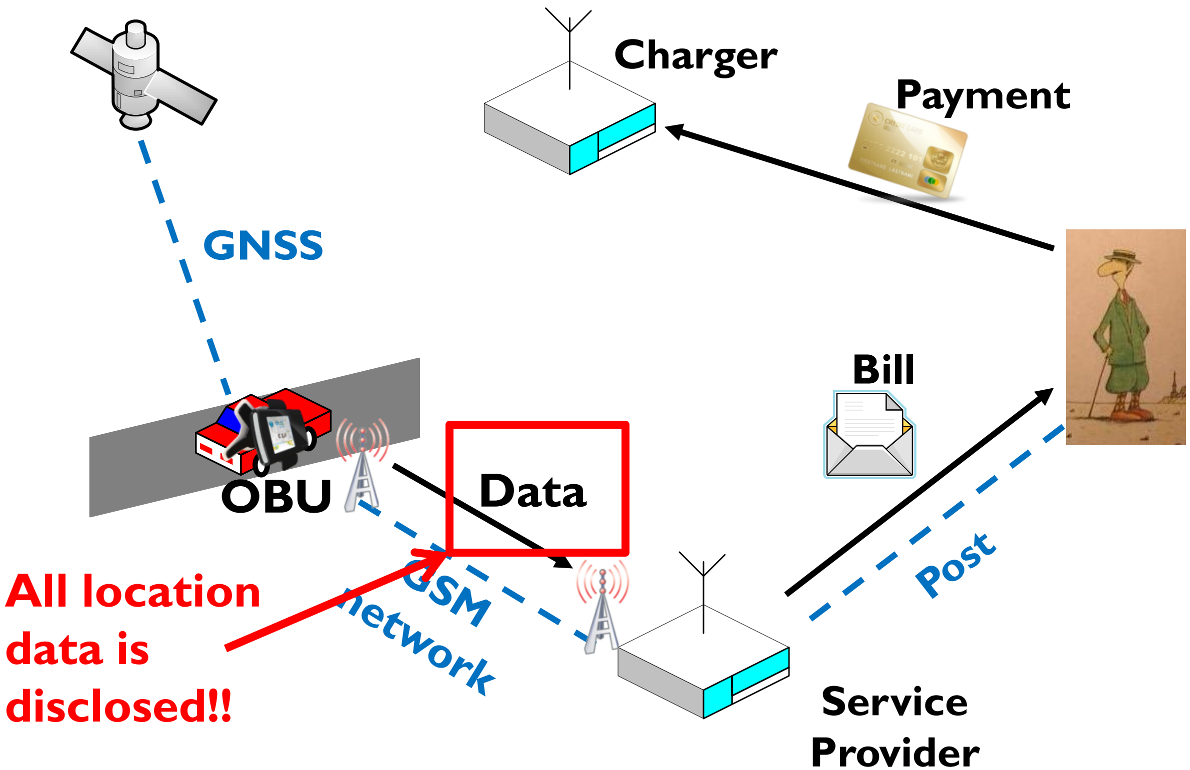
[3] Impact of Network Topology on Anonymity and Overhead in Low-Latency Anonymity Networks, C. Diaz, S. J. Murdoch, and C. Troncoso 10th Privacy Enhancing Technologies Symposium(PETS 2010)

Part II: Design of privacy-preserving systems

Pay-as-you-drive applications

- Pay-As-You-Drive: the concept
  - Concept:
    - Users should pay depending on their use of the car and roads:
      - Long drives, high density roads, rush hours: higher fee
      - Sporadic use, second vehicle for weekends, young drivers with small salary: smaller fee
  - Applications
    - Road pricing (ETP) - European Electronic Toll Service
      - Mandatory for vehicles above 3.5 tons by 2012
      - All vehicles by 2014
    - Vehicle insurance (PAYD)

Straightforward implementation



- Location data is highly sensitive
- Trust organization for privacy protection
- Third parties involved

Our contribution

- Two architectures for PAYD systems that fulfill privacy and security requirements
  - PriPAYD [4,5]
    - Key idea: processing of sensitive data local to the user
  - PrETP [6]
    - Key idea: advanced cryptography to fulfill security requirements

  - Holistic analysis
  - Ready to deploy in the real world

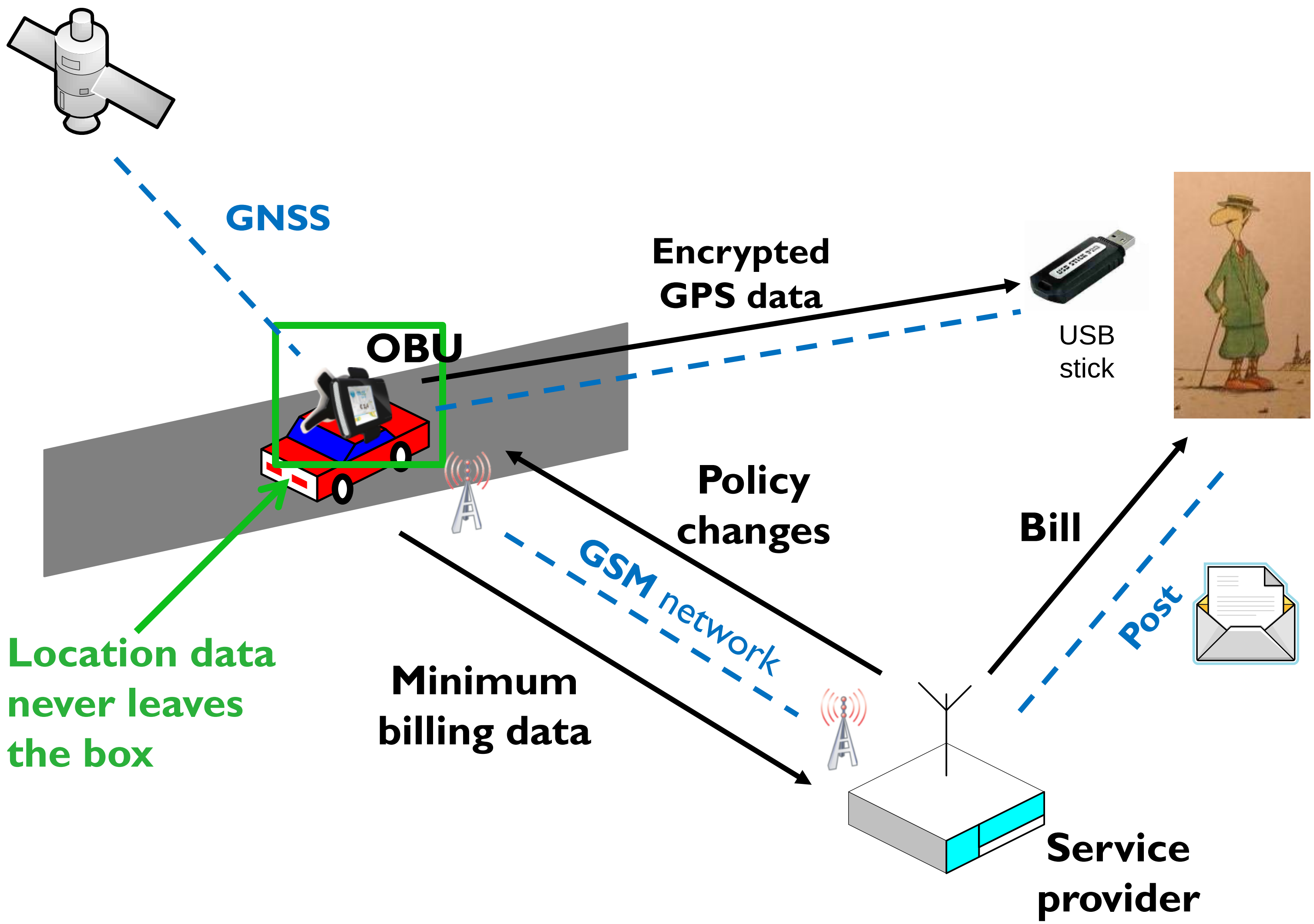
- Identification of design principles that lead to systems that offer strong privacy guarantees to their users

[4] PriPAYD: Privacy Friendly Pay-As-You-Drive Insurance, C. Troncoso, G. Danezis, E. Kosta and B. Preneel. WPES 2007
[5] PriPAYD: Privacy Friendly Pay-As-You-Drive Insurance, C. Troncoso, G. Danezis, E. Kosta, J. Balasch and B. Preneel. IEEE TDSC 2011
[6] PrETP: Privacy-preserving Electronic Toll Pricing J. Balasch, A. Rial, C. Troncoso, C. Geuens, B. Preneel, and I. Verbauwhede. Usenix Security 2010

Privacy-preserving Pay-as-you-drive

- Privacy issues?
  - Pay *as you drive*
  - Fine grained GPS data allows for inferences
- What data is necessary?
  - Final fee that the user must pay to the provider/government
    - No need to collect everyone's detailed location data
- Legal / service integrity issues
  - Actors must not be able to cheat
  - Actors must be held liable when misusing the system

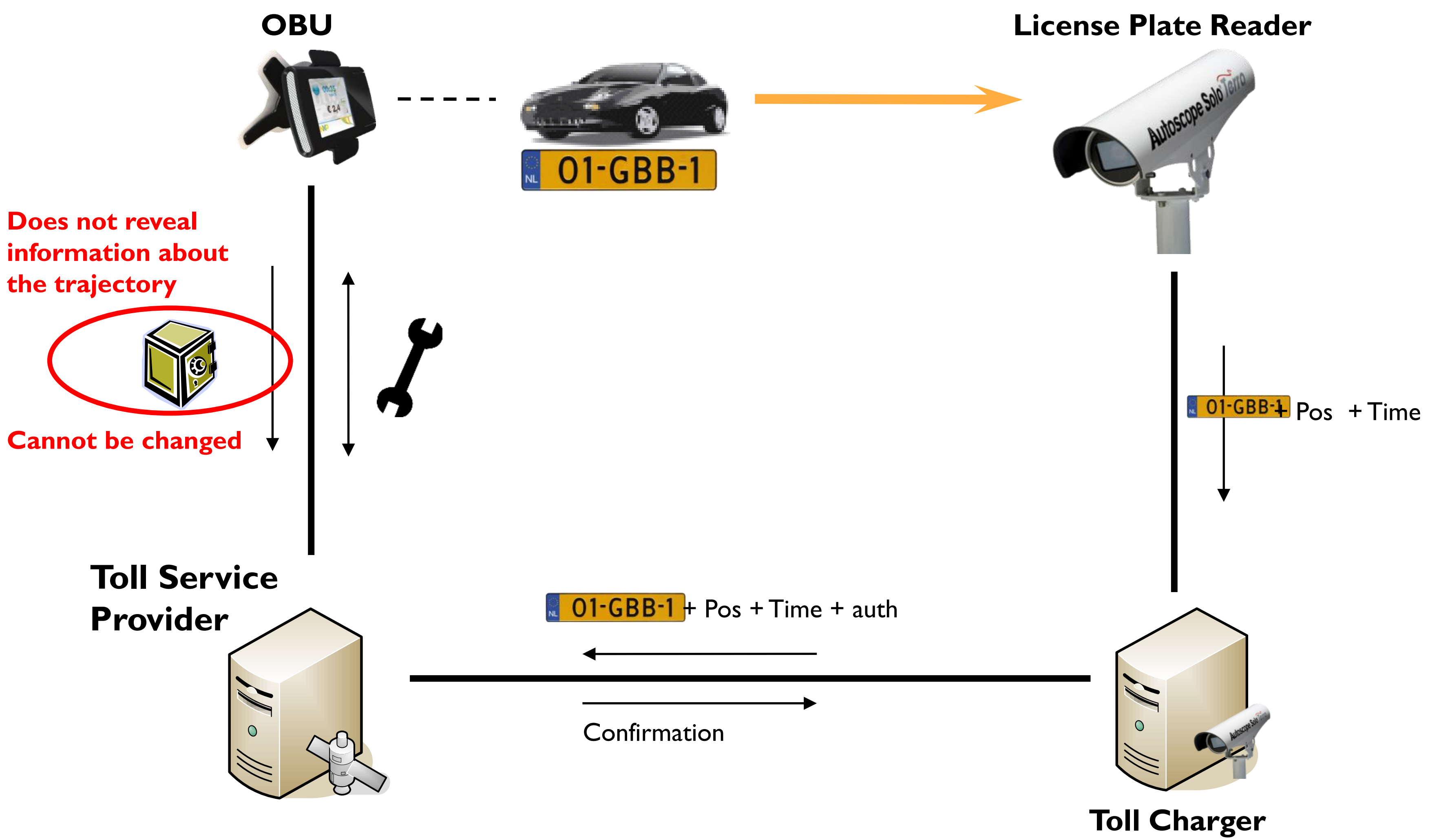
Local processing of location data



Service integrity

- OBU in hands of the user
  - Incentives to lower the premium
- Fraud-detection should include:
  - vehicles with inactive OBUs
  - vehicles reporting false location data
  - vehicles using incorrect road prices
  - vehicles reporting false final fees
- Random spot checks to detect cheating

How does it work?



What can we prove?

- OBU was active
  - A commitment with the committed location must be available
- OBU used correct prices
  - Prices signed by Toll Service Provider
  - Check correct pricing upon commitment opening
- OBU was at reported location
  - Compare photo location with committed location
- OBU made correct operations
  - Homomorphic commitments: prices in the "vaults" can be added to verify that they correspond to the reported final fee without being opened

Lessons learned

- In order to obtain strong privacy guarantees
  - The goal of the system must be well defined and feasible
  - Identify the minimal set of data needed for fulfilling this goal
  - Identify and model potential adversaries, multilateral security analysis

- Implement a solution that fulfills the requirements while revealing the minimal amount of private data

Conclusions

"Part of what makes a society a good place in which to live is the extent to which it allows people freedom from the intrusiveness of others. A society without privacy protection would be suffocation."
(Solove)

- Our actions and interactions are increasingly mediated by technology
- We leave digital traces everywhere

We need robust privacy-preserving technologies

Conclusions

- The analysis of privacy-preserving systems
  - Method to uncover relationships that takes into account all users simultaneously
  - Bayesian inference and Markov Chain Monte Carlo methods for traffic analysis
    - Systematic approach
    - Answers arbitrary questions about the entities in the system
    - Sampling reduces computational requirements
- The design of privacy-preserving systems
  - Two systems for privacy-preserving pay-as-you-drive applications
    - Local processing of sensitive data
    - Advanced privacy-preserving cryptographic primitives for security
    - Reduced risk and cost

Future work

- The analysis of privacy-preserving systems
  - Extend the Bayesian methods to other fields
    - location privacy (Shorki et al. framework S&P11,PETS11)
    - social networks
    - suggestions welcome!
  - Automate the modeling and analysis
- The design of privacy-preserving systems
  - Technical:
    - Integrate design and analysis (embed adversarial knowledge: CCS12)
  - Methodological:
    - More use cases to refine the principles
    - Full-fledged methodology

Thanks for your attention

http://homes.esat.kuleuven.be/~ctroncos/

Publication list (1/2)

2012

- F. Perez-Gonzalez, and C. Troncoso, "**A Least Squares Approach to User Profiling in Pool Mix-based Anonymous Communication Systems**," In *4th IEEE International Workshop on Information Forensics and Security (WIFS 2012)*, IEEE, 6 pages, 2012
- R. Shokri, G. Theodorakopoulos, C. Troncoso, J. Hubaux, and J. Le Boudec, "**Protecting Location Privacy: Optimal Strategy against Localization Attacks**," In *Proceedings of the 19th ACM Conference on Computer and Communications Security (CCS 2012)*, ACM, 11 pages, 2012
- F. Perez-Gonzalez, and C. Troncoso, "**Understanding Statistical Disclosure: A Least Squares approach**," In *Privacy Enhancing Technologies - 12th International Symposium, PETS 2012*, Lecture Notes in Computer Science 7384, S. Fischer-Huebner, and M. Wright (eds.), Springer-Verlag, pp. 38-57, 2012
- E. Balsa, C. Troncoso, and C. Diaz, "**OB-PWS: Obfuscation-Based Private Web Search**," In IEEE Symposium on Security and Privacy 2012, IEEE, pp. 491-505, 2012.

2011

- J. A. Elices, F. Perez-Gonzalez, and C. Troncoso, "**Fingerprinting Tor's Hidden Service Log Files Using a Timing Channel**," In 3rd IEEE International Workshop on Information Forensics and Security (WIFS 2011), IEEE, 6 pages, 2011.
- P. Mittal, F. Olumofin, C. Troncoso, N. Borisov, and I. Goldberg, "**PIR-Tor: Scalable Anonymous Communication Using Private Information Retrieval**," 20th USENIX Security Symposium , USENIX, 17 pages, 2011.
- C. Troncoso, E. Costa-Montenegro, C. Diaz, and S. Schiffner, "**How the Vehicle Infrastructure Integration anonymous certificates enable the tracking and re-identification of vehicles**," *Computer Networks* - Special Issue on Vehicle-2-x Communication 55(14), pp. 3199-3210, 2011.
- S. F. Gürses, C. Troncoso, and C. Diaz, "**Engineering Privacy by Design**," In Computers, Privacy & Data Protection, 25 pages, 2011.
- C. Troncoso, G. Danezis, E. Kosta, J. Balasch, and B. Preneel, "**PriPAYD: Privacy Friendly Pay-As-You-Drive Insurance (Journal version)**," *IEEE Transactions on Dependable and Secure Computing* 8(5), pp. 742-755, 2011.

2010

- R. Shokri, C. Troncoso, C. Diaz, J. Freudiger, and J. Hubaux, "**Unraveling an Old Cloak: k-anonymity for Location Privacy**," In Proceedings of the 9th ACM workshop on Privacy in the electronic society (WPES 2010), K. Frikken (ed.), ACM, pp. 115-118, 2010.
- J. Balasch, A. Rial, C. Troncoso, C. Geuens, B. Preneel, and I. Verbauwhede, "**PrETP: Privacy-Preserving Electronic Toll Pricing**," In 19th USENIX Security Symposium 2010, Usenix, pp. 63-78, 2010.
- P. Mittal, N. Borisov, A. Rial, and C. Troncoso, "**Scalable Anonymous Communication with Provable Security**," In 5th USENIX Workshop on Hot Topics in Security 2010, USENIX, 7 pages, 2010.
- G. Danezis, C. Diaz, C. Troncoso, and B. Laurie, "**Drac: An Architecture for Anonymous Low-Volume Communications**," In 10th International Symposium, PETS 2010, LNCS 6205, M. J. Atallah, and N. J. Hopper (eds.), Springer-Verlag, pp. 202-219, 2010
- C. Diaz, S. Murdoch, and C. Troncoso, "**Impact of Network Topology on Anonymity and Overhead in Low-Latency Anonymity Networks**," In 10th International Symposium, PETS 2010, LNCS 6205, M. J. Atallah, and N. J. Hopper (eds.), Springer-Verlag, pp. 184-201, 2010

Publication list (2/2)

2009

- G. Danezis, C. Diaz, E. Käsper, and C. Troncoso, "**The wisdom of Crowds: attacks and optimal constructions**," In *14th European Symposium on Research in Computer Security (ESORICS 2009)*, LNCS 5789, M. Backes, and P. Ning (eds.), Springer-Verlag, pp. 406-423, 2009
- C. Troncoso, and G. Danezis, "**The Bayesian Analysis of Mix Networks,**" In *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS 2009)*, E. Al-Shaer, S. Jha, and A. D. Keromytis (eds.), ACM, pp. 369-379, 2009
- G. Danezis, and C. Troncoso, "V**ida: How to use Bayesian inference to de-anonymize persistent communications,**" In *Privacy Enhancing Technologies - 9th International Symposium, PETS 2009*, LNCS 5672, M. J. Atallah, and I. Goldberg (eds.), Springer-Verlag, pp. 406-423, 2009

2008

- B. Gierlichs, C. Troncoso, C. Diaz, B. Preneel, and I. Verbauwhede, "**Revisiting A Combinatorial Approach Toward Measuring Anonymity,**" In *Proceedings of the 7th ACM workshop on Privacy in the electronic society (WPES 2008)*, V. Atluri , and M. Winslett (eds.), ACM, pp. 111-116, 2008
- C. Diaz, C. Troncoso, and B. Preneel, "**A Framework for the Analysis of Mix-Based Steganographic File Systems,**" In *13th European Symposium on Research in Computer Security (ESORICS 2008)*, LNCS 5283, S. Jajodia, and J. Lopez (eds.), Springer-Verlag, pp. 428-445, 2008
- C. Diaz, C. Troncoso, and A. Serjantov, "**On the Impact of Social Network Profiling on Anonymity**," In *8th International Symposium, PETS 2008*, LNCS 5134, N. Borisov, and I. Goldberg (eds.), Springer-Verlag, pp. 44-62, 2008
- C. Troncoso, B. Gierlichs, B. Preneel, and I. Verbauwhede, "**Perfect Matching Disclosure Attacks,**" In *Privacy Enhancing Technologies - 8th International Symposium, PETS 2008*, LNCS 5134, N. Borisov, and I. Goldberg (eds.), Springer-Verlag, pp. 2-23, 2008
- C. Troncoso, D. De Cock, and B. Preneel, "**Improving Secure Long-Term Archival of Digitally Signed Documents**," In *4th International Workshop on Storage Security and Survivability (StorageSS 2008)*, Y. Kim, and B. Yurcik (eds.), pp. 27-36, 2008

2007

- C. Troncoso, G. Danezis, E. Kosta, and B. Preneel, **"PriPAYD: Privacy Friendly Pay-As-You-Drive Insurance**," In *Proceedings of the 6th ACM workshop on Privacy in the electronic society (WPES 2007)*, T. Yu (ed.), ACM, pp. 99-107, 2007
- G. Danezis, C. Diaz, S. Faust, E. Käsper, C. Troncoso, and B. Preneel, "**Efficient Negative Databases from Cryptographic Hash Functions**," In *Information Security - 10th International Conference, ISC 2007*, LNCS 4779, J. A. Garay, A. K. Lenstra, M. Mambo, and R. Peralta (eds.), Springer-Verlag, pp. 423-436, 2007
- G. Danezis, C. Diaz, and C. Troncoso, "**Two-Sided Statistical Disclosure Attack**," In *Proceedings of Privacy Enhancing Technologies, 7th International Workshop, PET 2007*
- C. Troncoso, C. Diaz, O. Dunkelman, and B. Preneel, "**Traffic Analysis Attacks on a Continuously-Observable Steganographic File**," In *Information Hiding, 9th International Workshop, IH 2007*, LNCS 4567, F. Cayre, G. J. Doërr, and T. Furon (eds.), Springer-Verlag, pp. 220-236, 2007
- C. Diaz, C. Troncoso, and G. Danezis, "**Does additional information always reduce anonymity?**," In *Proceedings of the 6th ACM workshop on Privacy in the electronic society (WPES 2007)*, T. Yu (ed.), ACM, pp. 72-75, 2007

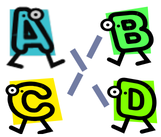
Publication list

- 27 publications
  - 2 international journals

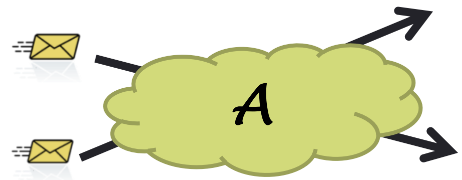
  - 7 Privacy Enhancing Technologies Symposium
  - 4 ACM Workshop on Privacy in the Electronic Society
  - 2 USENIX Security Symposium
  - 2 European Symposium on Research in Computer Security
  - 2 ACM Conference on Computer and Communications Security
  - 8 other international conferences and workshops

Bayesian inference to de-anonymize persistent communications

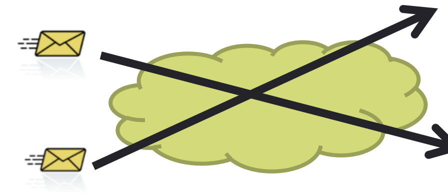
Ψ – User Profiles



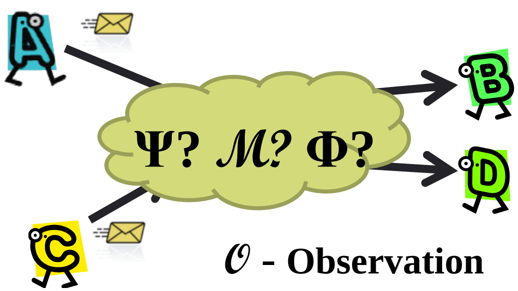
$\mathcal{M}$ – Sender-Receiver match



$\mathcal{A}$ – Anonymity system



Φ – Assignment



$\mathcal{O}$ - Observation

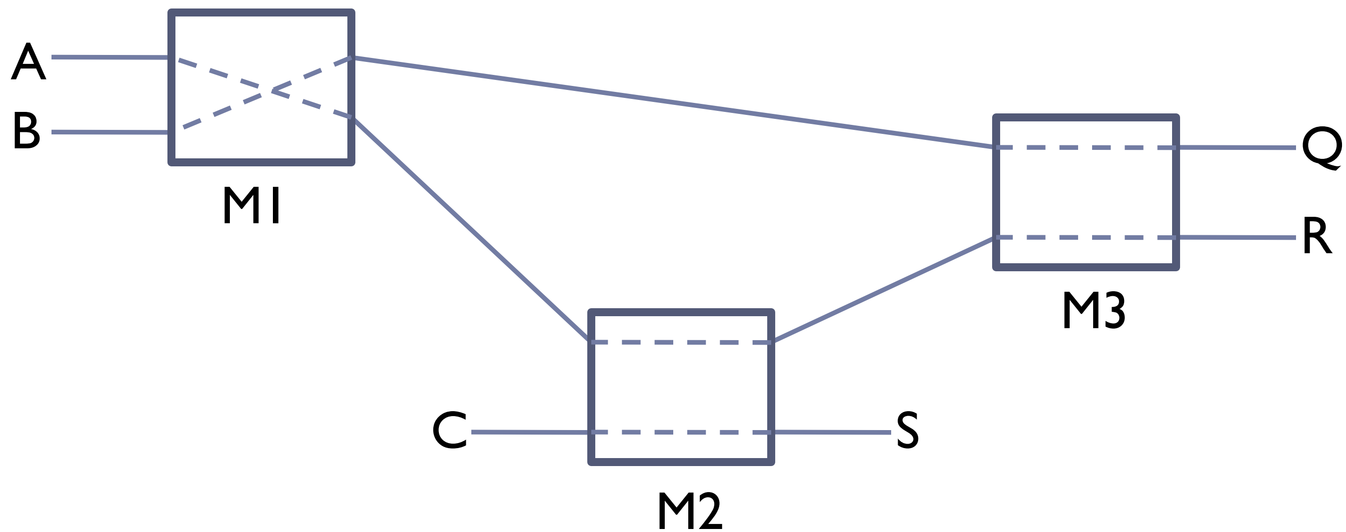
$$\Pr(M,\Phi,\Psi \mid O,A) = \frac{\Pr(M \mid \Psi)\cdot \Pr(\Phi \mid A)}{\Pr(O \mid A) \equiv Z} \Pr(\Psi \mid A)$$

$$(M,\Phi,\Psi)_1,(M,\Phi,\Psi)_2,(M,\Phi,\Psi)_3,\ldots \sim \Pr(M,\Phi,\Psi \mid O,A)$$

- **Markov Chain Monte Carlo Methods**
  - construct a Markov Chain with stationary distribution equal to the target distribution
- Gibbs sampling
  - Efficient for sampling joint distributions
  - Eliminate the need to compute Z

Redefining the traffic analysis problem

- *"Hidden State" + Observation = Paths*



$P_1 \rightarrow$ A — M1 — M2 — M3 — R

$P_2 \rightarrow$ B — M1 — M3 — Q

$P_3 \rightarrow$ C — M2 — S

$$\Pr(HS \mid O, C) = \frac{\Pr(O \mid HS, C) \cdot \Pr(HS \mid C)}{\sum_{HS} \Pr(HS, O \mid C)} = \frac{\Pr(Paths \mid C)}{\sum_{Paths} \Pr(Paths \mid C)}$$

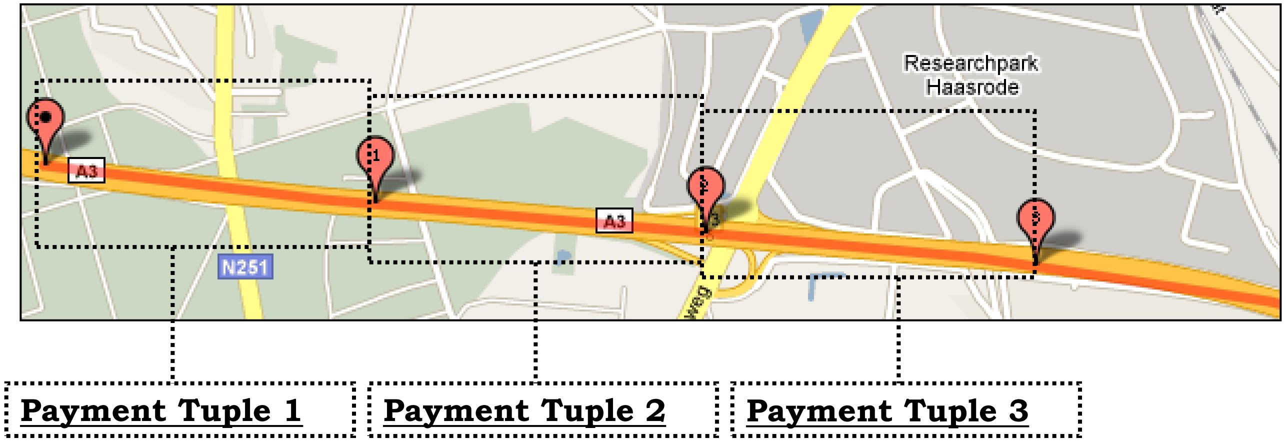
Performance

Nmix	t	Nmsg	RAM (Mb)	iter	Full analysis (min)	One sample (ms)
3	3	10	16	6011	4.24	509.12
3	3	50	18	6011	4.80	576.42
10	20	50	18	7011	5.34	641.28
10	20	1 000	24	7011	5.97	706.12
10	20	10 000	125	-	-	-

- RAM requirements
  - Size of network and population
- Time requirements (1443 LOC Python)
  - Operations are O(1)

Creating commitments

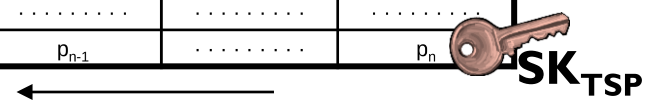
- Slice trajectory in segments (e.g., 1 Km)

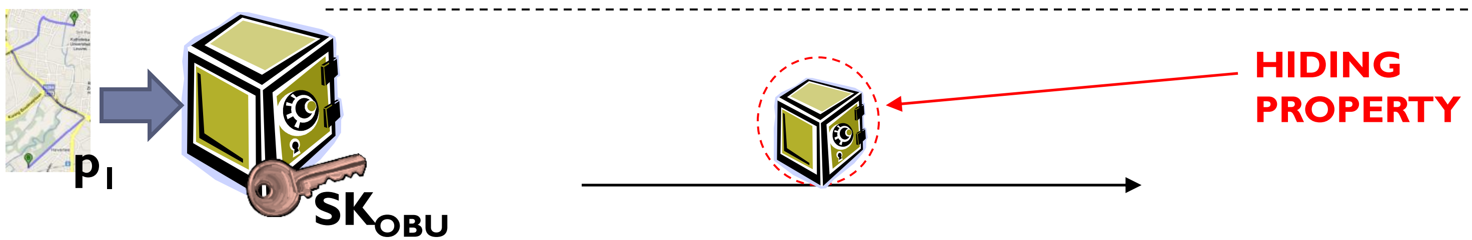


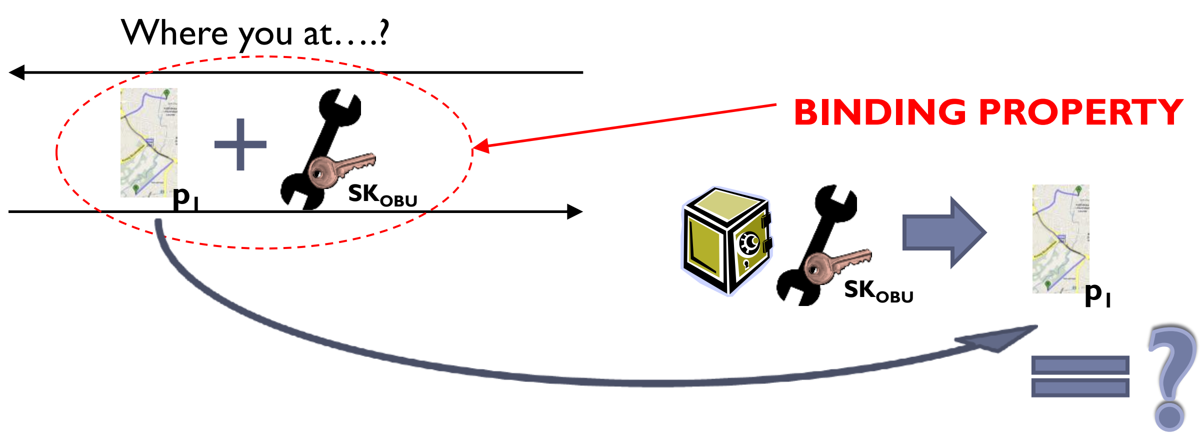
- Each segment has assigned a price per Km p_i
- This price is specified by the policy, example:
  - $p_i = f$ (*type road, time day*)
- A commitment per segment is created

Non-Interactive Commitment Schemes

	00u00 – 07u00	....	22u00 – 00u00
Highway	p_1	....	p_2
Primary	p_3	....	p_4
....	....	....	....
Residential	p_{n-1}	....	p_n







Homomorphic commitments

- The content of the vaults can be added up without being known