SIGNAL PROCESSING FOR ANONYMOUS COMMUNICATIONS

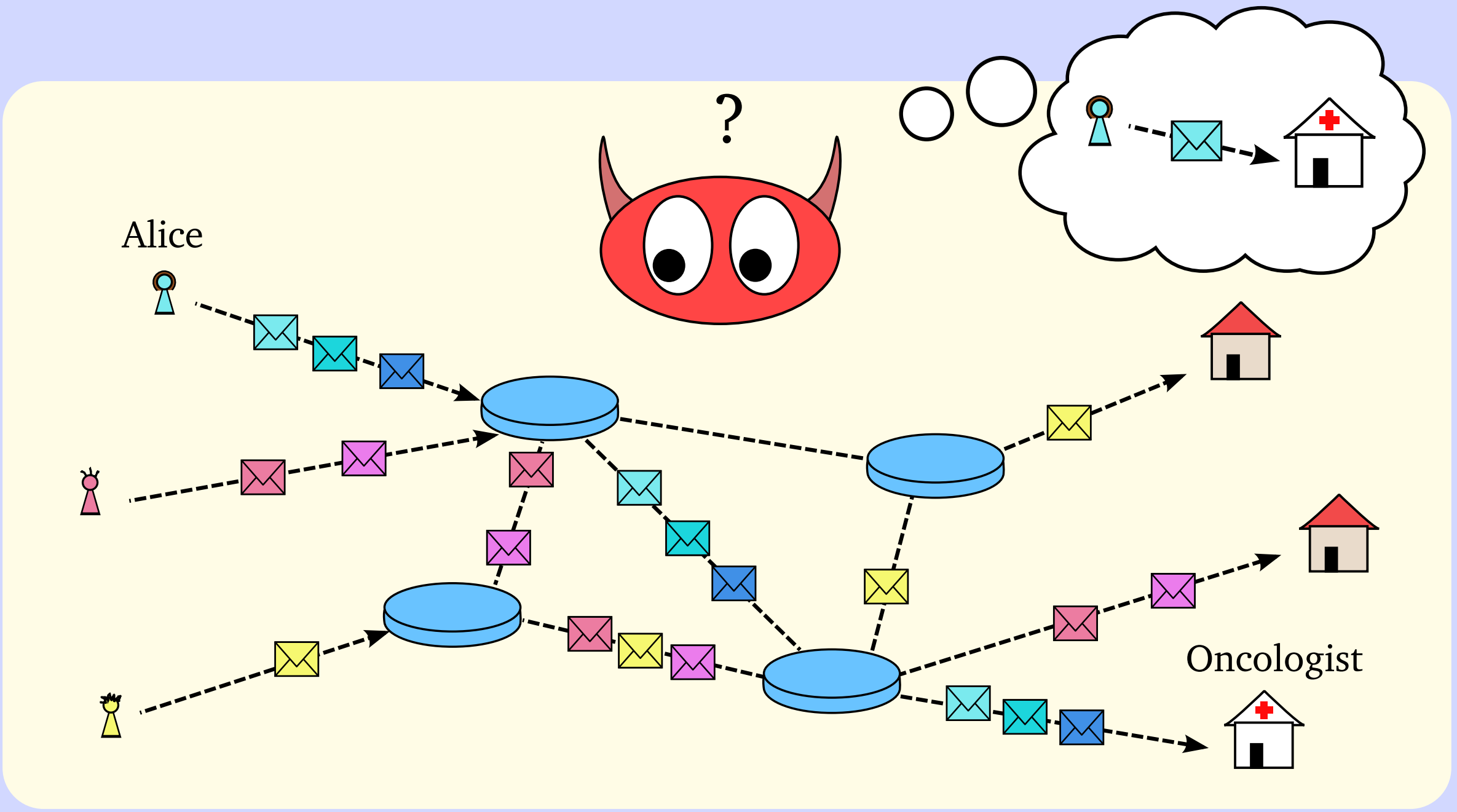
Simon Oya, Carmela Troncoso, and Fernando Pérez-González

simonoya@gts.uvigo.es carmela.troncoso@imdea.org fperez@gts.uvigo.es

UniversidadeVigo GPSC Signal Processing in Communications Group

MOTIVATION OF THE WORK

Need for anonymity in the communications.



Current Analyses: ☹

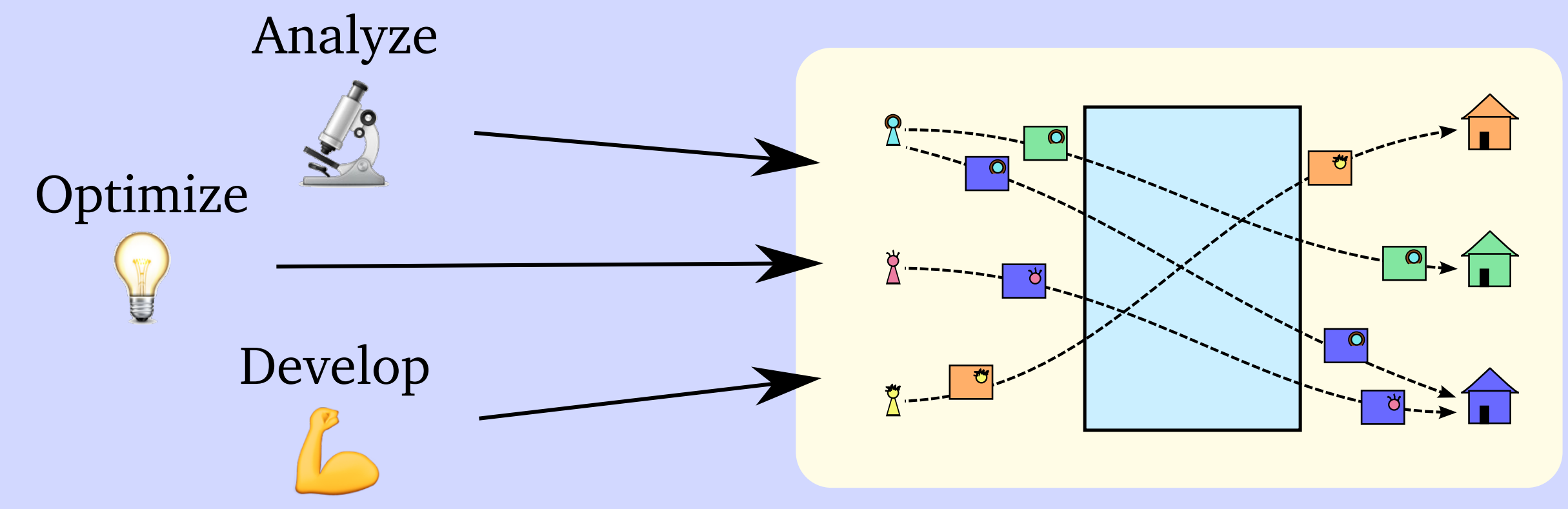
- Simplify the problem with unrealistic hypotheses. → Applicable to very complex problems (digital communications, forensics, etc).
- Rely on very complex mathematical devices. → Simplifies the problem.
- Provide only empirical results. → Provides analytical results.

Idea!! Signal Processing! 💡

THESIS OBJECTIVES

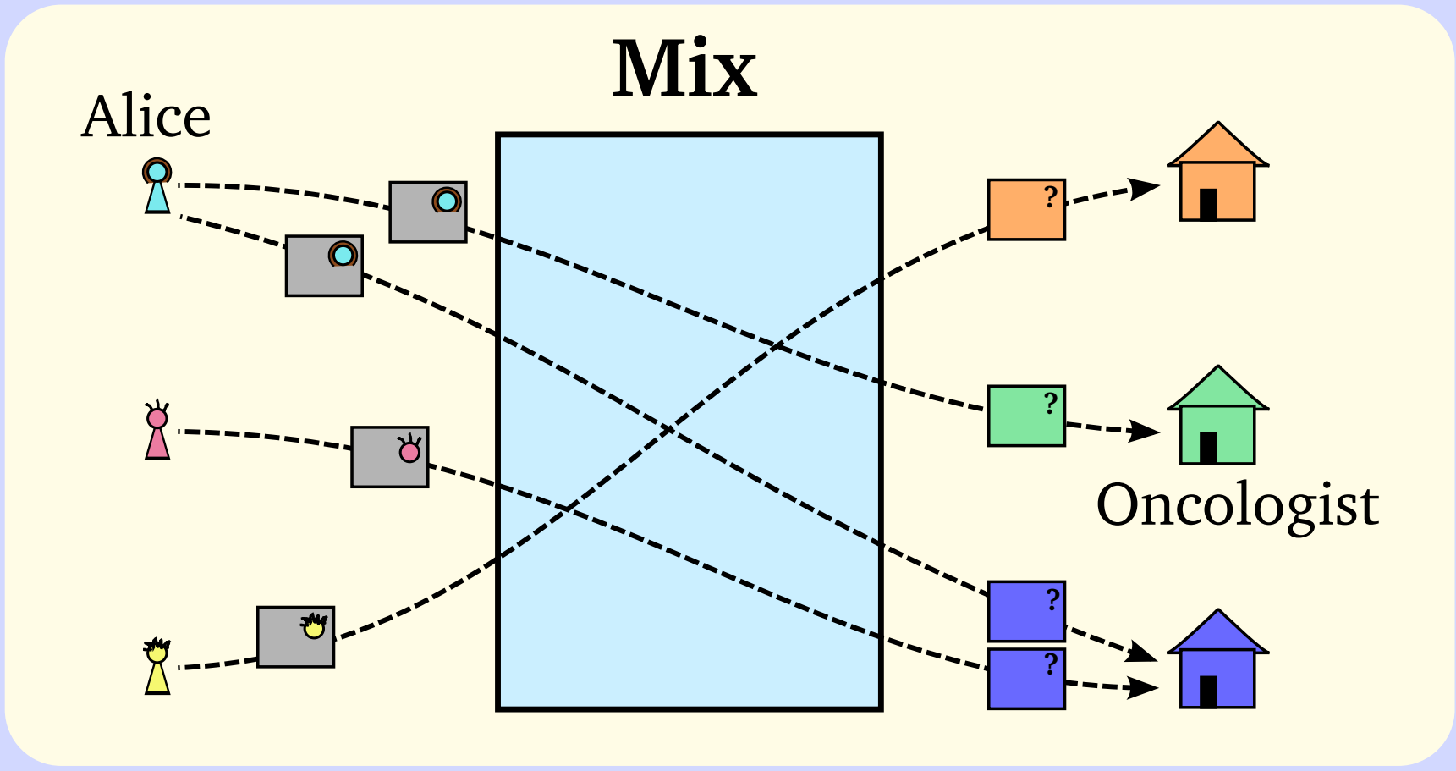
General objective

Apply signal processing tools to anonymous communications.



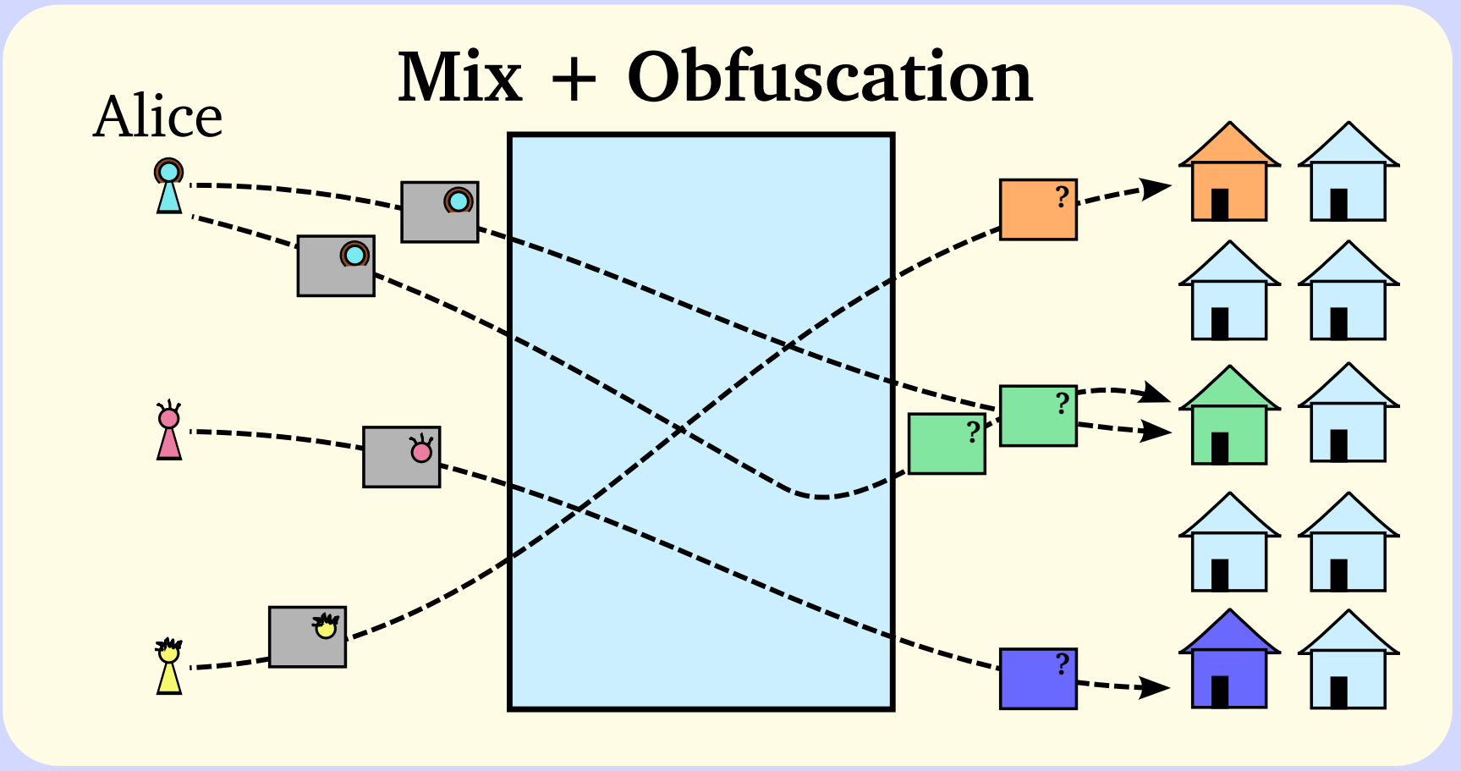
We will study two scenarios:

Delay-based communication systems [1][2]



- Delaying messages is allowed!!
- We cannot change recipients.

Location privacy [3][4]

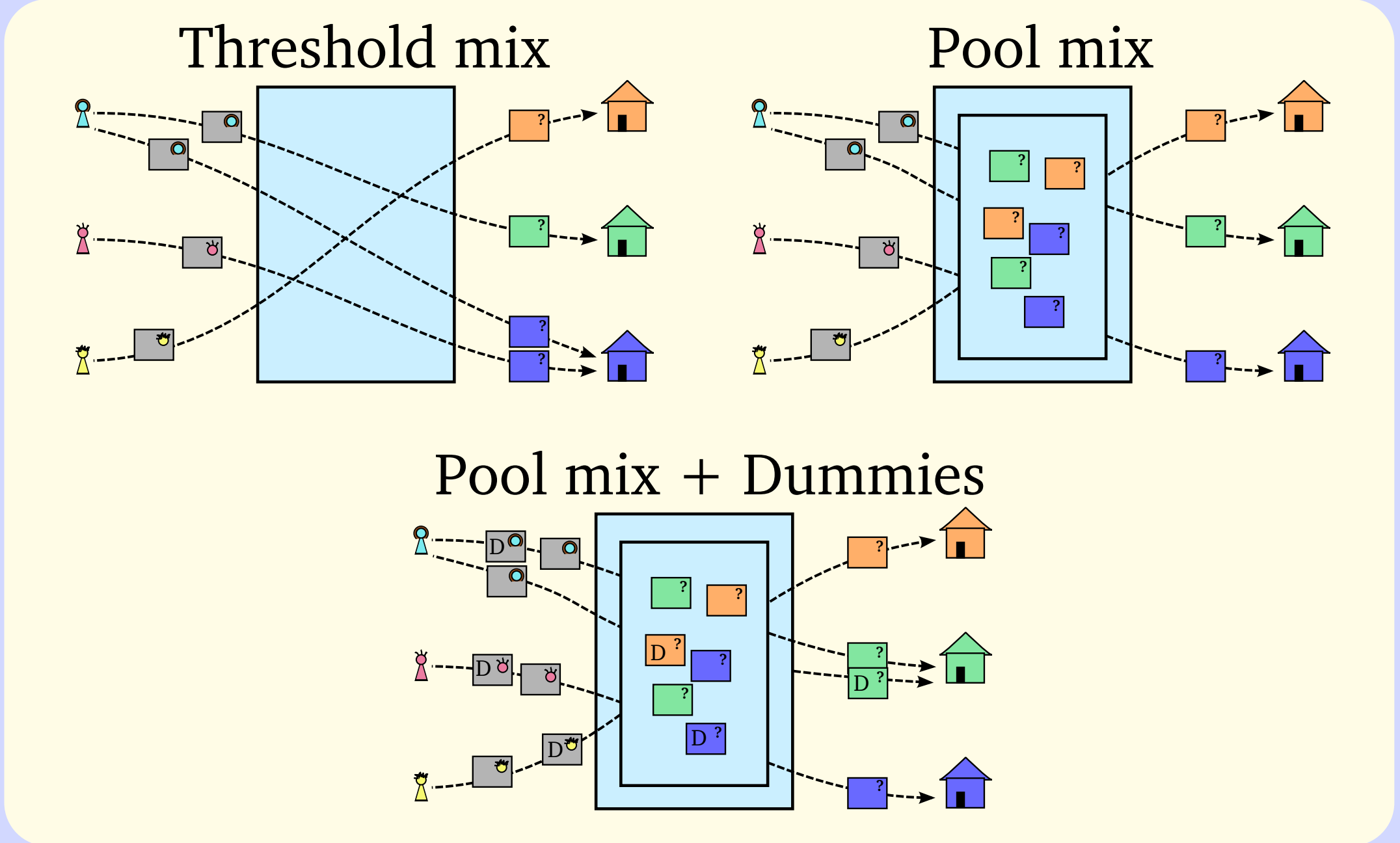


- Recipients are locations, we can obfuscate them to confuse the adversary.

RESEARCH PLAN

6 m.
- Study the state of the art (mixes).

21 m.
- Delay-based anonymous communications:

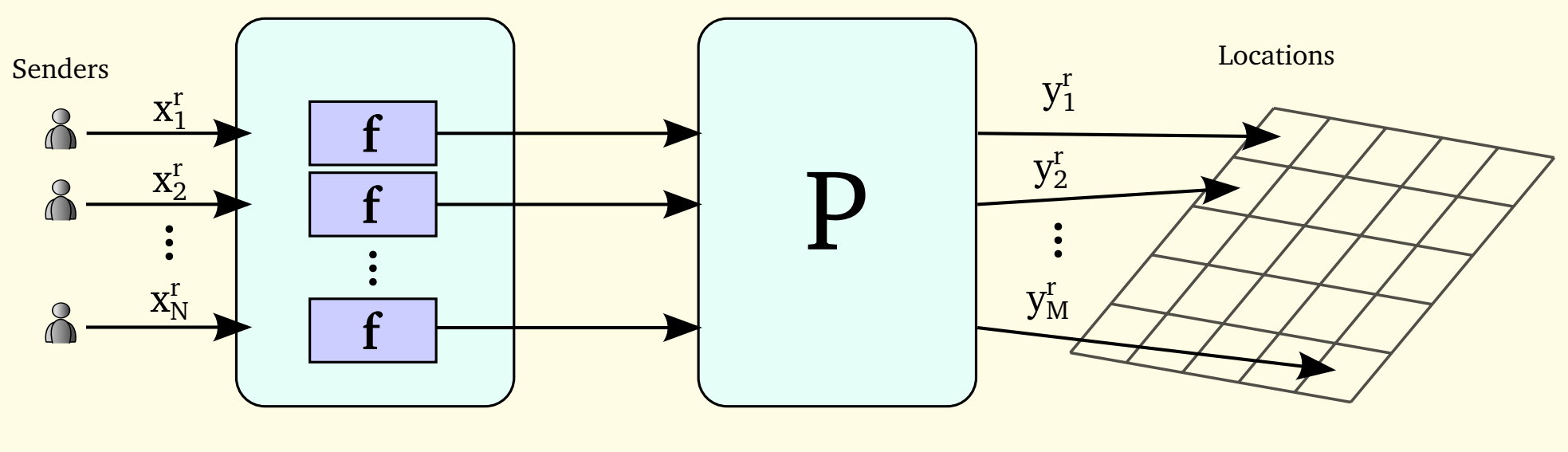


1 m.
- Study the state of the art (location privacy).

17 m.
- Location Privacy

- Short-term attacks
- Long-term attacks

Obfuscation Timed mix



Methodology

1. Develop theoretical models.
2. Apply signal processing tools to analyze the privacy properties.
3. Optimize the privacy mechanisms.
4. Propose new protection mechanisms.
5. Empirical evaluation of our findings.

WE'RE HERE

2 m.

4 m.
- Wrapping up, conclusions and writing.

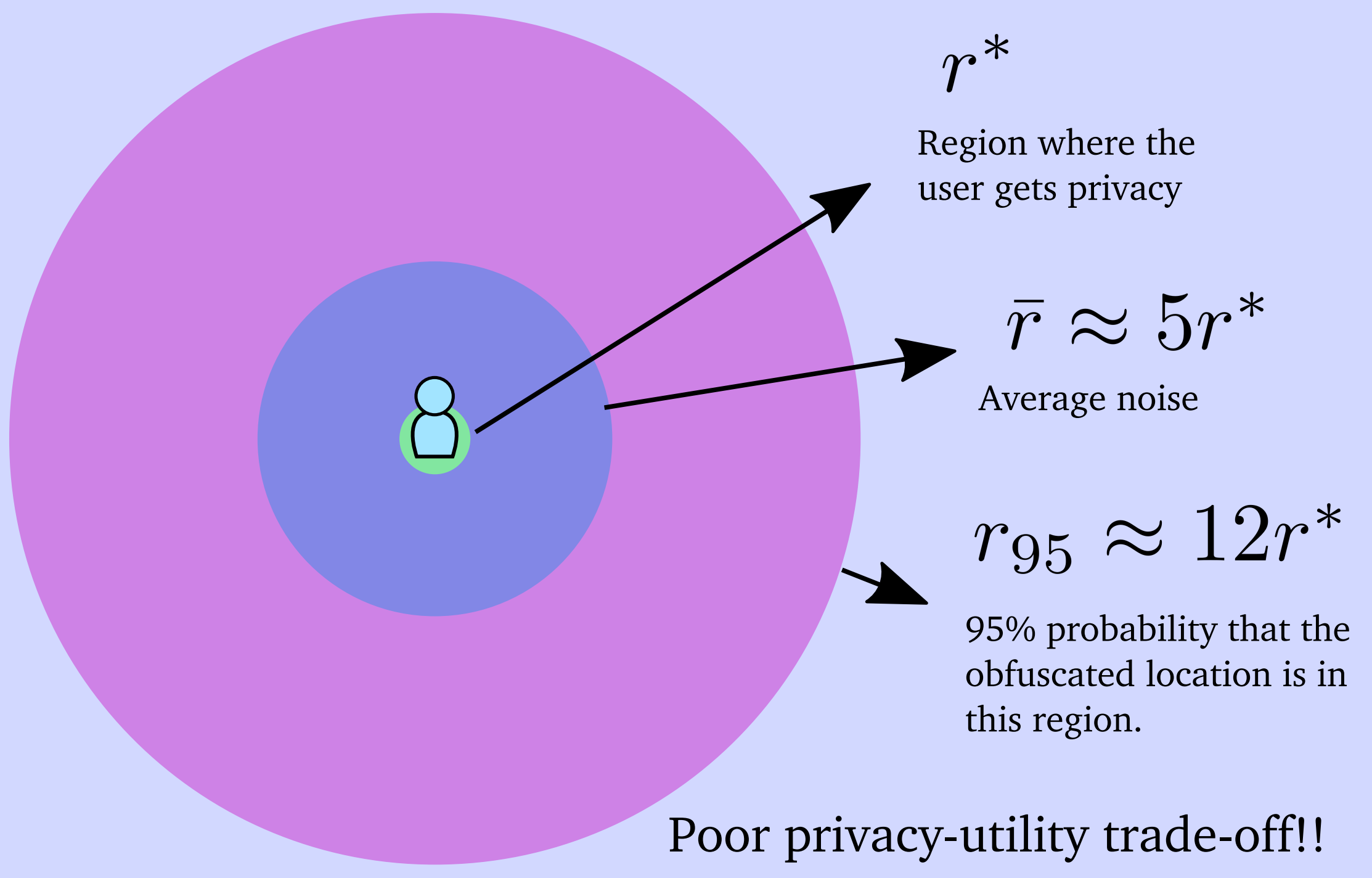
PREVIOUS RESULTS

- Proof that LSDA outperforms SDA [5].
- Analysis of a pool mix with dummies [6].
- In-depth study of LSDA on pool mixes [7].
- Analysis of the mix in real scenarios [8].
- Study of pool mixes in real scenarios [9].
- Filter design applied to pool mixes [10]
- Multi-dimensional notion of location privacy [11].

NEW RESULTS

- Issues of geo-indistinguishability [12]

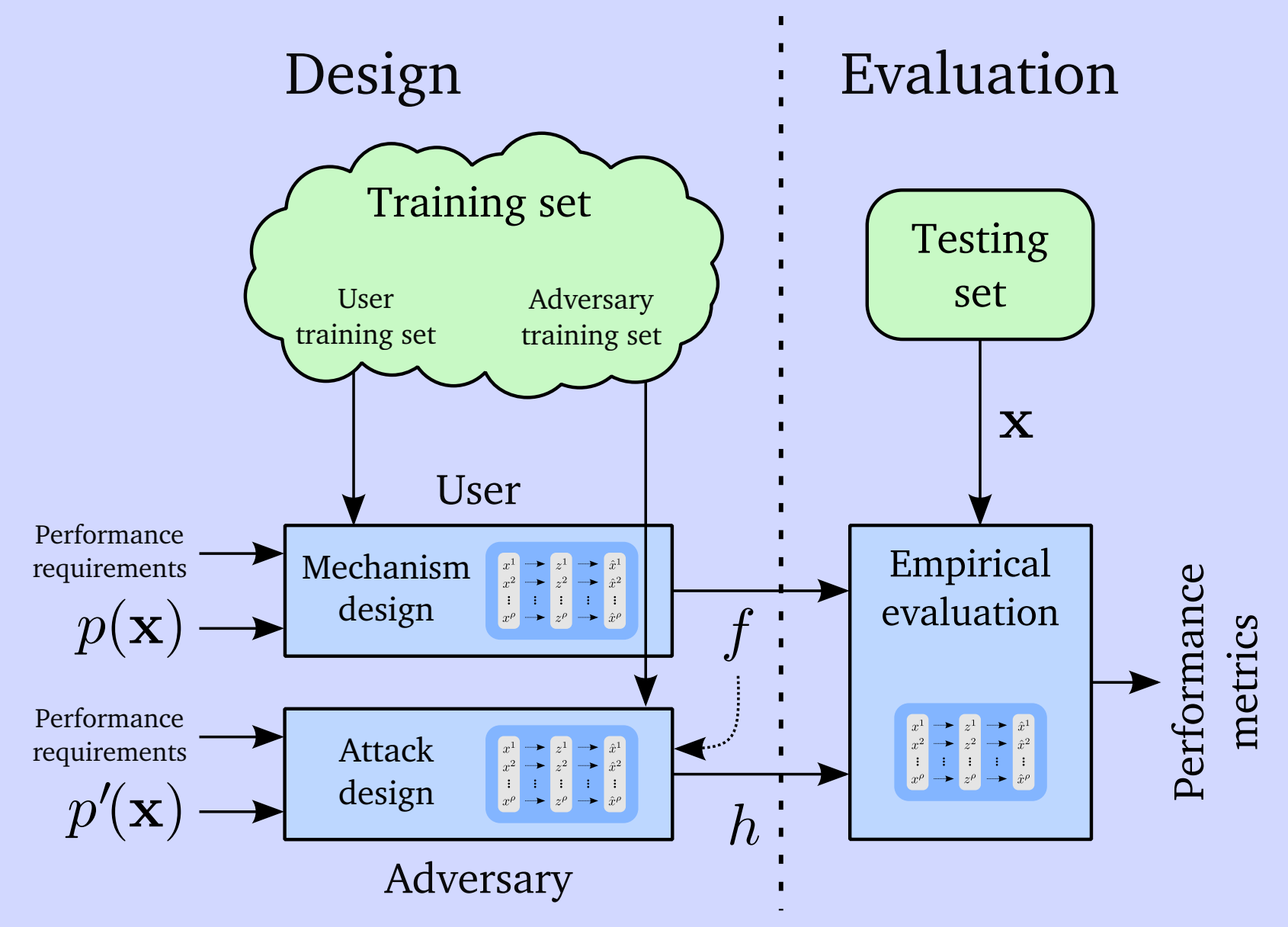
We find numeral issues with geo-indistinguishability, a widespread **location privacy** notion.


r^*
Region where the user gets privacy
$\bar{r} \approx 5r^*$
Average noise
$r_{95} \approx 12r^*$
95% probability that the obfuscated location is in this region.

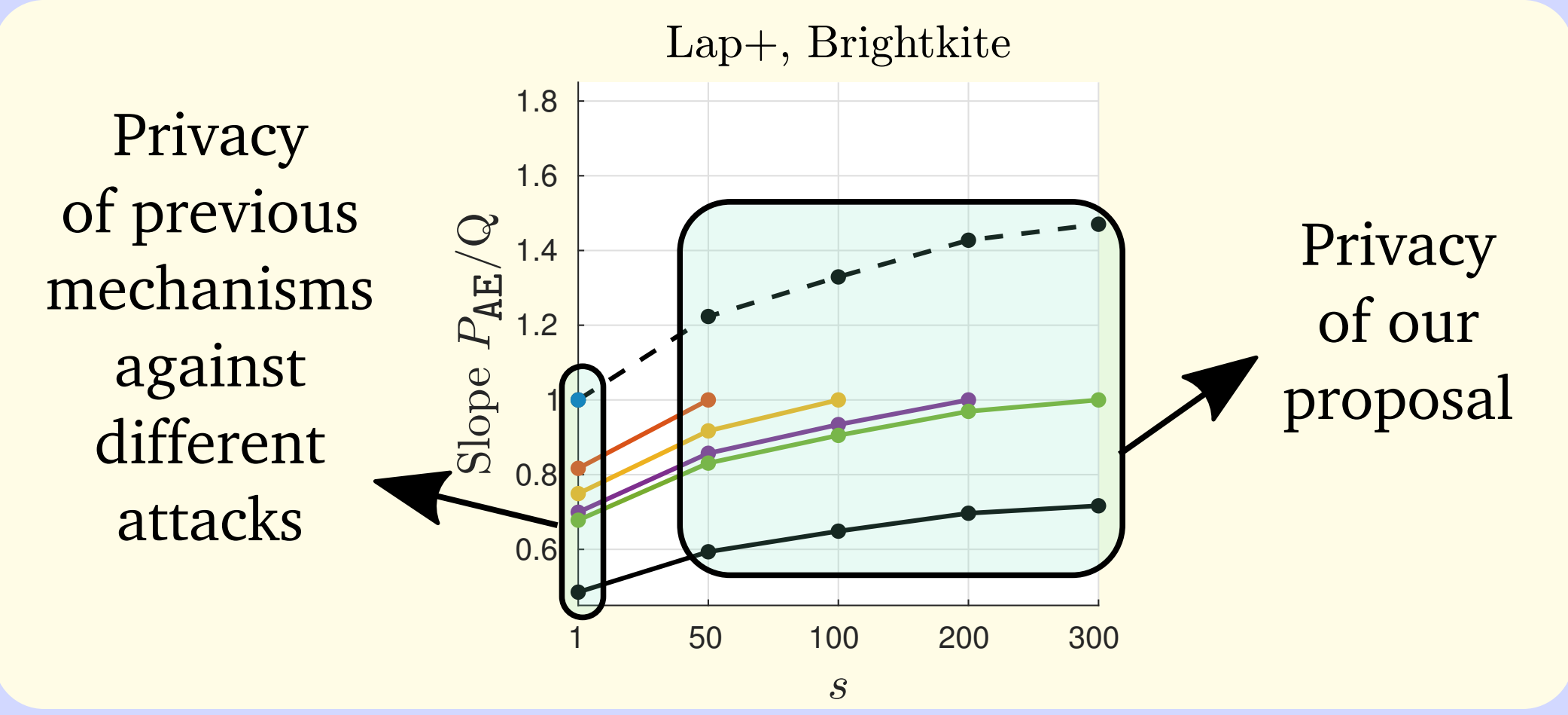
Poor privacy-utility trade-off!!

- Adaptive mechanisms for location privacy [13] (under submission)

We add training/testing set separation to the LPPM design and evaluation framework.



We find better models for user behavior that account for differences between training and testing sets. This allows us to build adaptive LPPMs



NEXT YEAR PLANNING

- Application of mixing and de-mixing techniques to cryptocurrencies.
- Wrapping up and writing.
- Hopefully finish by December 2018.

BIBLIOGRAPHY

[1] Chaum, David L. "Untraceable electronic mail, return addresses, and digital pseudonyms." Communications of the ACM 24.2 (1981): 84-90.

[2] Diaz, Claudia, and Bart Preneel. "Taxonomy of mixes and dummy traffic." Information Security Management, Education and Privacy. Springer US, 2004. 217-232.

[3] Shokri, Reza, George Theodorakopoulos, Jean-Yves Le Boudec, and Jean-Pierre Hubaux. "Quantifying location privacy." Security and privacy (sp), 2011 IEEE Symposium on. IEEE, 2011.

[4] Andrés, Miguel E., Nicolás E. Bordenabe, Konstantinos Chatzikokolakis, and Catuscia Palamidessi. "Geo-indistinguishability: Differential privacy for location-based systems." Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM, 2013.

[5] **S. Oya**, C. Troncoso, and F. Pérez-González, "Meet the family of statistical disclosure attacks," IEEE Global Conference on Signal and Information Processing, p. 4p, 2013.

[6] **S. Oya**, C. Troncoso, and F. Pérez-González, "Do dummies pay off? limits of dummy traffic protection in anonymous communications," in 14th Symposium on Privacy Enhancing Technologies, 2014.

[7] F. Pérez-González, C. Troncoso, and **S. Oya**, "A least squares approach to the static traffic analysis of high-latency anonymous communicationsystems," IEEE Transactions on Information Forensics and Security,vol. 9, no. 9, pp. 1341–1355, Sept 2014.

[8] **S. Oya**, C. Troncoso, and F. Pérez-González, "Understanding the effects of real-world behavior in statistical disclosure attacks," in IEEE Workshop on Information Forensics and Security, 2014.

[9] **S. Oya**, F. Pérez-González, and C. Troncoso, "Design of Pool Mixes Against Profiling Attacks in Real Conditions", IEEE /ACM Transactions on Networking, 2016.

[10] **S. Oya**, F. Pérez-González, and C. Troncoso, "Filter Design for Delay-Based Anonymous Communications", ICASSP 2017.

[11] **S. Oya**, C. Troncoso, and F. Pérez-González, "On the the design of optimal location privacy-preserving mechanisms", CCS 2017.

[12] **S. Oya**, C. Trocoso, and F. Pérez-González. "Is Geo-Indistinguishability What You Are Looking for?." ACM Workshop on Privacy in the Electronic Society, 2017.

[13] **S. Oya**, C. Troncoso, and F. Pérez-González. "Adaptive Mechanisms for Location Privacy". Under submission.