

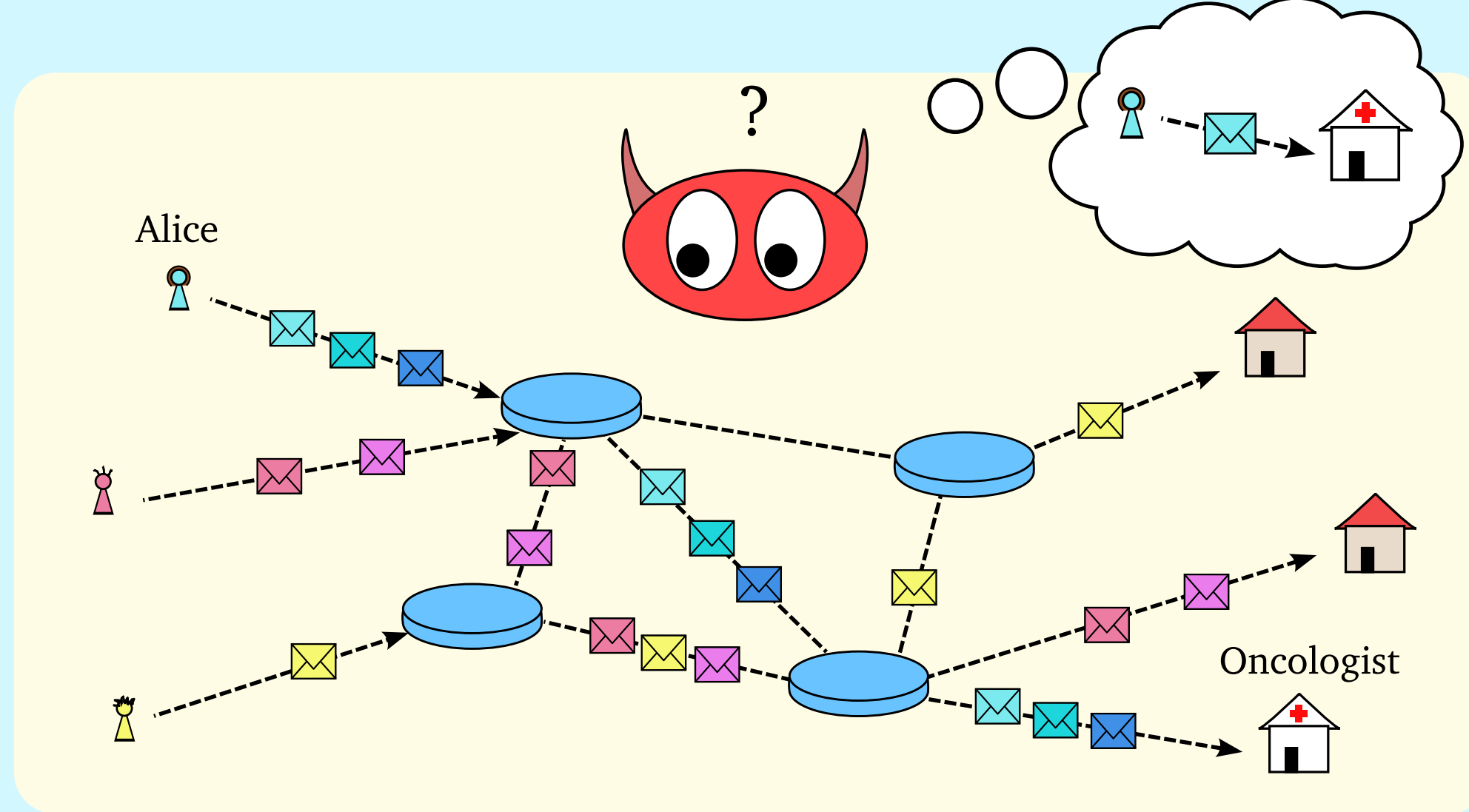
SIGNAL PROCESSING FOR ANONYMOUS COMMUNICATIONS

Simon Oya, Carmela Troncoso, and Fernando Pérez-González

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

MOTIVATION OF THE WORK

Need for anonymity in the communications.



Current Analyses: 😞

- Simplify the problem with unrealistic hypotheses.
- Rely on very complex mathematical devices.
- Provide only empirical results.

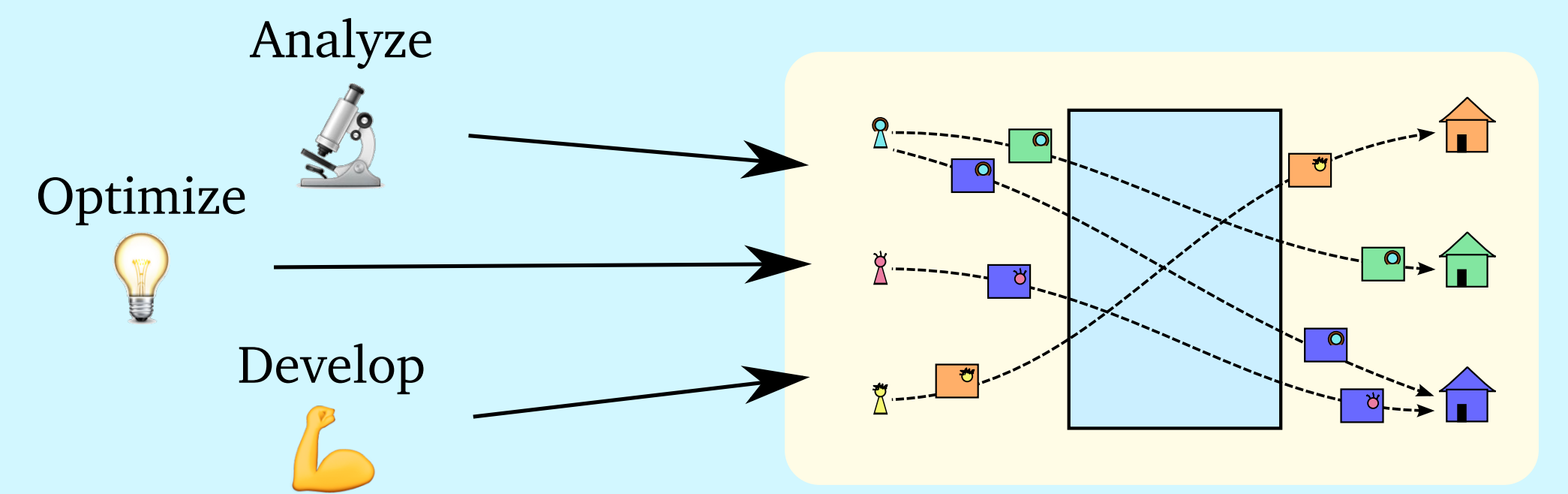
Idea!! Signal Processing! 💡

- Applicable to very complex problems (digital communications, forensics, etc).
- Simplifies the problem.
- Provides analytical results.

THESIS OBJECTIVES

General objective

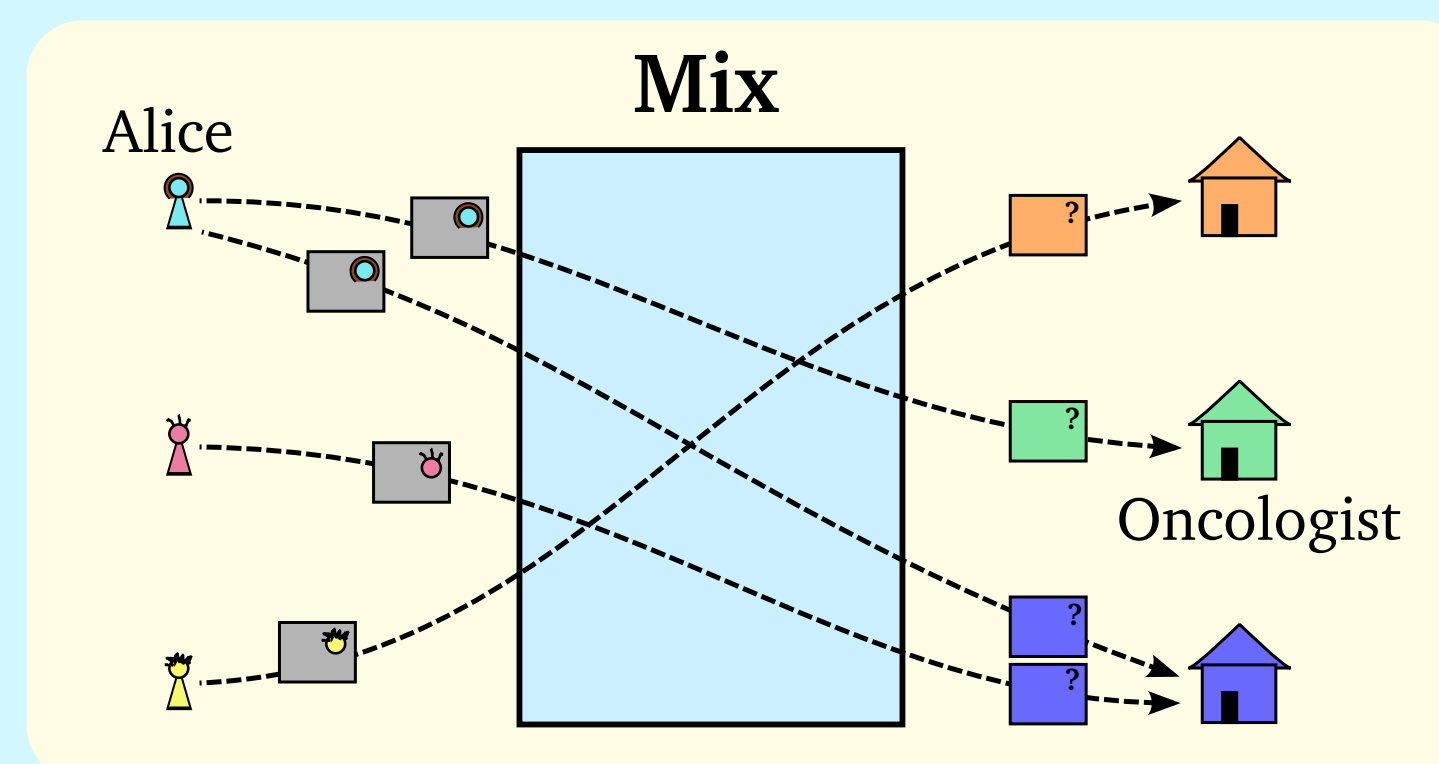
Apply signal processing tools to anonymous communications.



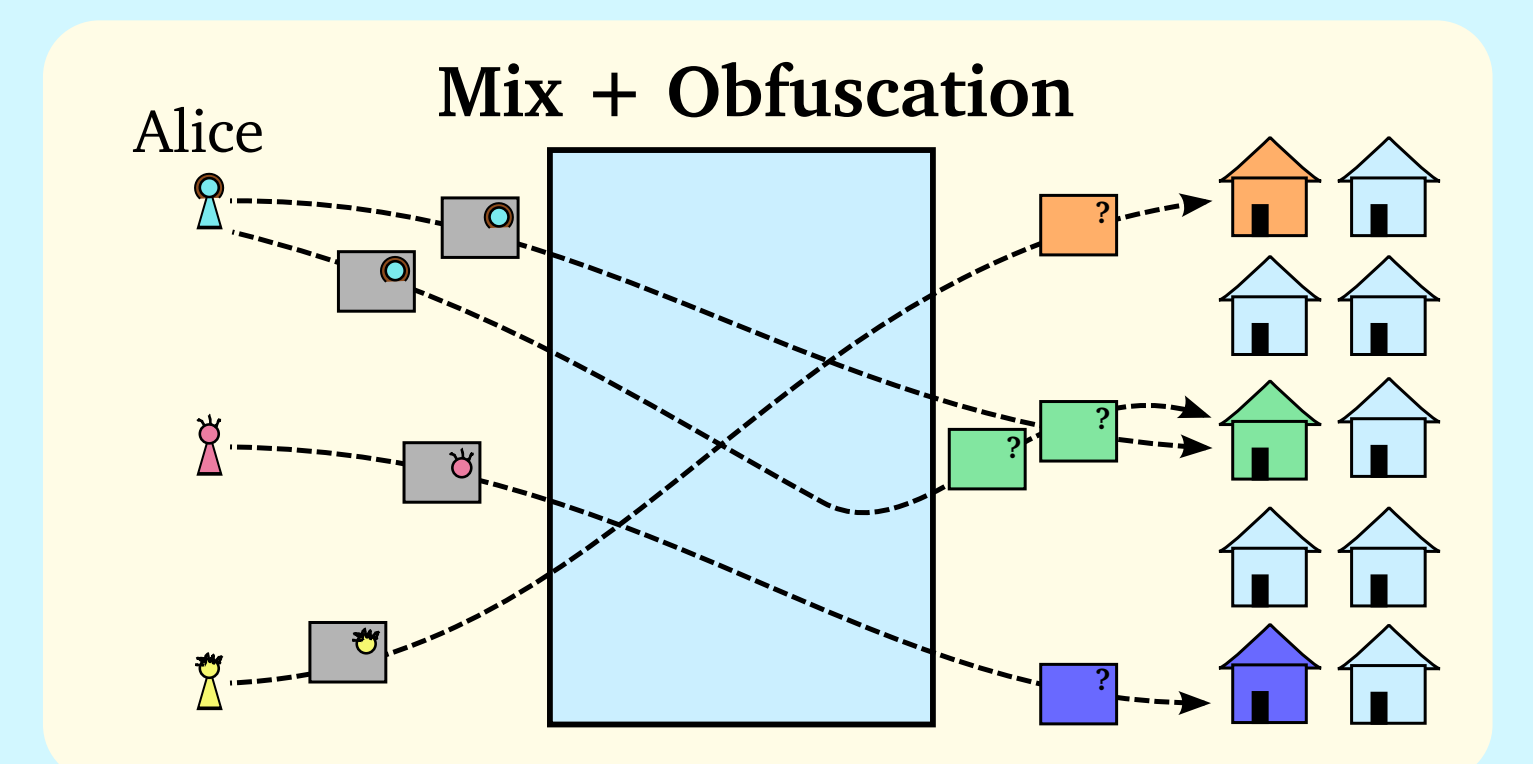
We will study two scenarios:

Delay-based communication systems [1][2]

Location privacy [3][4]



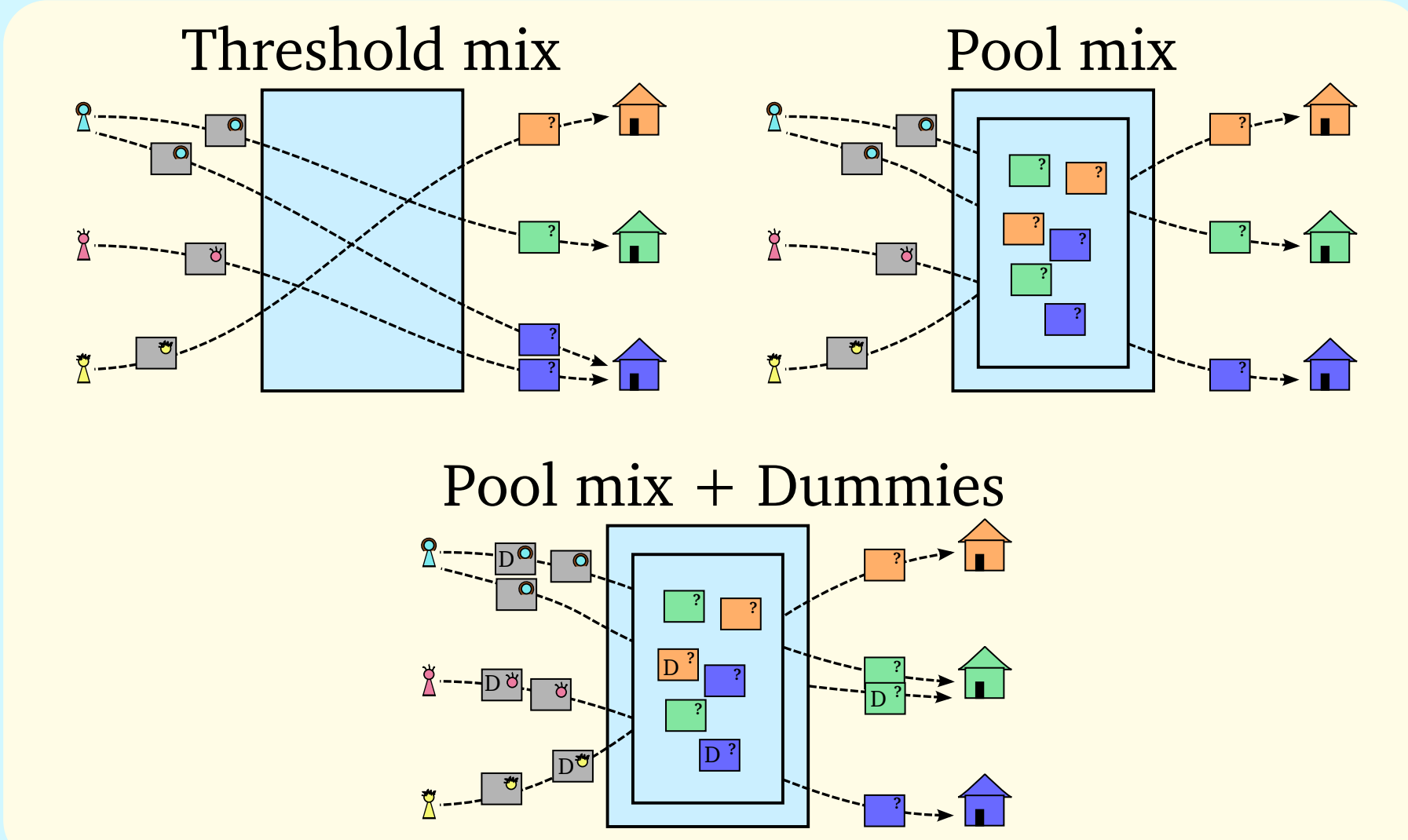
- Delaying messages is allowed!!
- We cannot change recipients.



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

RESEARCH PLAN

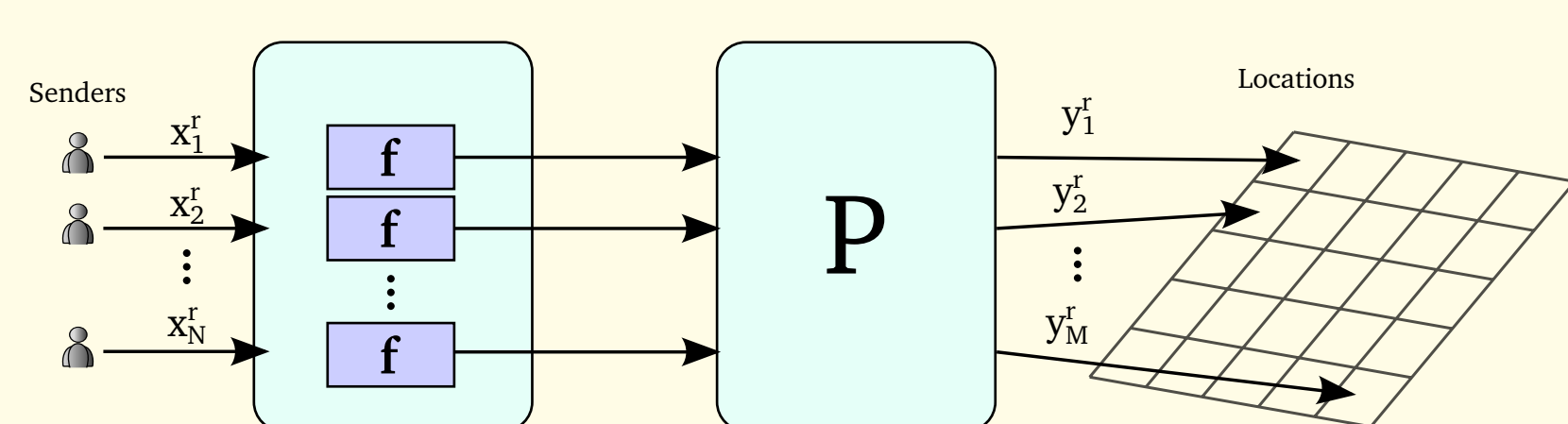
- 6 m.
- Study the state of the art (mixes).
 - Delay-based anonymous communications:



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

- Short-term attacks
- Long-term attacks

Obfuscation Timed mix



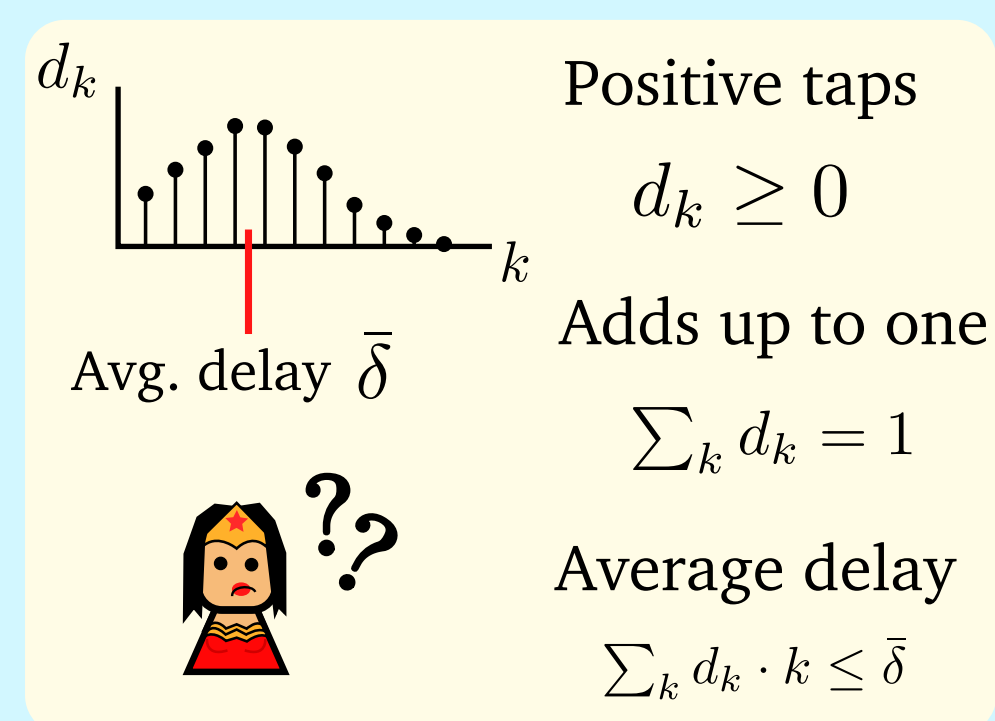
1. Develop theoretical models.
2. Apply signal processing tools to analyze the privacy properties.
3. Optimize the privacy mechanisms.
4. Propose new protection mechanisms.
5. Empirical evaluation of our findings.

- 2 m.
- Wrapping up, conclusions and writing.

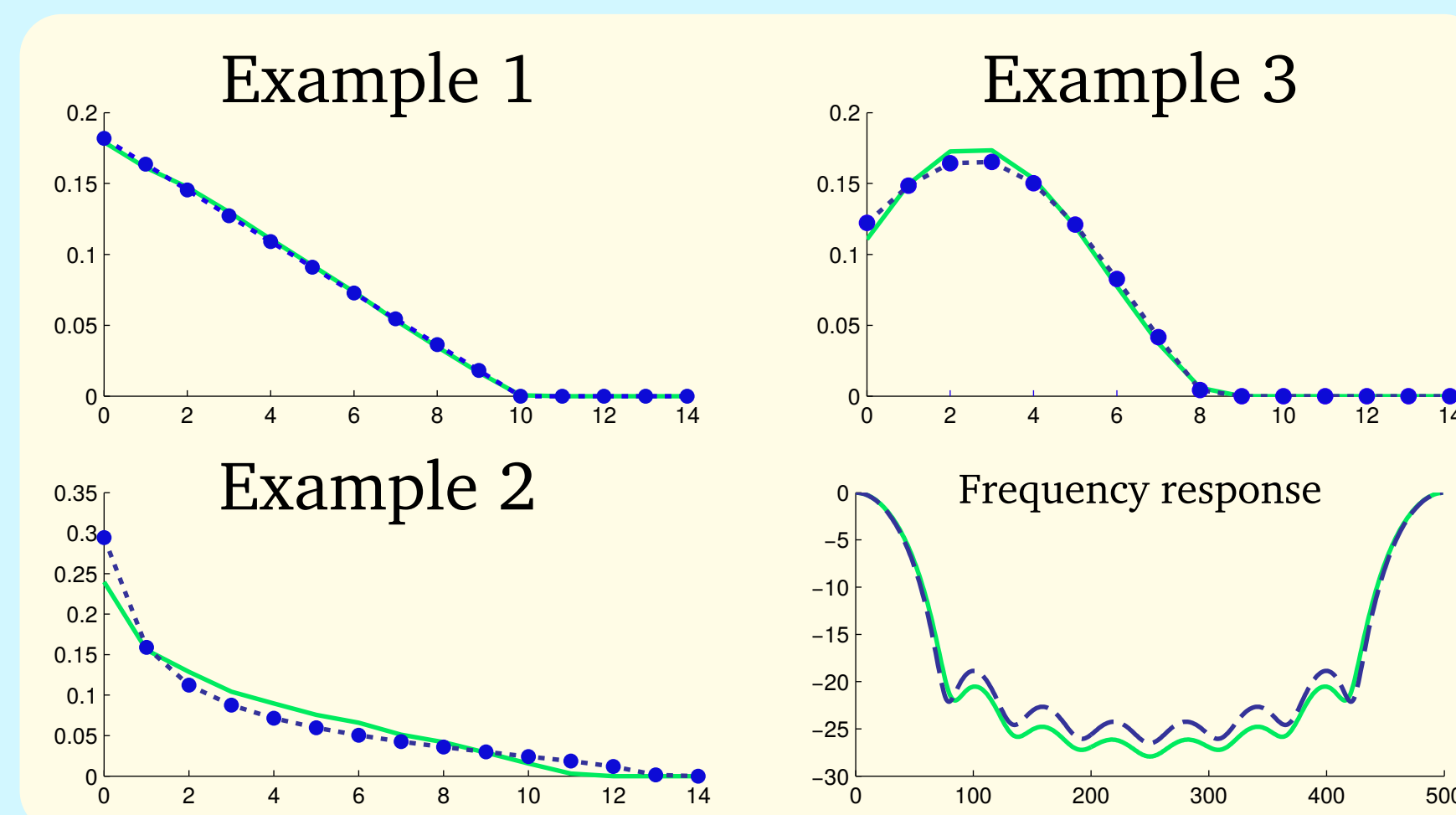
Methodology

NEW RESULTS

- Filter design applied to pool mixes [10]



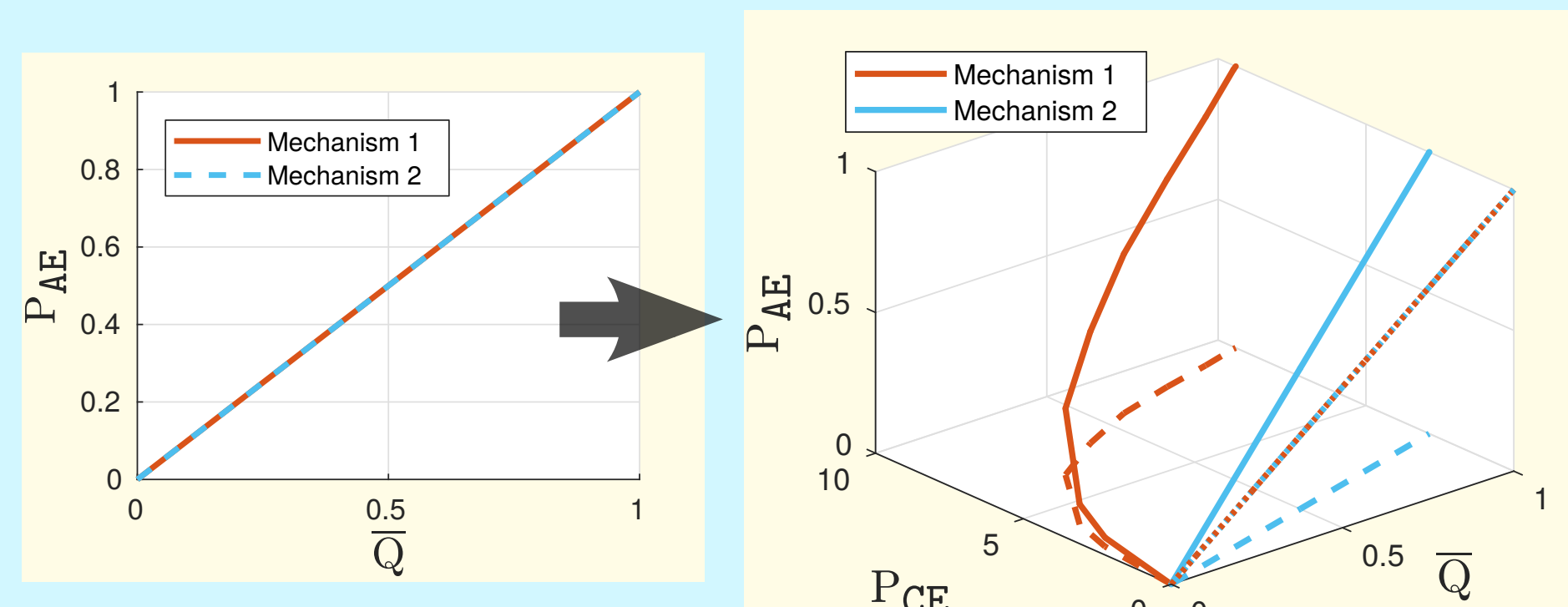
- Numerical, from real data.
- Analytical, from the filter design problem.



The **analytical** designs are very close to the **numerical** solutions with real-data experiments!

- Revisiting the design of optimal location privacy mechanisms (under submission) [11]

A useless privacy mechanism can be considered optimal according to traditional evaluation methods [3]. We need other privacy metrics, the entropy looks promising.



NEXT YEAR PLANNING

- Geo-indistinguishability, an extension of differential privacy to location privacy, is another standard evaluation technique. We have found that people are overestimating this privacy guarantee.
- Develop location privacy mechanisms for semantic and geographic privacy.
- Delay-based location privacy.

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 communications systems," *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 (submitted).

PREVIOUS RESULTS

- Proof that LSDA outperforms the family of statistical disclosure attacks [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].