Institute of Computer Science, University of Bern
Privacy and Data Security, HS 2021

Prof. Christian Cachin
Orestis Alpos, Luca Zanolini

Exercise 8

8.1 Location privacy (10pt)

In this exercise we investigate a probabilistic model for privacy-preserving location reporting. We use a Bayesian network as explained in the guest talk [HAHT17, Sec. 2.2].

Our model consists of n independent users moving for m discrete periods of time in a space that simply consists of R regions. We assume the location of a user at time t depends only on its location at time $t-1$. Let the random variable $X_{it} \in \{1, \ldots, R\}$ denote the location of user $i \in \{1, \ldots, n\}$ at time $t \in \{1, \ldots, m\}$. The initial locations of the users are assumed known.

a) Represent this model as a Bayesian network (and clarify what each node represents). Give a factorized formula for the joint distribution $P_{\mathbf{X}}$ for $\mathbf{X} = [X_{it}]$ that describes the overall behaviour of all users throughout the m time periods.

b) Now assume additionally that users have a mechanism to report an obfuscated location O_{it} at every time. The mechanism is probabilistic, and the reported location lies in the range $\{1, \ldots, R\}$ and depends on the actual location of the user at time t. Upgrade your model and formula to account for this mechanism.

c) Finally, in addition to the previous assumptions, users now report pairwise co-locations as follows. *If* two users are at the same location at time t, they report this with probability q (the report includes the fact that they are in the same location but not the location); *otherwise*, i.e., when they are not at the same location, they do not report such a co-location (i.e., the report has probability 0). Define the appropriate random variables and express the conditional probability functions for reporting co-locations. Give a new model and factorized formula for the joint distribution over all defined events.

References

[HAHT17] M. Humbert, E. Ayday, J. Hubaux, and A. Telenti, *Quantifying interdependent risks in genomic privacy*, ACM Trans. Priv. Secur. **20** (2017), no. 1, 3:1–3:31, `https://doi.org/10.1145/3035538`.