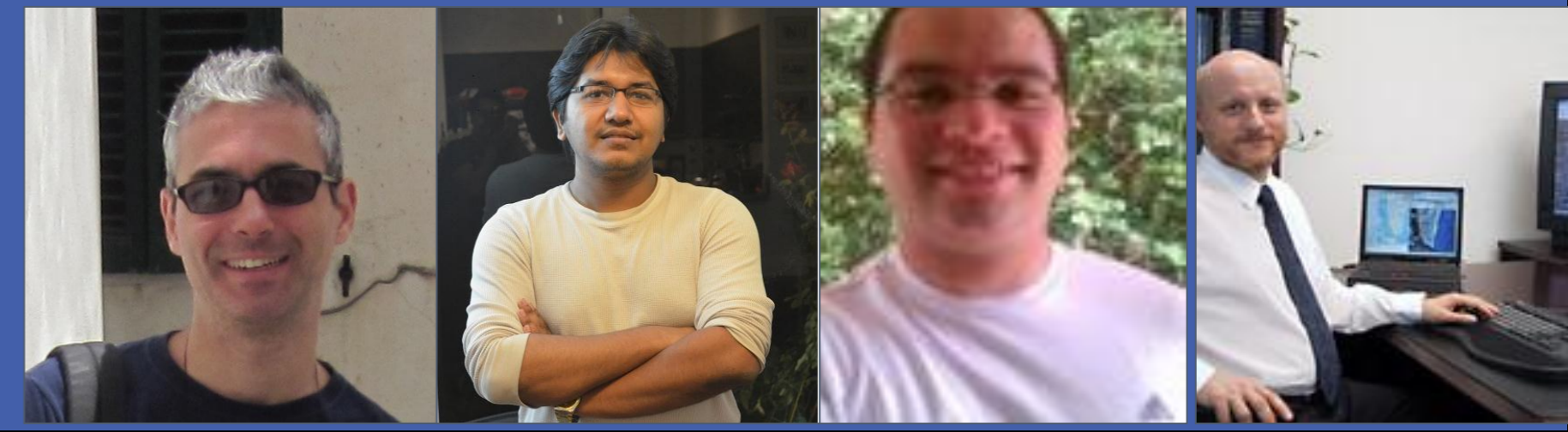


Private Location Centric Profiles for GeoSocial Networks

Bogdan Carbutar, Mahmudur Rahman, Jaime Ballesteros, Naphtali Rishe

Florida International University



Introduction

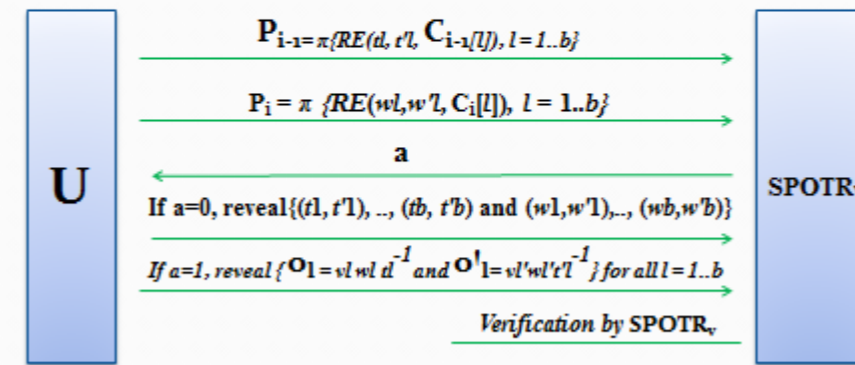
Providing input to targeted advertising, profiling social network users is an important source of revenue for geosocial networks. Since profiles contain personal information, their construction introduces a trade-off between user privacy and incentives of participation for businesses and geosocial network providers.

We take first steps toward breaking this deadlock.



ZK-CTR: Proof of Correctness

U and SPOTR_v run the following steps s times:

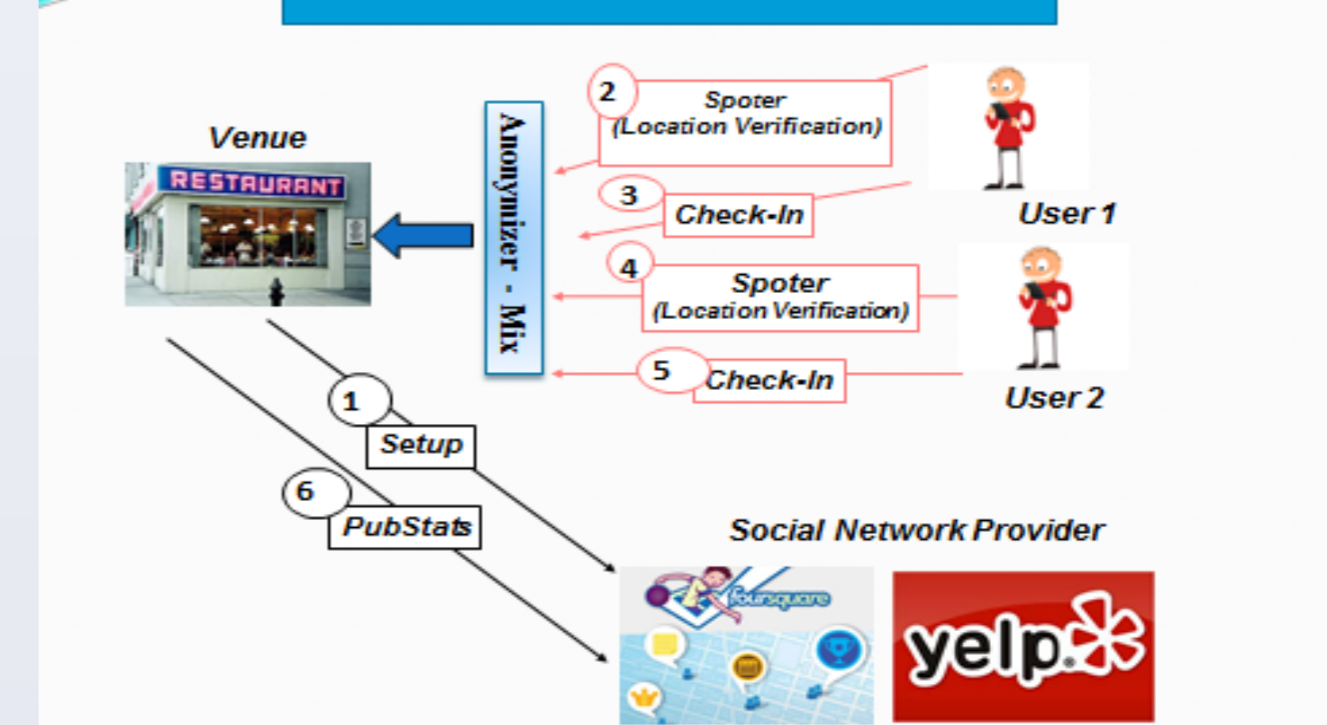


Experiment Setup

- Samsung Admire smartphone running Android OS Gingerbread 2.3 with a 800MHz CPU
- Dell laptop equipped with a 2.4GHz Intel Core i5 processor and 4GB of RAM for the server
- 802.11b/g Wi-Fi interface

All reported values are averages taken over at least 10 independent protocol runs.

Solution Architecture (k=2)



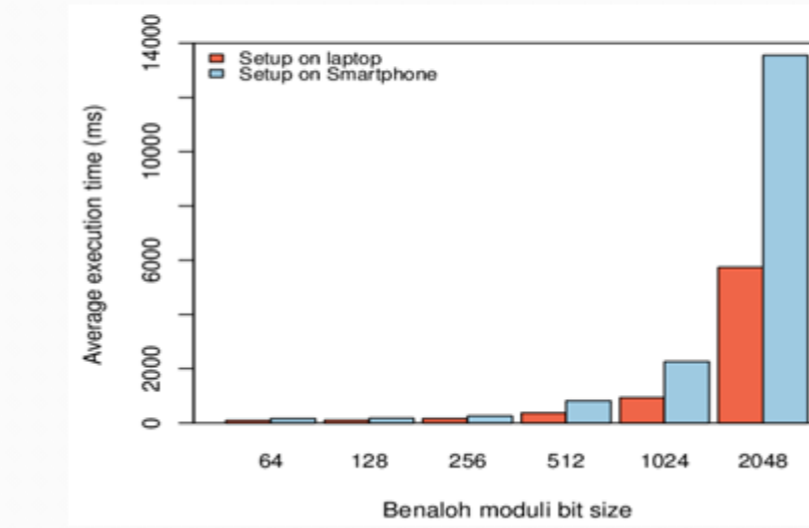
Our Contribution

- Introduce the concept of *location centric profiles* (LCPs)
- Propose PROFIL_R, a framework that
 - allows the construction of LCPs based on present user profiles
 - ensures privacy and correctness of participants.
- Consider two correctness components
 - location correctness
 - LCP correctness
- Propose a venue centric PROFIL_R

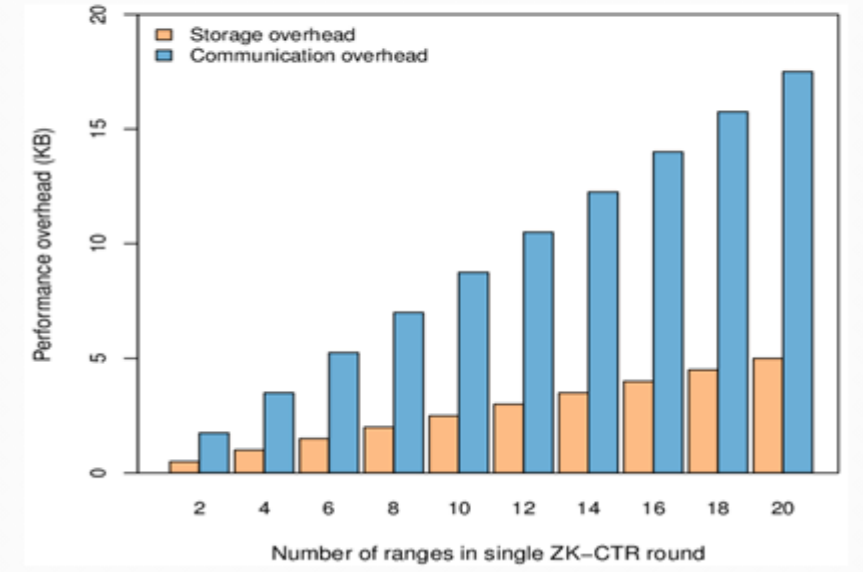
Location Centric Profiles (LCPs)

- Each user has a profile $P_U = \{u_1, u_2, \dots, u_d\}$
- Given a set of users U at location L , $LCP(L)$ is the set $\{S_1, S_2, \dots, S_d\}$
- We focus on a single profile dimension, D
- The aggregate statistics S for dimension D of $LCP(L)$ consists of b counters c_1, c_2, \dots, c_b

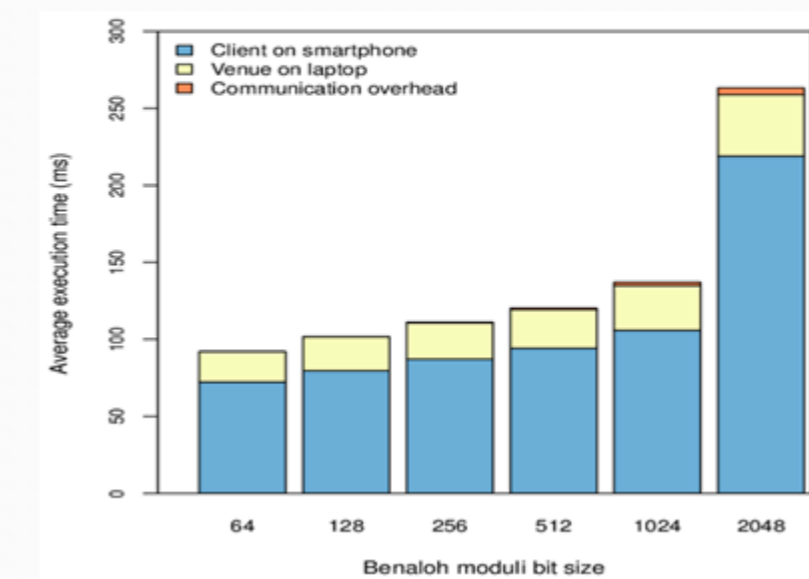
Setup dependence on Benaloh modulus size



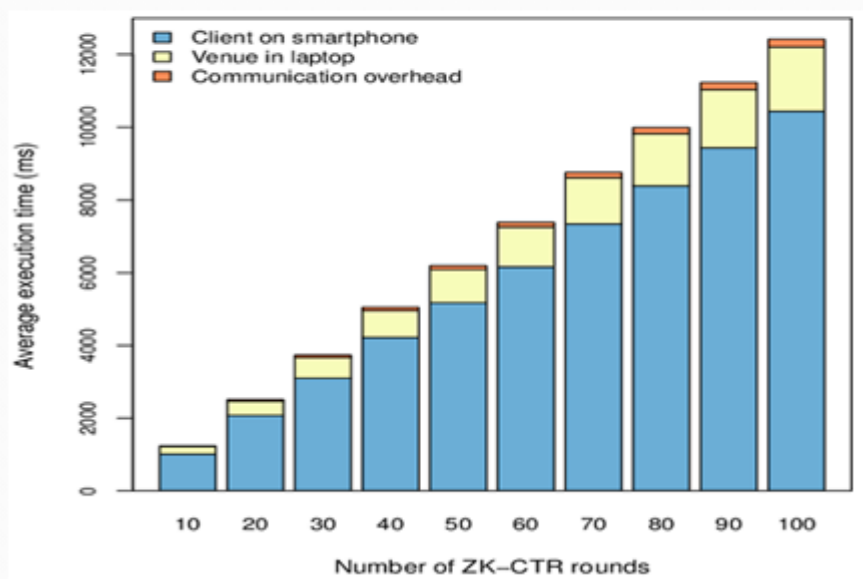
Storage and Communication overhead



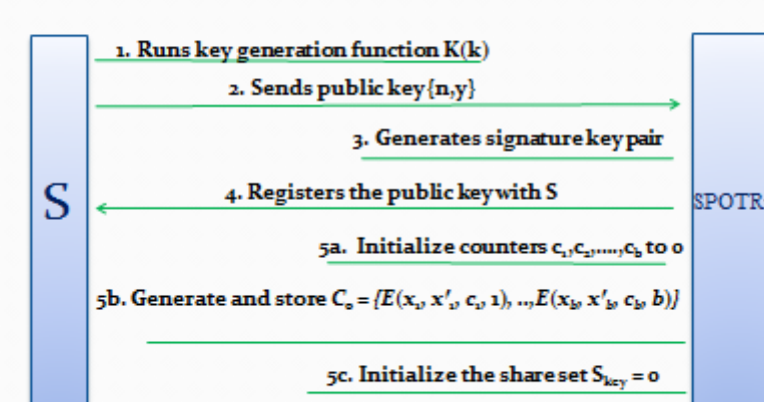
ZK-CTR Performance (Single round)



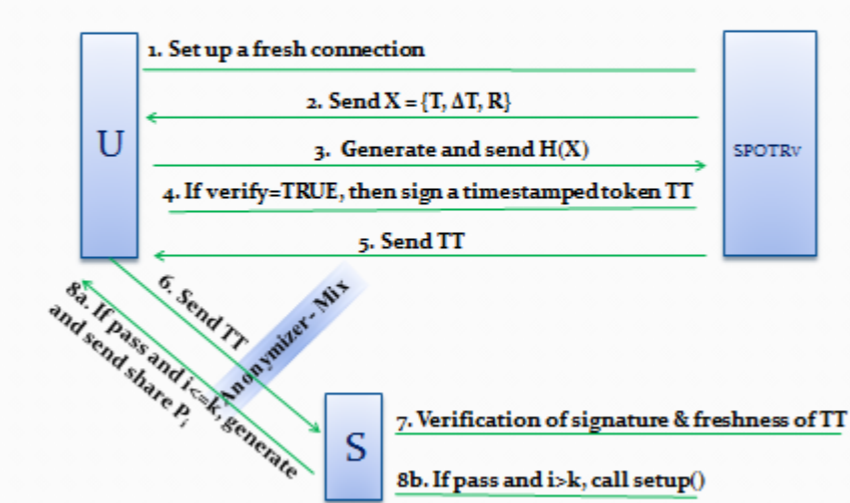
ZK-CTR Performance (Multiple rounds)



Setup(v_l, S(k))

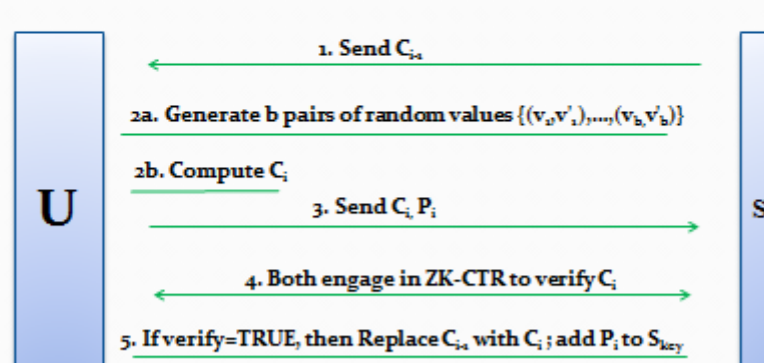


Spoter(u_(k), v_(l), S(k))



CheckIn(u_(p), n, v_(l), V(n, y, C_{i-1}, S_{key}))

If Spoter is successful, then do the following:



PubStats(v_(ck, Sh, V), S(p, q))

Steps:

- If $|Sh| < k$, abort.
- If $|Sh| = k$, use the k shares to reconstruct p
- Use p and $q = n/p$ to decrypt each record in C_k
- Publish results.

Conclusions

- Propose novel mechanisms for building aggregate location-centric profiles
- Maintain privacy of the participating users
- Ensure users' honesty during the process.
- Show that our solution is efficient, even when running on resource constrained mobile devices

References

- [1] Balachander Krishnamurthy and Craig E. Wills. On the leakage of personally identifiable information via online social networks. *Computer Communication Review*, 40(1):112–117, 2010.
- [2] Emily Steel and Geoffrey Fowler. Facebook in privacy breach. <http://online.wsj.com/article/SB1000042405220230477280457553848407523.html>
- [3] Foursquare Official Blog. On foursquare, cheating, and claiming mayorships from your couch. <http://goo.gl/FiYn5>, 2011.
- [4] Philippe Golle, Frank McSherry, and Ilya Mironov. Data collection with self-enforcing privacy. In Rebecca Wright, Sabrina De Capitani di Vimercati, and Vitaly Shmatikov, editors, *ACM Conference on Computer and Communications Security—ACM CCS 2006*, pages 69–78. ACM, October 2006.
- [5] Vincent Toubiana, Arvind Narayanan, Dan Boneh, Helen Nissenbaum, and Solon Barocas. Adnostic: Privacy preserving targeted advertising. In *NDS5*, 2010.

Contact

Mahmudur Rahman

Mobile: +1 305-7985490

E-mail: mrahm004@cs.fiu.edu

Office: ECS 264, SCIS, Florida Intl University