Cryptology ePrint Archive: Report 2011/445

Privacy-Preserving Friend Search over Online Social Networks

Huang Lin and Sherman S. M. Chow and Dongsheng Xing and Yuguang Fang and Zhenfu Cao

Abstract: Friendships or social contacts represent an important attribute characterizing one's social position and significantly impact one's daily life. Over online social networks (OSNs), users may opt to hide their social circle, membership or connections to certain individuals or groups for privacy concern. On the other hand, this prohibits a major benefit of OSNs -- building social connections. In order to enable OSN users to search for contacts they interested and leverage friends-of-friends relationship to grow their social network, we study the following privacy-preserving profiles searching (PPPS) problem: user P_1 wants to seek for contacts possessing a certain set of attributes from the contacts of P_2, while the contacts of P_2 remain hidden from P_1 and the criteria of P_1 is unknown to P_2 unless P_2 indeed having such contacts.

While the PPPS problem can be solved with the help of oblivious transfer with hidden access control (OT-HAC) which in turn can be built by anonymous identity-based encryption (IBE) with blind key extraction (BKE) protocol, the designs of existing systems are often complicated and the efficiency are not satisfactory. A simple and efficient approach is especially important for P_2 since he is playing a helping role in the protocol.

In this paper, we propose efficient BKE protocols, for an anonymous IBE and an anonymous hierarchical IBE attributed to Ducas in CT-RSA '10. Our protocol for IBE is conceptually simpler and more efficient than an existing proposal by Camenisch $\etal$ in PKC '09. Our protocol for HIBE is the first of its kind in the literature to the best of our knowledge. When compared with the OT-HAC system proposed by Camenisch $\etal$ in PKC '11, our protocol is again conceptually simpler, supports predicates defined by vectors from a large-domain instead of bit-vectors, and allows retrieval of multiple items in one invocation. Finally, we demonstrate their practicality by our performance analysis on prototypes implementation.

Category / Keywords:

Date: received 15 Aug 2011

Contact author: huanglin at ufl edu