Cryptology ePrint Archive: Report 2011/462

Secure Outsourced Computation of Iris Matching

Marina Blanton and Mehrdad Aliasgari

Abstract: Today biometric data propagate more heavily into our lives. With more ubiquitous use of such data, computations over biometrics become more prevalent as well. While it is well understood that privacy of biometric data must be protected, often computations over biometric data involve untrusted participants or servers, let it be a cross check between different agencies who are not permitted to share the data or a researcher testing a new biometric matching algorithm on a large scale that forces the computation to be placed on a grid. Unarguably, it would be desirable to secure computation over sensitive biometric data in such environments. Currently, no secure techniques for outsourcing biometric comparisons or searching are readily available, and this work makes the first step at designing solutions for secure outsourcing iris identification to one or more untrusted servers. We develop new solutions for the single-server (i.e., non-interactive) and multiple-server settings that use significantly different techniques. Furthermore, we carry out extensive experimentation on a database of iris codes to both validate the findings and achieve efficiency improvements.

Category / Keywords: cryptographic protocols /

Publication Info: To appear in Journal of Computer Security

Date: received 23 Aug 2011, last revised 16 Mar 2012

Contact author: mblanton at nd edu