MAP-i: Doctoral Programme in Computer Science

2013-14

Ph.D. Proposal

January 17, 2014

**Supervisor:** Manuel Barbosa
HASLab – INESC TEC and Univ. Minho

**Host R&D Unit:** HASLab – INESC TEC and Univ. Minho

**External Advisor:** Bogdan Warinschi
Dep. Comp. Science, University of Bristol

## Thematic Area

This proposal fits in the broad topic of Secure Multiparty Computation (SMPC), an area of cryptography that addresses the problem in which a number of players agree to compute a function on their private inputs in a secure way. Yao's millionaire problem, in which two people are trying to decide which one is richer without revealing the value of their wealth is a simple and well known example of SMPC. Modern implementations allow for more complex computations over private data, such as data mining algorithms over joint data from multiple companies.

SMPC was initially considered not usable in practice, due to high inherent computation and communication demands, but state-of-the-art research is constantly improving its viability. Tools and frameworks such as VIFF [Geisler, 2010], Sharemind [Bogdanov et al., 2008] and FairplayMP [Ben-David et al., 2008], are examples of approaches that aim towards providing efficient implementations of SMPC for practical usage.

Evaluating the security of SMPC protocols is, however, not trivial. Security proofs for such protocols typically make use of the Universally Composability framework [Canetti, 2001] and can be extremely complex. This means that they are usually presented at a high level of abstraction, often lacking the desired rigor expected from security justifications.

Domain-specific languages such as SecreC [Jagomägis, 2010] or SFDL [Malkhi et al., 2004] adequately support the implementation of SMPC functions, but still lack formal correctness and security validation mechanisms.

By combining these languages with tools for computer-aided cryptography, the resulting implementations could be validated to a high degree of assurance for a given security model, resulting in more robust cryptographic implementations.

As such, research possibilities arise from the need to bridge SMPC implementations with the appropriate security and correctness guarantees. This Ph.D. project aims to improve the implementation of high-assurance SMPC protocols by contributing to the design of appropriate development, validation and verification tools.

## References

[Ben-David et al., 2008] Ben-David, A., Nisan, N., and Pinkas, B. (2008). Fairplaymp: a system for secure multi-party computation. In *Proceedings of the 15th ACM conference on Computer and communications security*, pages 257–266. ACM.

[Bogdanov et al., 2008] Bogdanov, D., Laur, S., and Willemson, J. (2008). Sharemind: A framework for fast privacy-preserving computations. In *Computer Security-ESORICS 2008*, pages 192–206. Springer.

[Canetti, 2001] Canetti, R. (2001). Universally composable security: A new paradigm for cryptographic protocols. In *Foundations of Computer Science, 2001. Proceedings. 42nd IEEE Symposium on*, pages 136–145. IEEE.

[Geisler, 2010] Geisler, M. J. B. (2010). *Cryptographic Protocols:: Theory and Implementation.* PhD thesis, Aarhus UniversitetAarhus University,[Enhedsstruktur før 1.7. 2011] Aarhus University, Det Naturvidenskabelige FakultetFaculty of Science, Datalogisk InstitutDepartment of Computer Science.

[Jagomägis, 2010] Jagomägis, R. (2010). Secrec: a privacy-aware programming language with applications in data mining. *Master's thesis, University of Tartu.*

[Malkhi et al., 2004] Malkhi, D., Nisan, N., Pinkas, B., and Sella, Y. (2004). Fairplay-secure two-party computation system. In *USENIX Security Symposium*, pages 287–302.