Private Multi-party Matrix Multiplication and Trust Computation

Jean-Guillaume Dumas, Pascal Lafourcade, Jean-Baptiste Orfila
Maxime Puys

In this talk, we present new results on secure distributed matrix multiplication. Each player owns only one row of both matrices and wishes to learn about one distinct row of the product matrix, without revealing its input to the other players. We first improve on a weighted average protocol, in order to securely compute a dot-product with a quadratic volume of communications and linear number of rounds. We also propose a protocol with five communication rounds, using a Paillier-like underlying homomorphic public key cryptosystem, which is secure in the semi-honest model or secure with high probability in the malicious adversary model. Using ProVerif, a cryptographic protocol verification tool, we are able to check the security of the protocol and provide a countermeasure for each attack found by the tool. We also give a randomization method to avoid collusion attacks. As an application, we show that this protocol enables a distributed and secure evaluation of trust relationships in a network, for a large class of trust evaluation schemes.

References

[Amirbekyan and Estivill-Castro, 2007] Amirbekyan, A. and Estivill-Castro, V. (2007). A new efficient privacy-preserving scalar product protocol. In *AusDM 2007*, volume 70 of *CRPIT*, pages 209–214.

[Batir, 2011] Batir, N. (2011). Sharp bounds for the psi function and harmonic numbers. *Mathematical inequalities and applications*, 14(4).

[Ben-Or et al., 1988] Ben-Or, M., Goldwasser, S., and Wigderson, A. (1988). Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *STOC'88*. ACM.

[Benaloh, 1994] Benaloh, J. (1994). Dense probabilistic encryption. In *SAC'94*.

[Bendlin et al., 2011] Bendlin, R., Damgård, I., Orlandi, C., and Zakarias, S. (2011). Semi-homomorphic encryption and multiparty computation. In *EUROCRYPT'11*, LNCS.

[Blanchet, 2001] Blanchet, B. (2001). An efficient cryptographic protocol verifier based on prolog rules. In *IEEE CSFW'01*.

[Blanchet, 2004] Blanchet, B. (2004). *Cryptographic Protocol Verifier User Manual*.

[Chaum et al., 1986] Chaum, D., Evertse, J., van de Graaf, J., and Peralta, R. (1986). Demonstrating possession of a discrete logarithm without revealing it. In *CRYPTO'86*.

[Damgård et al., 2012] Damgård, I., Pastro, V., Smart, N., and Zakarias, S. (2012). Multiparty computation from somewhat homomorphic encryption. In *CRYPTO'12*, LNCS. Springer.

[Delaune, 2006] Delaune, S. (2006). An undecidability result for agh. *Theor. Comput. Sci.*

[Dolev et al., 2010] Dolev, S., Gilboa, N., and Kopeetsky, M. (2010). Computing multi-party trust privately: in $O(n)$ time units sending one (possibly large) message at a time. In *SAC'10*. ACM.

[Du and Atallah, 2001] Du, W. and Atallah, M. J. (2001). Privacy-preserving cooperative statistical analysis. In *ACSAC '01*, pages 102–110.

[Du and Zhan, 2002] Du, W. and Zhan, Z. (2002). A practical approach to solve secure multi-party computation problems. In *NSPW'02*. ACM.

[Dumas and Hossayni, 2012] Dumas, J.-G. and Hossayni, H. (2012). Matrix powers algorithm for trust evaluation in PKI architectures. In *STM'12, ESORICS 2012*, LNCS.

[Foley et al., 2010] Foley, S. N., Adams, W. M., and O'Sullivan, B. (2010). Aggregating trust using triangular norms in the keynote trust management system. In *STM'2010*.

[Fousse et al., 2011] Fousse, L., Lafourcade, P., and Alnuaimi, M. (2011). Benaloh's dense probabilistic encryption revisited. In *AFRICACRYPT'11*.

[Goethals et al., 2005] Goethals, B., Laur, S., Lipmaa, H., and Mielikäinen, T. (2005). On private scalar product computation for privacy-preserving data mining. In *ICISC'04*, LNCS. Springer.

[Guha et al., 2004] Guha, R. V., Kumar, R., Raghavan, P., and Tomkins, A. (2004). Propagation of trust and distrust. In *WWW'2004*.

[Huang and Nicol, 2010] Huang, J. and Nicol, D. M. (2010). A formal-semantics-based calculus of trust. *IEEE Internet Computing*.

[Jøsang, 2007] Jøsang, A. (2007). Probabilistic logic under uncertainty. In *CATS'2007*.

[Lafourcade and Puys, 2015] Lafourcade, P. and Puys, M. (2015). Performance evaluations of cryptographic protocols verification tools dealing with algebraic properties. In *FPS'15*.

[Lindell, 2009] Lindell, Y. (2009). Secure computation for privacy preserving data mining. In *Encyclopedia of Data Warehousing and Mining, Second Edition 4 Volumes)*. IGI Global.

[Michalas et al., 2012] Michalas, A., Dimitriou, T., Giannetsos, T., Komninos, N., and Prasad, N. R. (2012). Vulnerabilities of decentralized additive reputation systems regarding the privacy of individual votes. *Wireless Personal Commnications*, 66(3):559–575.

[Mohassel, 2011] Mohassel, P. (2011). Efficient and secure delegation of linear algebra. *IACR Cryptology ePrint Archive*.

[Ozarow and Wyner, 1984] Ozarow, L. H. and Wyner, A. D. (1984). Wire-tap channel II. In *EUROCRYPT'84*.

[Paillier, 1999] Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. In *EUROCRYPT'99*.

[Yao, 1982] Yao, A. C. (1982). Protocols for secure computations. *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*.