Abuse-Free Optimistic Contract Signing Using RSA for Multiuser Systems

Tristan Claverie
950418P612
trcl16@student.bth.se

Santosh Bharadwaj Rangavajjula
9408124635
sara16@student.bth.se

***Abstract*—Multi-party contract signing (MPCS) is a way for signers to agree on a predetermined contract by exchanging their signature. This matter has become crucial with the growing number of communications. In this paper we focus mainly on studying the state of the art protocols and more specifically the cryptography involved. We identify the major advances in MPCS and highlight a few gaps with the current protocols.**

I. Group members participation

The group members participated in the idea creation and report writing with the amount of involvement displayed in table I.

Group member	Idea creation	Report writing
Sri Harsha Arakatavemula	50%	50%
Santosh Bharadwaj Rangavajjula	50%	50%

Table I
Work repartition

II. Introduction

A. Context

B. Background

C. Objectives

D. Methods

E. Results

III. Review Question

IV. Review Methodology

V. Included and Excluded Studies

VI. Quality Assessment Criteria

VII. Results

VIII. Discussion

IX. Limitations

X. Conclusion

References

[1] Juan A. Garay, Markus Jakobsson, and Philip D. MacKenzie. Abuse-free optimistic contract signing. In Michael J. Wiener, editor, *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, volume 1666 of *Lecture Notes in Computer Science*, pages 449–466. Springer, 1999.

[2] Taher El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.

[3] N. Asokan, Victor Shoup, and Michael Waidner. Optimistic fair exchange of digital signatures. *IEEE Journal on Selected Areas in Communications*, 18(4):593–610, 2000.

[4] Aybek Mukhamedov and Mark Ryan. Improved multi-party contract signing. In Sven Dietrich and Rachna Dhamija, editors, *Financial Cryptography and Data Security, 11th International Conference, FC 2007, and 1st International Workshop on Usable Security, USEC 2007, Scarborough, Trinidad and Tobago, February 12-16, 2007. Revised Selected Papers*, volume 4886 of *Lecture Notes in Computer Science*, pages 179–191. Springer, 2007.

[5] G. Wang. An abuse-free fair contract-signing protocol based on the rsa signature. *IEEE Transactions on Information Forensics and Security*, 5(1):158–168, 2010. cited By 24.

[6] M. Fischlin. *Trapdoor Commitment Schemes and Their Applications*, 2001. cited By 22.

[7] Barbara Kordy and Saša Radomirović. Constructing optimistic multi-party contract signing protocols. In Stephen Chong, editor, *25th IEEE Computer Security Foundations Symposium, CSF 2012, Cambridge, MA, USA, June 25-27, 2012*, pages 215–229. IEEE, 2012.

[8] Juan A. Garay and Philip D. MacKenzie. Abuse-free multi-party contract signing. In Prasad Jayanti, editor, *Distributed Computing, 13th International Symposium, Bratislava, Slavak Republic, September 27-29, 1999, Proceedings*, volume 1693 of *Lecture Notes in Computer Science*, pages 151–165. Springer, 1999.

[9] Sjouke Mauw and Sasa Radomirovic. Generalizing multi-party contract signing. In Riccardo Focardi and Andrew C. Myers, editors, *Principles of Security and Trust - 4th International Conference, POST 2015, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2015, London, UK, April 11-18, 2015, Proceedings*, volume 9036 of *Lecture Notes in Computer Science*, pages 156–175. Springer, 2015.

[10] Giuseppe Ateniese. Efficient verifiable encryption (and fair exchange) of digital signatures. pages 138–146, 1999. cited By 94.

[11] X. Chen, F. Zhang, H. Tian, Q. Wu, Y. Mu, J. Kim, and K. Kim. Three-round abuse-free optimistic contract signing with everlasting secrecy. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 6052 LNCS:304–311, 2010. cited By 0.

[12] W. Gao, F. Li, and B. Xu. An abuse-free optimistic fair exchange protocol based on bls signature. volume 2, pages 278–282, 2008. cited By 3.

[13] X. Li, Z. Wang, L. Chen, and Q. Wang. A multi-party contract signing protocol and its formal analysis in strand space model. volume 3, pages 556–559, 2009. cited By 0.

[14] X. Chen, F. Zhang, H. Tian, Q. Wu, Y. Mu, J. Kim, and K. Kim. Three-round abuse-free optimistic contract signing with everlasting secrecy. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 6052 LNCS:304–311, 2010. cited By 4.

[15] S. Heidarvand and J.L. Villar. A fair and abuse-free contract signing protocol from boneh-boyen signature. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 6711 LNCS:125–140, 2011. cited By 1.

[16] A.A. Al-Saggaf and L. Ghouti. Efficient abuse-free fair contract-signing protocol based on an ordinary crisp commitment scheme. *IET Information Security*, 9(1):50–58, 2015. cited By 0.