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 involvment displayed in table I.

Group member	Idea creation	Report writing
Tristan Claverie	50%	50%
Santosh Bharadwaj Rangavajjula	50%	50%

Table I
Work repartition

II. Introduction

A. Context

Signing a paper contract between two users may be very simple, but signing a paper contract between 2 000 signers is very difficult. The same problematic arise if the contract involves only 10 people scattered around the globe. In such cases the ability to sign a contract using a computer becomes very handy. One thing necessary for such a protocol is *fairness*, that is signer A can not get the signature of any other honest signer unless signer A has committed to the contract. An easy way to solve this problem would be for every signer to send his signature to a *Trusted Third Party* (TTP), then the TTP sends back a fully signed contract to everyone. However, by doing this the TTP would become an necessary element of any contract signature and would end up being a bottleneck. Another approach is to share the load between all signers, and to refer to the TTP only in case of problem during the signature. This kind of MPCS is called *optimistic*.

B. Background

We are interested in the notion of *abuse-freeness* as defined in [1]. A protocol is abuse-free if no group of signer can prove that he holds the power to complete or abort the contract signature. Garay et al. introduce a new cryptographic object called *Private Contract Signature* in [1] based on ElGamal crypto system [2] and use it to define a two-party contract signing and a three-party contract signing. These construction are proven to be fair, optimistic and abuse-free. In [3] an optimistic protocol for exchanging fairly signatures was proposed by Asokan et al.. Mukhamedov et al. proposed another optimistic MPCS for any number of signers in [4] also base on private contract signatures. Wang proposed an abuse-free, optimistic two-party contract signing in [5] using RSA and trapdoor commitment schemes [6]. Kordy et al. proved an equivalence between a mathematical sequence and the fairness of an MPCS protocol in [7], it is based on private contract signature. The obtained protocol is abuse-free, optimistic, fair and efficient because it reaches the lower bounds in terms of bandwidth and message complexity determined by Garay et al. in [8]. In [9] Mauw et al. extend the work of Kordy et al. using a labeled DAG instead of a linear sequence, and achieving as well an optimistic abuse-free fair and efficient MPCS.

C. Objectives

A common point to optimistic MPCS is that at some point, a commitment is exchanged before sending the signature. At first, *verifiable escrows* [3] and *verifiable encrypted signature* [10] were used as commitments but the consequent schemes were not abuse-free. RSA crypto system is now an industry standard, but there are only two protocols which use it and guarantee abuse-freeness and optimism, however it only works for a two-party contract as show in table IV. This paper focuses on finding an MPCS protocol which is abuse-free, optimistic and fair for any number of signers. A secondary objective is its efficiency, *i.e.* it has to be usable in practice without heavy computation and should stick to the RSA industry standard.

D. Methods

We chose contract signing as our research field because it is a very specific field and it will probably become more and more crucial with time. It involves heavy cryptography and mathematics which makes it very interesting to work in. We started by looking at the first articles we could find about contract signing on IEEE Xplore in order to gain some basic knowledge about it. From there, we were able to orient our research to be more and more specific, by adding the

"optimistic" and searching on Scopus. There were 63 results, so we looked at the older ones first. This allowed us to add the "abuse-free" keyword and get down to 13 results (14 but one is plagiarised from another). After applying our inclusion and exclusion criteria, we were left with 8 articles. By doing a forward search from [1], we were able to find two more articles that are expected to be abuse-free free, though the proof wasn't in the paper.

E. Results

A summary of the included papers in this SLR is provided in table IV. We discuss the method for obtaining those in section IV. and V. We discuss the results in section VII. and give limits of this paper in section VIII.

III. Review Question

Q1.How can contract signing be made trust worthy and optimal ?

This research question is framed for acquiring knowlegde on studying the current state of art in contract signing protocols. Contract signing is an important part of the E commerce transactions and hence, it is very important to have a basic understanding of the contract signing mechanisms. The steps followed, actionstaken and trust mechanisms are gathered from the exising studies.

Q2.How can we eliminate the trusted third party in the optimistic contract signing?

In order to implement trust in fool proof systems, trusted third party (TTP) is used in the literature. As TTPs are not completely abuse-free, charge a subscription fee and use bandwidth, they become bottle necks in multi user transactions. Therefore, this research question is framed to get knowledge about eliminating the TTPs in contract signing. The question allows us to explore the other systems which do not use TTPs in digital contract signing.

IV. Review Methodology

Pilot study:
Firstly, we wanted to work to improve security in networks and chose a specific topic "Contract signing". On searching in the IEEE Explore with "Contract Signing", we found that its a huge topic (336 results) and required a lot more time.So we reformulated the question by adding two new keywords "Abuse-free" and "optimistic" to narrow down the search and also get more relevant papers. With a basic search on the IEEE Explore we found 4 papers and using this research question, we want to move forward on the SLR in addressing gaps with contract signing over the network for more than 2 parties.

Search Strings:
Security in networks is the domain chosen initially for exploring the subject and "Contract Signing" is chosen as the topic of interest .As, topic is huge and takes a lot more time, the search is narrowed down by adding keywords "Abuse-free" AND "Optimistic" as we are more interested in the field. A basic search along with the new keywords is performed, papers found are analysed and synthesised.

V. Included and Excluded Studies

The inclusion criterion involves:

1) Articles that have full text.
2) Articles in English language.
3) Research articles that are Peer reviewed.
4) Research article that are Journal articles and conference proceedings.
5) Research articles that have insight of any crypto system

The Exclusion criterion involves:

1) Articles that cost money
2) Research articles in languages other than English
3) Research articles that are not peer reviewed
4) Research articles that are not related to Computer Science

VI. Quality Assessment Criteria

The acquired information from literature is assessed based on how we utilise it in our research.

QC1: Are the objectives clear ?
QC2: Are the mechanisms applicable for more than 2 parties ?
QC3: Are the limitations stated clearly ?
QC4: Are the techniques applicable with RSA keys ?

VII. Results

We present our results in this section. They are based on the different articles we have read and present an overview of what is state of the art contract signing.

- **Problem of implementation** Most of the protocols we came across are not fit to the real world. By that, we mean that there are only two optimistic, abuse-free fair MPCS using the RSA standard but they are valid for only two signers. One is using trapdoor commitment scheme [5] and the other has modifid the verifiable encrypted singature and defined a new object called *verifiable encryption of chameleon signature* [11] to define a protocol. We think that there is still some work to be conducted in order to get an MPCS using RSA which would ensure optimism, abuse-freeness and fairness for any number of signers.
- **Private Contract Signature** Using private contract signatures to define an MPCS protocol seems to be very appreciated. Several protocols have been defined and have attained very interesting properties. Unlike verifiable encrypted signature, PCSs are defined only for the ElGamal cryptosystem, which makes them useful and interesting but not that powerful. However, by looking at the construction of those cryptographic object as in [1], we may be able to create an object with the same properties working for RSA.
- **Generalization** Abuse-free optimistic MPCS are still studied separately in the sense that there is yet no protocol

Reference papers	QC1	QCQ2	QCQ3	QC4
Ref[1]	YES	YES	YES	YES
Ref[8]	YES	YES	YES	YES
Ref[12]	YES	YES	YES	YES
Ref[13]	YES	YES	YES	YES
Ref[5]	YES	YES	YES	YES
Ref[14]	YES	YES	YES	YES
Ref[7]	YES	YES	YES	YES
Ref[9]	YES	YES	YES	YES
Ref[16]	YES	YES	YES	YES

Table II
QUALITY ASSESSMENT TABLE

Reference papers	QC1	QCQ2	QCQ3	QC4
Ref[1]	YES	YES	YES	YES
Ref[8]	YES	YES	YES	YES
Ref[12]	YES	YES	YES	YES
Ref[13]	YES	YES	YES	YES
Ref[5]	YES	YES	YES	YES
Ref[14]	YES	YES	YES	YES
Ref[7]	YES	YES	YES	YES
Ref[9]	YES	YES	YES	YES
Ref[16]	YES	YES	YES	YES

Table III
QUALITY ASSESSMENT TABLE

that have managed to guarantee those properties for any one-way function. However, such objects like trapdoor commitment schemes can be created from any one-way function, so maybe there will be a breakthrough in a few years.

This SLR was aimed at finding an MPCS for any number of signers with interesting properties which could use RSA. This was not attained in any of the protocols we've studied, and here is the overview of our results is given in table IV for the following Data Extraction Questions :

- **DEQ1** What are the results of the study ?
- **DEQ2** What are the limitations of the study ?
- **DEQ3** What encryption scheme(s) does the protocol support
- **DEQ4** What is the cryptographic object used as commitment ?

VIII. DISCUSSION

- This study is about finding a protocol which is abuse-free, optimistic and fair for any number of signer, and we've provided examples of such protocols. All the optimistic protocols we've seen have the same structure : Signers exchange during one or several rounds their commitment to a pre-agreed contract. When those rounds are over, signers send their signature, and the TTP is able to derive a signer's signature from his commitment.
- Another point of interest was the load on the TTP. Optimistic protocols are great at reducing the load because the TTP is only called in case of failure in the protocol. Meaning, during a normal execution of a contract signature, the TTP is not called. Ways to handle the TTP differ amongst protocols. The RSA based protocols [5][14] require a step of registration to the TTP, whereas in [7] and [9] the TTP is not even aware of the signature.
- The final step would be to throw away the TTP, which is theoretically possible using a peer-to-peer network, but hard to put in practice. However, we believe that by using a structure inspired by bitcoin's protocol it is possible to create an abuse-free, fair MPCS without any TTP.

IX. LIMITATIONS

- This SLR was intended to be as complete as possible, however we may have missed crucial information by narrowing our research string to abuse-free protocols. As an example, [7] and [9] were not in the first paper set.
- Some paper might be invalidated in the future due to a flaw discovered in the commitments of in the signature schemes.
- Some paper might be invalidated due to a flaw in a protocol not yet discovered.
- We might have excluded papers that other find relevant, proceeding to an exclusion bias.

X. CONCLUSION

In this paper we conducted an SLR about optimistic abuse-free contract signing. In table IV we summarized the relevant work in this field along with the major results. We mainly focused on the different cryptographic primitive used rather than the protocols or their efficency. We highlighted some gaps into the current protocols and we will strive to address one in a further research.

Reference papers	DEQ1	DEQ2	DEQ3	DEQ4
Ref[1]	Building an optimistic abuse-free fair MPCS, and definition of a new cryptographic object	The protocol is defined for 2 and 3 signers	ElGamal	Private Contract Signature
Ref[8]	Building an optimistic abuse-free fair MPCS, for n > 3 signers	Proven to be unfair for n $\geq$ 4	ElGamal	Private Contract Signature
Ref[12]	First optimistic abuse-free fair MPCS using BLS signature	Two signers	BLS	non-interactive proof of knowledge
Ref[13]	Optimistic abuse-free fair MPCS for any number of signers. Modeling and analysis of MPCS	-	ElGamal	Private Contraact Signature
Ref[5]	Optimistic abuse-free fair MPCS	Only for 2 signers	RSA	Trapdoor Commitment Scheme
Ref[14]	Optimistic abuse-free fair MPCS	Only for 2 signers	RSA	Verifiable encryption of Chameleon Signature
Ref[15]	Optimistic abuse-free fair MPCS using a variant of Boneh-Boyen signature	Only for 2 signers	A variant of Boneh-Boyen	Partial Signature Scheme
Ref[7]	Optimistic abuse-free fair MPCS. Equivalence between a sequence and an MPCS	Abuse-freeness not proven	ElGamal	Private Contract Signature
Ref[9]	Optimistic abuse-free fair MPCS. Equivalence between a labeled DAG and an MPCS	Abuse-freeness not proven	ElGamal	Private Contract Signature
Ref[16]	Optimistic abuse-free fair MPCS. Defines a framework for the commitment	Only for 2 signers	-	Ordinary Crisp Commitment Scheme

Table IV
RESULTS OVERVIEW

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.