

# Secure Web Services Protocol for Fair Contract Signing with Off-line Semi-Trusted Third Party

吳宗潔、曹偉駿

E-mail: 9314379@mail.dyu.edu.tw

## ABSTRACT

Fairness becomes a key factor while a data exchange since the transaction is conducted over the Internet. To start the data exchange, confidential data, payments, and signatures need to be transmitted. Main parties are afraid of they cannot get electronic documents from the other side safely while the data exchange. To ensure the fairness of data exchange, the protocol needs a trusted third party be a judge when the dispute occurs, and has to give a guarantee to main parties during the data exchange. Online contract signing is a kind of fair exchange. In addition to traditional contract signing, online contract signing has become a flexible method in business. Online contract signing consists of three main parties, including two signers and trusted third party. Currently, in the studies, most of the third parties are either online semi-trusted third party or off-line trusted third party. To eliminate the third party's connectional time and enhance its security, a secure and efficient protocol for fair contract signing with off-line semi-trusted third party has proposed in the proposed protocol, where a flexible method for selecting a semi-trusted third party is proposed actually. The online contract signing is still fair while the third party is off-line and main parties can rely on the semi-trusted with third party. Finally, in the thesis, the proposed protocol is extended to Web services so that it can be used for main parties in different platforms.

Keywords : Fair Data Exchange, Online Contract Signing, Off-line Semi-Trusted Third Party, Web Services

## Table of Contents

簽名頁 授權書	iii
中文摘要	v
ABSTRACT	vi
誌謝	vii
Contents	viii
List of Figures	xi
List of Tables	xii
Chapter I.	
INTRODUCTION	1
1.1 Background and Motivation	1
1.2 Purpose	4
1.3 Scope	4
1.4 Research Procedure	5
1.5 Thesis Organization	7
Chapter II. PREVIOUS WORKS	8
2.1 Fair Exchange	8
2.2 Contract Signing	9
2.3 DSS-Based Signature	10
2.2.1 Signature Generation	12
2.2.2 Signature Verification	13
2.4 Group-Oriented Digital Multisignature Scheme	14
2.5 XML Security	16
2.5.1 XML Digital Signature	16
2.5.2 XML Encryption	20
2.6 Web Services	22
2.6.1 SOAP	24
2.6.2 XKMS	26
2.7 WS-Security	29
Chapter III. RESEARCH METHODS	30
3.1 Semi-Trusted Third Party Selection Phase	30
3.2 Normal Phase-Signature Verification	32
3.3 Normal Phase- Contract Signing	33
3.4 Dispute Phase	34
3.1.1 Case I: dispute in party B	35
3.1.2 Case II: dispute in party A	36
Chapter IV. PROPOSED PROTOCOL FOR WEB SERVICES	38
4.1 Semi-Trusted Third Party Selection Phase	38
4.2 Normal Phase- Signature Verification	41
4.3 Normal Phase-Contract Signing	44
4.4 Dispute Phase	47
4.4.1 Case I: dispute in party B	47
4.4.2 Case II: dispute in party A	50
Chapter V. SECURITY ANALYSIS AND PERFORMANCE EVALUATION	53
5.1 Security Analysis	53
5.1.1 A semi-trusted third party	53
5.1.2 Scenarios	53
5.1.3 Completeness and Privacy	54
5.1.4 WS-Security	55
5.2 Performance Evaluation	55
5.3 Comparisons	56
Chapter VI.	
CONCLUSIONS	59
BIBLIOGRAPHY	61

## REFERENCES

- [1]M. Abadi, N. Glew, B. Home, and B. Pinkas, "Certified Email with a Light On-line Trusted Third Party Design and Implementation," in Proc. of the Eleventh International Conference on World Wide Web, pp. 387-395, 2002.
- [2]N. Asokan, M. Schunter, and M. Waidner, "Optimistic protocol for fair exchange," in Proc. of 4th ACM Conference on Computer and Communications Security, pp. 7-17, 1997.
- [3]N. Asokan, V. Shoup, and M. Waidner, "Optimistic Fair Exchange of Digital Signature," IEEE Journal on Selected Areas in Communications, vol. 18, pp. 593-610, 2000.
- [4]G. Avoine and S. Vaudenay, "Fair Exchange with Guardian -Angels," in Information Security Applications, LNCS 2908, pp. 188-202, 2004.
- [5]G. Avoine and S. Vaudenay, "Optimistic Fair Exchange Based on Publicly Verifiable Secret Sharing," in Proc. of 9th Australasian Conference on Information Security and Privacy, LNCS 3108, pp. 74-85, 2004.
- [6]B. Baur-Waidner and M. Waidner, "Round-Optimal and Abuse-Free Optimistic Multi-party Contract Signing," in ICALP, LNCS 1853, pp. 524-535, 2000.
- [7]B. Baur-Waidner, "Optimistic Asynchronous Multi-party Contract Signing with Reduced Number of Rounds," in Proc. of 28th International

- Colloquium on Automata, Languages and Programming, LNCS 1853, pp. 898-911, 2001.
- [8]M. Ben-Or, O. Goldreich, S. Micall, and R. L. Rivest, "A Fair Protocol for Signing Contracts," IEEE Transactions on Information Theory, vol. 36, pp. 40-46, 1990.
- [9]K. Bhargavan, C. Fournet, and A. D. Gordon, "A Semantics for Web Services Authentication," in Proc. of ACM POPL'04, pp. 198-209, 2004.
- [10]C. Boyd and P. Kearney, "Exploring Fair Exchange Protocols Using Specification Animation," in Proc. of Third International Workshop on Information Security, LNCS 1975, pp. 101-108, 2003.
- [11]G. Brose, "Gateway to Web Services Security- Securing SOAP with Proxies," in Web Services - ICWS-Europe, LNCS 2853, pp. 209-223, 2000.
- [12]C. Cachin and J. Caenisch, "Optimistic Fair Secure Computation," in Proc. of the 20th Annual International Cryptology Conference on Advances in Cryptology, pp.1-23, 2003.
- [13]R. Chadha, J. C. Mitchell, A. Scedrov, and V. Shmatikov, "Contract Signing, Optimism, and Advantage," in CONCUR- Concurrency Theory, LNCS 2761, pp. 366-382, 2003.
- [14]K. Chavda, "Anatomy of a Web Service," The Journal of Computing in Small Colleges, pp. 124-134, 2004.
- [15]D. Cohen, M. Jacovi, M. Herscovici, Y. S. Maarek, N. Meshulam, A. Soffer, and V. Soroka, "Leveraging web services for information discovery," Proc. of the IEEE International Conference on Software: Science, Technology and Engineering, pp. 123-132, 2003.
- [16]J. Cole and Z. Milosevic, "Extending Support for Contract in eXML," in Proc. of the Workshop on Information Technology for Virtual Enterprises, pp. 119-127, 2001.
- [17]B. Elisa, C. Barbara, and F. Elena, "XML Security," Information Security Technical Report, vol. 6, pp. 45-58, 2001.
- [18]J. L. Ferrer-Gomila, M. Payeras-Capell?, and L. Huguet-Roter, "Efficient Optimistic N-Party Contract Signing Protocol," in Proc. of 4th International Conference on Information Security, LNCS 2200, pp. 394-407, 2001.
- [19]J. L. Ferrer-Gomila, A.-I. Martinez-Nadal, M. Payeras-Capell?, and L. Huguet-Roter, "A Juridical Validation of a Contract Signing Protocol," in Proc. of Third International Conference on E-Commerce and Web Technologies, LNCS 2455, pp. 343-352, 2002.
- [20]M. K. Franklin and M. K. Reiter, "Fair Exchange with a Semi-Trusted Third Party," in Proc. of the 4th ACM conference on Computer and Communication Security, pp. 1-6, 1997.
- [21]J. A. Garay and C. Pomerance, "Timed Fair Exchange of Standard Signatures [Extended Abstract]," in Financial Cryptography, LNCS 2742, pp. 190-207, 2003.
- [22]O. Goldreich, "A Simple Protocol for Contract Signing," in Advances in Cryptology, pp. 133-136, 1984.
- [23]N. Gonzalez-Deleito and O. Markowitch, "An Optimistic Multi-party Fair Exchange Protocol with Reduced Trust Requirements," in Proc. of 4th International Conference on Information Security and Cryptology, LNCS 2288, pp. 258-267, 2002.
- [24]A. Goodchild, C. Herring, and Z. Milosevic, "Business Contracts for B2B," in Workshop on Infrastructures for Dynamic B2B Service Outsourcing, pp.1-11, 2000.
- [25]A. D. Gordon and R. Pucella, "Validating a Web Service Security Abstraction by Typing," in Proc. of ACM Workshop on XML Security, pp. 18-29, 2002.
- [26]L. Harn, "Group-oriented threshold signature scheme and digital multisignature," in IEEE Proc. of Computer and Digital Technology, vol. 141, pp. 307-313, 1994.
- [27]K. Harumoto and S. Shimojo, "A P2P platform architecture for context-sensitive applications and its implementation using web services," in IEEE Proc. of Communications, Computers and Signal, pp. 185-188, 2000.
- [28]A. L. Heuer, F. Losemann, and C. Meinel, "Logging and Signing Document-Transfers on the WWW- A Trusted Third Party Gateway," in Proc. of the First International Conference on Web Information Systems Engineering, vol. 1, pp. 146-152, 2000.
- [29]K. Hogg, P. Chilcott, M. Nolan, and B. Srinivasan, "An Evaluation of Web Services in the Design of a B2B Application," in Proc. of the 27th Conference on Australasian Computer Science, pp. 331-340, 2004.
- [30]B. Ingham, F. Panzieri, and S. K. Shrivastava, "Constructing Dependable Web Services," in Distributed Systems, LNCS 1752, pp. 277-294, 2000.
- [31]C. Ito, M. Iwaihara, and Y. Kambayashi, "Fair Exchange under Limited Trust," in Proc. of Third International Workshop on Technologies for E-Services, LNCS 2444, pp. 161-169, 2002.
- [32]C. Li and C. Pahl, "Security in the Web Services Framework," in Proc. of the 11th International Symposium on Information and Communication Technologies, pp. 481-486, 2003.
- [33]O. Marowitch and S. Kremer, "An Optimistic Non-repudiation Protocol with Transparent Trusted Third Party," in Proc. of 4th International Conference on Information Security, LNCS 2200, pp. 363-378, 2001.
- [34]O. Marowitch and S. Saeednia, "Optimistic Fair Exchange with Transparent Signature Recovery," in Proc. of 5th International Conference on Financial Cryptography, LNCS 2339, pp. 339-350, 2002.
- [35]H. Maruyama, T. Nakamura, and T. Hsieh, "Optimistic Fair Contract Signing for Web Services," in Proc. of the 2003 ACM workshop on

XML security, pp. 79-85, 2003.

[36]S. Micali, "Simple and Fast Optimistic Protocols for Fair -Electronic Exchange," in Proc. of the Twenty-second Annual Symposium on Principles of Distributed Computing, pp. 12-19, 2003.

[37]C. Mohan, "Dynamic E-business: Trends in Web Services," in Proc. of Third International Workshop on Technologies for E-Services, LNCS 2444, pp. 1-5, 2002.

[38]D. Molnar, "Signing Electronic Contracts," in Crossroads, 2000.

[39]Y. Mu, K. Q. Nguyen, and V. Varadharajan, "A Fair Electronic Cash Scheme," in Proc. of Second International Symposium on Topics in Electronic Commerce, LNCS 20-40, pp. 20-32, 2001.

[40]J. M. Park, K. P. Chong, and H. J. Siegel, "Constructing Fair-Exchange Protocols for E-commerce via Distributed Computation of RSA Signatures," in Proc. of the Twenty-second Annual Symposium on Principles of Distributed Computing, pp. 127-181, 2003.

[41]M. Payeras-Capella, J. L. Ferrer-Gomila, and L. Huguet-Rotger, "Fair Exchange to Achieve Atomicity in Payments of High Amounts Using Electronic Cash," in Proc. of Third International Workshop on Technologies for E-Services, LNCS 3043, pp. 831-840, 2004.

[42]M. Pierce, C. Youn, and G. Fox, "The Gateway Computational Web Portal: Developing Web Services for High Performance Computing," in Proc. of International Conference on Computational Science, LNCS 2329, pp. 503-512, 2002.

[43]M.-C. Pong, "EC-SignGate: Electronic Contract Signing -Gateway," in IEEE Proc. of 25th Annual International Computer Software and Applications, pp. 245-248, 2001.

[44]I. Ray and I. Ray, "An Optimistic Fair Exchange E-commerce Protocol with Automated Dispute Resolution," in Proc. of First International Conference on Electronic Commerce and Web Technologies, LNCS 1875, pp. 84-93, 2000.

[45]I. Ray and I. Ray, "An Anonymous Fair Exchange E-Commerce -Protocol," in Proc. of First International Workshop on Internet Computing and E-commerce, pp. 1790-1797, 2001.

[46]O. Shi, N. Zhang, and M. Merabti, "Signature-based approach to fair document exchange," in IEEE Proc. of Communications, pp. 21-27, 2003.

[47]H. Vogt, "Asynchronous Optimistic Fair Exchange Based on -Revocable Items," in Financial Cryptography, LNCS 2742, pp. 208-222, 2003.

[48]Wang C. F., Ge J.H., Du X. J., Qu J., Zhao T. S., and Yang S. Y., "A Multi-Party Non-Repudiation Protocol with Semi-Trusted Third Party," in Proc. of IEEE TENCON'02, pp. 188-191, 2002.

[49]Y. Watanabe and H. Imai, "Reducing the round complexity of a sealed-bid auction protocol with an off-line TTP," in Proc. of the 7th ACM Conference on Computer and Communications Security, pp. 80-86, 2000.

[50]C.-H. Wang, "Untraceable Fair Network Payment Protocol with Off-Line TTP," in ASIA -CRYPT, LNCS 2894, pp. 173-187, 2003.

[51]C.-K. Wu and V. Varadharajan, "Fair Exchange of Digital -Signature with Off-line Trusted Third Party," in Proc. of Third International Conference on Information and Communications Security, LNCS 2229, pp. 466-470, 2001.

[52]Xu Y., Tang H., and Zhang P., "An advanced text-to-speech -server system based on SOAP protocol," in Proc. of the IEEE International Conference on Acoustics, Speech, and Signal, vol. 1, pp. I-728- I-731, 2003.

[53]C. H. Yin and C. H. Wang, "An Efficient Contract Signing Protocol with Secret Protection," in Information Security Conference, pp. 119-127, 2004.

[54]J. Zhou, R. Deng, and F. Bao, "Some Remarks on a Fair -Exchange Protocol," in Proc. of Third International Workshop on Practice and Theory in Public Key Cryptosystems, LNCS 1751, pp. 46-57, 2000.

[55]"The Electronic Signature Law," Department of Commerce 0910080314, Ministry of Economic Affairs, R.O.C., 2001.

[56]DSS-Signature, [www.itl.nist.gov/fipspubs/fip186.htm](http://www.itl.nist.gov/fipspubs/fip186.htm) [57]XML Encryption, [www.w3.org/TR/xmlenc-core/](http://www.w3.org/TR/xmlenc-core/) [58]XML Signature,

[www.w3.org/Signature/](http://www.w3.org/Signature/) [59]XKMS, [www.w3.org/TR/xkms2/](http://www.w3.org/TR/xkms2/) [60]WS-Security,

[msdn.microsoft.com/library/default.asp?url=/library/en-us/dnglobsec/html/ws-security.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnglobsec/html/ws-security.asp)