以網路服務為基礎之具離線半信任第三者的公正簽約協定

吳宗潔、曹偉駿

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

摘 要

自從交易模式從傳統面對面躍上網際網路後，公平性便成為資料交換極重要考量要點。一旦要進行資料交換，便需進行資料保密、資料付費及雙方簽章等三種事項。事實上，當進行資料交換時，雙方最擔心的莫過於無法安全地取得對方的電子文件。為確保資料交換的公平性，協定需有公正第三者來解決爭端且給予雙方在簽署時公正的保證。　　線上合約簽署亦是公平電子文件交換的一種。在商業交易行為中，除了傳統簽署的方式以外，線上合約簽署亦成為較具彈性的方式。線上合約簽署應包含三方：簽署雙方及可信任的第三者。目前相關研究中，第三者大多是線上半信任第三者或離線可信任第三者。為了同時降低第三者的連線時間及提升其安全性，本研究提出了既安全又有效率的「離線半信任第三者」之公正簽約協定，其中，本研究實際提出一套具彈性的半信任第三者挑選方式，使得第三者在離線且對第三者可半信任的前提下，線上簽約仍具公正性。最後，本研究亦將所提出之協定擴展至網路服務上，使得雙方在不同平台上亦能使用本協定。

關鍵詞 : 公平電子文件交換，線上合約簽署，離線半信任第三者，網路服務

目錄

參考文獻

[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 Verifi -able Secret Sharing," in Proc. of 9th Australasian Conference on Informatio -n Security and Privacy, LNCS 3108, pp. 74-85, 2004.

[6]B. Baurn-Waidner and M. Waidner, "Round-Optimal and Abuse-Free Optimistic Mul -ti-party Contract Signing," in ICALP, LNCS 1853, pp. 524-535, 2000.

[7]B. Baurn-Waidner, "Optimistic Asynchronous Multi-party Contract Signing with R -educed Number of Rounds," in Proc. of 28th International Colloquium on Automa -ta, 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 Sig -ning 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 Auth -entication," 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 Infor -mation 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 Confer -ence 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 Theo -ry, LNCS 2761, pp. 366-382, 2003.
[14]K. Chavda, "Anatomy of a Web Service," The Journal of Computing in Small Colleg -es, pp. 124-134, 2004.
[15]D. Cohen, M. Jacovi, M. Herscovici, Y. S.Maarek, N. Meshulam, A. Soffer, an -d V. Soroka, "Leveraging web services for information discovery," Proc. of th -e IEEE International Conference on Software: Science, Technology and Engineerin -g, pp. 123-132, 2003.
[16]J. Cole and Z. Milosevic, "Extending Support for Contract in -ebXML, " 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 Tech -nical Report, vol. 6, pp. 45-58, 2001.
[18]J. L. Ferrer-Gomila , M. Payeras-Capell?, and L. Huguet-Roter, "Efficient Optim -istic N-Party Contract Signing Protocol," in Proc. of 4th International Confe -rence on Information Security, LNCS 2200, pp. 394-407, 2001.
[19]J. L. Ferrer-Gomila, A.-l. Martinez-Nadal, M. Payeras-Capell?, and L. Hugu -et-Roter, "A Juridical Validation of a Contract Signing Protocol," in Pro -c. of Third International Conference on E-Commerce and Web Technologies, LNC -S 2455, pp. 343-352, 2002.
[20]M. K. Franklin and M. K. Reiter, "Fair Exchange with a Semi-Trusted Third Par -ty, " in Proc. of the 4th ACM conference on Computer and Communication Securi -ty, pp. 1-6, 1997.
[21]J. A. Garay and C. Pomerance, "Timed Fair Exchange of Standard Signatures [Ex -tended 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. Gonz?lez-Deleito and O. Markowitch, "An Optimistic Multi-party Fair Exch -ange Protocol with Reduced Trust Requirements, "in Proc. of 4th Internationa -l 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 Works -hop on Infrastructures for Dynamic B2B Service Outsourcing, pp.1-11, 2000.
[25]A. D. Gordon and R. Pucella, "Validating a Web Serivce Security Abstraction by T -yping," in Proc. of ACM Workshop on XML Security, pp. 18-29, 2002.
[26]L. Harn, "Group-oriented threshold signature scheme and digital multisignatur -e," in IEE 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 ap -plications and its implementation using web services," in IEEE Proc. of Communic -ations, Computers and Signal, pp. 185-188, 2000.
[28]A. L. Heuer, F. Losemann, and C. Meinel, "Logging and Signing Document-Trans -fers on the WWW- A Trusted Third Party Gateway," in Proc. of the First Internati -onal Conference on Web Information Systems Engineering, vol. 1, pp. 146-152, 2000.
[29]K. Hogg, P. Chilcott, M. Nolan, and B. Srinivasn, "An -Evaluation of Web Services in the Design of a B2B Application," in Proc. of th -e 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 P -roc. of Third International Workshop on Technologies for E-Services, LNCS 2444, p -p. 161-169, 2002.
[32]C. Li and C. Pahl, "Security in the Web Services Framework," in Proc. of the 1 - t International Symposium on Information and Communication Technologies, p -p. 481-486, 2003.
[33]O. Marowitch and S. Kremer, "An Optimistic Non-repudiation Protocol with Transpar -ent Trusted Third Party," in Proc. of 4th International Conference on Informatio -n 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 Fin -ancial Cryptography, LNCS 2339, pp. 339-350, 2002.
[35]H. Maruyama, T. Nakamura, and T. Hsieh, "Optimistic Fair Contract Signing for We -b 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 Princip -les of Distributed Computing, pp. 12-19, 2003.
[37]C. Mohan, "Dynamic E-business: Trends in Web Services," in Proc. of Third Intern -ational 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 Pro -c. 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 Protoc -ols for E-commerce via Distributed Computation of RSA Signatures," in Pr -oc. of the Twenty-second Annual Symposium on Principles of Distributed Computi -ng, 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: Develop -ing Web Services for High Performance Computing," in Proc. of International Conf -erence 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 Appl -ications, pp. 245-248, 2001.
[44]I. Ray and I. Ray, "An Optimistic Fair Exchange E-commerce Protocol with Automate -d Dispute Resolution," in Proc. of First International Conference on Electron -ic 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-co -mmerce, pp. 1790-1797, 2001.
[46]O. Shi, N. Zhang, and M. Merabti, "Signature-based approach to fair document exc -hange," in IEE 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-Par -ty Non-Repudiation Protocol with Semi-Trusted Third Party," in Proc. of IEE -E TENCON'02, pp. 188-191, 2002.
[49]Y. Watanabe and H. Imai, "Reducing the round complexity of a sealed-bid auct -ion protocol with an off-line TTP," in Proc. of the 7th ACM Conference on Com -puter 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 Internat -ional 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 S -ecret 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 The -ory in Public Key Cryptosystems, LNCS 1751, pp. 46-57, 2000.
[55]"The Electronic Signature Law," Department of Commerce 0910080314, Ministry of Economic Affairs, RO.C., 2001.
[56]DSS-Signature, www.itl.nist.gov/fipspubs/fip186.htm [57]XML Encryption, www.w3.org/TR/xmlenc-core/ [58]XML Signature, www.w3.org/Signature/ [59]XKMS, www.w3.org/TR/xkms2/ [60]WS-Security, msdn.microsoft.com/library/default.asp?url=/library/en-us/dnglobsp -ec/html/ws-security.asp