公平电子合同协议的模块化设计方法*)

庞辽军　柳　毅　王育民
(西安电子科技大学综合业务网国家重点实验室　西安710071)

摘　要　电子合同协议的研究越来越受到人们的重视。本文提出一种模块化的方法来设计公平电子合同协议。通过对电子合同的签定过程进行分析，定义了一套协议模块，利用这些模块可以有效地构造公平电子合同协议。该方法不仅能降低协议设计和分析的复杂度，而且使得设计者可以根据不同的应用需求，灵活地设计公平性程度不同的电子合同协议。

关键词　电子商务，电子合同，数字签名

A Modular Method of Designing Fair Electronic Contract Protocols

PANG Liao-Jun　LIU Yi　WANG Yu-Min
(National Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071)

Abstract　Electronic contract protocol is receiving more and more attention. In the paper, a modular method of designing fair electronic contract protocols is proposed. Through the analysis of the electronic contract signing process, a set of protocol modules are defined and these protocol modules can be used to construct fair electronic contract protocols efficiently. Besides reducing the complexity of the protocol's design and analysis, this method enables designer to design an electronic contract protocol with a proper degree of fairness according to the practical application.

Keywords　Electronic commerce, Electronic contract, Digital signature

1　引言

随着 Internet 上电子商务的飞速发展，作为电子商务重要组成部分的电子合同也逐渐受到人们的重视，制定公平的电子合同协议是电子合同得以应用的关键。一般的合同签定，都需要当事人同时在场，进行同时签约，这样就避免了一方当事人通过欺诈而处于比其它当事人有利的地位。而 Internet 上的电子合同的签定不要求当事人谋面，因而并不具有这样的特点。

合同当事人甲乙通过 Internet 签定电子合同时，如果甲将自己对合同的数字签名发送给乙之后，而没有收到乙对合同的数字签名，这时甲就处于不利地位。因为，一旦发生合同纠纷，当合同内容对乙有利时，乙可以拿出甲对合同的数字签名，证明甲曾经与自己签定过这份合同。而当合同内容对乙不利时，甲拿不出乙对合同的数字签名，乙会矢口否认曾经与甲签定过这份合同。为了保障合同当事人的利益，需要制定公平的电子合同协议。对于一个电子合同协议，如果按照该协议签定电子合同，任意一个当事人不会因为其他当事人的作弊或通信线路故障而使自己处于不利地位，就称之为公平电子合同协议。

目前，密码学家对电子合同协议进行了大量研究，取得了不少成果。按照是否带有可信第三方可分为两类：带有可信第三方的协议，如文[1～3]等，和不带有可信第三方的协议，如文[4～6]等。这些协议都是为某特定的应用环境设计的，因而所需的系统资源以及所提供的公平性程度必然不同。这些协议看起来好像根本无法相互比较，尤其是对其公平性进行比较，因为还没有适合描述电子合同协议公平性程度的相关定义。本文基于文[7,8]的有关公平性定义的思想，对电子合同签定过程进行分析，给出适合描述电子合同协议公平性程度的定义。在此基础上，提出了一种模块化的方法来设计公平电子合同协议。通过对合同签定系统模型进行分析，定义一套协议模块，利用这些模块可以有效地构造公平电子合同协议。该方法具有模块化设计的优点，将复杂的协议分解成一组简单的协议模块，易于协议的设计和分析；另一个优点是可以根据不同的应用需求，灵活地设计公平性程度不同的电子合同协议。不带可信第三方的协议对计算和通信性能要求很高，且通信量过大而难以得到实际应用[2]。本文仅考虑带有可信第三方且只有两个合同当事人的情况。

为了准确地进行描述，本文用到了如下符号和约定：

TTP	可信第三方
A,B	合同当事人 A,B
$A\rightarrow B:m$	A 向 B 发送消息 m
M	合同内容
$H(X)$	对 X 求哈希值
$Sign_S(X)$	S 使用自己的签名私钥对消息 X 进行数字签名的签名结果
$E_K(),D_K()$	关于对称密钥 K 的对称加，解密算法
$e_X(),d_X()$	关于 X 的公、私钥的非对称加，解密算法

2　公平性的定义

通常，电子合同协议的公平性都是用一种很直观的方法来描述：协议完成后，合同的当事人都得到了对方对该合同的有效数字签名，或者，由于某种原因，协议没有进行完成，任何一方都不能得到对方对该合同的有效数字签名，那么，就认为该电子合同协议保证了公平性。除了这两种情况的其它情况

*)基金项目：国家973项目(G1999035803)资助课题。庞辽军　博士生，主要研究方向为电子商务中的安全理论与技术。柳　毅　博士生，主要研究方向为电子商务安全，网络安全。王育民　博士生导师，主要研究方向为信息论，密码，编码。

都是不公平的，因为某一方会得到比对方更大的有利条件。如果电子合同协议总是能够保证公平性，那么就称电子合同协议是公平的。

很明显，这个公平性概念，只能区分两种情况，公平的和非公平的，而不能刻画公平性的程度。因此，要设计具有不同程度公平性的电子合同协议，首先需要对公平性进行有强弱级别的定义。许多研究人员关于公平性的定义做了大量的研究[7~9]，其中最重要的是由 Asokan 提出的定义[7]，他提出了强公平性和弱公平性概念。Holger Vogt[8]进行了更深入的研究，他的基本思想是：由协议本身提供的公平性要比求助于协议外部仲裁所提供的公平性强。这是因为多一个参与者就会对协议的结果增加更多的不确定性，不确定性越大，协议提供的公平性就越弱。这种思想还可以进一步扩展：要求合作的参与者越少，所提供的公平性越强，因为参与者可能会欺诈而导致协议结果的不确定性变大。基于他们思想，我们给出以下适合于电子合同协议的公平性定义：

Fairness A：由协议本身提供，且不要求当事人进行合作。

Fairness B：由协议本身提供，但要求当事人进行合作。

Fairness C：需要协议外部的仲裁，但不要求当事人进行合作。

Fairness D：需要协议外部的仲裁，且要求当事人进行合作。

Fairness E：不提供任何公平性。

可以看出，Fairness A ～ Fairness D 强于 Fairness E，因为 Fairness E 本来就不具有公平性；Fairness A 和 Fairness B 强于 Fairness C 和 Fairness D，因为 Fairness A 和 Fairness B 由协议本身所提供，而 Fairness C 和 Fairness D 需要外部仲裁的协作；Fairness A 和 Fairness C 分别强于 Fairness B 和 Fairness D，因为前者不需要当事人的合作，而后者则需要当事人的合作。Fairness A 和 Fairness B 对应于 Asokan 的强公平性概念，而 Fairness C 和 Fairness D 对应于其弱公平性概念，这是因为在 Asokan 的定义中并没有强调是否需要当事人的合作。因此，可以得出结论：从 Fairness A 到 Fairness E，公平性的程度逐步降低。

3 电子合同协议的模块分析

首先给出协议的系统模型：假定协议的参与者包括当事人 A，当事人 B，以及 TTP。其中，TTP 可以是离线的(off-line)，只有在发生合同纠纷的时候参与合同的签定，也可以是在线的(on-line)，直接参与合同的签定过程；TTP 与当事人 A 和 B 之间的通信信道能够保证可靠的通信，因为 TTP 肯定会遵守协议约定；A 和 B 间的信道不需要保证可靠的通信，因为他们随时可能恶意地终止协议。在给出这个协议模型后，我们对协议过程进行分析，定义以下5个模块。在构成协议时，这五个模块的前后顺序不能变。

3.1 Module1：协商模块

在合同签定之前，当事人 A 和 B 需要对所签合同的内容条款进行协商并达到一致。除此之外，当事人双方还应视合同的重要程度协商采取何种协议，不同的协议由不同的协议模块构成，并且协商潜在的 TTP。这是协议的起始模块，也是必不可少的一个模块。

3.2 Module2：承诺模块

电子合同的签定一般是在当事人不谋面的情况下进行的，因而不能保证其同时性。如果 A 将其对合同的电子签字送给了 B，但却得不到 B 的电子签字，这样 A 就可能处于不利地位。为了保证公平性，在进行真正的签字之前，必须要求后给出签字的一方，如 B，给出承诺：如果 A 送给 B 正确的签字，那么 B 承诺一定会将自己的签字送给 A。这种承诺是可以验证的，比如通过仲裁者验证，如果 B 拒绝给出承诺，那么签约协议就会终止，这时双方都没有进行签字，可以保证公平性 Fairness A。可以任意规定当事人签字的前后顺序，显然这种顺序不会影响协议的公平性。因此，以下过程中，我们不妨都假设 A 先给出自己的签字。

3.3 Module3：签字模块

A 对合同进行签字，并将该数字签字送给 B；然后 B 验证签字的正确性，如果验证正确，那么他将自己的签字送给 A。可能产生的结果如下：

a)双方都得到对方的有效签字，

b)双方都没有得到对方的有效签字，

c)B 得到了 A 的有效签字，而 A 并没有得到 B 的有效签字。

对于 a)和 b)来说，公平性 Fairness A 得到保证，协议可以到此结束。如果出现情况 c)，必须执行后面的模块 Module4 或 Module5，或者求助于外部的仲裁者(可保证 Fairness C 或 Fairness D)，以重建公平性。

3.4 Module4：无须 TTP 进行签字验证的公平性重建模块

如果 A 持有 B 的有效承诺向 TTP 求助时，TTP 帮助 A 打开承诺，但 TTP 不需亲自计算和验证 B 的签字，可以减少 TTP 的计算负载。如果 A 在 TTP 的帮助下能够计算出 B 的有效签字，那么协议可以结束，可以保证公平性 Fairness A。如果 A 得到的不是 B 的有效签字，有两种方法解决：一种是继续执行后面的模块 Module5；另一种是求助于协议外的仲裁者以重建公平性。在大多情况下，TTP 不需要参与合同的签定过程，因为在模块 Module2，B 已经做了承诺，这将作为一个证据，使得他即使进行欺诈也得不到任何好处。

3.5 Module5：需要 TTP 进行签字验证的公平性重建模块

与 Module4不同的是，这里 TTP 需要亲自计算 B 的数字签字并进行验证。如果验证失败或者不能得到 B 的有效签名，它将恢复协议的初始状态，这样，A 和 B 谁也得不到对方的有效数字签字，从而保证了公平性 Fairness A。

4 模块功能的实现

4.1 Module1的实现

在这里，A 和 B 需要对所要签定的合同条款内容进行协商并达到一致。除此之外，他们还应视合同的重要程度协商采取何种协议，以及潜在的 TTP。这个过程可以直接表示如下。

Implementation1：

A→B:B,A,TTP,M,Protocol

B→A:A,B,TTP,M,Protocol

其中 Protocol 表示 A 和 B 所协商的协议，它决定了电子合同协议的组成模块。这个过程可以重复多次，直至当事人双方对协商内容达到一致。

4.2 Module2的实现

承诺模块实现如下。

Implementation 2：

	计算 $h=H(M)$
B:	计算对合同 M 的签字 $SB=Sign_B(h)$
	选择一个随机数 R
	用 R 对 SB 加密得 $ER(SB)$
	用 TTP 的公钥加密 R 得 $e_{TTP}(R)$
	计算签字 $SignB=Sign_B(h,\text{TTP},E_R(SB),e_{TTP}(R))$
$B\rightarrow A$:	$SignB,E_R(SB),e_{TTP}(R)$
	计算 $h=H(M)$
A:	验证签字 $SignB$
	如果验证不正确,终止协议

其中 $SignB,E_R(SB),e_{TTP}(R)$代表 B 做出的承诺。如果签字 $SignB$ 验证不通过,那么 A 可以什么也不做就终止协议,Fairness A 就可以得到保证。

当 TTP 为在线第三方时,可以用下面的实现来等价替换。

Implementation 2':

$A\rightarrow$TTP:	A,B,TTP,M,SA
$B\rightarrow$TTP:	B,A,TTP,M,SB

其中 $SA=Sign_A(h)$表示 A 对合同的数字签字。

4.3 Module3的实现

签字模块实现如下。

Implementation 3:

$A\rightarrow B$:	SA
	验证 SA 是否为 A 对 M 的有效签字
B:	如果验证不正确,终止协议
$B\rightarrow A$:	R
	用 R 解密 $ER(SB)$得到 SB
A:	验证 SB 是否为 B 对 M 的有效签字
	如果验证正确,则协议完成
	否则,执行后面的模块 Module4或 Module5或求助仲裁者以重建公平性

在这个模块中,A 首先产生对 M 的签字 $SA=Sign_A(h)$,并将其送给 B;B 通过验证后将 R 送给 A,否则什么也不用做;A 利用 R 可以解密 $E_R(SB)$得到 SB,$SB=D_R(E_R(SB))$。这样 A 和 B 都可以得到对方的签字。如果发生合同纠纷,如 B 的签字 SB 验证不通过,A 可以执行后面的模块 Module4或 Module5或求助仲裁者以重建公平性。如果 B 知道他的欺诈得不到任何好处,他就会按照协议来执行,在这种情况下,合同的签定可以在没有 TTP 参与的情况下公平的进行,从而减小了 TTP 的负载。

同样,当 TTP 为主动的参与者时,可以用下面的实现来等价替换。

Implementation 3':

TTP:	计算 $h=H(M)$
	验证 SA,SB 的正确性
	如果都正确
	TTP$\rightarrow A$: SB
	TTP$\rightarrow B$: SA
	否则,终止协议

4.4 Module4的实现

Module4用来重建公平性,实现如下。

Implementation 4:

$A\rightarrow$TTP:	$SA,M,TTP,SignB,E_R(SB),e_{TTP}(R)$
TTP:	计算 $h=H(M)$
	验证签字 SA 和 $SignB$
	如果都正确,解密 $e_{TTP}(R)$得到 R,$R=d_{TTP}(e_{TTP}(R))$
	否则,终止协议
TTP$\rightarrow B$:	SA
TTP$\rightarrow A$:	R
A:	用 R 解密 $E_R(SB)$得到 SB
	验证 SB 是否为 B 对 M 的有效签字
	如果验证正确,则协议完成
	否则,执行后面的模块 Module5或求助仲裁者以重建公平性

其中,TTP 解密得到 R,并用它和 A 的 SA 进行交换,并将 SA 送给 B。由于 A 自己解密得到 B 的签名 SB,所以,它必须验证 SB 的正确性。如果 B 送给 A 的 R 是正确的,协议可以公平地结束,否则,公平性得不到保证,A 可能得不到 B 的正确签名。这时 A 可以执行 Module5或求助仲裁者以重建公平性。

4.5 Module5的实现

在这里,TTP 需要验证 B 的签字,如果不正确,它将向双方发送一个消息 $SignTTT=Sing_{TTP}(A,B,h)$,取消本次协议的执行,双方的签字都无效。这样就可以保证公平性 $Fairness\ A$。实现如下。

Implementation 5:

$A\rightarrow$TTP:	$SA,M,\text{TTP},SignB,E_R(SB),e_{TTP}(R)$
	计算 $h=H(M)$
TTP:	验证签字 SA 和 $SignB$
	如果不全正确,终止协议,否则继续
	解密得到 R
	用 R 解密 $ER(SB)$得到 SB
	验证签字 SB
	如果正确
	TTP$\rightarrow A$: SB
	否则
	TTP$\rightarrow A$: $Sing_{TTP}(A,B,h)$
	TTP$\rightarrow B$: $Sing_{TTP}(A,B,h)$

其中 $Sign_{TTT}$将作为 A 的证据,证明其对合同签字无效,因为 B 此前可能已经得到了 A 的有效数字签字。

5 合成协议

前面讨论了电子合同协议的组成模块及其实现,下面我们通过实例来描述如何用这些协议模块来合成公平电子合同协议。我们已经知道,在构成协议时,这五个模块的顺序不能改变,每一个模块都决定了下一步如何来选取适当的模块(我们也将外部仲裁看成一个特殊的模块)。因此,我们可以从起始模块 Module1开始,按照模块间的关系,逐个选取适当的模块,直至所构成的协议能够保证公平性 Fairness A,或 Fairness B,或 Fairness C,或 Fairness D。这样我们就可以得到一个协议树,如图1所示,代表了一类电子合同协议。

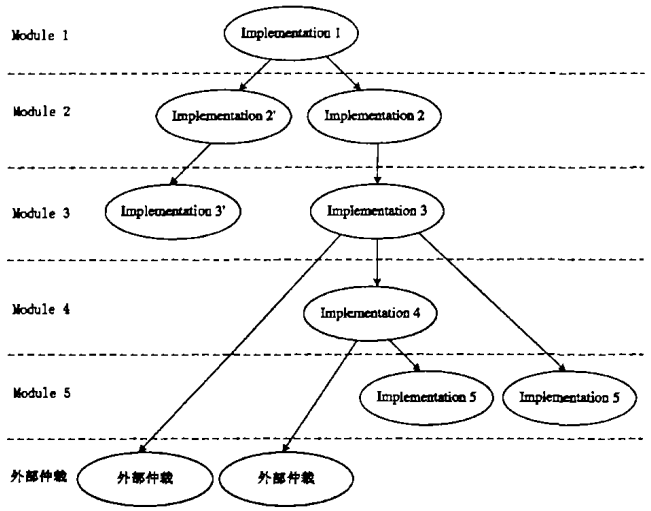

图1 带有 TTP 的电子合同协议的协议树

其中,每个中间结点和叶子结点分别代表一个模块(包括外部仲裁模块);从根结点到叶子结点的每一条路经就是一个协议。带有 TTP 的公平电子合同协议有如下5个:

Protocol1:{ Implementation 1, Implementation 2', Implementation 3'},可以保证公平性 Fairness A。

Protocol2:{ Implementation 1, Implementation 2, Implementation 3,外部仲裁},这个协议只能保证公平性 Fairness D 或 Fairness C。

Protocol3:{ Implementation 1, Implementation 2, Implementation 3, Implementation 4,外部仲裁},这个协议也只能保证公平性 Fairness D 或 Fairness C。

Protocol4:{ Implementation 1, Implementation 2, Implementation 3, Implementation 4, Implementation 5}可以在协议内部保证公平性 Fairness A。

Protocol5:{ Implementation 1, Implementation 2, Implementation 3, Implementation 5},可以在协议内部保证公平性 Fairness A。

如果将某些协议模块的实现部分稍作改变,还可以得到另外一些协议,如{ Implementation 1, Implementation 2, Implementation 4,外部仲裁}和{ Implementation 1, Implementation 2, Implementation 5 },它们都可看作 Protocol1的变种,因此不再列出。

通过比较,可以得到如下结论:比起其它的协议,Protocol1需要一个在线的 TTP 参与,但 TTP 可能成为协议的性能瓶颈,其类似于文[10]的思想;Protocol2和 Protocol3需要一个外部仲裁,公平性不高,其中 Protocol3是一个新协议;Protocol4和 Protocol5需要一个离线的 TTP,但在大多数情况下不需要 TTP 的参与就可以保证 Fairness A,是很有效的协议,其中 Protocol4实质上等同于文[3,10]的思想,Protocol5就是文[1]采用的思想。

结论 公平电子合同协议已成为电子商务领域的一个热点问题,是推动电子商务发展的一个重要因素。本文提出一种模块化的方法,对电子合同签定过程进行分析,定义了一套协议模块。利用这些协议模块可以设计公平性程度不同的电子合同协议,其中包括一些已经发表的著名协议,可见这种方法非常有效。该方法不仅具有模块化设计的优点,使得对协议的设计和分析变成对单个模块的设计和分析,降低了复杂度,而且还使得协议设计者能够根据不同的应用需求,灵活地设计公平性程度不同的电子合同协议。进一步的工作是如何对有任意多参与者的系统进行建模,定义协议模块,以构建多方公平电子合同协议,以及对其它电子商务协议设计方法的研究。

参 考 文 献

1 Bao F, Deng B H, Mao W. Efficient and practical fair exchange protocols with off-line TTP [A]. In: Proc. IEEE Symp. Security Privacy[C], 1998. 77～85

2 Pfitzmann B, Schunter M, Waidner M. Optimal efficiency of optimistic contract signing[EB/OL]. IBM Research Report RZ 2994 (# 93040), IBM Zurich Research Lab., Http://www.semper.org/direne/publ/PFSW.98PODC98.ps.gz.03/02/1998

3 Asokan N, Shoup V, Waidner M. Optimistic fair exchange of digital signatures [J]. IEEE Journal on Selected Areas In Communications, 2000, 18(4): 593～610

4 Even S, Goldreich O, Lempel A. A randomized protocol for signing contracts [J]. ACM, 1985, 28(6): 637～647

5 Goldreich O. A simple protocol for signing contracts [A]. Crypto'83[C], New York: Plenum Press, 1984. 133～136

6 Ben-Or M, Goldreich O, Micali S, Rivest R L. A fair protocol for signing contracts [J]. IEEE Transactions on IT, 1990, 36(1): 40～46

7 Asokan N, Schunter M, Waidner M. Optimistic protocols for fair exchange [A]. In: Proc. 4th ACM Conf. Computer Commun. Security [C], 1997. 6～17

8 Vogt H, Pagnia H, Grtner F C. Modular fair exchange protocols for electronic commerce [A]. In: Proc. of the 15th Annual Computer Security Applications Conf. [C], pp. 3～11

9 Tygar J D. Atomicity in electronic commerce [A]. In: Proc. of the 15th Annual ACM Symposium on Principles of Distributed Computing (PODC'96)[C], New York, 1996. 8～26

10 Bürk H, Pfitzmann A. Value exchange systems enabling security and unobservability. Computers Security, 1990, 9: 715～721