具有非泄露性的公平签约协议

樊玫玫[1,2],彭长根[1,2]
FAN Mei-mei[1,2],PENG Chang-gen[1,2]

1.贵州大学 计算机软件与理论研究所,贵阳 550025
2.贵州大学 理学院 数学系,贵阳 550025
1.Institute of Computer Science,Guizhou University,Guiyang 550025,China
2.Department of Mathematic,College of Science,Guizhou University,Guiyang 550025,China
E-mail:sci.mmfan@gzu.edu.cn

FAN Mei-mei,PENG Chang-gen.Fair contract signing protocol with non-disclosure.Computer Engineering and Applications,2009,45(5):101-103.

Abstract: A concept of non-disclosure contract signing protocol is given because those disadvantages of existed fair contract signing protocol.Based on the elements of designated-receiver signature scheme and giving an improved aggregate signature scheme,design a non-disclosure contract signing protocol.At last,an analysis of this protocol property is given.
Key words: bilinear pairings;fair exchange;contract signing protocol;non-disclosure

摘 要:针对目前已有的公平签约协议存在的不足,提出了签约协议非泄露性的概念,结合具有指定接受方签名方案的原理,改进双线性聚集签名方案,构建了一种具有非泄露性的公平签约协议,并对协议性质进行了分析。
关键词:双线性对;公平交换;签约协议;非泄露性
DOI:10.3778/j.issn.1002-8331.2009.05.029 **文章编号**:1002-8331(2009)05-0101-03 **文献标识码**:A **中图分类号**:TP309

1 引言

签约是电子商务的重要组成部分。所谓公平签约协议,就是必须保证在协议结束的时候,要么双方都能得到对方真实有效的签名,要么双方什么也得不到。

为了实现公平性,一般都使用了第三方(TTP)[1-2]。但是随着第三方的引入,也出现了一些不可避免的问题。首先是效率的问题,第三方的参与使得通信量大大增加,如何降低通信量,提高效率,成为研究的重要问题。其次是第三方的诚实性问题,由于完全可信第三方很容易成为协议的瓶颈,且使用这种第三方的协议效率极其低下,何况在网络环境下,找一个完全可信的第三方是不现实的,因此现在使用较少,而半可信第三方虽不与参与协议的某一方合谋[3],但可能向对该签约行为感兴趣的实体透露签约意图甚至签名等。

为了提高协议的效率,Boneh 等[4]提出了双线性聚集签名方案,该方案基于 co-Diffie-Hellman 假设的双线性对和椭圆曲线上的双线性映射,签名长度短、计算简便。李梦东等[5]在双线性聚集签名方案的基础上,实现了一种简单的公平签名交换方案,但是该方案在进行仲裁时,交易双方的签名将留在第三方。C.H.Wang 等在文献[6]中提出的签名方案可以保证第三方在进行仲裁时不能得到任何一方的真实签名,但是该方案是公开可验证的,这就使得在协议非正常结束的情况下,也会留下证据,使得参与协议的某一方可以向其他方"炫耀"对方同意和我签署协议,从而造成签约意图的泄露。

提出了签约协议非泄露性的概念,包含以下两个性质:(1)如果签约协议没有正常结束,协议的参与方(包括第三方)不可能留下任何"证据",通过这个"证据"可使其他方相信签约双方或其中一方的签约意图;(2)如果签约完成,并且第三方参与仲裁,那么第三方不能得到任何一方的真实有效签名,只有签约双方才能获得对方的签名。

结合具有指定接受方签名方案的原理,改进了双线性聚集签名方案,构建了一种公平的签约协议,该协议利用了双线性聚集签名的高效性,实现了签约协议的有效性、公平性、非泄露性、时限性、优化性等,具有较强的利用价值。

2 协议基础

2.1 双线性对[3]

G_1 和 G_2 是两个素数阶 p 的乘法循环群,g_1 是 G_1 的生成元,g_2 是 G_2 的生成元,$\psi:G_2\to G_1$ 是一个可计算的同构映射,另有与 G_1,G_2 同阶加法群 G_T。映射 $e:G_1\times G_2\to G_T$ 称为双线性映射,只需满足:

(1)双线性:$\forall u\in G_1$,$v\in G_2$,及 $\forall a,b\in Z$,有 $e(u^a,v^b)=e(u,v)^{ab}$;

基金项目:贵州省自然科学基金(the Natural Science Foundation of Guizhou of China under Grant No.20052107)。
作者简介:樊玫玫(1981-),女,助教,主研密码学与信息安全;彭长根(1963-),男,博士,教授,硕士生导师,主研密码学与信息安全。
收稿日期:2007-09-20 **修回日期**:2007-11-30

(2)非退化性:$e(g_1,g_2)\neq 1$;

(3)可计算性:$\forall u\in G_1, v\in G_2$,存在一个有效的方法计算$e(u,v)$。

这些性质可以导出更多的属性:对$\forall u_1,u_2\in G_1, v\in G_2$,有$e(u_1u_2,v)=e(u_1,v)e(u_2,v)$;对$\forall u,v\in G_2$,有$e(\psi(u),v)=e(\psi(v),u)$。

2.2 签名方案

签名方案由4个过程组成:Initialize,ParaExchange,Sign,Verify。

2.2.1 Initialize

u_A随机选择$x_A\in Z_p$作为私钥,计算$y_A=g^{x_A}$作为其公钥。u_B类似地计算$(x_B,y_B=g^{x_B})$作为其私/公钥对。半可信第三方T计算作$(x_T,y_T=g^{x_T})$为其私/公钥对。m为将要签约的文件,H为单向无冲突的哈希函数。

2.2.2 ParaExchange

u_B利用其私/公钥对$(x_B,y_B=g^{x_B})$计算$K=\psi(y_B)^{x_B}$,将K发送给u_A。

2.2.3 Sign

步骤 1 u_A计算$\sigma_A=h^{x_A}$,其中$h=H(m)\in G_1$;

步骤 2 u_A随机选择$r_B\in Z_p, r_T\in Z_p$,计算$\mu_B=\psi(g)^{r_B}$,$\mu_T=\psi(g)^{r_T}$,$\rho_B=K^{r_B}$,$\rho_T=\psi(y_T)^{r_T}$;

步骤 3 u_A生成指定接收方的可验证加密签名$\omega_A=\sigma_A\rho_B\rho_T$,则$(\omega_A,\mu_B,\mu_T)$构成$u_A$对消息的签名。

2.2.4 Verify

u_B验证方程$e(\omega_A,g)=e(h,y_A)e(\mu_B^{x_B},y_B)e(\mu_T,y_T)$是否成立,如果验证通过,则确认$\omega_A$为$u_A$的加密签名。

2.3 方案分析

(1)方案的正确性

$$\begin{aligned}e(\omega_A,g)&=e(h^{x_A}\cdot K^{r_B}\cdot\psi(y_T)^{r_T},g)=\\&e(h^{x_A},g)\cdot e(K^{r_B},g)\cdot e(\psi(y_T)^{r_T},g)=\\&e(h,g)^{x_A}\cdot e(\psi(y_B),g)^{x_B\cdot r_B}\cdot e(\psi(y_T),g)^{r_T}=\\&e(h,g^{x_A})\cdot e(\psi(g)^{r_B\cdot x_B},y_B)\cdot e(\psi(g)^{r_T},y_T)=\\&e(h,y_A)\cdot e(\mu_B^{x_B},y_B)\cdot e(\mu_T,y_T)\end{aligned}$$

(2)只有指定的接受方u_B才能验证u_A的签名

因为验证方程$e(\omega_A,g)=e(h,y_A)e(\mu_B^{x_B},y_B)e(\mu_T,y_T)$是否成立,只有$u_B$才知道他自己的私钥$x_B$,故其他方不能通过该方程验证签名的有效性,并且$u_B$也无法向对该签约行为感兴趣的实体透露签约意图。

(3)u_A的加密签名ω_A需要u_B和T的合作才能解密

$$\begin{aligned}\text{因为 } e((\omega_A/\mu_B^{x_B^2})/\mu_Y^{x_T},g)&=e(\omega_A,g)\cdot e(\mu_B,g)^{-x_B^2}\cdot e(\mu_T,g)^{-x_T}=\\&e(\omega_A,g)\cdot e(\mu_B^{x_B},y_B)^{-1}\cdot e(\mu_T,y_T)^{-1}=e(h,y_A)\end{aligned}$$

所以$\sigma_A=(\omega_A/\mu_B^{x_B^2})/\mu_T^{x_T}=(\omega_A/\mu_T^{x_T})/\mu_B^{x_B^2}$。即使$T$进行仲裁,对$\omega_A$解密,也不能得到$u_A$的真实签名。因此$T$也无法向对该签约行为感兴趣的实体透露签名。

3 具有非泄露性的公平签约协议

本章应用前面提出的签名方案,构建了一个公平的签约协议。该协议包括3个子协议:Exchange协议、Resolve协议和Abort协议。

3.1 Exchange协议

步骤 1 u_B首先用函数ψ和自己的私钥x_B,公钥y_B,计算$K=\psi(y_B)^{x_B}$,将K发送给u_A;

步骤 2 u_A若能收到K,则计算具有指定接收方的加密签名(ω_A,μ_B,μ_T):$h=H(m)$,$\sigma_A=h^{x_A}$,随机选择$r_B\in Z_p, r_T\in Z_p$,计算$\mu_B=\psi(g)^{r_B}$,$\mu_T=\psi(g)^{r_T}$,$\rho_B=K^{r_B}$,$\rho_T=\psi(y_T)^{r_T}$,$\omega_A=\sigma_A\rho_B\rho_T$,然后将$(\omega_A,\mu_B,\mu_T)$发送给$u_B$,否则退出协议;

步骤 3 u_B若能收到u_A的加密签名并且验证通过,则计算自己的签名$\sigma_B=h^{x_B}$并发送给u_A,否则退出协议;

步骤 4 u_A若能收到u_B的签名σ_B并且验证通过,则计算自己的签名$\sigma_A=h^{x_A}$并发送给u_B,否则执行Abort协议后退出;

步骤 5 u_B若能收到u_A的签名σ_A并且验证通过,则正常退出,签约成功完成,否则执行Resolve协议后退出。

3.2 仲裁协议

Abort协议:u_A向T提出放弃申请,T收到请求后,首先检查是否已经执行Resolve协议,若执行则将(ω_B,μ_A)发送给u_A,否则将不再接受u_B的解密请求。

Resolve协议:当u_B发送自己的真实签名σ_B给u_A后,却没有收到u_A的真实签名,此时,u_B可以向半可信第三方T申请仲裁。

步骤 1 u_B随机选择$r_A\in Z_p$,计算$\mu_A=\psi(g)^{r_A}$,$\rho_A=\psi(y_A)^{r_A}$,$\omega_B=\sigma_B\rho_A$,将可验证加密签名(ω_B,μ_A)以及在交换协议中第二步中收到的(ω_A,μ_B,μ_T)发送给T;

步骤 2 T首先检查是否执行过Abort协议,如果没有执行,则验证是否有$e(\omega_B,g)=e(h,y_B)e(\mu_A,y_A)$,验证通过则进入下一步,否则停止协议;

步骤 3 如果验证通过,T计算$\omega_A/\mu_T^{x_T}$并发送给u_B,T同样将(ω_B,μ_A)发送给u_A。

4 协议分析

结论 1 协议满足有效性。

证明 如果签约双方u_A和u_B都是诚实的,他们严格按照协议流程发送消息,只需要4次信息交互,不需要第三方的参与,签约双方均能获得对方的签名。

结论 2 协议满足公平性。

从以下四个方面来证明:

(1)u_A,u_B均是诚实的。他们严格按照协议流程发送消息,不需要第三方仲裁,则协议正常完成,u_A,u_B均能收到对方的真实有效签名。

(2)u_A诚实但u_B不诚实。在签约过程中u_A当她把自己的加密签名ω_A发送给u_B后,没有接收到u_B的有效签名σ_B。此时,u_A

可以申请执行 Abort 协议,u_B 虽然得到了 u_A 的加密签名,没有 T 的帮助,他也无法得到 u_A 的真实签名,由于 T 执行了 Abort 协议,因此 u_B 即使申请执行 Resolve 协议,T 也不会进行 ω_A 的解密,所以 u_A 和 u_B 都不会得到对方的签名。

(3)u_B 诚实但 u_A 不诚实。在签约过程中 u_B 当他把自己的真实有效签名 σ_B 发送给 u_A 后,却没有收到 u_A 的签名,此时,u_B 可以启动 Resolve 协议,向 T 申请仲裁,T 计算 $\omega_A/\mu_T^{x_T}$ 并发送给 u_B,同样将(ω_B,μ_A)发送给 u_A,从而 u_A 和 u_B 都能获得对方的签名。

(4)u_A,u_B 都不诚实。在这样的情况下,双方都不诚实,则他们什么都得不到。

由以上分析可知,u_A,u_B 要么都能获得对方签名,要么什么也得不到,所以协议满足公平性。

结论 3 协议满足非泄露性。

从以下两个方面来证明:

(1)在 Exchange 协议第三步,u_B 收到了 u_A 发送的加密签名(ω_A,μ_B,μ_T),因为验证 $e(\omega_A,g)=e(h,y_A)e(\mu_B^{x_B},y_B)e(\mu_T,y_T)$ 必须要用到 u_B 的私钥 x_B,所以只有 u_B 可以验证签名的有效性,避免了在签约非正常结束的情况下,向其他方泄露对方即将和我签约的意图。

(2)当第三方 T 参与仲裁时,因为 T 接收到 u_B 发送的(ω_B,μ_A)和(ω_A,μ_B,μ_T)都是加密签名,(ω_B,μ_A)必须要通过 u_A 的私钥 x_A 解密才能得到 u_B 真实签名 σ_B,T 计算 $\omega_A/\mu_T^{x_T}=\sigma_A\rho_B$,仍然是加密签名,必须通过 u_B 的私钥 x_B 解密才能得到 u_A 的真实签名 σ_A,因此,T 参与仲裁但不能得到任何一方的真实签名。

由以上分析可知,即使签约非正常结束,签约双方都不能得到对方的签名,但任何一方都不能向对协议感兴趣的实体泄露签约意图,并且即使第三方 T 参与仲裁,他也不能得到任何一方的真实签名,所以协议满足非泄露性。

结论 4 协议满足时限性。

证明 协议运行之前,u_A 和 u_B 商定一个时限,当对方超时,通过执行 Abort 协议或 Resolve 协议,并确信在有限的时间内能够收到 T 的回复,不必无限地等待对方,保证协议的公平进行。因此,本协议是满足时限性的。

结论 5 协议满足优化性。

证明 在本协议中,第三方工作在优化方式。在正常情况下,签约双方严格按照签名交换执行协议,没有争议发生,则第三方的不需参与协议,协议的参与者只有 u_A 和 u_B。只有在发生争议时,才需要第三方的介入来保证协议的公平性。

5 结束语

基于双线性映射的性质,结合具有指定接受方签名方案的原理,改进了双线性聚集签名方案,构建了一种公平的签约协议。该协议与现有的签约协议相比较,不仅具有复杂度较低和计算量较小的特点,而且实现了签约协议的有效性、公平性、非泄露性、时限性、优化性。

参考文献:

[1] Asokan N,Shoup V,Waidner M.Optimistic fair exchange of digital signature[J].IEEE Journal on Selected Areas in Communications,2000,18(4):593-610.

[2] Bao F,Deng R H,Mao W.Efficient and practical fair exchange protocols with off-line TTP[C]//Proceeding of 1998 IEEE Symp on Security and Privacy.Oakland:IEEE Computer Press,1998:77-85.

[3] Franklin M,Tsudik G.Secure group barter:multi-party fair exchange with semi-trusted neutral parties[C]//Proceeding of FC'98.Berlin:Springer-Verlag,1998:90-102.

[4] Boneh D,Gentry C,Lynn B,et al.Aggregate and verifiably encrypted signatures from bilinear maps[C]//Proceeding of Eurocrypt 2003.Berlin:Springer-Verlag,2003:416-432.

[5] 李梦东,杨义先,马春光,等.利用双线性聚集签名实现公平的签名交换方案[J].通信学报,2004,25(12):59-64.

[6] Wang C H,Kuo Y S.An efficient contract signing protocol using the aggregate signature scheme to protect signers' privacy and promote reliability[J].ACM SIGOPS Operating Systems Review,2000,39(4):66-79.

(上接 100 页)

保证了剩余能量多的节点优先成为簇头,并且能够使簇头在网络内均匀分布,成簇的通信开销较小;普通节点在加入簇头的过程中,优先选择转发到下一跳总功耗最小的簇头加入,减小了能量的总功耗开销,有效延长了网络生存时间。

下一步工作将引入流量工程,对网络的能量均衡消耗作进一步研究,以更有效地延长网络生存时间。

参考文献:

[1] 李建中,李金宝,石圣飞.传感器网络及其数据管理的概念、问题与进展[J].软件学报,2003,14(10):1717-1727.

[2] 孙利民.无线传感网络[M].北京:清华大学出版社,2005:1-15.

[3] Akyildiz I F,Su W,Sankarasubramaniam Y,et al.Wireless sensor networks:a survey[J].Computer Networks,2002,38(4):393-422.

[4] Chong C Y,Kumar S P.Sensor networks:Evolution,opportunities and challenges[C]//Proc IEEE,2003,91:1247-1256.

[5] EstrinD.Tutorial/Wirelesssensornetworks0partIV:sensor network protocols[EB/OL].http://nest1.ee.ucla.edu/tuto2rials/mobicom02/2002/2005211.

[6] Heinzelman W R,Kulik J,Balakrishnan H.Adaptive protocols for information dissemination in wireless sensor networks[C]//Proc of the 5th Ann Int'l Conf on Mobile Computing and Networking,2001:174-185.

[7] HeinzelmanWendiB,ChandrakasanAnanthaP,Bal-akrishnanHari.An-Application-SpecificProtocolArchitech-tureforWirelessMicrosensor-Networks[J].IEEE Trans Wireless Communication,2002,1:660-670.

[8] Younis O,Fahmy S.HEED:A hybrid,energy-efficient,distributed clustering approach for Ad-hoc sensor networks[J].IEEE Transactions on Mobile Computing,2004,3(4):366-379.