文章编号:1001 - 9081(2010)06 - 1493 - 02

基于同时生效签名的 PayWord 协议公平性改进

刘　军
(南京财经大学 电子商务系,南京 210046)
(LJ1918@ sohu. com)

摘　要:PayWord 协议出于对效率和成本的考虑,对于支付公平性方面缺乏支持。基于 PayWord 协议提出了一个新型的公平支付方案,通过在 PayWord 协议中引入同时生效签名对消费者的支付承诺提供保护,并且设计了模糊商品服务承诺对商家提供保护,从而提高了 PayWord 协议的公平性。由于方案避免使用公开密钥算法,因而在保证支付的公平性的基础上还兼顾了支付效率。

关键词:同时生效签名;微支付;PayWord 协议;公平性
中图分类号: TP309. 3　　**文献标志码**:A

Fairness improvement of PayWord protocol based on concurrent signature

LIU Jun
(*Department of E-commerce, Nanjing University of Finance and Economics, Nanjing Jiangsu* 210046, *China*)

Abstract: In consideration of efficiency and cost, PayWord protocol lacks fairness. A new solution based on PayWord protocol was proposed to protect the payment commitment of consumer and the service commitment of provider with concurrent signature, so as to enhance the fairness of PayWord protocol. The analysis results show that the new solution can better meet the requirements of micro-payment for efficiency and fairness.

Key words: concurrent signature; micro-payment; PayWord protocol; fairness

0　引言

PayWord[1]作为一种基于信用的微支付协议,应用 Hash 链技术较好地解决了微支付中的效率和成本控制的问题,但是支付的有效性和不可否认性方面考虑不多,对于支付活动中发生的纠纷没有给出相应的解决机制[2]。有关学者对 PayWord 进行改进以提高其公平性。文献[2]提出把一个 Hash 值分成两部分,作为对一个单位信息商品的支付。先支付前一半,得到一个单位信息商品后,再支付另一半,这样交易双方无论谁先中断协议运行都得不到好处。文献[3]根据分次支付的思想把用于一次性数字签名的双哈希链方案引入移动支付协议。文献[4]提出了一种预付费方案,通过银行在消费者消费前验证其支付指令的合法性并进行授权,在支付结束时删除对应于该消费者的银行授权信息,从而有效地防止了消费者进行重复花费。

本文在保证支付系统的高效和低成本的前提下,将同时生效签名[5-6]技术引入到 PayWord 支付系统,通过消费者和商家分别对支付信息和商品信息进行同时生效签名,从而有效地解决 PayWord 系统的交易公平性缺失的问题。

1　同时生效签名

同时生效签名是通过签名双方分别对各自的消息进行模糊签名,然后交换模糊签名,此时任何第三方不能把模糊签名与签名者的身份对应起来,即签名是无效的;只有签名发起人公布了一个"重要信息",此时才能将签名与签名者的身份对应起来,也即这两个模糊签名同时生效了。同时生效签名算法由 4 部分组成,具体如下。

1.1　初始化算法

首先选择两个大素数 p、q(其中 $q(q \mid p-1)$),g 是群 $\mathbf{Z}_q^*$ 的一个 q 阶生成元,生成两个 Hash 函数 H_1,H_2:$\{0,1\}^* \rightarrow \mathbf{Z}_q$。在生成算法完成之后,假设参与协议的双方为 Alice 和 Bob,Alice 得到其私钥 $X_A \in \mathbf{Z}_q$ 和公钥 $y_A = g^{x_A} (\bmod p)$,Bob 则得到私钥 $X_B \in \mathbf{Z}_q$ 和公钥 $y_B = g^{x_B} (\bmod p)$。

1.2　模糊签名算法

模糊签名算法的输入参数包括 y_i、x_i、t、$f(y_i$ 是对方公钥,x_i 是己方私钥,t 为随机数且 $t \in \mathbf{Z}_q$,$f = H_1(k)$,k 为随机比特串),算法输出结果为模糊签名。举例如下:

Alice 要对消息 M_A 签名,那么首先选择一个随机比特串 k,计算:

$f = H_1(k)$

$h = H_2((g^t y_B^f (\bmod p)) \| M_A)$; $\|$ 表示比特串联

$h_A = (h - f) \bmod q$

$S_A = (t - h_A x_A) \bmod q$

得到 Alice 对消息 M_A 的模糊签名 $\sigma_A = (S_A, h_A, f, y_A, y_B, M_A)$。

1.3　模糊签名验证算法

模糊签名验证算法的输入参数是一个模糊签名,输出是"TRUE"或"FALSE"。假设 Bob 收到 Alice 传来的签名 $\sigma_A = (S_A, h_A, f, y_A, y_B, M_A)$,首先检查 h_A 与 f 是否相等,如果相等,则中止协议并输出"错误";若不等,则验证等式:

$$h_A + f \equiv (H_2((g_1^{S_A} y_A^{h_A} y_B^f \bmod p) \| M_A)) \bmod q$$

若成立,输出"TRUE";反之,则输出"FALSE"。

在证实 Alice 的模糊签名是正确的之后,Bob 直接利用 Alice 发送给他的 f 生成消息 M_B 的模糊签名 $\sigma_B = (S_B, h_B, f, y_B, y_A, M_B)$,将其传给 Alice。Alice 收到 σ_B 后,如果证实模糊签名的正确性,则将 k 告知 Bob 或将 k 公开,至此 Alice 和 Bob 完成对消息 M_A 和 M_B 的交换并各自得到了对方对其所发送消息的模糊签名。

收稿日期:2009 - 12 - 29;**修回日期**:2010 - 03 - 01。
基金项目:国家自然科学基金资助项目(70572024);江苏省高校自然科学基础研究项目(06KJB120032)。
作者简介:刘军(1971 -),男,河南洛阳人,副教授,博士,主要研究方向:电子商务。

1.4 身份验证算法

身份验证算法的输入为(k,σ)，输出为模糊签名 σ 的签名人的身份。验证者(通常是独立的第三方)得到 k 和模糊签名 $\sigma=(S,a_1,a_2,y_B,y_A,M)$ 后(其中 S 为 S_A 或 S_B，a_1、a_2 分别为 h_i 或 f，$i\in\{A\mid B\}$)，首先验证等式：

$$\alpha_1+\alpha_2\equiv H_2(g^S y_A^{a_1} y_B^{a_2}(\bmod p)\parallel M)(\bmod q) \quad (1)$$

如果等式(1)成立，则分别将 a_1、a_2 和 $H_1(k)$ 的值比较，如果 $a_1=H_1(k)$，那么 Bob 是该签名的生成者，Alice 是接收者；反之，则可以确定 Alice 是该签名的生成者，Bob 是接收者。

如果不成立，交换参数继续验证等式(判断方法同上)：

$$\alpha_1+\alpha_2\equiv H_2(g^S y_A^{a_2} y_B^{a_1}(\bmod p)\parallel M)(\bmod q)$$

由此可以看到，一旦关键数 k 被公布，则两个签名同时生效，并且在生效之前被签名的消息内容均经过了接收方的审阅和认可。因此采用同时生效签名算法，可以很好地解决电子支付协议的公平性问题。

2 公平微支付协议描述

系统的参与者包括：消费者(C)、商家(V)、经纪人(B)。本模型协议包括 4 个子协议：离线开户子协议、服务协商认证子协议、支付子协议和结算子协议。

2.1 符号定义

协议中使用的参数说明：

Z 为实体的标志，$Z\in\{C,B,V\}$；SK_Z 为实体 Z 的私钥；PK_Z 为实体 Z 是公钥；CSK_Z 为实体 Z 的同时签名私钥；CPK_Z 为实体 Z 的同时签名公钥；$\{M\}_{PK_Z}$ 为消息 M 使用 PK_Z 加密的密文；$Sign_{SK_B}(M)$ 为消息 M 及其数字签名；$A\rightarrow B:\{X\}$ 表示 A 向 B 发送消息 X。

2.2 协议流程

1) 离线开户子协议。

消费者 C 选择一个匿名标识 ID_C，发送给经纪人 B 进行开户，B 将 ID_C 与 C 的真实身份信息进行绑定。B 运行同时生效签名初始化算法，生成 CSK_C 和 CPK_C，将 CSK_C、SK_C 以及 PayWord 证书 $C_C=Sign_{SK_B}(ID_B,ID_C,PK_C,CPK_C,H_1,H_2,A_C,E_C)$ 发送给 C，A_C 为 C 地址或邮箱，E_C 为 C 证书有效期。同样，V 开户时也发送匿名标识 ID_V，B 亦将 ID_V 与其真实身份进行绑定，并生成同时签名公钥 CSK_V 以及证书 $C_V=Sign_{SK_B}(ID_B,ID_V,CPK_V,H_1,H_2,A_V,E_V)$，$A_V$ 为商家地址。

2) 服务协商认证子协议。

在这一阶段，消费者 C 生成订单信息 O_I，向商家 V 发送模糊支付承诺，商家 V 经过验证后发送模糊商品服务承诺。具体如下：

① 消费者 C 生成 PayWord 支付承诺的模糊签名。消费者 C 选取随机数 W_n，根据消费金额生成 PayWord 链：$W_0,W_1,\cdots,W_n$，其中 $W_i=h(W_{i+1})$。消费者 C 作为同时签名的发起者在关键数集合中选择一个随机数 k，计算 $f=H_2(k)$，生成支付承诺 $M_C=\{ID_V,C_C,W_0,O_I\}$ 的模糊签名 $\sigma_C=CSign(CPK_C,CPK_V,CSK_C,f,M_C)$，发送给 V。

$$C\rightarrow V:\{M_C,CPK_C,\sigma_C,f\}_{PK_V}$$

② 商户 V 发送模糊商品服务承诺。商户 V 收到消费者 C 的模糊签名后，验证模糊签名 σ_C。如果验证通过，则商户构造消息 $M_V=H_1(PRODUCT_{ID})$，$PRODUCT_{ID}$ 为消费者要购买的商品或服务的唯一标志，然后对 M_V 进行模糊签名得到 $\sigma_V=CSign(CPK_V,CPK_C,CSK_V,f,M_V)$，即模糊商品服务承诺，发送回复消息给消费者 U。

$$V\rightarrow C:\{ID_C,C_V,M_V,CPK_V,\sigma_V,f\}_{PK_C}$$

3) 支付子协议。

消费者 C 收到来自商户 V 的模糊签名 σ_V 之后，执行模糊签名验证算法，如果验证通过则将关键数 k 和 PayWord 支付对发送给商户 V，而商户在收到消息后，提供商品。

$$C\rightarrow V:\{k,w_i,i\}$$

$$V\rightarrow C:\{PRODUCT\}$$

4) 结算子协议。

商家在结算时将消费者 C 的支付承诺 Commitment 和其最后的 PayWord 支付对(w_i,i)提交给经纪人 B，经纪人 B 验证支付对的有效性后，进行相应的结算操作。如果消费者 C 与商家 V 关于交易发生纠纷，可以由其中任意一方向 B 提交 k 及相关同时生效签名，由 B 进行仲裁。

3 协议分析

3.1 安全性分析

对于交易中的敏感信息如 σ_C 和 σ_V，采用加密密钥进行保护，因而敏感信息在传输和处理过程中是安全的，攻击者无法对模糊签名进行伪造和篡改。消费者 C 的身份使用随机标识 ID_C 代替，有效地保护了消费者的真实身份。

3.2 公平性分析

在协议的服务协商认证子阶段，在消费者公布关键数 k 之前，任意方如果终止协议，对于消费者 C 虽然将支付承诺发送给了商家 V，但是由于没有公布关键数 k 而其签名没有生效，因此不会有任何损失，对于商家 V 由于消费者 C 没有公开关键数 k 自然也不会发送商品。当消费者 C 将关键数 k 公开后，如果商家 V 没有提供产品而直接向经纪人 B 提交 W_i 而获取资金，则消费者 C 可以向经纪人 B 投诉并提供商家 V 签发的包括 $PRODUCT_{ID}$ 的模糊商品服务承诺。如果消费者 C 恶意透支，则商家 V 可以提供消费者 C 签名的模糊支付承诺和关键数 k 作为证据要求消费者支付。

3.3 效率分析

在消费者 C 方面，相对于原有的 PayWord 支付方案，改进后的协议对计算负荷的影响主要在服务协商认证阶段中对支付承诺的处理，主要变化表现为：1) 将原有协议的一次对称密钥签名改为模糊签名，两者相比计算量变化不大；2) 添加了一次对模糊签名的验证运算，该计算以 Hash 计算为主，计算强度低。因此就消费者而言新协议的效率几乎与 PayWord 协议一样。

对于经纪人 B 增加了同时签名初始化运算，但是由于该部分计算为离线进行，因此可以接受。对于商家 V 增加了一次同时签名验证运算和一次同时签名运算，由于商家 V 采用的计算平台通常为高性能计算平台，因此对于商家 V 也是可以接受的。

4 结语

本文通过在 PayWord 协议中引入同时生效签名技术对其支付公平性进行改进，主要工作包括：1) 在离线开户子协议中，设计了包含同时生效签名私钥的 PayWord 支付证书。由于消费者和商家的同时生效签名私钥是在经纪人 B 处离线生成进行的，因此对消费者 C 和商家 V 不会产生影响。2) 在服务协商认证子协议和支付子协议，引入了支付承诺模糊签名和模糊商品服务承诺，由于模糊签名的生成与验证以 Hash 计算为主，因此增加的计算负荷十分有限，这对于计算能力相对较弱的消费者 C 有着非常重要的现实意义。3) 结算子协议，在结算阶段如果消费者 C 与商家 V 关于交易发生纠纷，可以由任

(下转第 1675 页)

相似度最大的原则。

4) 在每一个类 C_j 中,顺序选取类中一个句子 $S_i \in C_j$,计算用其取代现在的 Medoids 所增加的类中相似度总和 E_i,选取最大的 E_i,确定新的句子作为新的 Medoids,这样 Medoids 就改变了。

5) 接下来转到第3) 步,循环计算直到 K 个 Medoids 固定下来,这样所有的句子就被分配到 K 个类中。

6) 经过改进型 K-Medoids 算法后,所有的句子被归入类中。在每一类中,根据下面公式为每一个句子打分,这个打分衡量句子出现在摘要中的重要性。

$$Score(S_i) = \sum_{S_j \in C_K - S_i} sim(S_i, S_j)$$

其中:$Score(S_i)$ 衡量的是每一个句子 S_i 在类 C_j 中与其他同类中的句子的相似度之和。

7) 从每一类中选出相似度之和最高的句子,即 max $Score(S_i)$,组成最后的摘要。

2　实验及结果分析

实验数据选用文档理解会议 DUC2002 上任务 2 的数据集[6]。该数据集包含 60 个文档集合,其中每个文档集中有 10 篇用于摘要的文章,还有 4 篇用于评测的理想摘要(手工生成)。分别做 200 词和 50 词的摘要,然后计算摘要准确率的平均值。

本文选用 ROUGE 作为评测工具。ROUGE 现已成为摘要抽取评测技术的通用标准,被广泛应用于 DUC 的摘要评测任务中。ROUGE 准则基于摘要中 n 元词(n-gram)的共现信息来评价摘要,是一种面向 n 元词召回率的评价方法。ROUGE 准则由一系列的评价方法组成,包括 *ROUGE*-1、*ROUGE*-2、*ROUGE*-3、*ROUGE*-4,以及 *ROUGE*-*L*、*ROUGE*-*W* 等(其中 *ROUGE*-1 至 *ROUGE*-4 分别基于 1 元词到 4 元词)。*ROUGE*-*N* 的计算公式如下:

$$ROUGE\text{-}N = \frac{\sum_{S \in \{\text{ReferenceSummaries}\}} \sum_{n\text{-gram} \in S} Count_{\text{match}}(n\text{-gram})}{\sum_{S \in \{\text{ReferenceSummaries}\}} \sum_{n\text{-gram} \in S} Count(n\text{-gram})}$$

其中:n-gram 表示 n 元词,{ReferenceSummaries} 表示参考摘要,$Count_{\text{match}}(n\text{-gram})$ 表示系统摘要和参考摘要中同时出现 n-gram 的个数,$Count(n\text{-gram})$ 则表示参考摘要中出现的 n-gram 个数。

将基于向量空间模型(Vector Space Model, VSM)的摘要系统,以及基于知网和 K-Medoids 模型(Hownet based K-Medoids,HKM)的摘要系统与本文提出的单文档摘要 HMKM 分别在 200 词和 50 词的摘要上做性能比较。

表 1　在 200 词摘要上性能比较

方法	*ROUGE*-1	*ROUGE*-2	*ROUGE*-*W*
HMKM	0.352	0.069	0.106
VSM	0.214	0.043	0.078
HKM	0.318	0.061	0.102

表 2　在 50 词摘要上性能比较

方法	*ROUGE*-1	*ROUGE*-2	*ROUGE*-*W*
HMKM	0.368	0.078	0.129
VSM	0.285	0.061	0.103
HKM	0.342	0.062	0.113

从表 1 和表 2 中可以看出,本文提出的 HMKM 在性能上要好于 VSM 和 HKM。其中 VSM 性能最差,因为基于空间向量的模型只考虑了统计的信息,而 HMKM 系统和 HKM 系统都运用了知网,从语义的角度计算,效果得到了明显提高。新算法在改进了原来的 K-Medoids 算法后性能得到进一步提高。总的来说,基于语义的单文档摘要系统提高了单文档摘要的准确性。

3　结语

基于语义的单文档摘要算法是在从语义推理角度上研究自然语言处理的一个探索,适当的运用语义信息有助于更好地理解文本的意思。通过 DUC2002 的实验数据测试可以看出,本文的方法在 200 词和 50 词的自动摘要均超过了 VSM 和 HKM 方法,这说明适当地语义推理能更好地提高摘要的准确性。今后将继续研究语义层面上句子相似度计算的方法,并运用知网在语义方面进行进一步的研究和探索。

参考文献:

[1] MANI I. Automatic summarization [M]. Amsterdam: John Benjamins Publishing Company, 2001.

[2] 张燕,赵广社,郭培胜. 一种英文自动摘要方法[J]. 计算机工程与应用,2009,45(7):135 - 137.

[3] GONG Y, LIU X. Generic text summarization using relevance measure and latent semantic analysis [C]// Proceedings of the 24th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval. New York: ACM Press, 2001: 19 - 25.

[4] 董振东,董强. 知网[EB/OL]. [2008 - 10 - 10]. http://www.keenage.com.

[5] 张滨. 中文文档分类技术研究[D]. 武汉:武汉大学,2004.

[6] LIN C Y, HOVY E. Automatic evaluation of summaries using n-gram co-occurrence statistics [C]// Proceedings of the 2003 Conference of the North American Chapter of the Association for Computational Linguistics on Human Language Technology. Edmonton, Canada: Association for Computational Linguistics, 2003: 71 - 78.

(上接第 1494 页)

意一方向经纪人 B 提交 k 及相关同时生效签名,由 B 进行仲裁。总之,通过在 PayWord 协议中引入同时生效签名既提高了支付协议的公平性,又避免引入大负荷的计算,因此非常适用于弱计算能力下的商务环境,例如移动商务场合。

参考文献:

[1] RIVEST R, SHAMIR A. PayWord and MicroMint: Two simple micropayment schemes [EB/OL]. [1996 - 05 - 07]. http://theory.lcs.mit.edu/~rivest/RivestShamir-mpay.ps.

[2] 姬东耀,王育民. 基于 PayWord 的小额电子支付协议[J]. 电子学报,2002,30(2):301 - 303.

[3] 曹华,金瓯,贺建飚. 基于双哈希链的公平移动支付协议的设计和分析[J]. 计算机测量与控制,2007,15(1):117 - 119.

[4] 谭运猛,付雄,郎为民. 基于多 PayWord 链的新型高效微支付方案[J]. 华中科技大学学报,2004,32(5):29 - 31.

[5] CHEN L, KUDLA C, PATERSON K G. Concurrent signatures [C]// Advances in Cryptology-EUROCRYPT 2004. Berlin: Springer, 2004: 287 - 305.

[6] 肖海燕,张敏情,杨晓元,等. 一种基于同时生效签名的公平交易协议[J]. 计算机工程与应用,2009,45(23):206 - 207,210.