(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 110941858 B
(45)授权公告日 2021.10.26

(21)申请号 201911336219.8

(22)申请日 2019.12.23

(65)同一申请的已公布的文献号
申请公布号 CN 110941858 A

(43)申请公布日 2020.03.31

(73)专利权人 上海源庐加佳信息科技有限公司
地址 200120 上海市浦东新区双桥路1255号2006室

(72)发明人 杨炜祖 李从恺 顾军

(74)专利代理机构 北京恒泰铭睿知识产权代理有限公司 11642
代理人 周成金

(51)Int.Cl.
G06F 21/62(2013.01)
G06F 21/60(2013.01)

(56)对比文件
US 2014059345 A1,2014.02.27
CN 106203169 A,2016.12.07
CN 1933629 A,2007.03.21
CN 109615376 A,2019.04.12
陈渊 等.基于零知识证明的安全认证方案.《计算机与数字工程》.2015,第43卷(第7期),第1279-1282页.

审查员 周瑞瑞

权利要求书1页 说明书4页

(54)发明名称

一种基于零知识证明的个人网络消费信息保护方法

(57)摘要

本发明涉及个人网络消费信息保护技术领域,且公开了一种基于零知识证明的个人网络消费信息保护方法,包括:在客户数据库存储个人网络消费信息之前,在二进制域F_2^m上随机选定一条椭圆曲线$E_p(a,b)$,在该椭圆曲线$E_p(a,b)$上随机选取一点R作为基点,并根据消费用户A在弹出的交互式通信对话框中随机选择的在二进制域F_2^m上的私有密钥k自动生成在二进制域F_2^m上的公开密钥K;在客户数据库内存储的个人网络消费信息被访问之前,通过验证$SR=R_1+bK$成立与否,来验证访问用户B的身份是否合法。本发明解决了目前存储在购物网站数据库内的个人消费信息,存在被非法访问、以及存在被非法获取的技术问题。

CN 110941858 B

1.一种基于零知识证明的个人网络消费信息保护方法,其特征在于,包括以下步骤:

步骤一:在客户数据库存储个人网络消费信息之前,个人网络消费信息保护系统的个人信息加密验证模块自动执行以下操作:

(1)锁定客户个人信息输入页面;

(2)在二进制域F_2^m上随机选定一条椭圆曲线$E_p(a,b)$,在该椭圆曲线$E_p(a,b)$上随机选取一点R作为基点;

(3)在客户个人信息输入页面之上弹出与用户A进行交互式通信的对话框,该交互式通信对话框具备无痕迹通信功能,即对话框内的所有交互通信内容均没有任何备份记录;

(4)个人信息加密验证模块提示消费用户A在弹出的交互式通信对话框中随机选择一个在二进制域F_2^m上的私有密钥k,该私有密钥k为唯一合法的证明密钥,且该私有密钥k仅为消费用户A单独拥有,即个人信息加密验证模块并不知晓私有密钥k;

(5)个人信息加密验证模块在交互式通信对话框中自动生成在二进制域F_2^m上的公开密钥K,且使K=kR成立,交互式通信对话框同步消失;

步骤二:在客户数据库内存储的个人网络消费信息被访问之前,个人网络消费信息保护系统的个人信息加密验证模块自动执行以下操作:

(1)锁定客户数据库内存储的客户个人信息;

(2)在客户数据库的访问页面之上弹出与访问用户B进行交互式通信的对话框,该交互式通信对话框具备无痕迹通信功能,即对话框内的所有交互通信内容均没有任何备份记录;

(3)提示访问用户B在弹出的交互式通信对话框中随机选取一个在二进制域F_2^m上的r,并计算$R_1=rR$,使R_1在椭圆曲线$E_p(a,b)$上;

(4)在交互式通信对话框中自动生成在二进制域F_2^m上的随机数b;

(5)提示访问用户B计算S=r+bk,并将所计算的数据输入到交互式通信对话框中;

步骤三:个人信息加密验证模块验证访问用户B的身份,如果$SR=R_1+bK$成立,则说明验证通过,即访问用户B身份合法,但是访问用户B仅可以访问客户数据库内与其合法访问身份相匹配的个人信息;

其中,所述个人网络消费信息保护系统的个人信息加密验证模块将椭圆曲线$E_p(a,b)$、基点R、公开密钥K传送给客户数据库;

所述客户数据库执行以下操作:(1)将消费用户A输入的明文数据形式的个人信息编码到$E_p(a,b)$上的一点M,并生成一个在二进制域F_2^m上的随机数s,且使M=sR成立;(2)计算消费用户A输入的个人信息的加密密文C=M+sK;

所述访问用户B接到加密密文C之后,根据唯一合法的证明密钥,即私有密钥k,计算C=M+sK=sR+sK=sR+skR=(1+k)sR,解密得到加密密文C的明文数据形式的个人信息。

一种基于零知识证明的个人网络消费信息保护方法

技术领域

[0001] 本发明涉及个人网络消费信息保护技术领域，具体为一种基于零知识证明的个人网络消费信息保护方法。

背景技术

[0002] 大数据背景下，消费者的个人信息对商家越来越重要，但个人信息的安全性常常也是消费者网络购物时最担心的问题之一，在网上交易时，消费者在网站注册、填写订单、支付等过程中需要输入自己的个人信息(姓名、联系电话、电子邮箱、家庭地址、银行账号)，如果网络技术水平不足，客户数据库安全等级不高，或者商家不注重对消费者信息的保护，甚至为了一己私利出卖消费者的个人信息，都将造成个人信息的泄露、盗用或滥用。

[0003] 此外，消费者在网上浏览网页的过程中，会留下一些浏览痕迹，不良商家可以利用大数据技术对这些痕迹进行跟踪，从而了解消费者的需求、消费情况。如果消费者以前浏览过的网页被嵌入了跟踪代码，那么下次再次访问时，容易遭受第三方跟踪，导致个人信息泄露。

发明内容

[0004] (一)解决的技术问题

[0005] 针对现有技术的不足，本发明提供了一种基于零知识证明的个人网络消费信息保护方法，解决了目前存储在购物网站数据库内的个人消费信息，存在被非法访问、以及存在被非法获取的技术问题。

[0006] (二)技术方案

[0007] 为实现上述目的，本发明提供如下技术方案：

[0008] 一种基于零知识证明的个人网络消费信息保护方法，包括以下步骤：

[0009] 步骤一：在客户数据库存储个人网络消费信息之前，个人网络消费信息保护系统的个人信息加密验证模块自动执行以下操作：

[0010] (1)锁定客户个人信息输入页面；

[0011] (2)在二进制域F_2^m上随机选定一条椭圆曲线$E_p(a,b)$，在该椭圆曲线$E_p(a,b)$上随机选取一点R作为基点；

[0012] (3)在客户个人信息输入页面之上弹出与用户A进行交互式通信的对话框，该交互式通信对话框具备无痕迹通信功能，即对话框内的所有交互通信内容均没有任何备份记录；

[0013] (4)个人信息加密验证模块提示消费用户A在弹出的交互式通信对话框中随机选择一个在二进制域F_2^m上的私有密钥k，该私有密钥k为唯一合法的证明密钥，且该私有密钥k仅为消费用户A单独拥有，即个人信息加密验证模块并不知晓私有密钥k；

[0014] (5)个人信息加密验证模块在交互式通信对话框中自动生成在二进制域F_2^m上的公开密钥K，且使K=kR成立，交互式通信对话框同步消失；

[0015] 步骤二:在客户数据库内存储的个人网络消费信息被访问之前,个人网络消费信息保护系统的个人信息加密验证模块自动执行以下操作:

[0016] (1)锁定客户数据库内存储的客户个人信息;

[0017] (2)在客户数据库的访问页面之上弹出与访问用户B进行交互式通信的对话框,该交互式通信对话框具备无痕迹通信功能,即对话框内的所有交互通信内容均没有任何备份记录;

[0018] (3)提示访问用户B在弹出的交互式通信对话框中随机选取一个在二进制域F_2^m上的r,并计算$R_1=rR$,使R_1在椭圆曲线$E_p(a,b)$上;

[0019] (4)在交互式通信对话框中自动生成在二进制域F_2^m上的随机数b;

[0020] (5)提示访问用户B计算S=r+bk,并将所计算的数据输入到交互式通信对话框中;

[0021] 步骤三:个人信息加密验证模块验证访问用户B的身份,如果$SR=R_1+bK$成立,则说明验证通过,即访问用户B身份合法,但是访问用户B仅可以访问客户数据库内与其合法访问身份相匹配的个人信息。

[0022] 进一步的,所述个人网络消费信息保护系统的个人信息加密验证模块将椭圆曲线$E_p(a,b)$、基点R、公开密钥K传送给客户数据库。

[0023] 进一步的,所述客户数据库执行以下操作:

[0024] (1)将消费用户A输入的明文数据形式的个人信息编码到$E_p(a,b)$上的一点M,并生成一个在二进制域F_2^m上的随机数s,且使M=sR成立;

[0025] (2)计算消费用户A输入的个人信息的加密密文C=M+sK。

[0026] 进一步的,所述访问用户B接到加密密文C之后,根据唯一合法的证明密钥,即私有密钥k,计算C=M+sK=sR+sK=sR+skR=(1+k)sR,解密得到加密密文C的明文数据形式的个人信息。

[0027] (三)有益的技术效果

[0028] 与现有技术相比,本发明具备以下有益的技术效果:

[0029] 1.本发明采用“在客户数据库存储个人网络消费信息之前,在二进制域F_2^m上随机选定一条椭圆曲线$E_p(a,b)$,在该椭圆曲线$E_p(a,b)$上随机选取一点R作为基点,并根据消费用户A在弹出的交互式通信对话框中随机选择的在二进制域F_2^m上的私有密钥k自动生成在二进制域F_2^m上的公开密钥K”的技术手段,与“在客户数据库内存储的个人网络消费信息被访问之前,通过验证$SR=R_1+bK$成立与否,来验证访问用户B的身份是否合法”的技术手段,即采用基于零知识证明的信息访问验证机制,不仅使拥有私有密钥k的访问用户B在不泄露任何有关私有密钥k信息的前提下,就可以证明自己是个合法用户,而且使没有拥有私有密钥k的访问用户B,无法证明自己是个合法用户,进而无法访问客户数据库内存储的个人网络消费信息,从而解决了目前存储在购物网站数据库内的个人消费信息,存在被非法访问的技术问题。

[0030] 2.本发明采用“客户数据库将消费用户A输入的明文数据形式的个人信息编码到$E_p(a,b)$上的一点M,并生成一个在二进制域F_2^m上的随机数s,且使M=sR成立,计算消费用户A输入的个人信息的加密密文C=M+sK,访问用户B根据唯一合法的证明密钥,即私有密钥k,计算C=M+sK=sR+sK=sR+skR=(1+k)sR,解密得到加密密文C的明文数据形式的个人信息”的技术手段,即采用基于椭圆曲线密码的加解密方式,不仅使拥有私有密钥k的访问用户B可以

解密密文C,获取与其合法访问身份相匹配的明文数据形式的个人信息,而且使没有拥有私有密钥k的访问用户B,无法解密密文C,进而无法获取明文数据形式的个人信息,从而解决了目前存储在购物网站数据库内的个人消费信息,存在被非法获取的技术问题。

具体实施方式

[0031] 一种基于零知识证明的个人网络消费信息保护方法,包括以下步骤:

[0032] 步骤一:当消费用户A在网络消费平台的客户个人信息输入页面上准备输入个人信息时,客户数据库进入存储信息工作状态,在客户数据库进行存储个人网络消费信息之前,个人网络消费信息保护系统的个人信息加密验证模块自动执行以下操作:

[0033] (1)对客户个人信息输入页面进行锁定处理,使消费用户A无法在网络消费平台的客户个人信息输入页面上输入个人信息;

[0034] (2)在二进制域F_2^m上随机选定一条椭圆曲线$E_p(a,b)$,在该椭圆曲线$E_p(a,b)$上随机选取一点R作为基点;

[0035] (3)在客户个人信息输入页面之上弹出与用户A进行交互式通信的对话框,该交互式通信对话框具备无痕迹通信功能,即对话框内的所有交互通信内容均没有任何备份记录;

[0036] (4)个人信息加密验证模块提示消费用户A在弹出的交互式通信对话框中随机选择一个在二进制域F_2^m上的私有密钥k,该私有密钥k为唯一合法的证明密钥,且该私有密钥k仅为消费用户A单独拥有,即个人信息加密验证模块并不知晓私有密钥k;

[0037] (5)个人信息加密验证模块在交互式通信对话框中自动生成在二进制域F_2^m上的公开密钥K,且使K=kR成立,交互式通信对话框同步消失;

[0038] 其中,个人网络消费信息保护系统包括个人信息加密验证模块,该个人信息加密验证模块用于对输入到客户数据库的个人网络消费信息进行加密保护,同时用于验证访问用户的身份是否合法;

[0039] 步骤二:个人网络消费信息保护系统的个人信息加密验证模块将椭圆曲线$E_p(a,b)$、基点R、公开密钥K传送给客户数据库,同时对客户个人信息输入页面进行解锁处理,之后,消费用户A在网络消费平台的客户个人信息输入页面上输入个人信息;

[0040] 步骤三:客户数据库在接收到椭圆曲线$E_p(a,b)$、基点R、公开密钥K等信息之后,执行以下操作:

[0041] (1)将消费用户A输入的明文数据形式的个人信息编码到$E_p(a,b)$上的一点M,并生成一个在二进制域F_2^m上的随机数s,且使M=sR成立;

[0042] (2)计算消费用户A输入的个人信息的加密密文C=M+sK;

[0043] 步骤四:当访问用户B向客户数据库发送请求访问个人网络消费信息时,客户数据库进入接受数据访问工作状态,在客户数据库内存储的个人网络消费信息被访问之前,个人网络消费信息保护系统的个人信息加密验证模块自动执行以下操作:

[0044] (1)对客户数据库内存储的客户个人信息进行锁定处理;

[0045] (2)在客户数据库的访问页面之上弹出与访问用户B进行交互式通信的对话框,该交互式通信对话框具备无痕迹通信功能,即对话框内的所有交互通信内容均没有任何备份记录;

[0046] (3)提示访问用户B在弹出的交互式通信对话框中随机选取一个在二进制域F_2^m上的r,个人信息加密验证模块计算$R_1=rR$,并且使R_1在椭圆曲线$E_p(a,b)$上;

[0047] (4)在交互式通信对话框中自动生成在二进制域F_2^m上的随机数b;

[0048] (5)提示访问用户B计算S=r+bk,并将所计算的数据输入到交互式通信对话框中;

[0049] 步骤五:客户数据库验证访问用户B的身份,如果$SR=R_1+bK$成立,则说明验证通过,即访问用户B身份合法,但是访问用户B仅可以访问客户数据库内与其合法访问身份相匹配的加密密文C,与此同时客户数据库仅将加密密文C传送给访问用户B;

[0050] 步骤六:访问用户B接到加密密文C之后,根据唯一合法的证明密钥,即私有密钥k,计算$C=M+sK=sR+sK=sR+skR=(1+k)sR$,解密得到加密密文C的明文数据形式的个人信息。