基于 ECDLP 的高效承诺方案

赖 欣,喻秀英,何大可
LAI Xin,YU Xiu-ying,HE Da-ke

西南交通大学 信息安全与国家网格计算实验室,成都 610031
Information Security and National Computing Grid Laboratory(IS&NC),Southwest Jiaotong University,Chengdu 610031,China
E-mail:lxswjtu@163.cm

LAI Xin,YU Xiu-ying,HE Da-ke.Efficient commitment scheme based on ECDLP.Computer Engineering and Applications, 2008,44(3):136-138.

Abstract: Commitment scheme is not only the fundamental primitive in cryptographic protocols but also be used directly in the remote electronic voting,electronic voting,and electronic auction occasions.In this paper,based on the elliptic curve discrete logarithm problem a commitment scheme is proposed.In this scheme the information exchange among participants is not needed. Through the implementation of commitments phase and a decommitment phase a commitment of message can be achieved from the sender.A detailed security analysis of the scheme is given.Based on elliptic curve discrete logarithm problem the scheme is hiding and binding,also has the advantage in efficiency and communication bandwidth.

Key words: cryptographic protocols;commitment scheme;ECDLP;hiding property;binding property

摘 要:承诺方案不仅是许多密码协议中的核心部分,同时也被直接使用于远程电子投票、电子选举、电子拍卖等场合。提出一个基于椭圆曲线离散对数困难问题的承诺方案,该方案不需要在参与方之间进行信息交互,并通过执行一轮承诺阶段和公开承诺阶段就可以实现发送方对某一消息的承诺。对该方案进行详尽地分析,指出基于椭圆曲线离散对数困难问题该方案具有消息隐藏性和消息绑定性,且在执行效率和通信带宽上具有优势。

关键词:密码协议;承诺方案;椭圆曲线离散对数问题;隐藏性;绑定性
文章编号:1002-8331(2008)03-0136-03 **文献标识码**:A **中图分类号**:TN918.2

1 引言

承诺方案是许多密码协议中的基本成分,它通常作为零知识证明协议、多方安全计算、电子合同签署协议等的子协议,另外也被直接使用于远程电子投票、电子选举、电子拍卖等场合。承诺方案是一个两阶段协议,要求在第一阶段承诺方 S 通过对某一消息 x 进行承诺计算后,将该消息的承诺发送给接收方 R。一段时间后在第二阶段 S 需要通过公开承诺来证实他知道的消息 x。执行过程中承诺方案应当满足两个基本特性:(1)消息隐藏性,即在公开承诺前接收方 R 不能获得消息 x 的任何信息;(2)绑定性,即具有欺骗性的承诺者不能改变承诺,消息 x 的承诺必须和其公开承诺一一对应。

自 Blum1982 年提出基于大数分解困难性的比特承诺方案后[1],大量承诺方案被提出[2-5],这些承诺方案都建立在整数因子分解问题或有限域离散对数问题之上。1998 年由 Kobliz 和 Miller 各自提出了椭圆曲线公钥密码体制 ECC,该密码体制的安全性基于椭圆曲线离散对数困难问题(ECDLP),具有很强的安全性,且在密钥长度和执行效率上具有显著优势,因此得到广泛关注。本文根据 Crescenzo 等提出的完善隐藏承诺方案范例[6],利用椭圆曲线上的离散对数问题假设提出一个高效、非交互承诺方案,并对该方案相关特性了分析,该方案具有消息隐藏性、绑定性,非交互性等特点。且基于椭圆曲线离散对数问题的计算优势该承诺方案具有较高执行效率。

2 准备工作

2.1 承诺方案的形式化定义

在公开参数模型下,给出承诺方案,及其消息隐藏性、绑定性的形式化定义。

定义 1 承诺方案(TTP,S,R)是一个在概率多项式时间内,在承诺方 S 与验证方 R 之间进行的两阶段协议。在概率多项式时间算法 TTP 返回公开参数 σ 后开始执行。

第一阶段(承诺阶段):S 通过计算(com,dec)←$Comit(m,\sigma)$得到消息 m 的承诺与公开承诺对,并将承诺 com 发送给 R。

第二阶段(公开承诺阶段):S 向 R 展示消息 m 的公开承诺 dec。并由 R 检查公开承诺 $m/\perp \leftarrow Open(com,dec)$,如果无效,$R$ 输出一个停止符号,并拒绝接受消息 m;如果有效,R 接受消息 m。

定义 2 承诺方案的消息隐藏性:对某承诺方案,如果在给定攻击者 Adversary 公开参数 σ 和消息 m 的承诺 com 后,攻击者输出一个消息 m^*。如 $m^*=m$ 的概率是可以忽略的,即 $Prob[m^*=m|m^* \leftarrow Adversary(com,\sigma)]=\varepsilon$($\varepsilon$ 为可忽略量),那么该承诺方案

基金项目:国家部委科技重点实验室基金。

作者简介:赖欣,女,博士研究生,主要研究方向为密码学、信息安全技术;喻秀英,女,讲师,博士研究生,主要研究方向信息安全;何大可,教授,博士生导师,主要研究方向:密码学、信息安全。

具有消息隐藏性。

定义 3 绑定性:对某承诺方案,若(com,dec)是消息 m 的有效承诺和公开承诺,如果存在消息 m 的另一对有效承诺和公开承诺(com^*,dec^*),满足 $com^*=com$ 并且 $dec^*\neq dec$ 的概率是可以忽略的,即:$Prob[com^*=com \wedge (dec^*\neq dec)|(com,dec)\leftarrow Comit(m),(com^*,dec^*)\leftarrow Comit(m)]=\varepsilon$($\varepsilon$ 为可忽略量),那么该承诺方案具有绑定性。

2.2 完善隐藏非交互承诺方案范例

Crescenzo 等在文献[6]给出一个完善隐藏非交互串承诺方案范例,并对进行了安全性证明。范例简述如下,一个承诺方案的承诺可由三部分组成 $com=<A,B,Tag>$。其中第一部分 A 是对参数 r_1、r_2 的承诺,而参数 r_1、r_2 是对第二部分 B 进行认证时计算消息认证码所需的参数;第二部分 B 是对原始消息 m 的承诺计算,该承诺计算利用的参数必须依赖于第一部分的信息 A;第三部分 $Tag=MAC_{r_1,r_2}(B)$,即利用消息认证码函数 $MAC_{r_1,r_2}(\cdot)$ 对第二部分 B 进行认证。

2.3 椭圆曲线离散对数问题

椭圆曲线 $E(F_q)$上的点构造的群是现代密码学中非常重要的一类群,它与有限域上的乘法群 F_q^* 有很多相似之处,它们都是 Abel 群,且根据 Hasse 定理它们具有大致相同的元素个数。但对一个特定的 q 具有多个不同的椭圆曲线 $E(F_q)$,相比乘法群而言,椭圆曲线提供了更丰富的 Abel 群资源[7]。椭圆曲线离散对数问题 ECDLP 定义如下,假设 P 是 $E(F_q)$上的一个点,假设 Q 是 $E(F_q)$上为 P 的倍数点,即存在整数 $x>0$,使得 $Q=xP$,已知 P 和 Q 确定出 x 在计算上是不可行的,即 $Prob[x\in F_q|(P,Q)\in E(F_q)\wedge(Q=xP)]=\varepsilon_{ECDLP}$($\varepsilon_{ECDLP}$ 为可忽略量)。

3 基于 ECDLP 的高效承诺方案

本文根据 Crescenzo 承诺方案范例,以及椭圆曲线离散对数问题提出一个高效的非交互承诺方案。该方案分为三个执行步骤,详细描述如下:

建立公开参数阶段:选取一个大素数 p(比如广义梅森素数)。定义一个在有限域 F_p 上的曲线 $E_{(a,b)}:y^2=x^3+ax+b$。为抗击目前已有所有攻击,应满足椭圆曲线上有理点个数 $\#E_{(a,b)}$具有大素因子 n,满足 $n\geqslant 2^{160}$ 且 $n>4\sqrt{p}$,且 $E_{(a,b)}$是非超奇异的。在曲线上随机选取的三个非无穷远点 P_1、P_2、P_3,点 P_i 的坐标表示(x_{P_i},y_{P_i})。选择一个抗碰撞密码学杂凑函数 $H:F_p\|F_p\rightarrow F_p$ 和一个消息认证码函数 $MAC:\{0,1\}^*\rightarrow F_p$。对所有系统用户公开参数 $\sigma=<F_p,E_{(a,b)},P_1,P_2,P_3,H,MAC>$。

承诺阶段:承诺方 S 利用公开参数 σ 对原始消息 $m\in F_q$ 进行承诺计算。

(1)S 从 F_q 中均匀随机地选择四个随机数:$r_1,r_2,r_3,r_4\in_R F_p$;

(2)S 计算 A:$A\leftarrow r_1P_1+r_2P_2+r_3P_3$,为椭圆曲线上一点,坐标表示为$(x_A,y_A)$;

(3)S 计算 α:$\alpha\leftarrow H(x_A\|y_A)$,$\alpha\in F_p$;

(4)S 计算 B:$B\leftarrow m(\alpha P_1+P_2)+r_4P_3$,为椭圆曲线上一点,坐标表示为$(x_B,y_B)$;

(5)S 计算 Tag:$Tag\leftarrow MAC_{r_1,r_2}(x_B\|y_B)$,$Tag\in F_p$。

S 令 $com=<A,B,Tag>$作为对 m 的承诺发送给验证方 R,令 $dec=<m,r_1,r_2,r_3,r_4>$为 m 的公开承诺自己保留。

公开承诺阶段:承诺方 S 向验证方 R 展示公开承诺,验证方 R 验证。

(1)S 发送公开承诺给验证方 R:$dec=<m,r_1,r_2,r_3,r_4>$;

(2)R 验证:$A\overset{?}{=}r_1P_1+r_2P_2+r_3P_3$、$B\overset{?}{=}m(H(x_A\|y_A)P_1+P_2)+r_4P_3$、$Tag\overset{?}{=}MAC_{r_1,r_2}(x_B\|y_B)$。如果其中一项不成立则输出停止符 $\perp$ 并拒绝接受消息 m;若三项均验证成功,那么接受消息 m。

4 方案的性能分析

本方案的非交互性是显而易见的,整个承诺方案执行过程中,在承诺阶段发送方 S 发送计算的消息承诺、在公开承诺阶段发送公开承诺信息,与验证方 R 之间不存在相互之间的应答过程。下文对承诺方案的隐藏性和绑定性进行分析。

4.1 隐藏性分析

基于椭圆曲线离散对数问题困难的假设,对承诺方案的消息隐藏性和绑定性进行分析。消息 m 的保密性依赖于承诺值中的第二部分 $B=m\alpha P_1+mP_2+r_4P_3$,该式中 P_1、P_2、P_3 都是椭圆曲线的生成元,都可以独立构成椭圆曲线上点的循环群,且 r_1、r_2、r_3、r_4 是从 F_q 中均匀随机选择的,因此一组 r_1、r_2、r_3 唯一确定一个 A 点。攻击者获得消息 m 的承诺 $com=<A,B,Tag>$进行攻击分析时可以假定一个椭圆曲线的生成元 P,满足 $P_1=k_1P$、$P_2=k_2P$、$P_3=k_3P$,那么 $B=m\alpha P_1+mP_2+r_4P_3=(m\alpha k_1+mk_2+r_4k_3)P$。这样攻击者求解消息 m 将转化为已知 B、P 需首先求出$(m\alpha k_1+mk_2+r_4k_3)$,这是一个典型的求解椭圆曲线离散对数问题,即 $Prob[(m\alpha k_1+mk_2+r_4k_3)|(B,P)\wedge(B=(m\alpha k_1+mk_2+r_4k_3)P)]=\varepsilon_{ECDLP}$。而攻击者确定以下关系 $P_1=k_1P$、$P_2=k_2P$、$P_3=k_3P$,也将涉及求解椭圆曲线离散对数问题。因此攻击者成功恢复消息的概率等价于求解椭圆曲线离散对数问题概率,即 $Prob[m^*=m|m^*\leftarrow Adversary(com,\sigma)]=\varepsilon\approx\varepsilon_{ECDLP}$ 在离散对数问题困难假设下是一个可以忽略的量。

4.2 绑定性分析

根据绑定特性的定义,要求在公开承诺阶段接收者 R 可以确信公开信息中的 m 是承诺者 S 在第一阶段进行承诺计算的值,即强调消息要与消息承诺者存在对应关系。在本方案中这一对应关系由承诺值中第二部分 B 和第三部分 $Tag=MAC_{r_1,r_2}(x_B\|y_B)$来保证,且基于椭圆曲线中群点计算特性,给定一个椭圆曲线上的点 P 和一个整数 x,将唯一确定椭圆曲线上的点 Q,满足 $Q=xP$,即 $Prob[Q=Q^*|Q=xP,Q^*=x^*P,P\in E(F_q),x\neq x^*]=0$。绑定性证明过程中,假设存在另一组公开承诺$dec^*=<m,r_1^*,r_2^*,r_3^*,r_4^*>$计算得点 B^*,满足 $B^*=B$ 即 $m(\alpha P_1+P_2)+r_4P_3=m(\alpha^*P_1+P_2)+r_4^*P_3$,仍然不妨假设存在一个椭圆曲线的生成元 P,满足 $P_1=k_1P$、$P_2=k_2P$、$P_3=k_3P$,那么存在$(m\alpha k_1+mk_2+r_4k_3)P=(m\alpha^*k_1+mk_2+r_4^*k_3)P$。在椭圆曲线上点唯一确定条件下,要使等式成立,必须满足 $m\alpha k_1+r_4k_3=m\alpha^*k_1+r_4^*k_3$,即在 $k_1\neq 0,k_2\neq 0,m\neq 0$ 时只有$(\alpha=\alpha^*)\wedge(r_4=r_4^*)$时 $B^*=B$ 才成立。

假定攻击者获得最好的攻击条件,即他公布的公开承诺 $dec^*=<m,r_1^*,r_2^*,r_3^*,r_4^*>$中的 r_4^* 等于原来真实公开承诺 $dec=<m,r_1,r_2,r_3,r_4>$中的 r_4,他只需要考虑满足 $\alpha=\alpha^*$。然而只要$<r_1,r_2,r_3>$其中之一不等于$<r_1^*,r_2^*,r_3^*>$中对应值,那么 $r_1P_1+r_2P_2+r_3P_3\neq r_1^*P_1+r_2^*P_2+r_3^*P_3$,即$(x_A^*,y_A^*)\neq(x_A^*,y_A^*)$。因此攻击者在最好条件下攻击绑定特性成功的概率将转化为在$(x_A^*,y_A^*)\neq(x_A^*,y_A^*)$的条件下 $H(x_A\|y_A)=H(x_A^*\|y_A^*)$的概率。由定义已知 H 是抗碰

撞密码学杂凑函数,因此 $Prob[H(x_A \| y_A)=H(x_A^* \| y_A^*) \wedge (x_A,y_A)\neq(x_A^*,y_A^*)] \leqslant \varepsilon_{collision}$。综上考虑本方案的绑定特性可知 $Prob[(com^*=com) \wedge (dec^* \neq dec) \wedge (com,dec) \leftarrow Comit(m), (com^*,dec^*) \leftarrow Comit(m)] = \varepsilon \leqslant \varepsilon_{collision}$ 是可以忽略的量。第三部分 $Tag=MAC_{r_1,r_2}(x_B \| y_B)$ 计算,相当于利用承诺者已知的"私钥"$<r_1,r_2>$ 对第二部分计算值进行了签名,这样保证了数据在传输过程中的真实性。

4.3 执行效率分析

分析承诺方案执行过程可知,在承诺计算和公开承诺验证阶段各需要进行椭圆曲线上的数乘运算,点加运算、抗碰撞杂凑函数运算以及 *MAC* 函数运算。抗碰撞杂凑函数运算和 *MAC* 函数运算的执行效率与具体所选用的算法有关。相比以整数分解或离散对数为数学基础的承诺方案而言,在同等安全条件下,椭圆曲线上进行的模运算只需要更小的模数,这就使得基于 ECDLP 的承诺方案在计算效率上较原来基于整数因子分解问题或有限域离散对数问题提出的承诺方案有更大的改进。Certicom 公司曾对椭圆曲线密码体制和基于整数因子分解的密码体制进行了对比,在实现相同安全强度下,以 40 MHz 的时钟频率实现 155 bit 规模的椭圆曲线运算,每秒钟能完成 40 000 次,其速度比 1 024 bit 规模的整数因子分解问题和离散对数问题快近 10 倍。另一方面,本方案中承诺的第一部分 *A* 计算与实时消息无关,完全可以实现预计算。这就使得承诺阶段中接近一半椭圆曲线运算可以离线进行。承诺计算与验证过程中不存在承诺方和接收方之间的信息交互。在这对实时性要求很高的场合具有现实意义。

本文提出的承诺方案中,承诺 $com=<A,B,Tag>$ 包含了两个椭圆曲线上的点,以及由 *MAC* 函数计算得到的基域 F_p 上的数 *Tag*,所占用的通信带宽 $|com| \approx 5|F_p|$($|F_p|$ 为表示一个有限域 F_p 中元素所使用的带宽)。而在公开承诺阶段 $dec=<m,r_1,r_2,r_3,r_4>$,所占用的通信带宽 $|dec| \approx 5|F_p|$。由此可见本方案的通信带宽取决于基域中元素所占用带宽。由上述实例已知取得相同的安全强度,椭圆曲线离散对数问题所需要的基域规模更小,可以极大减小通信中带宽开销。可见基于 ECDLP 的承诺方案对功耗、存储空间和成本受限的环境是一个较好的选择。

5 结语

承诺方案在许多密码协议以及实际的应用场合都有重要的价值。本文讨论了承诺方案及其消息隐藏性、绑定性的形式性化定义。在椭圆曲线离散对数困难问题假设下给出了一个高效的承诺方案,经证明本方案不仅具有消息隐藏性和绑定性,还在执行效率和占用通信带宽上具有优势。本方案可作为高效密码协议中的子协议,同时也可以应用于远程电子投票、电子选举、电子拍卖等场合。(收稿日期:2007 年 7 月)

参考文献:

[1] Blum M.Coin flipping by telephone:a protocol for solving impossible problems[C]//Proc of 24th IEEE Computers Conference.[S.l.]:ACM Press,1983:23-27.

[2] Goldwasser S,Micali S,Rivest R.A digital signature scheme secure against adaptive chosen-message attacks[J].SIAM Journal of Computing,1988,17(2):281-308.

[3] Bleumer G,Pfitzman B,Waidner M.A remark on a signature scheme where forgery can be proved[C]//LNCS 473:Proc of Eurocrypto'90.Berlin:Springer-Verlag,1990:441-445.

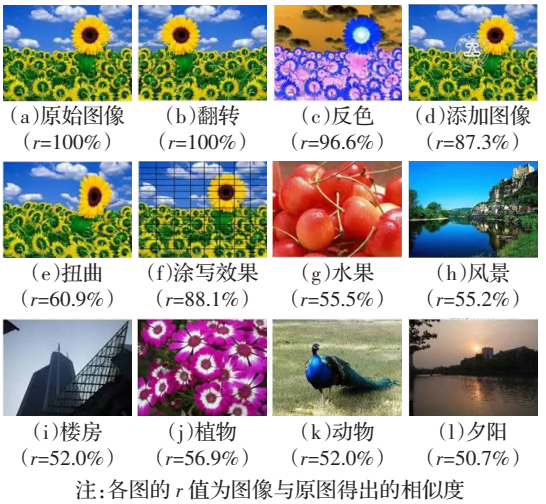
[4] Chaum D,van Heijst E,Pfitzmann B.Cryptographiclly strong undeniable signature,unconditionally secure for signer[C]//LNCS 576:Proc of Crypto'91.Berlin:Springer-Verlag,1992:470-484.

[5] Damgard I B.Practical and provably secure release of a secret and exchange of signature[C]//LNCS 765:Proc EuroCrypto'93.Berlin:Springer-Verlage,1994:200-217.

[6] Crescenzo G D,Ishai Y,Ostrovsky R.Non-interactive and non-malleable commitment[C]//Proc 30th Annual ACM Symposium on Theory of Computing,1998:141-150.

[7] 周玉洁,冯登国.公开密钥密码算法及其快速实现[M].北京:国防工业出版社,2002.

(上接 121 页)



(a)原始图像 (r=100%) (b)翻转 (r=100%) (c)反色 (r=96.6%) (d)添加图像 (r=87.3%)

(e)扭曲 (r=60.9%) (f)涂写效果 (r=88.1%) (g)水果 (r=55.5%) (h)风景 (r=55.2%)

(i)楼房 (r=52.0%) (j)植物 (r=56.9%) (k)动物 (r=52.0%) (l)夕阳 (r=50.7%)

注:各图的 r 值为图像与原图得出的相似度

图 3 实验结果分析

印等保护方法所存在的问题。因此,在完全不影响原图画质的前提下,本文提出了一种利用图像的特征值对图像进行保护的方法,该方法不需要对原始图像进行修改,可对原图提取特征数据,能有效抵抗一些常见的图像修改方式,最终以相似度百分比的形式给出图像相似度,从而确定图像是否被盗用。实验仿真结果证明了该方案的有效性。由于该方法对原始图像的保护不会对原始图像产生损伤,具有很高的实际应用价值。(收稿日期:2007 年 8 月)

参考文献:

[1] Gordy J D.Performance evaluation of digital watermarking algorithm[D].Canada:University of Calgar,2000.

[2] Barni M,Bartolini F,De Rosa A.Capacity of full frame DCT image watermarks[J].IEEE Transactions on A Piva-Image Processing,2000.

[3] 陈俊文,杨树堂,倪佑生,等.基于 DCT 变换的图像类水印认证算法[J].上海交通大学学报,2006,40(1):41-45.

[4] 闫晓涛,刘宏伟.基于 DWT 和 DCT 域的二值图像数字水印算法[J].计算机与数字工程,2007,3:5-7.

[5] Piva A,Barni M,Bartolini F,et al.DCT-based watermark recovering without resorting to the uncorrupted original[C]//Proc International Conference on Image Processing,1997,1:520-523.

[6] 杨福生,洪波.独立分量分析的原理与应用[M].北京:清华大学出版社,2006.

[7] Fridich J.Combing low frequency and spectrum watermarking[C]//SPIE International Symposium on Optical Science,Engineering and Instrumentation.San Diego:[s.n.],1998:203-212.