DOI:10.16749/j.cnki.jecjtu.2015.04.019

文章编号:1005-0523(2015)04-0110-07

一种基于无双线性对映射的无证书代理签密方案

查文刚

(华东交通大学现代教育技术中心,江西 南昌 330013)

摘要:无证书签密是公钥密码体制的一个重要应用,与传统的先签名后加密相比,其计算量和通信成本都要低。借鉴国密SM2标准签名方案设计技巧,提出了一个新的基于无双线性对映射的无证书代理签密方案。随后对协议的正确性、安全性、参数选择和效率进行分析,在适应性选择消息和存在第二类攻击者给出了随机预言机模型下的安全性证明。新方案基于离散对数问题困难假设,由于避免了使用双线性对,因此性能良好;通过与其它方案的对比,计算开销明显低于其它签密方案,分析表明新方案具备较高安全性和效率。

关键词:数字签名;双线性映射;随机预言机模型;代理签密;无双线性对映射

中图分类号:TP309 **文献标志码**:A

Al Riyami和Paterson 2003首次提出无证书密码体制[1],给出了无证书公钥密码系统的概念同时并提出了首个无证书签名方案。这种签名方案的部分秘钥是由用户和KGC共同协议产生,解决了基于身份的密码系统中的密钥托管问题,提高了效率。1997年Zheng首次提出的签密[2]的概念,能同时完成签名和加密,在计算量和成本上,远远低于传统的先签名后加密的密码体制缺点是不满足公开验证性。Bao针对公开验证性分别给出了改进的可公开验证的签密方案[3], Shin指出文献[3]的方案不满足语义安全,并给出了改进方案[4]。随后不少研究者在此基础上提出了不少高效的签密方案及其变种[5-9]。

代理签密是由Gamage于1999年首次提出,Gamage等人提出的代理签密方案,实现了一个代理签密人代替原始签密人进行签密,但此方案没对安全性进行证明[10]。2004年,Li提出了一种基于身份的代理签密方案[11],然而,Wang指出文献[10]的方案不具有不可伪造性和前向安全性,并给出了改进的方案[12]。无证书代理签密可以结合无证书签密和代理签名的特点,不存在密钥托管问题,而且不需要证书来认证公钥,安全性高,效率高。所以,无证书代理签密在实际工程中中应用更广泛。2009年,王会歌提出的高效的无证书可公开验证签密方案,安全性存在问题,方案不能抵抗公钥替换攻击,而且运用了双线性对运算,计算效率低[12]。2010年,Yu提出了一种基于椭圆曲线上的无证书代理签密方案,这个方案简单可行,但是安全性不高[14]。本文在文献[15]的基础上提出了一种基于无双线性对映射的无证书代理签密方案,整个方案只运用了加法和乘法运算,大大的减少了算法的计算量和通信成本,易于在移动通讯的敏感数据交换技术中应用。

1 预备知识

定义1 (离散对数困难问题假设)设G是阶为q的一个加群, P为G的生成元,对于任意的$a\in Z_q^*$,已知aP, P,计算a是离散对数问题,在概率多项式时间(PPT)内,对于任意攻击算法A,在解决DLP困难问

收稿日期:2015-02-27

作者简介:查文刚(1983—),男,助理工程师,研究方向为信息安全,计算机技术。

题的优势 $Adv_{DLP}(\mathrm{A})=\Pr[\mathrm{A}(uP,P)=u \mid u\in \boldsymbol{Z}_q^*]$ 是可忽略的。

2　基于无双线性对映射的无证书代理签密方案

2.1　参数选取和密钥生成

KGC利用有效算法 $L(1^k)$，生成参数 (G,q,P)，其中 G 为具有素数阶 q 的循环群（以下不加说明默认为椭圆曲线群）。选择安全hash函数：$H_1:\{0,1\}^*\times G\times G\times G\rightarrow \boldsymbol{Z}_q^*$，$H_2:G\times\rightarrow \boldsymbol{Z}_q^*$，$H_3:\{0,1\}^*\times G\rightarrow \boldsymbol{Z}_q^*$，$H_4:\{0,1\}^*\times\{0,1\}^*\times G\times G\times G\times G\rightarrow \boldsymbol{Z}_q^*$，$H_5:\{0,1\}^*\times\{0,1\}^*\times\{0,1\}^*\times G\times G\rightarrow \boldsymbol{Z}_q^*$。

KGC选择 x_{kgc} 作为其主私钥，计算其主公钥 $y_{kgc}=x_{kgc}P$。

假定用户 A_i 的身份为 ID_i（可以是用户私人相关有效信息），A_i 随机选择一个 $x_i\in Z_q^*$ 作为自己的长期私钥（以下简称私钥），计算 $y_i=x_iP$ 作为其长期公钥（以下简称公钥）。将 y_i 发给密钥生成中心KGC。A_i 将 (ID_i,y_i) 发送给KGC申请另一部分密钥。

KGC秘密选择随机数 $u_i,v_i\in \boldsymbol{Z}_q^*$，计算：$U_i=u_iP$，$V_i=v_iP$，$\bar{x}_i=u_i+v_i+x_{kgc}H_1(ID_i,U_i,V_i,y_i)$，$\bar{y}_i=\bar{x}_iP$。

$\bar{x}_i$ 作为 A_i 的另一部分私钥（以下简称部分私钥），将 $(\bar{y}_i,U_i,V_i)$ 公开作为 A_i 的另一部分公钥（以下简称部分私钥）。KGC将 $\bar{x}_i$ 通过安全可靠渠道发送给用户 A_i。于是用户 A_i 完整私钥为 $(x_i,\bar{x}_i)$，完整公钥为 $(y_i,\bar{y}_i,U_i,V_i)$。

2.2　委托过程

假设Alice对Bob进行委托，Alice的身份为 ID_A，完整私钥为 $(x_A,\bar{x}_A)$，完整公钥为 $(y_A,\bar{y}_A,U_A,V_A)$，Bob的身份为 ID_B，完整私钥为 $(x_B,\bar{x}_B)$，完整公钥为 $(y_B,\bar{y}_B,U_B,V_B)$。

1）Alice随机选取秘密值 $k_1,k_2\in \boldsymbol{Z}_q^*$，计算 $K_1=k_1P$，$K_2=k_2P$，并计算：$e_1=H_2(K_1,K_2)$，$e_2=H_2(K_2,K_1)$，$w=e_1x_A+e_2\bar{x}_A+k$，$W=wP$ 将 K_1、K_2 和 W 发送给Bob，w 通过安全信道发送给Bob。

2）Bob计算 $e_1'=H_2(K_1,K_2)$，$e_2'=H_2(K_2,K_1)$，验证等式 $W=wP=e_1'y_A+e_2'\bar{y}_A+K_1+K_2$，若不成立，拒绝Alice的委托，若成立，则计算代理签名密钥 $x=w+e_1'x_B+e_2'\bar{x}_B$，公开其对应公钥 $y=xP$。

2.3　代理签密的生成过程

代理签密的参与者为Bob与Cock，Bob的身份为 ID_B，完整私钥为 $(x_B,\bar{x}_B)$，完整公钥为 $(y_B,\bar{y}_B,U_B,V_B)$，代理签名密钥 x，对应公钥 y。Cock的身份为 ID_C，私钥为 $(x_C,\bar{x}_C)$，公钥为 $(y_C,\bar{y}_C,U_C,V_C)$。需传递数据信息为 m，数据信息加密采用安全对称加密算法（记加密过程为 E_{key}，解密过程为 D_{key}）。Bob随机选择对称密钥 $key\in \boldsymbol{Z}_q^*$，加密后得到密文 $s=E_{key}(m)$，计算 $M=H_3(m)$。

1）随机选取 $t\in \boldsymbol{Z}_q^*$，计算 $T=tP$，$K=key\oplus H_5(ID_A,ID_B,ID_C,(x+t)(y_C+\bar{y}_C),T)$。

2）计算 $s=t(x+h)^{-1}$，$h=H_4(ID_B,ID_C,K,M,T,K_1+K_2)$。

将 $S=(h,s,T,K,M,K_1,K_2)$ 作为签密数据发送给Cock。

2.4　代理签密的签名验证和解密过程

Cock验证等式 $h\stackrel{?}{=}H_4(ID_B,ID_C,K,M,s(y+hP),K_1+K_2)$，若不成立则接受拒绝签名，否则接受签名，并计算对称密钥 $key=K\oplus H_5(ID_A,ID_B,ID_C,(x_C+\bar{x}_C)(y+T),T)$，并通过 $m=D_{key}(s)$ 得到明文 m。

2.5　代理签名的注销过程

Alice向签名用户广播一条消息，声明任何含有 (K_1,K_2) 的签密数据 $S=(h,s,T,K,M,K_1,K_2)$ 为无效信息。

3　安全性与效率分析

3.1　方案正确性

1）代理密钥生成过程的正确性

接收者收到 (K_1,K_2,w) 之后验证下列式子

$$e_1' y_A + e_2' \bar{y}_A + K_1 + K_2 = e_1' x_A P + e_2' \bar{x}_A P + k_1 P + k_2 P$$
$$= (e_1' x_A + e_2' \bar{x}_A + k_1 + k_2)P = wP$$

2）解签密过程的正确性

$$H_4(ID_B, ID_C, K, M, s(y + hP), K_1 + K_2) = H_4(ID_B, ID_C, K, M, s(xP + hP), K_1 + K_2)$$
$$= H_4(ID_B, ID_C, K, M, s(x + h)P, K_1 + K_2) = H_4(ID_B, ID_C, K, M, tP, K_1 + K_2)$$
$$= H_4(ID_B, ID_C, K, M, T, K_1 + K_2) = h$$

3.2 随机预言机下可证安全性

本文方案包括一个原始签密者、一个代理签密者和签密接受者，签密方案包括以下过程：系统参数的选取，密钥的生成，委托过程，代理签密的生成，代理签密的签名验证和解密，代理签密的注销。对于无证书的签密方案都存在两种类型的攻击者：（类型1）攻击者 Q_1 无法获知系统的主密钥，但是可以替换任意用户的长期公钥；（类型2）攻击者 Q_2 不能替换用户的公钥，但可以获得系统的主密钥。

由于类型2的攻击更具有破坏力，攻击成功则影响所有用户，本文只证明对类型2攻击下是可证安全的，对于类型1的证明过程基本类似（只是询问过程有些不同，证明过程也可参考文献[15]中的定理2和定理3）。

定理1 （类型2攻击下的不可伪造性）在随机预言机模型和第二类攻击假设下，若存在算法 Q 在多项式时间 t 内，通过进行有限多项次询问，以不可忽略的概率 ε 伪造一个有效的签密，那么存在一个挑战者 Ω 在多项式时间 t' 内，以不可忽略的概率 ε' 解决ECDLP。

证明 已知 $y=xP\in G$，为了计算 x（x 为用户 ID^* 的长期私钥），$x\in \boldsymbol{Z}_q^*$，假设挑战者 Ω 为求解 x，将算法 Q 作为自己的子程序，并与攻击者算法 Q 进行游戏交互，且在多项式时间内最多允许攻击者算法 Q 执行 q_{H_1} 次 H_1 询问、q_{H_2} 次 H_2 询问、q_{H_3} 次 H_3 询问、q_{H_4} 次 H_4 询问、q_{H_5} 次 H_5 询问、q_{BM} 次部分密钥提取询问、q_{SK} 次长期私钥提取询问、q_{PK} 次长期公钥提取询问、q_{DK} 次代理密钥提取询问、q_{QM} 次代理签密询问、q_{JM} 次解密询问。挑战者 Ω 维持列表 L_{H_1}，L_{H_2}，L_{H_3}，L_{H_4}，L_{H_5}，L_{BM}，L_{LK}，L_{DK}，L_{QM}，L_{JM} 分别用于应对 H_1 询问、H_2 询问、H_3 询问、H_4 询问、H_5 询问、部分密钥提取询问、长期密钥提取询问、代理密钥提取询问、代理签密询问、解密询问，并初始化所有列表为空。

挑战者 Ω 生成系统参数 $param=\{G, q, P, H_1, H_2, H_3, H_4, H_5, y_{kgc}\}$ 并将系统参数发送给攻击者。挑战者 Ω 随机选择 $x_{kgc}\in \boldsymbol{Z}_q^*$ 作为KGC私钥，KGC公钥为 $y_{kgc}=x_{kgc}P$。C 随机选取 $k, 0\leqslant k\leqslant q_{PK1}$，身份标示 $ID^*=ID_k$，对应的用户长期公钥为 $y_k=x_kP$，用 x_k 来模拟 ID_k 的长期私钥。显然询问过程不能询问 ID^* 的长期私钥。

3.2.1 H_1 询问

当挑战者 Ω 收到攻击者 Q 关于 $H_1(ID_i,U_i,V_i,y_i)$ 的 H_1 询问，Ω 首先查询列表 L_{H_1}，如果 $(ID_i,U_i,V_i,y_i,h_{1i})$ 存在于列表 L_{H_1} 中，则 Ω 将 h_{1i} 返回给 Q；否则，Ω 随机选择 $h_{1i}\in \boldsymbol{Z}_q^*$，将其作为回答返回给 Q_1，并且将 $(ID_i,U_i,V_i,y_i,h_{1i})$ 添加到列表 L_{H_1} 中。

3.2.2 H_2 询问

当 Ω 收到 Q 关于 $H_2(K_{1i},K_{2i})$ 的 H_2 询问，Ω 首先查询列表 L_{H_2}，如果 (K_{1i},K_{2i}, e_i) 在列表 L_{H_2} 中，那么 Ω 将 e_i 返回给 Q；否则，Ω 随机选择 $e_i\in \boldsymbol{Z}_q^*$，将其作为回答返回给 Q，并且将 (K_{1i},K_{2i}, e_i) 添加到列表 L_{H_2} 中。

3.2.3 H_3 询问

当 Ω 收到 Q 关于 $H_3(m_i)$ 的 H_3 询问，Ω 首先查询列表 L_{H_3}，如果 (m_i,M_i) 在列表 L_{H_3} 中，那么 Ω 将 M_i 返

回给 Q;否则,Ω 随机选择 $M_i \in \boldsymbol{Z}_q^*$,将 M_i 作为回答返回给 Q,并且将 (m_i, M_i) 添加到列表 L_{H_3} 中。

3.2.4 H_4 询问

当 Ω 收到 Q 关于 $H_4(ID_{Bi}, ID_{Ci}, K_i, M_i, K_{1i}+K_{2i})$ 的 H_4 询问,Ω 首先查询列表 L_{H_4},如果 $(ID_{Bi}, ID_{Ci}, K_i, M_i, K_{3i},\ h_{4i})$ 在列表 L_{H_4} 中,那么 Ω 将 h_{4i} 返回给 Q;否则,Ω 随机选择 $h_{4i} \in \boldsymbol{Z}_q^*$,将其作为回答返回给 Q,并将 $(ID_{Bi}, ID_{Ci}, K_i, M_i, K_{3i}, h_{4i})$ 添加到列表 L_{H_4} 中。

3.2.5 H_5 询问

当 Ω 收到 Q 关于 $H_5(ID_{Ai}, ID_{Bi}, ID_{Ci}, E_i, T_i)$ 的 H_5 询问,Ω 首先查询列表 L_{H_5},如果 $(ID_{Ai}, ID_{Bi}, ID_{Ci}, E_i, T_i, h_{5i})$ 在列表 L_{H_5} 中,那么 Ω 将 h_{5i} 返回给 Q;否则 Ω 随机选择 $h_{5i} \in \boldsymbol{Z}_q^*$,将其作为回答返回给 Q,并将 $(ID_{Ai}, ID_{Bi}, ID_{Ci}, E_i, T_i, h_{5i})$ 添加到列表 L_{H_5} 中。

3.2.6 部分密钥提取询问

当 Ω 收到 Q 关于 (ID_i, U_i, V_i) 的询问,Ω 首先查询列表 L_{BM},如果 $(ID_i, U_i, V_i, \bar{x}_i, \bar{y}_i)$ 在表 L_{BM} 中,那么 Ω 将相应的值发送给 Q;否则 Ω 先运行 H_1 询问提取 h_{1i},随机选择 u_i,$v_i \in \boldsymbol{Z}_q^*$,计算 $U_i = u_i P, V_i = v_i P$,$\bar{x}_i = u_i + v_i + x_{kgc} h_{1i}$,$\bar{y}_i = \bar{x}_i P$,将 $(ID_i, U_i, V_i, \bar{x}_i, \bar{y}_i)$ 记录到列表 L_{BM} 中,将 $(\bar{x}_i, \bar{y}_i)$ 返回给 Q。

3.2.7 长期私钥提取询问

当 Ω 收到 Q 关于 ID_i 的私钥提取询问,Ω 先检查列表 L_{LK}。若 (ID_i, x_i, y_i) 在列表 L_{LK} 中,那么 Ω 将相应的 x_i 发送给 Q;否则

1)当 $i \neq k$ 时:Ω 先做关于 ID_i 的 H_1 询问,然后再执行部分私钥提取询问得到 $\bar{x}_i$,随机选择 $x_i \in z_q^*$,计算 $y_i = x_i P$。把 (ID_i, x_i, y_i) 添加到列表 L_{LK},将相应的 x_i 发送给 Q;

2)当 $i = k$ 时:算法停止。

3.2.8 长期公钥提取询问

当 Ω 收到 Q 关于 ID_i 的公钥提取询问,Ω 先检查列表 L_{LK}。如果 (ID_i, x_i, y_i) 在列表 L_{LK} 上,则 Ω 将 y_i 发送给 Q;否则

1)当 $i \neq k$ 时:随机选择 $x_i \in \boldsymbol{Z}_q^*$,计算 $y_i = x_i P$ 把 (ID_i, x_i, y_i) 添加到列表 L_{LK},将 y_i 发送给 Q;

2)当 $i = k$ 时:而用户私钥用 $\perp$ 表示,公钥为 y_k,将 y_k 发送给 Q,并且将 $(ID_i, \perp, y_k)$ 添加到列表 L_{LK}。

3.2.9 代理密钥提取询问

当 Ω 收到 Q 关于 (ID_{Ai}, ID_{Bi}) 的部分代理密钥询问,若 $(ID_{Ai}, ID_{Bi}, k_{1i}, k_{2i}, K_{1i}, K_{2i}, W_i, x_{pi}, y_{pi})$ 在列表 L_{DK} 中,则返回 (x_{pi}, y_{pi}) 给 Q;否则当 $ID_{Ai} \neq ID_k$ 且 $ID_{Bi} \neq ID_k$ 时:Ω 随机选取秘密值 $k_{1i}, k_{2i} \in \boldsymbol{Z}_q^*$,计算 $K_{1i} = k_{1i} P$,$K_{2i} = k_{2i} P$,接着执行 H_2 询问获取 e_{1i}, e_{2i},部分密钥提取询问获取 $(\bar{x}_{Ai}, \bar{y}_{Ai})$ 和 $(\bar{x}_{Bi}, \bar{y}_{Bi})$,长期私钥提取询问获得 (x_{Ai}, x_{Bi}) 和长期公钥提取获得 (y_{Ai}, y_{Bi}),然后计算:$w_i = e_{1i} x_{Ai} + e_{2i} \bar{x}_{Ai} + k_{1i} + k_{2i}$,$x_{pi} = w_i + e_{1i} x_{Bi} + e_{2i} \bar{x}_{Bi}$,$y_{pi} = x_{pi} P$,$W_i = w_i P$。同时将 $(ID_{Ai}, ID_{Bi}, k_{1i}, k_{2i}, K_{1i}, K_{2i}, W_i, x_{pi}, y_{pi})$ 记录到列表 L_{DK} 中,将 (x_{pi}, y_{pi}) 返回给 Q。

3.2.10 代理签密询问

当 Ω 收到 Q 关于 $(ID_{Ai}, ID_{Bi}, ID_{Ci})$ 和 m_i 的代理签名询问,查询列表 L_{JM},若在列表 L_{JM} 中已经存在记录 $(m_i, ID_{Ai}, ID_{Bi}, ID_{Ci}, h_{4i}, s_i, T_i, K_i, M_i, K_{1i}, K_{2i})$,则返回 $(h_i, s_i, T_i, K_i, M_i, K_{1i}, K_{2i})$,Ω 运行代理密钥提取询问得到 $(K_{1i}, K_{2i}, x_{pi}, y_{pi})$,运行 H_3 询问获得 M_i,运行 H_4 询问获得 h_{4i},运行 H_5 询问获得 h_{5i},随机选择 $t_i \in \boldsymbol{Z}_q^*$,$key_i \in \boldsymbol{Z}_q^*$,计算 $T = tp$,$K_i = key_i \oplus h_{5i}$,$s_i = t_i (x_{pi} + h_{4i})^{-1}$,得到 (m_i, ID_{Ai}, ID_{Bi}) 的签密 $(h_{4i}, s_i, T_i, K_i, M_i, K_{1i}, K_{2i})$,将 $\sigma = (h_{4i}, s_i, T_i, K_i, M_i, K_{1i}, K_{2i})$ 发送给 Q,并将 $(m_i, ID_{Ai}, ID_{Bi}, ID_{Ci}, h_{4i}, s_i, T_i, K_i, M_i, K_{1i}, K_{2i})$ 添加到 L_{JM}。易验证若算法不终止,签密信息可以通过签名和验证。

3.2.11 解签密询问

当 Ω 收到 Q 关于 $(ID_{Ai},ID_{Bi},ID_{Ci})$ 的一个签密 $(h_{4i},s_i,T_i,K_i,M_i,K_{1i},K_{2i})$ 时，查询列表 L_{JM}，若在列表 L_{JM} 中已经存在记录 $(m_i,ID_{Ai},ID_{Bi},ID_{Ci},h_{4i},s_i,T_i,K_i,M_i,K_{1i},K_{2i})$，则返回 m_i 给 Q，否则

1）当 $ID_{Ci}\neq ID_k$：Ω 首先根据签密者和接收者的身份以及公钥从列表 L_{H_4} 中查询 h_{4i}，若在 L_{H_4} 查找出匹配的 h_{4i}，验证查找出的 h_{4i} 与接收到的 h'_{4i} 是否相等，如果不相等，则拒绝对 $(h_{4i},s_i,T_i,K_i,M_i,K_{1i},K_{2i})$ 解签密；若相等，则 Ω 从列表 L_{BM} 和 L_{LK} 中查找出 ID_{Ci} 的完整私钥 $(x_{Ci},\bar{x}_{Ci})$，若在 L_{H_5} 查找出匹配的 h_{5i}，计算 $key_i=K_i\oplus h_{5i}$，执行解密算法即可得到 m。

2）当 $ID_{Ci}=ID_k$：Ω 首先根据签密者和接收者的身份以及公钥查询列表 L_{H_4}，若在 L_{H_4} 不存在匹配的 h_{4i}，则终止协议；若能在 L_{H_4} 查找出匹配的 h_{4i}，并验证查找出的 h_{4i} 与接收到的 h'_{4i} 是否相等，如果不相等，则拒绝对 $(h_{4i},s_i,T_i,K_i,M_i,K_{1i},K_{2i})$ 解签密；如果相等，那么 Ω 查询列表 L_{H_5}，查找出 h_{5i}，执行以下算法：

① $\alpha=1$；

② 若 $\alpha<q_{H_5}$，则在列表 L_{H_5} 中查询出 $h_{5\alpha}$，计算 $key=K\oplus h_{5\alpha}$，用这个 key 和所接收到的 s 来解密，即 $m_\alpha=D_{key}(s)$；

③ 查询列表 L_{H_3}，若存在 (m_α,M_α)，则返回 m_α，否则执行④；

④ $\alpha=\alpha+1$，执行②。

最后 Ω 将输出的 m_α 发送给 Q。

Q 进行至多有限次多项式次询问后，在概率多项式时间 t 内，以不可忽略的概率 ε，产生一个有效的签密数据。设代理签名密钥 x，对应公钥 y，利用分叉规约技术对 H_4 进行分叉，根据分叉引理，通过对 Q 的哈希重放，Ω 可以得到消息 m 的两个有效的签密信息：$S=(h,s,T,K,M,K_1,K_2)$ 和 $S'=(h',s',T,K,M,K_1,K_2)$。

由 $s(y+hP)=s'(y+h'P)$ 退出 $s(x+h)=s'(x+h')$，计算可得 $x=\dfrac{s'h'-sh}{s-s'}$，因此求解了离散对数问题 $y=xP$。

以下我们给出算法 Ω 成功的优势和执行的时间粗估计（精细估计方法可参考文献[15]）：对于没有询问过程算法没有停止的概率至少为 $\dfrac{1}{q_{H_1}q_{H_2}q_{SK}^3q_{DK}q_{QM}}$，成功伪造签密的概率至少为 $\dfrac{1}{(q_{H_4})^{1/2}q_{H_5}}$，因此，算法 Ω 成功的优势 $\varepsilon'\geq\dfrac{\varepsilon}{q_{H_1}q_{H_2}q_{H_4}^{1/2}q_{H_5}q_{SK}^3q_{DK}q_{QM}}$，假设 t_{H_1}，t_{H_2}，t_{H_3}，t_{H_4}，t_{H_5}，t_{BM}，t_{SK}，t_{PK}，t_{DK}，t_{QM}，t_{JM} 分别为 H_1 询问，H_2 询问，H_3 询问，H_4 询问，H_5 询问，部分密钥提取询问，长期私钥提取询问，长期公钥提取询问，代理密钥提取询问，代理签密询问，解密询问一次所需时间，算法 Ω 执行完成的时间 t' 满足

$$t'\leq 10^6U\frac{t_{H_1}q_{H_1}+2t_{H_2}q_{H_2}+t_{H_3}q_{H_3}+t_{H_4}q_{H_4}+t_{H_5}q_{H_5}+t_{BM}q_{BM}+t_{SK}q_{SK}+t_{PK}q_{PK}+t_{DK}q_{DK}+t_{QM}q_{QM}+t_{JM}q_{JM}+2t}{\varepsilon}$$

其中：$U=q_{H_1}q_{H_2}q_{SK}^3q_{DK}q_{QM}$。

通过以上分析，Ω 能在概率多项式时间 t' 内，以不可忽略的概率 ε'，解决 $y=xP$ 求出 x。这与离散对数问题的困难性矛盾，所以针对类型2攻击本文方案具有不可伪造性。

4 效率以及与其它方案的性能比较分析

本文方案不需要双线性对运算和指数运算，签密运算和解签密运算只进行椭圆曲线上的数乘运算，文献[12]运用了双线性对运算，目前快速双线性对运算时间是椭圆曲线上点乘所需时间的20倍左右，因此效率与本文的方案相比要低。而文献[14]虽然是基于无双线性对映射的，但是运用了指数运算，而且其为了保证方案的前向安全性，其代理授权过程计算量比较大，效率并不高。我们用 H 表示哈希函数运算，用 M 表示椭圆曲线上的数乘运算，E 表示指数运算，P 表示双线性对运算，具体的方案效率分析及比较见表1。

表1　与其它方案的性能比较

Tab.1　Comparison of efficiency results between our scheme and other signcryption schemes

方案	代理委托过程	代理签密	解签密及验证过程
文献[12]	3M+2E+3P+1H	2M+2E+2P+1H	0M+5E+5P+2H
文献[14]	6M+2E+0P+5H	3M+3E+0P+5H	2M+2E+0P+4H
本文	9M+0E+0P+2H	2M+0E+0P+3H	2M+0E+0P+2H

5　结论

1）本方案没有运用双线性对运算和指数运算,能够抵抗公钥替换攻击,在随机预言机模型中,方案对于适应性选择消息攻击具有机密性和不可伪造性。

2）本方案在设计和实现上借鉴了国密SM2标准签名方案的参数和技巧,计算开销明显低于其他方案,提高了方案的效率。

参考文献:

[1] AL-RIYAMI, PATERSON. Certificateless public key cryptography[C]//Advances in Cryptology-ASIACRYPT 2003. Berlin: Springer-Verlag Berlin Heideberg, 2003: 452-473.

[2] YANG ZHENG. Digital signcryption or how to achieve cost (signature & encryption) [C] //Advances in Cryptology-CRYPTO'97. Berlin: Springer-Verlag Berlin Heideberg, 1997:165-179.

[3] BAO F, DENG R. A signcryption scheme with signature directly verifiable by public key[C] //Advances in Cryptology-CRYPTO'98. Berlin: Springer-Verlag Berlin Heideberg, 1998:55-59.

[4] SHIN J B, LEE K, SHIM K. New DSA-verifiable signcryption schemes[C]//Information Security and Cryptology-ICISC 2002. Berlin: Springer-Verlag Berlin Heideberg, 2003:35-47.

[5] 汤鹏志,陈仁群,左黎明. 一种基于椭圆曲线的门限部分盲签名方案[J]. 华东交通大学学报,2014,31(6):96-102.

[6] 左黎明,汤鹏志,刘二根.一种辫群上代理签名方案[J].计算机应用,2011, 31(11),2979-2982.

[7] 左黎明, 陈仁群, 郭红丽.可证安全的基于身份的签密方案[J].计算机应用,2015,35(3): 712-716.

[8] SHARMIL S D S,VIVEK S S,RANGAN C P. Cryptanalysis of certificateless signcryption schemes and an efficient construction without pairing[C]//Information Security and Cryptology. Berlin:Springer-Verlag Berlin Heideberg, 2011:75-92.

[9] LIU Z H, HU Y P. Certificateless signcryption scheme in the standard model[J]. Information Sciences,2010(7):452-464.

[10] GAMAGE C, LEIWO J, ZHENG Y. An efficient scheme for secure message transmission using proxy signcryptio[C]/ /Proceedings of 22nd Australasian Computer Science Conference. Berlin:Springer-Verlag, 1999:420-431

[11] LI XIANGXUE, CHEN KEFEI. Identity- based proxy signcryption scheme from pairing[C]//Proceedings of the IEEE International Conference on Services Computing (SCC2004). Berlin:Springer-Verlag Berlin Heideberg,2004:494- 497.

[12] 王会歌, 王彩芬, 易玮, 等. 高效的无证书可公开验证签密方案 [J]. 计算机工程, 2009,35(5):147-149.

[13] 王琴.一种基于身份的代理签密体制[J].计算机工程,2011,37(19) :120-121.

[14] 俞惠芳,王彩芬,王之仓.基于 ECC 的自认证代理签密方案[J]计算机科学,2010,37(7):91- 92.

[15] 文佳骏,左黎明,李彪.一个高效的无证书代理盲签名方案[J]. 计算机工程与科学,2014,36(3):452-457.

Certificateless Agent Signcryption Scheme without Bilinear Pairing

Zha Wengang

(Modern Education Technology Center, East China Jiaotong University, Nanchang 330013, China)

Abstract: Certificateless signcryption is one of the most important applications in certificateless public key cryptography. Compared with the traditional practice of signature before encryption, it has less costs for computation and communication. By reference to the signature scheme design skills in National Secret Algorithm SM2 Standard, this paper proposes a certificateless agent signcryption scheme without pairing scheme. The analysis of its correctness, security, efficiency and parameter choice are subsequently presented, and a detailed formal security proof in the random oracle model is given. The new scheme, based on the discrete logarithm problem (DLP) and DLP assumption, has significantly lower computational overhead than other certificateless agent signcryption schemes. By avoiding the use of bilinear map, the proposed scheme shows better performance with higher security and efficiency.

Key words: digital signature;bilinear map;random oracle model;proxy signcryption; non-bilinear pairing

(责任编辑 姜红贵)

(上接第89页)

Designing of New Sliding-mode Controller for MMC

Song Pinggang, Luo Shanjiang, Yang yao, Wen Fa, Ma Weidong

(School of Electrical and Electronic Engineering, East China Jiaotong University, Nanchang 330013, China)

Abstract: At present, controllers of MMC mostly adopt the double closed loops PI control system with voltage and current loop based on d-q coordinate, and the sliding-mode control strategy hasn't yet been used to MMC control due to its unique pulse generation style. After in-depth study of the two control strategies, this paper proposes a new sliding-mode control system, which reduces the PI regulation link, simplifies the debugging of parameters and improves the adaptiveness of the system. Finally, a simulation model is constructed in MATLAB/Simulink and the simulation results validate the feasibility and superiority of the proposed control strategy.

Key words: modular multilevel converter; high voltage direct current; sliding-mode control; double closed loop; adaptiveness

(责任编辑 刘棉玲)