文章编号：1674-8085(2016)04-0043-03

基于离散对数的门限解签密方案

*殷凤梅，王筱薇倩，张　江

（合肥师范学院公共计算机教学部，安徽，合肥 230601）

摘　要：为了降低门限解签密算法的计算开销，基于离散对数问题提出了一种新的门限解签密方案。该方案通过随机数和私钥生成签密密钥来签密消息，引入门限共享思想获取解签密钥来恢复消息。与现有方案相比，该方案的计算开销明显较小。在离散对数假设和 DDH 假设的前提下，该方案满足机密性、不可伪造性、不可否认性和不相关性。

关键词：签密；解签密；门限性；离散对数

中图分类号：TP309.7　　**文献标识码**：A　　DOI:10.3969/j.issn.1674-8085.2016.04.009

A THRESHOLD UNSIGNCRYPTION SCHEME BASED ON DLP

YIN Feng-mei, WANG Xiao-weiqian, ZHANG Jiang

(Department of Public Computer Teaching, Hefei Normal University, Hefei, Anhui 230601, China)

Abstract: In order to reduce the computational cost of the algorithm, a new threshold unsigncryption scheme based on DLP (discrete logarithm problem) is proposed. In the scheme, the key of the signcryption is generated by the random number and the private key to sign the message. Furthermore, the key of the unsigncryption is gained by introducing the threshold sharing to recover the message. Compared with the existing schemes, the computational cost of the proposed scheme is obviously smaller. On the premise of DLP assumption and DDH assumption, the scheme has been proved to satisfy confidentiality, unforgeability, non-repudiation and non-correlation.

Key words: signcryption; unsigncryption; threshold; DLP

0　引　言

签密的概念由 Zheng[1]首次提出，其可以实现一次性对明文消息进行签名和加密功能。门限共享概念最早由 Shamir 和 Blakley 分别提出，其主要思想是将秘密在 n 个人中分享，其中至少 t 个人合作才能恢复出秘密。若将门限共享思想和签密概念相结合，可产生两种不同类型的方案，即门限签密方案[2-5]和门限解签密方案[6-10]，分别实现签密与解签密的分散管理和合理监督。

陈瑞虎等[6]结合 Shamir 门限共享思想提出具有指定接收组的门限解签密方案，但该方案不满足前向安全性。周宣武等[7]对该方案进行改造，实现具有前向安全性的门限解签密方案。Herranz 等[8]提出门限解签密的安全性要求，Selvi 等[9]给出门限解签密的安全性形式化证明。在这两个方案的基础上，Herranz 等[10]提出了完全安全的门限解签密方案，但由于该方案基于双线性对运算，计算量较大。

为了降低计算代价，基于离散对数假设和 DDH 假设，本文提出了一种新的门限解签密方案，

收稿日期：2016-03-12；修改日期：2016-04-18
基金项目：国家自然科学青年科学基金项目(61503112)；安徽省高校优秀青年人才支持计划重点项目(gxyqZD2016231)
作者简介：*殷凤梅(1981-)，女，安徽肥东人，讲师，硕士，主要从事网络与信息安全研究(E-mail:yinfm@163.com);
王筱薇倩(1988-)，女，安徽合肥人，助教，硕士，主要从事图像处理与信息安全研究(E-mail:wangxiaoweiqian@126.com);
张　江(1981-)，女，江苏扬州人，讲师，硕士，主要从事图像处理与信息安全研究(E-mail: 99034871@qq.com).

该方案满足解签密的安全性需求。

1 基本概念

1.1 离散对数(DLP)假设

p 和 q 是 2 个大素数，且 $q|p-1$，q 阶 $g \in Z_p$，则不存在概率多项式时间算法 A，其能以不可忽略的概率从 g^a 中获得 a。

1.2 Decisional Diffie-Hellman(DDH)假设

p 和 q 是 2 个大素数，且 $q|p-1$，q 阶 $g \in Z_p$，$a,b,c \in Z_q$，$A_1=(g,g^a,g^b,g^c)$，$A_2=(g,g^a,g^b,g^{ab})$，则不存在概率多项式时间算法 A，其能以不可忽略的概率区分出 A_1 和 A_2。

2 门限解签密方案

本方案主要包含 3 个算法：系统参数生成算法、签密算法和门限解签密算法。

2.1 系统参数生成算法

本方案中含有n个成员$A_i(1\le i\le n)$，对应的身份标识符$x_i(1\le i\le n)$。p和q是2个大素数，且$q|p-1$，q阶 $g \in Z_p$，$H:\{0,1\}^* \to Z_q$为单向哈希函数，(E,D)为对称加/解密算法。每个成员A_i选取私钥$s_i(1\le i\le n)$，计算对应的公钥 $y_i=g^{s_i} \bmod p$。公开系统参数 $\{p,q,y_i,H,(E,D)\}$。

2.2 签密算法

签密者A_k为消息m生成签密σ，发送给t个成员 $\{A_1,A_2,\cdots,A_t\}$，$L=\{y_1\|\cdots\|y_t\}$（符号“||”表示串联)。

1) 选择随机数r，使用t个成员的$(x_i,y_i^r)(1\le i\le t)$按照(1)式构造t-1次Lagrange插值多项式 $f(x)$ 并计算 $f(0)$，按照(3)式计算R，按照(4)式计算$F(0)$。

$$f(x)=\sum_{i=1}^{t} y_i^r a_i \bmod p \tag{1}$$

$$a_i=\prod_{\substack{j=1\\ j\ne i}}^{t}\frac{x-x_j}{x_i-x_j} \bmod q \tag{2}$$

$$R=g^r \bmod p \tag{3}$$

$$F(0)=g^{f(0)} \bmod p \tag{4}$$

2) 计算b和B、z和Z，按照(9)式计算签密密钥k，使用k对消息m加密生成密文c。

$$b=H(L\|m\|y_k\|f(0)) \tag{5}$$

$$B=g^b \bmod p \tag{6}$$

$$z=hs_k+ry_k \tag{7}$$

$$Z=g^z \bmod p \tag{8}$$

$$k=F(0)^z \bmod p \tag{9}$$

$$c=E_k(m) \tag{10}$$

3) 按照(11)式产生消息m的签密σ，并发送给t个成员。

$$\sigma=(L,c,B,R,Z) \tag{11}$$

2.3 门限解签密算法

t 个成员 $\{A_1,A_2,\cdots,A_t\}$ 收到签密 $\sigma=(L,c,B,R,Z)$ 后，首先解签密σ获得消息m'，然后验证签密是否正确。

1) 每个成员按照(12)式计算 w_i，t个成员合作可获得w和解签密钥 k'，使用 k' 按照(15)式解密密文c获得消息 m'。

$$w_i=R^{s_i}a_i \bmod q \tag{12}$$

$$w=\sum_{i=1}^{t} w_i \bmod q \tag{13}$$

$$k'=Z^w \bmod p \tag{14}$$

$$m'=D_{k'}(c) \tag{15}$$

2) 若等式(16)式成立，则接受消息 m'；否则拒绝 m'。

$$g^{H(L\|m\|y_k\|w)} \bmod p \overset{?}{=} B \tag{16}$$

3 方案分析与比较

3.1 正确性

定理 1 2.3 节中的门限解签密过程是正确的，即密钥 $k'=k$，消息 m 可以被正确解出。

证明：由于 $k'=Z^w \bmod p=Z^{\sum_{i=1}^{t} w_i} \bmod p=$

$Z^{\sum_{i=1}^{t} R^{s_i}a_i} \bmod p=Z^{\sum_{i=1}^{t} R^{s_i}\prod_{\substack{j=1\\ j\ne i}}^{t}\frac{x-x_j}{x_i-x_j}} \bmod p=Z^{\sum_{i=1}^{t} g^{rs_i}\prod_{\substack{j=1\\ j\ne i}}^{t}\frac{x-x_j}{x_i-x_j}} \bmod p=$

$Z^{\sum_{i=1}^{t} y_i^r\prod_{\substack{j=1\\ j\ne i}}^{t}\frac{x-x_j}{x_i-x_j}} \bmod p=Z^{f(0)} \bmod p=g^{zf(0)} \bmod p=$

$F(0)^z \bmod p=k$

因此，$m'=D_{k'}(c)=D_{k'}(E_k(m))=D_k(E_k(m))=m$

即 t 个成员门限解签密密文 c，可获得消息原文 m。

定理 2 2.3 节中的验证过程是正确的，即当门限解签密过程正确时，验证等式 $g^{H(L\|m\|y_k\|w)} \bmod p=B$ 成立。

证明：从定理 1 的证明过程可知

$$H(L\|m\|y_k\|w)=H(L\|m\|y_k\|\sum_{i=1}^{t}w_i)=$$

$$H(L\|m\|y_k\|\sum_{i=1}^{t}R^{s_i}a_i)=H(L\|m\|y_k\|f(0))=b$$

因此，$g^{H(L\|m\|y_k\|w)} \bmod p = g^b \bmod p = B$。

即当门限解签密过程正确时，验证等式成立，解签密获得的消息 m 正确。

3.2 安全性

3.2.1 机密性

攻击者试图获取消息 m 有两种可能的方法：一是通过获取对称加密密钥 k，解密获得

$$D_k(E_k(m))=m$$

由于 $k=F(0)^z \bmod p=g^{f(0)z} \bmod p=g^{f(0)(hs_k+ry_k)} \bmod p$，$k$ 的计算涉及签密者 A_k 的私钥 s_k 和随机数等信息，在 DDH 假设的前提下，其他成员是不可能获取这些隐私信息的，因而无法获得密钥 k，也就无法解出消息 m，消息 m 是安全的。二是通过获取签密 $\sigma=(L,c,B,R,Z)$ 中的 $B=g^b \bmod p=g^{H(L\|m\|y_k\|f(0))} \bmod p$ 获取消息 m。在离散对数假设的前提下，这是不可能做到的，因而消息 m 是安全的。

3.2.2 不可伪造性

攻击者伪造签密者 A_k 对消息 m 的签密 σ'，并试图通过解签密认证。从 2.2 节可知，签密 σ' 的生成需要用到签密者 A_k 的私钥 s_k，这就需要从公开的公钥 y_k 中获得。在离散对数假设的前提下，这是不可能做到的，因此，攻击者无法获得 A_k 的私钥 s_k，也就无法伪造签密 σ'。

3.2.3 不可否认性

从不可伪造性的证明可知，签密者 A_k 对消息 m 的签密 $\sigma=(L,c,B,R,Z)$，需要使用自身的私钥 s_k。因为只有 A_k 自己知道 s_k，只能 A_k 一人可以完成签密 σ，因而签密满足不可否认性。

3.2.4 不相关性

签密者 A_k 的每次签密，都会选择不同的随机数 r，构造不同的 Lagrange 插值多项式 $f(x)$，生成不同的签名 σ，因而不能判定两次签密是否是来自同一个人。

3.3 计算代价比较

本文基于离散对数问题提出了一种门限解签密方案，与同类方案在性质和计算代价上的比较具体如下：

1) 性质比较

与现有的门限解签密方案相比，本文方案同样具有机密性、不可伪造性、不可否认性、不相关性、门限解签密等性质。

2) 计算代价比较

在同样具备门限解签密安全性性质的前提下，本节主要将本文方案与同样基于离散对数问题的陈瑞虎等[6]方案和 Herranz 等[10]方案在计算代价上进行比较。

门限解签密方案的计算代价主要包含 3 个算法：系统参数生成、签密和门限解签密。为了方便比较，我们使用 exp 表示指数运算次数，mul 表示标量乘运算次数，pair 表示双线对运算次数。3 个方案的计算开销比较如表 1 所示。表 1 中的数据显示，在本文方案中，系统参数生成算法只需 n 次 exp，签密算法需要 t+4 次 exp 和 3 次 mul，门限解签密算法需要 t+2 次 exp 和 1 次 mul。可见，本文方案的计算代价明显少于陈瑞虎等方案和 Herranz 等方案。

表 1 计算代价比较

Table 1 Comparison of computational cost

方案	系统参数生成			签密			门限解签密		
	exp	mul	pair	exp	mul	pair	exp	mul	pair
Herranz 等[10]方案	4t+1	1	0	3	0	1	7t	2t+3	5t+2
陈瑞虎等[6]方案	2n+t-1	t-1	0	2	2	0	5t	2t+1	0
本文方案	n	0	0	t+4	3	0	t+2	1	0

4 结束语

本文方案允许成员自主选择私钥，签密算法中通过随机数和私钥生成签密密钥来签密消息，解签密算法中引入门限共享思想获取解签密钥来恢复消息。通过分析与证明，本文方案满足签密的安全性需求：机密性、不可伪造性、不可否认性和不相关性。与 Herranz 等方案相比，本方案计算代价明显较小。下一步我们将对多接收者的门限解签密方案进行深入研究，拓宽解签密方案的应用范围。

(参考文献[1]- [10]转第 62 页)

通过对图3~图5某车型被动悬架和主动悬架性能指标的仿真结果对比分析，可发现主动悬架系统相对于被动悬架系统在相关性能指标方面都有所改善。但是有些方面的改善是明显的，有些则不是很明显，甚至超出了主动悬架系统，而且通过仿真结果可发现前后左右四个悬架系统在悬架动挠度和轮胎动位移两个性能方面的输出是不相同的，对于前后输出不同首先是应为车身的质心位置不是中间，前后不是对称的；其次是前后悬架系统在减震器阻尼和弹簧刚度等方面不同引起的；最后是由于轮胎和地面的接触时间以及车身重量等方面所造成的。而对于左右悬架系统在左右弹簧刚度和减震器阻尼相同的情况下，车身左右不对称引起左右输出不一致，除此之外还有其他一些外在影响因素。

4 结论

通过分块控制的方法对汽车主动悬架进行研究，发现该控制方法相对于其它控制方法在理论计算方面简便了很多；对 1/4 车体模型是利用的天棚阻尼控制，对 1/2 车体模型是利用 PID 控制方式。这两种控制方法目前研究得都比较成熟，易于实现;该控制方法可提高汽车的行驶平顺性、操纵稳定性和舒适性等相关性能。

参考文献：

[1] 兰波. 车辆主动悬架 LQG 控制器的设计与仿真分析[J]. 农业机械学报,2004,35(1):13-17.

[2] 喻凡. 汽车系统动力学[M].北京:机械工业出版社,2005:1-283.

[3] 万百五. 控制论—概念、方法与应用[M].北京:清华大学出版社,2009:80-153.

[4] 刘海生. Simulik 在汽车主动悬架 LQG 控制仿真中的应用[J].机械设计与制造,2008(8):106-107.

[5] 朱命怡,杨丽云. 汽车主动悬架的整车控制方法及仿真研究[J].机械设计,2008,25(6):17-20.

[6] 张海涛,高洪. 整车模型被动悬架的建模与仿真分析[J]. 井冈山大学学报: 自然科学版, 2013, 34(3): 58-62.

[7] 张海涛,高洪,查为民,等. 具有 LQG 控制器的主动悬架半车模型动力学分析与仿真[J]. 安徽工程大学学报, 2012, 27(1): 42-45.

(上接第45页)

参考文献：

[1] Zheng Y. Digital signcryption or how to achieve cost (signature & encryption)≪ cost (signature)+ cost (encryption)[C].Annual International Cryptology Conference. Springer Berlin Heidelberg, 1997: 165-179.

[2] Chen S, Bian G. A new group-oriented publicly veriable threshold signcryption scheme [J]. Journal of Electronics, 2013, 30(6):567-573.

[3] Qin H, Dai Y, Wang Z. Identity-based multi-receiver threshold signcryption scheme[J]. Security & Communication Networks, 2011, 4(11):1331-1337.

[4] Zhang J, Chen Z, Xu M. On the security of ID-based multi-receiver threshold signcryption scheme[C]. International Conference on Consumer Electronics, Communications and Networks. IEEE, 2012: 1944-1948.

[5] Chien-Hua T, Su P. Multi-document threshold signcryption scheme [J]. Security & Communication Networks, 2015, 8:2244-2256.

[6] 陈瑞虎,高峰修,马传贵. GOST 门限签密方案[J]. 微计算机信息, 2005, 21(11X): 9-10.

[7] 周宣武,刘开华,金志刚,等. 基于椭圆曲线的门限共享解签密改进方案[J]. 计算机工程, 2014, 40(12): 121-125.

[8] Herranz J, Ruiz A, Sáez G. Fully secure threshold unsigncryption[C]. International Conference on Provable Security. Springer Berlin Heidelberg, 2010: 261-278.

[9] Selvi S S D, Vivek S S, Rangan C P, et al. On the security of identity based threshold unsigncryption schemes[C].International Conference on Network & System Security. IEEE, 2010:554-559.

[10] Herranz J, Ruiz A, Sáez G. Signcryption schemes with threshold unsigncryption, and applications[J]. Designs Codes & Cryptography, 2014, 70(3): 323-345.