·安全技术· 文章编号：1000-3428(2018)08-0151-04 文献标志码：A 中图分类号：TP391

基于异构密码系统的混合盲签密方案

牛淑芬，杨喜艳，王彩芬，田 苗，贾向东

（西北师范大学 计算机科学与工程学院，兰州 730070）

摘 要： 现有的异构密码体制不具备可加密任意长度消息的能力，无法在签名者不知道消息内容的情况下进行签名。为此，提出一种由基于身份的密码（IBC）体制到无证书密码（CLC）体制的混合盲签密方案。私钥生成器（PKG）和密钥生成中心（KGC）能够分别在 IBC 体制和 CLC 体制中产生各自的系统主密钥，而且具有可加密任意长消息和盲签密的能力。分析结果表明，与现有的签密方案相比，该方案具有速度快、效率高、计算量小等特点，在随机预言模型下具有更高的可行性。

关键词： 异构密码系统；混合签密；基于身份的密码体制；无证书密码体制；盲签密

中文引用格式： 牛淑芬，杨喜艳，王彩芬，等. 基于异构密码系统的混合盲签密方案[J]. 计算机工程，2018，44(8)：151-154，160.

英文引用格式： NIU Shufen，YANG Xiyan，WANG Caifen，et al. Hybrid blind signcryption scheme based on heterogeneous cryptosystem[J]. Computer Engineering，2018，44(8)：151-154，160.

Hybrid Blind Signcryption Scheme Based on Heterogeneous Cryptosystem

NIU Shufen，YANG Xiyan，WANG Caifen，TIAN Miao，JIA Xiangdong

（College of Computer Science and Engineering，Northwest Normal University，Lanzhou 730070，China）

【Abstract】 Existent heterogeneous cryptosystems don't have the ability of encrypting any lengths of messages，as well as no ability to sign a signature without knowing the content of the message. Therefore，this paper proposes a hybrid blind signcryption scheme from Identity-based Cryptosystem（IBC） to Certificateless Cryptosystem（CLC）. Private Key Generation（PKG） in IBC and Key Generation Center（KGC） in CLC can generate their own system master keys and have the ability to encrypt any long message and blind signcryption. Analysis results show that compared with existent signcryption schemes，the scheme has high speed and efficiency，and small computation，which is more feasible under the random oracle model.

【Key words】 heterogeneous cryptosystem；hybrid signcryption；Identity-based Cryptosystem（IBC）；Certificateless Cryptosystem（CLC）；blind signcryption

DOI： 10.19678/j.issn.1000-3428.0047898

0 概述

异构密码系统中的消息在传输过程中需要具备保密性和认证性，数字签密[1]使得签密密文同时具有保密性和认证性。近年来很多学者研究了各种签密方案[2-4]，包括基于身份的签密方案[5-8]和无证书签密方案[9]，其中不乏对特殊签密的研究，例如，代理签密方案[10-12]和异构签密方案[13-15]。文献[16]提出了从传统公钥密码到身份公钥密码的异构签密方案。文献[17]提出了 2 个异构签密方案，第 1 个方案是由公钥基础设施（Public Key Infrastructure，PKI）到基于身份的密码体制（Identity-based Cryptosystem，IBC），第 2 个方案是由 IBC 到 PKI。文献[18]提出了匿名 CLPKC-TPKI 异构签密方案。文献[19]提出了异构系统下的双向签密方案。但现有的异构密码系统大多采用公钥加密技术，而公钥加密技术由于对长消息的加密速度较慢，通常只适合加密短消息。在实际的安全通信中往往使用混合加密或者混合签密的方式。文献[20]提出了新的基于身份的混合签密。文献[21]提出了可证安全的无证书混合签密。上述文献都是签名者在知道明文的环境下进行的签名，在特殊的环境下签名者对于明文是未知的。

基金项目： 国家自然科学基金（61562077，61462077，61662071，61662069）；甘肃省杰出青年基金（1308RJDA007）；西北师范大学青年教师科研提升计划项目（NWNU-LKQN-14-7）。

作者简介： 牛淑芬（1976—），女，副教授、博士，主研方向为云计算、大数据安全；杨喜艳，硕士研究生；王彩芬，教授；田 苗，硕士研究生；贾向东，副教授、博士。

收稿日期： 2017-07-11 **修回日期：** 2017-09-18 **E-mail：** sfniu76@nwnu.edu.cn

为解决这一类特殊情况的签名,学者们首次提出了对盲签名的定义并进行了深入研究[22-24]。此后,又有学者提出了一系列盲签密方案[25-27]。

上述异构方案均没有实现既可对任意长度的消息签密的方案,也没有满足在特殊环境中明文消息对签名者具有盲性的特点,同时,在不同的密码体制内共享相同的主密钥是不现实的。为此,本文提出一个基于异构密码系统的混合盲签密方案,该方案是一个从 IBC 到无证书密码体制(Certificateless Cryptosystem,CLC)(IBC→CLC)的异构签密算法。

1 双线性映射

设 G_1 是生成元为 P、阶为 q 的循环加法群,G_2 是阶为 q 的循环乘法群,$e:G_1\times G_1\rightarrow G_2$ 是一个双线性映射,并且具有以下 3 个性质。

1)双线性性:任意 $a,b\in Z_p^*$,$e(aP,bP)=e(P,P)^{ab}$。

2)非退化性:$e(P,P)\neq 1_{G_2}$。

3)可计算性:任意 $P,Q\in G_1$,存在一个有效的算法计算 $e(P,Q)$。

2 具体方案

2.1 系统建立算法

设 G_1 是生成元为 P、阶为 q 的循环加法群,G_2 是阶为 q 的循环乘法群,$e:G_1\times G_1\rightarrow G_2$ 是一个双线性映射。定义 3 个安全的 Hash 函数 $H_1:\{0,1\}^*\rightarrow G_1$,$H_2:G_2\rightarrow\{0,1\}^n\times\{0,1\}^n$ 和 $H_3:\{0,1\}^*\times G_1\rightarrow Z_P^*$。$(E,D)$ 是一个对称加密体制的加密算法和解密算法。输入参数 1^k,输出系统参数 *params* 和主密钥 s_1 和 s_2。PKG 保密 s_1,并计算相应的公钥 $P_1=s_1^{-1}P$,KGC 保密 s_2,并计算相应的公钥 $P_2=s_2^{-1}P$。系统参数为 $\{G_1,G_2,q,e,P,n,E,D,H_1,H_2,H_3\}$。

2.2 IBC 密钥生成算法

IBC 密钥生成算法由 PKG 完成,输入用户身份 ID_A,计算用户私钥 $S_A=s_1Q_A$,其中,$Q_A=H_1(ID_A)$,最后通过安全方式发送给用户。

2.3 CLC 密钥生成算法

CLC 密钥生成算法分为以下 3 个子算法:

1)部分私钥生成算法。该算法由 KGC 完成,输入系统参数 *params* 和用户身份 ID_B,计算用户部分私钥 $D_B=s_2^{-1}Q_B$,其中,$Q_B=H_1(ID_B)$,最后通过安全方式发送给用户。

2)用户密钥生成算法。输入系统参数 *params* 和用户身份 ID_B,输出 ID_B 的秘密值 x_B 和公钥 $P_B=x_BP$。

3)私钥生成算法。输入系统参数 *params*、部分私钥 D_B 和秘密值 x_B,输出一个完全的私钥 $S_B=x_BD_B$。

2.4 签密

A 为盲签密者,M 为消息拥有者,签密过程如下:

1)A 随机选择 $a\in Z_P^*$,计算 $R=aQ_A$,然后将 R 发送给 M。

2)M 随机选取 $r\in Z_P^*$,计算 $U_1=rP$,$U_2=rR$,$U_3=rQ_A$,$t=H_2(U_2,m)$,$h=H_3(U_1,U_2,U_3,t,ID_A,Q_A)$,然后将 h 发送给 A。

3)A 计算 $V=(a+h)S_A$,$W=e(P_B,P_2Q_AQ_B)^a$,然后将 (V,W) 发送给 M。

4)M 计算 $W^*=W^r$,$V^*=r^{-1}V$,$K=H_2(U_1,U_2,U_3,W^*,rP_B,ID_B)$,$c=DEM.Enc(K,m)$。

5)M 输出 $\sigma=(c,U_1,U_2,U_3,V^*,R)$。

2.5 解签密

验证 $e(P_1U_1,V^*)=e(P^2,R+hQ_A)$ 是否成立,若成立,则进行以下操作:

1)B 计算 $W^*=e(U_1,PR)^{S_B}$。

2)B 计算 $K=H_2(U_1,U_2,U_3,W^*,x_BU_1,ID_B)$。

3)B 计算 $m=DEM.Dec(K,c)$。

4)输出 m 或 $\perp$。

3 正确性分析

正确性分析推导过程如下:

$$\begin{aligned}W^*&=W^r=e(P_B,P_2Q_AQ_B)^{ar}=e(x_BP,S_2^{-1}PQ_AQ_B)^{ar}=\\&e(x_BP,S_2^{-1}PRQ_B)^r=e(rP,x_Bs_2^{-1}PRQ_B)=\\&e(U_1,S_BPR)=e(U_1,PR)^{S_B}\end{aligned}$$

$$\begin{aligned}e(P_1U_1,V^*)&=e(s_1^{-1}PrP,r^{-1}(a+h)s_1Q_A)=\\&e(P^2,aQ_A+hQ_A)=e(P^2,R+hQ_A)\end{aligned}$$

4 安全性分析

4.1 盲性

盲性指签名者对所签署的内容是不可见的。由签密过程 2)可知,M 计算 $U_1=rP$,$U_2=rR$,$U_3=rQ_A$,$t=H_2(U_2,m)$,$h=H_3(U_1,U_2,U_3,t,ID_A,Q_A)$,其中,$r$ 是盲因子,$t=H_2(U_2,m)$ 是对消息的盲化过程,最后将 h 发送给 A。由签密过程 3)可知,当 M 收到 (V,W) 时,对签名 V 进行去盲,去盲过程为 $V^*=r^{-1}V$。显然,盲签名者 A 不知道所签署的内容。

4.2 不可跟踪性

不可跟踪性指 A 对签署的密文具有不可跟踪的特性。当 B 将密文 (c,U_1,U_2,U_3,V^*,R) 公开时,虽然 A 拥有 (a,R,h,V,W,S_A),但是不能通过密文 (c,U_1,U_2,U_3,V^*,R) 计算出 (s,r,W^*,x_B,D_B,S_B),所以本文方案具有不可跟踪的特性。

4.3 保密性

保密性指敌手通过密文 σ 计算不出消息 m。假

设除了 M 和 B 之外,还有其他用户(假设是 A)能从密文 σ 中得到消息 m。由于在盲签密过程中 M 给的是关于消息的哈希函数,A 想要得到消息 m 只能通过密文 σ 得到,因此 A 必须计算 W^* 和 K 才能恢复出消息 m。已知 A 拥有的值有($c,U_1,U_2,U_3,V^*,R,h,V,W,S_A$),但是 A 依然从等式 $h=H_3(U_1,U_2,U_3,t,ID_A,Q_A)$,$t=H_2(U_2,m)$ 中无法恢复消息 m,因为等式含有未知数 m 和 t。A 要求解双线性映射的逆运算是困难的,不能通过 $W^*=W^r=e(P_B,P_2Q_AQ_B)^{ar}$ 计算出 W^*。所以,除 M 和 B 知道消息 m 之外,其他用户无法得知消息 m。

4.4　公开验证性

公开验证性指在不需要 B 的私钥 S_B 的情况下,任意第三方验证者都能直接通过(U_1,U_2,U_3,V^*,h,R)验证盲签密的有效性。

任何第三方验证者从 B 处得到(U_1,U_2,U_3,V^*,h,R)并验证等式 $e(P_1U_1,V^*)=e(P^2,R+hQ_A)$ 是否成立,如果成立,验证通过;否则,该盲签密无效。在上述过程中无需 A 和 B 的私钥 S_A 和 S_B,所以本文方案具有公开验证性。

4.5　不可否认性

不可否认性指 A 如果协助 M 创建一个有效盲签名之后,就不可否认自己的盲签名。

如果 A 否认自己的盲签名时,因为本文方案具有公开验证性,任意第三方得到(U_1,U_2,U_3,V^*,h,R)并验证等式 $e(P_1U_1,V^*)=e(P^2,R+hQ_A)$ 是否成立,若成立,(U_1,U_2,U_3,V^*,h,R)是消息 m 的有效盲签名。所以接收者 B 只需公开(U_1,U_2,U_3,V^*,h,R)就可证明本文方案具有不可否认的特性,无需公开私钥 S_B。

4.6　前向安全性

前向安全性指即使 A 的私钥 S_A 意外泄漏,敌手也能恢复 A 签署消息的明文。

如果敌手已经在公开信道上截获密文(c,U_1,U_2,U_3,V^*,R),同时盲签名者 A 的私钥 S_A 意外泄漏,因为敌手不知道 B 的私钥 S_B,所以不能从 $W^*=e(U_1,PR)^{S_B}$,$K=H_2(U_1,U_2,U_3,W^*,x_BU_1,ID_B)$ 中获得对称密钥 K。如果敌手想要得到对称密钥 K,只能通过 $W^*=W^r=e(P_B,P_2Q_AQ_B)^{ar}$,$K=H_2(U_1,U_2,U_3,W^*,rP_B,ID_B)$ 得到,但等式内含 a、r、W^* 3 个未知数。因为敌手需要解决椭圆曲线离散困难问题和离散对数困难问题,所以即使拥有截获的 R、U_1、U_2、U_3,也不能通过 $R=aQ_A$,$U_1=rP$,$U_2=rR$,$U_3=rQ_A$ 计算出 a 和 r。因此,无法获得对称密钥 K,仅通过密文恢复不出明文。所以本文方案具有前向安全的特性。

4.7　不可伪造性

不可伪造性指敌手无法通过一个消息 m 伪造合法盲签密。

本文方案的签名虽然有 A 选择的随机数 a 和 A 的私钥 S_A,然而因为 A 需要解决单向散列函数的逆的困难问题,通过 $h=H_3(U_1,U_2,U_3,t,ID_A,Q_A)$,$t=H_2(U_2,m)$ 无法恢复出消息 m,并且 A 不知道 M 选择的随机数 r,所以 A 不能伪造盲签密。

如果 B 称(c,U_1,U_2,U_3,V^*,R)是来自 M 的密文,需要通过 $W^*=W^r$ 计算出 r,并伪造(U_1,U_2,U_3,V^*),使伪造数据能够通过验证。但是 B 无从得知 A 选择的随机数 a,通过 $W^*=W^r=e(P_B,P_2Q_AQ_B)^{ar}$ 计算不出 r。即使 B 已经在公开信道上截获了 W,但是需要解决双线性映射的逆的困难问题,通过 $W^*=W^r$ 计算不出 r。所以 B 不能伪造盲签密。

如果 M 想要伪造一个合法的盲签密,首先他不知道 A 的私钥 S_A,其次他不知道 A 选择的随机数 a。即使 A 的私钥 S_A 意外泄漏,M 想要通过等式 $R=aQ_A$ 计算出 a 是不可行的,因为 M 需要解决离散对数困难问题,所以 M 无法伪造盲签密。

如果任意第三方敌手想伪造合法盲签密,即使他拥有从公开信道上截获的($c,U_1,U_2,U_3,V^*,R,h,W,V,S_A,D_B$),但他不知道($s,x_B,S_B,a,r$),所以一样无法伪造盲签密。

5　效率分析

本节通过理论和数值实验进行效率分析。在理论分析中,由于现有可供查阅的文献中没有 IBC→CLC 的异构混合盲签密方案。因此,无法与同类 IBC→CLC 的异构混合盲签密方案进行效率比较。文献[26]是基于无证书的盲签密方案。比较 2 个方案的计算复杂性,主要包括 4 种运算:点乘运算(M),指数运算(E),对运算(P),异或运算(X)。由表 1 可知,在签密过程中本文方案的指数运算比文献[26]方案少 2 个,并且没有异或运算,在解签密过程中本文方案比文献[26]方案少 1 个异或运算。所以本文方案明显优于文献[26]方案。

表 1　2 种方案计算成本比较

方案	签密	解签密
文献[26]方案	$3M+4E+P+X$	$E+3P+X$
本文方案	$6M+2E+P$	$E+3P$

在数值实验分析中,利用 C 语言的 PBC 库对 IBC→CLC 的异构混合盲签密方案进行仿真模拟。在仿真过程中,群 G_1、G_2 的长度为 1 024 bit,利用的参数类型为椭圆曲线 $y^2=x^3+x \bmod q$,用户身份为 160 bit,消息取 160 bit,并且用户身份和消息随机生

成。仿真环境的配置如表 2 所示,双线性对包参数 Type 的性质如表 3 所示。

表 2 实验环境配置

参数	配置
电脑型号	HP Compaq2032
CPU	i5-2400@3.10 GHz
内存	4 GB
操作系统	Win7
虚拟机	VMware9
内核	Ubuntu2.6.35

表 3 各参数的取值

参数	取值
类型	a
基域/bit	512
Dlog 安全/bit	1 024
椭圆曲线次数	2

本文方案与文献[26]方案在通信过程中都是单消息。在数值实验分析中,本文方案的总体运行时间、签密运行时间、解签密运行时间取 50 次运行结果的平均值,如表 4 所示。

表 4 本文方案运行时间 s

类别	运行时间
总体	0.044 1
签密	0.012 7
解签密	0.001 8

为了比较本文方案和文献[26]方案在签密和解签密过程中的计算效率,对本文方案和文献[26]方案进行同样的仿真,仿真结果取 50 次运行结果的平均值,如图 1 所示,从中可以看出,本文方案的运行时间明显小于文献[26]方案的运行时间。

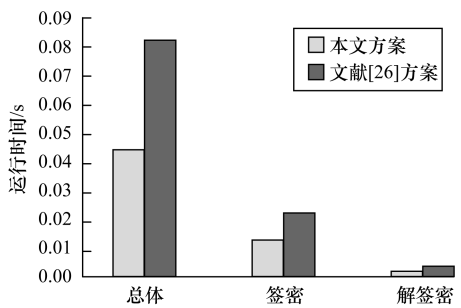

图 1 2 种方案的计算效率对比

6 结束语

现有的异构签密方案的系统主密钥的产生方式大多相同,不但不能加密任意长度的消息,而且不具备盲签密的能力。为此,本文提出一个由 IBC 到 CLC 的基于异构密码系统的混合盲签密方案。PKG 和 KGC 分别在 IBC 密码体制和 CLC 密码体制中产生各自的系统主密钥,而且具有可加密任意长消息和盲签密的能力。与现有的签密方案相比,该方案具有速度快、效率高、计算量小等特点,在随机预言模型下满足盲性、保密性、不可跟踪性、公开验证性、不可否认性、不可伪造性和前向安全性。

参考文献

[1] ZHENG Yuliang. Digital signcryption or how to achieve cost(signature & encryption) < <cost(signature) + cost(encryption)[M]. New York,USA:ACM Press,1997.

[2] 俞惠芳. 基于自认证的签密体制的研究[D]. 兰州:西北师范大学,2009.

[3] 李瑞婷. 基于双线性映射的可验证加密签名方案的研究与应用[D]. 秦皇岛:燕山大学,2010.

[4] 周才学. 几个签密方案的密码学分析与改进[J]. 计算机工程与科学,2016,38(11):2246-2253.

[5] 石 秀,张少武,夏洪平,等. 基于身份的门限签密方案的分析与设计[J]. 计算机工程与设计,2009,30(21):4858-4860.

[6] 项顺伯. 有效的基于身份的广义签密方案[J]. 广东石油化工学院学报,2012,22(4):36-39.

[7] 张 雪,冀会芳,李光松,等. 基于身份的跨信任域签密方案[J]. 计算机科学,2015,42(5):165-168.

[8] PANG Liaojun,GAO Lu,LI Huixian,et al. Anonymous multi-receiver ID-based signcryption scheme[J]. IET Information Security,2015,9(3):194-201.

[9] ZHOU Yanwei,YANG Bo,ZHANG Wenzheng. Provably secure and efficient leakage-resilient certificateless signcryption scheme without bilinear pairing[J]. Discrete Applied Mathematics,2016,204(3):185-202.

[10] 俞惠芳,赵海兴,王之仓,等. 无可信中心的自认证多代理签密方案[J]. 计算机工程与科学,2010,32(8):14-16.

[11] 陈善学,周淑贤,姚小凤,等. 高效的基于身份的代理签密方案[J]. 计算机应用研究,2011,28(7):2694-2696.

[12] 杨小东,高国娟,周其旭,等. 基于代理重签名的电子政务数据安全交换方案[J]. 计算机工程,2017,43(2):183-188.

[13] HUANG Qiong,WONG D S,YANG Guoming. Heterogeneous signcryption with key privacy[J]. Computer Journal,2011,54(4):525-536.

[14] FU Xiaotong, LI Xiaowei, LIU Wen. IDPKC-to-TPKC construction of multi-receiver signcryption [C]// Proceedings of International Conference on Intelligent Networking and Collaborative Systems. Washington D.C., USA:IEEE Press,2013:335-339.

[15] 党小超,李 琦,郝占军,等. 适用于 WSN 的在线/离线异构签密方案[J]. 计算机工程,2017,43(8):161-168.

[16] SHAMIR A. Identity-based cryptosystems and signature schemes[M]. Berlin,Germany:Springer,1984.

[17] LI Fagen, ZHANG Hui, TAKAGI T. Efficient signcryption for heterogeneous systems[J]. IEEE Systems Journal,2013,7(3):420-429.

(下转第 160 页)

$N_A=\{n_R,n_I,n_{EP},n_{EF}\}$, $E_A=\{(n_R,n_I),(n_I,n_{EP}),(n_{EP},n_{EF})\}$。$AT_A^{N_A}=\{T_R,T_I,T_{EP},T_{EF}\}$。$f_A=\{n_R\rightarrow T_R,n_I\rightarrow T_I,n_{EP}\rightarrow T_{EP},n_{EF}\rightarrow T_{EF}\}$。因此,APT-HRM 模型完全能够表示 DUQU 2.0 APT 攻击。

4 结束语

本文建立一种窃密型 APT 攻击分层表示模型 APT-HRM。APT-HRM 对 APT 攻击进行了形式化定义,将 APT 攻击分为攻击链和攻击树 2 层。攻击链各阶段有其对应的由不同攻击策略和方法组成的攻击树,只有完成当前阶段攻击树中的攻击目标才能转入下一个攻击阶段。因此,可以针对各阶段的攻击手段进行防范,以切断 APT 攻击链并最终阻止 APT 攻击。对 DUQU 2.0 APT 攻击的建模分析结果表明,该模型能够有效描述窃密型 APT 攻击行为,可为 APT 攻击的预测和防御提供参考。

参考文献

[1] ROSS R. Managing information security risk:organization, mission and information system view[EB/OL]. [2017-06-30]. https://ws680. nist. gov/publication/get _ pdf. cfm?pub_id = 908030.

[2] AUTY M. Anatomy of an advanced persistent threat[J]. Network Security,2015(4):13-16.

[3] 胡 彬,王春东,胡思琦,等. 基于机器学习的移动终端高级持续性威胁检测技术研究[J]. 计算机工程,2017,43(1):241-246.

[4] KAUR R,SINGH M. A survey on zero-day polymorphic worm detection techniques[J]. IEEE Communications Surveys and Tutorials,2014,16(3):1520-1549.

[5] 潘道欣,王轶骏,薛 质. 基于网络协议逆向分析的远程控制木马漏洞挖掘[J]. 计算机工程,2016,42(2):146-150.

[6] 张小松,牛伟纳,杨国武,等. 基于树型结构的 APT 攻击预测方法[J]. 电子科技大学学报,2016,45(4):582-588.

[7] HONG J B,KIM D S. Assessing the effectiveness of moving target defenses using security models[J]. IEEE Transactions on Dependable and Secure Computing,2016,13(2):163-177.

[8] DOHERTY S, BANERJEE D. Orchestrating software defined networks (SDN) to disrupt the APT kill chain[EB/OL]. [2017-06-30]. https://www. rsaconference. com/events/us15/agenda/sessions/1555/orchestrating-software-defined-networks-sdn-to.

[9] LI M,HUANG W,WANG Y,et al. The study of APT attack stage model[C]//Proceedings of 2016 IEEE/ACIS International Conference on Computer and Information Science. Washington D. C. ,USA:IEEE Press,2016:1-5.

[10] BREWER R. Advanced persistent threats:minimising the damage[J]. Network Security,2014(4):5-9.

[11] CHOI J,CHOI C,LYNN H M,et al. Ontology based APT attack behavior analysis in cloud computing[C]//Proceedings of the 10th International Conference on Broadband and Wireless Computing,Communication and Applications. Washington D. C., USA: IEEE Press, 2015:375-379.

[12] IOANNOU G,LOUVIERIS P,CLEWLEY N,et al. A Markov multi-phase transferable belief model: an application for predicting data exfiltration APTs[C]//Proceedings of International Conference on Information Fusion. Washington D. C., USA: IEEE Press, 2013: 842-849.

[13] KOCH R, GOLLING M, RODOSEK G D. How anonymous is the tor network? a long-term black-box investigation[J]. Computer,2016,49(3):42-49.

[14] GEHL R W. Power/freedom on the dark Web:a digital ethnography of the dark Web social network[J]. New Media and Society,2016,18(7):1219-1235.

[15] 胡 飞,范建华,魏祥麟,等. 基于节点状态跳转统计分析的干扰攻击检测算法[J]. 计算机工程,2017,43(7):156-162.

[16] GReAT. The DUQU 2.0 Technical Details[R]. Moscow, Russia:Kaspersky Lab,2015.

编辑 吴云芳

(上接第 154 页)

[18] 张玉磊,张灵刚,张永洁,等. 匿名 CLPKC-TPKI 异构签密方案[J]. 电子学报,2016,44(10):2432-2439.

[19] 刘景伟,张俐欢,孙 蓉. 异构系统下的双向签密方案[J]. 电子与信息学报,2016,38(11):2948-2953.

[20] 金春花. 新的基于身份的混合签密[D]. 西安:西安电子科技大学,2011.

[21] 俞惠芳,杨 波. 可证安全的无证书混合签密[J]. 计算机学报,2015,38(4):804-813.

[22] 苏万力,张跃宇,张晓红,等. 无证书盲签名方案[J]. 电子科技大学学报,2009,38(4):533-536.

[23] 龙士工,伍 岳,王利军. 基于门限的无可信中心的盲签名方案[J]. 计算机应用研究,2010,27(7):2657-2660.

[24] 秦晓君. 盲签名设计及其在电子商务中的应用[D]. 西安:长安大学,2011.

[25] 俞惠芳,王彩芬,王之仓. 基于 DLP 的自认证盲签密方案[J]. 计算机工程与应用,2010,46(23):119-121.

[26] 俞惠芳,王彩芬,杨 林,等. 基于无证书的盲签密方案[J]. 计算机应用与软件,2010,27(7):71-73.

[27] 宋明明,张 彰,谢文坚. 没有对运算的无证书盲签密方案[J]. 广西民族大学学报(自然科学版),2011,17(1):64-67.

编辑 顾逸斐