计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.201000002

基于认证及区块链的 CFL_BLP_BC 模型

廉文娟[1]　赵朵朵[1]　范修斌[1,2]　耿玉年[2]　范新桐[3]
1 山东科技大学计算机科学与工程学院　山东 青岛 266590
2 中国科学院软件研究所青岛分部　山东 青岛 266114
3 曲阜师范大学计算机学院　山东 日照 276800
(skd991457@sdust.edu.cn)

摘　要　5G 时代的到来给新兴信息产业的信息安全问题带来了新的挑战,现有的安全技术已不能满足 5G 时代下特定场景对毫秒级认证、可信认证等的相关需求。因此,以 CFL 技术为信息安全原点技术,提出了 CFL_BLP_BC 模型。CFL_BLP_BC 模型在局部修改原 BLP 模型安全公理的基础上,结合区块链技术对该模型的基本元素、安全公理和状态转换规则进行了形式化描述。该模型不仅支持信息安全五性,而且具有毫秒级、指令级、实证制等信息安全属性。该模型支持内生安全、先天免疫、主动防御技术,可为当今网络空间新兴信息产业提供重要的理论指标。

关键词:可信认证;CFL 认证体制;区块链;BLP 模型
中图法分类号　TP399

CFL_BLP_BC Model Based on Authentication and Blockchain

LIAN Wen-juan[1],ZHAO Duo-duo[1],FAN Xiu-bin[1,2],GENG Yu-nian[2] and FAN Xin-tong[3]
1 College of Computer Science & Engineering,Shandong University of Science and Technology,Qingdao,Shandong 266590,China
2 Qingdao Branch,Institute of Software,Chinese Academy of Sciences,Qingdao,Shandong 266114,China
3 School of Computer Science,Qufu Normal University,Rizhao,Shandong 276800,China

Abstract　The coming of 5G era brings new challenges to the information security of emerging information industries. The existing security technologies can't meet the requirements of millisecond level authentication and trusted authentication for specific scenarios in 5G era. Therefore,CFL technology is taken as the origin technology of information security. Based on the local modification of the security axioms of the original BLP model,combined with the Blockchain technology,CFL_BLP_BC model formally describes the basic elements,security axioms and state transition rules of the model. The model can support the construction of five aspects of information security,and has the attributes of millisecond level,instruction level and empirical system. The model belongs to endogenous safety,innate immunity and active defense technology. The model can provide important theoretical guidance for the emerging information industry.

Keywords　Trusted authentication,CFL authentication system,Blockchain,BLP model

1　引言

2015 年,国际电信联盟(International Telecommunication Union,ITU)在 ITU-RM.2083-0 建议书[1]中确定了 5G 的愿景,并在建议书中明确了 5G 支持的 3 大应用场景,包括增强型移动宽带(enhanced Mobile Broadband,eMBB)、大规模机器类型通信(massive Machine Type Communications,mMTC)以及超可靠和低延迟通信(ultra Relaible & Low Latency Communication,uRLLC)。mMTC 可连接大量设备,支撑百万级低功耗物联网设备终端的连接服务,满足智能家居、智能城市等大规模智能设备的通信问题[1-2]。新的使用案例、商业模式、技术和架构的引入,以及对隐私问题的日益关注,使得 5G 信息安全更具挑战性[3]。

许多低成本的 mMTC 设备在计算能力、能量支持、内存能力、安全物理结构方面都有局限性,这增大了大规模受损设备被劫持以对 5G 网络发起协同拒绝服务(Denial of Service,DoS)攻击的风险。许多 uRLLC 应用都涉及到人类的生命安全,且易受无线电干扰攻击和风暴信号攻击[3],因此 5G 需要有更高的吞吐量、更低的延迟、超高的可靠性、更大的连接密度和更高的移动范围来确保各应用的安全性,故迫切需要满足毫秒级的身份认证机制、轻量级的密码算法和更强大的信息安全技术。

到稿日期:2020-10-02　返修日期:2020-12-18　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:青岛市社科规划项目(QDSKL2001156)
This work was supported by the Qingdao Social Science Planning Project(QDSKL2001156).
通信作者:范修斌(fanxiubin1966@sina.com)

Gunther 等[4]讨论了 5G 网络的安全需求和策略；Samant 等[5]从高层次角度研究了 5G 用户隐私问题；Dirk 等[6]从数据平面的角度讨论了 5G 网络的安全性和性能。还有很多关于特定 5G 技术或领域的安全解决方案的讨论，但是以往的这些研究都局限于一定的视角或非广泛范围的解决方案，没有一种普适的 5G 安全解决方案。文献[7]指出了当今网络空间信息安全需要首先解决的认证问题，同时指出了目前的认证技术分为函数认证和参数认证，参数认证技术包括指纹、虹膜、刷脸等，因没有香农熵，其本质上不具有信息安全功能，函数认证技术包括公钥基础设施（Public Key Infrastructure，PKI）、基于标识的密码体系（Identity-Based Cryptograph，IBC），PKI 和 IBC 由于自身结构的原因，无法满足毫秒级的响应需求，在当今网络空间遇到了挑战。

本文提出了一种适用于 5G 环境下各新兴信息产业的信息安全模型——CFL_BLP_BC 模型。其中，CFL 是基于标识的证书认证体制，由 Chen 等发明且获得了国家认可[7]，该认证体制无需第三方参与，可实现毫秒级的认证。文献[8]给出的 CFL_BLP 模型是基于 CFL 的系统操作机密性模型，但是缺乏完整性保护方法。本文进一步给出了 CFL_BLP_BC 模型，同时根据实际需求局部修改了原 BLP 安全公理。CFL_BLP_BC 模型具有毫秒级、指令级、实证制等信息安全属性，支持内生安全、先天免疫、主动防御、可信计算等，在理论上可为当今网络空间的信息安全建设提供重要的指导作用，特别是针对 5G 等新兴信息产业。

2 基本知识

（1）CFL 认证体制

CFL 是具有我国自主知识产权的首个基于标识的证书认证体制，是证书认证技术 PKI 和标识认证技术 IBC 的继承和发展，同时规避了两种认证体制的不足，是当今网络空间的信息安全原点技术，有效解决了各新兴信息产业发展过程中遇到的有信息安全认证方面共性的“卡脖子问题”[7]。

CFL 具有以下安全性质：

性质 1[9-10] CFL 在理论上满足可证明在安全，在应用中满足零知识交互，即 CFL 的理论和应用都是安全的。

性质 2[7,11-12] CFL 证书在应用过程中不依赖第三方，可直接认证、现场认证、动态认证、进程认证、自主认证。

性质 3[7,11-12] CFL 一人一钥、防内鬼。

性质 4[7,11-12] CFL 支持毫秒级安全、指令级安全。

性质 5[8] CFL 支持 BLP 模型，即 BLP 模型的范畴权限可以作为 CFL 证书中的部分标识，即 CFL 可以支持基于 BLP 模型的操作机密性保护。

性质 6[13] CFL 支持 BC 模型，即 CFL 可以作为区块链的认证技术，与区块链的无中心相匹配。

CFL 技术在“一带一路”沿线的相关国家得到了重要应用，并获得了充分肯定。同时，在我国相关部门、相关单位、企业、大学、个人等中得到了广泛应用。

（2）BLP 模型

BLP 模型[14]是由 Bell 等于 1973 年提出的，该模型解决的本质问题是对具有密级划分的信息的访问控制。BLP 模型是对安全策略形式化的第一个数学模型，同时也是我国等级保护标识级以上级的核心模型，被广泛应用于描述计算机系统的安全问题。BLP 模型从“访问控制”的角度研究如何既保证主体能有效地访问客体，又使得系统的安全性不会遭到破坏的性质和规则，是一种在计算机系统内实施多级安全策略的访问控制模型，通过制定主体对客体的访问规则和操作权限来保证系统的安全性。

BLP 模型有两大特点，简单安全特性（不向上读，即下读），即一个主体只能读一个低级别或相同安全级别的对象；* 特性（不向下写，即上写），即一个主体只能写一个高级别或相同安全级别的对象。BLP 模型的“下读上写”为信息系统提供了机密性保护，但对完整性的保护不足。文献[8]给出了 CFL_BLP 模型，通过 CFL 和 BLP 模型的结合，保证了用户的 BLP 模型权限的完整性，同时也保证了 BLP 模型的可信性、安全性，在防范隐蔽信道的基础上实现了自主可控、满足高等级安全的信息系统。

（3）区块链

区块链（Blockchain，BC）最早由中本聪（Satoshi Nakamoto）提出[15-16]，是一种基于非对称加密算法的分布式基础设施和计算范式。区块链以高效、透明的方式记录所有交易信息，数据安全性高。区块链将数据分成不同的区块，区块通过前一区块哈希值链接到前一个区块，以呈现一组完整的连续数据。如图 1 所示，每个数据块通常包含两部分，区块头和区块体。

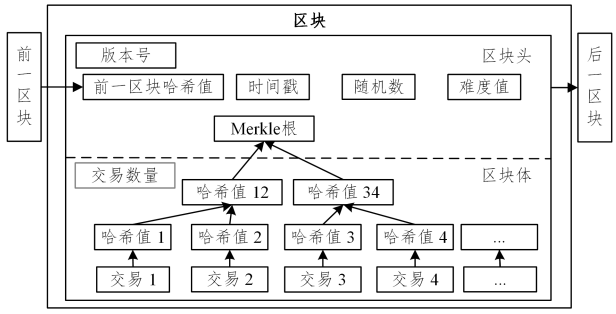

图 1 区块链数据结构

Fig. 1 Blockchain data structure

区块头中存储了当前版本号、前一区块的哈希值、时间戳、随机数、难度值和 Merkle 根[17]信息，区块通过哈希值链接到前一区块以形成链。区块体包括当前块中的事务数以及在块创建期间生成的所有已验证的事务记录。这些记录通过 Merkle 树的散列过程生成唯一的 Merkle 根，并将其记录在区块头中。数据块按时间顺序组合成一种特殊的数据结构，时间戳作为区块数据的存在性证明（proof of existence），可确保数据不被篡改或伪造[18]。区块链是实现静态完整性和动态完整性保护的当代技术，具有去中心化、匿名性、可审计性、可追溯等特性，可保护指令程序和文件等数据的完整性。文献[13，19-20]指出，CFL 可与区块链相结合，并可充分支持区块链中的认证。

（4）CFL_BLP 模型

文献[8]给出了 CFL_BLP 模型，定义了八元组。

定义 1[8] CFL_BLP 模型即为 $t\in T=\{0,1,2,\cdots,t,\cdots\}=N$ 时刻计算机系统 SY_t 的一个八元组，$SY_t=(S_t,O_t,RA,A,$

$D, M_t, BLP(S_t, O_t), CFL)$。

但 CFL_BLP 模型缺乏完整性保护方法，因此我们必须创设新的模型。

1977 年，Biba 提出了 Biba 模型，并发表于 Mitre 公司，它是与 BLP 模型对偶的完整性保护模型，正是由于两个模型的对偶性，使得同一个主体的两个模型的权限标识不具有独立性。因此，我们必须寻找新的完整性保护模型与 BLP 模型有机结合。经过探索，我们发现区块链模型可与 BLP 模型进行有机结合，由 CFL 的性质 5、性质 6 可知，CFL 支持 BLP 模型和区块链模型。为此，我们给出了 CFL_BLP_BC 模型。

3 CFL_BLP_BC 模型

3.1 CFL_BLP_BC 定义

CFL_BLP_BC 模型在 CFL_BLP 模型的基础上进行了元组改进和扩充，给出了新的定义。

定义 2 CFL_BLP_BC 模型即为 $t \in T = \{0, 1, 2, \cdots, t, \cdots\}$ 时刻计算机系统 SY_t 的一个 9 元组，即 $SY_t = (CFL, S_t, O_t, RA, A, D, \boldsymbol{M}_t, BLP(S_t, O_t), BC_t)$。

(1)CFL：实现 CFL_BLP_BC 模型中的 CFL 签名验证，CFL 的数据格式如下：

1)CFL 签名文件：明文 ‖ 创建者的 CFL 证书 ‖ 时间戳 ‖ 签名. 文件. cfl_sign。

2)CFL 对称加密文件：密文(明文格式为文件. cfl_sign) ‖ 创建者的 CFL 证书 ‖ 时间戳 ‖ 签名. 文件. cfl_bcipher。

3)CFL 电子信封文件：密文(明文格式为文件. cfl_sign) ‖ 创建者的 CFL 证书 ‖ 接收者的 CFL 证书 ‖ 时间戳 ‖ 签名. 文件. cfl_pcipher。

注：CFL 证书中都含有 BLP 权限标识，加密和签名使用了国产密码算法，包括公钥密码算法 SM2、分组密码算法 SM4 和密码杂凑算法 SM3。文献[7]证明纯软件算法本质上不具有信息安全功能，而 CFL_BLP_BC 模型中的密码算法是在硬件黑盒中实现的，保障了高效的边缘计算。

在系统中主体必须通过 CFL 证书认证后，才有权对客体进行访问操作，根据主体 CFL 证书中 BLP 模型的权限标识，确定主体的访问权限，再执行主体对客体的访问操作，操作过程包括 CFL_BLP_BC 模型中的请求、模型给出的请求回答、允许访问的方式等。

(2)$S_t^{[8,14]}$：$S_t = \{s_{t,i}\}_{i \in N}$，即 t 时刻计算机系统 SY_t 的所有主体，包括用户、设备、进程等。$S_t = S_t^c \cup S_t^{\bar{c}}$，其中 S_t^c 为 CFL_BLP_BC 模型中带 CFL 证书的主体，$S_t^{\bar{c}}$ 为 CFL_BLP_BC 模型中未带 CFL 证书的主体。

(3)$O_t^{[8,14]}$：$O_t = \{o_{t,j}\}_{j \in N}$，即 t 时刻计算机系统 SY_t 的所有客体，它是一个树型结构，指一系列的对象或资源，如数据、文件、程序、存储器等。$O_t = O_t^c \cup O_t^{\bar{c}}$，其中 O_t^c 为 CFL_BLP_BC 模型中带创建者 CFL 签名的客体，$O_t^{\bar{c}}$ 为 CFL_BLP_BC 模型中未带创建者 CFL 签名的客体。

(4)$RA^{[8,14]}$(Request Access)：

$RA = \{$get, release, give, rescind, change, create, delete$\}$

它是主体向系统发出请求命令的集合，下面对 7 种请求方式进行详细介绍。

1)get：

①在 t 时刻的主体集合中添加一个主体，并且给该主体赋值 BLP 一般权限。

②在 t 时刻的主体集合中添加一个主体，并且给该主体赋值 BLP 当前权限。

③在 t 时刻的客体集合中添加一个客体，并且给该客体赋值 BLP 权限。

2)$release$：

①从 t 时刻 BLP 模型主体中删除一个主体。

②从 t 时刻 BLP 模型客体中删除一个客体。

3)$give$：扩充 M_t 某点集合中的元素。

4)$rescind$：删减 M_t 某点集合中的元素。

5)$change$：更改 BLP 模型客体安全级，或 BLP 模型主体当前安全级。

6)$create$：创建一个新客体添加到当前的客体树型结构中，并给 BLP 权限以及自主访问控制矩阵赋值。

7)$delete$：从树型结构中删除一个客体，从而删除相关 BLP 赋值以及自主访问控制矩阵赋值。

(5)$A^{[8,14]}$：$A = \{\underline{e}, \underline{r}, \underline{a}, \underline{w}, \underline{c}\}$，即主体访问客体的访问方式的集合，其中：

1)$\underline{e}$：$execute$，执行(neither observantion nor alteration)。

2)$\underline{r}$：$only\ read$，只读(observation with no alteration)。

3)$\underline{a}$：$append$，只写(alteration with no observation)。

4)$\underline{w}$：$read\ and\ write$，读写(both observation and alteration)。

5)$\underline{c}$：$control$，指某主体用来授予或撤销另一主体对某客体的访问权限的能力。

(6)$D^{[8,14]}$：$D = \{yes, no\}$，系统接收到主体对客体的请求访问操作后，对请求访问操作进行判定，D 为判定结果集合，其中：

1)yes：表示请求被执行。

2)no：表示请求被拒绝。

(7)$\boldsymbol{M}_t^{[8,14]}$：即 t 时刻自主访问控制矩阵。其中的点是某主体对某客体可操作的集合，它是一个超矩阵。

当 $\forall\, m_{t,i,j} \subseteq A, 1 \leqslant i \leqslant \alpha_t, 1 \leqslant j \leqslant \gamma_t$ 时，$\boldsymbol{M}_t$ 为：

$$\boldsymbol{M}_t = \begin{pmatrix} m_{t,1,1}, & m_{t,1,2}, & m_{t,1,3}, & \cdots, & m_{t,1,\gamma_t} \\ m_{t,2,1}, & m_{t,2,2}, & m_{t,2,3}, & \cdots, & m_{t,2,\gamma_t} \\ m_{t,3,1}, & m_{t,3,2}, & m_{t,3,3}, & \cdots, & m_{t,3,\gamma_t} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ m_{t,\alpha_t,1}, & m_{t,\alpha_t,2}, & m_{t,\alpha_t,3}, & \cdots, & m_{t,\alpha_t,\gamma_t} \end{pmatrix}$$

其中，α_t 是 CFL_BLP_BC 模型在 t 时刻的主体集合的个数，γ_t 是 CFL_BLP_BC 模型在 t 时刻的客体集合的个数。

$\boldsymbol{M}_t$ 的性质如下：

$$\forall\, i, m_{t,i,\beta_t+1} = \varnothing, \begin{pmatrix} m_{t,1,1}, & m_{t,1,2}, & m_{t,1,3}, & \cdots, & m_{t,1,\gamma_t} \\ m_{t,2,1}, & m_{t,2,2}, & m_{t,2,3}, & \cdots, & m_{t,2,\gamma_t} \\ m_{t,3,1}, & m_{t,3,2}, & m_{t,3,3}, & \cdots, & m_{t,3,\gamma_t} \\ \vdots & \vdots & \vdots & & \vdots \\ m_{t,\alpha_t,1}, & m_{t,\alpha_t,2}, & m_{t,\alpha_t,3}, & \cdots, & m_{t,\alpha_t,\gamma_t} \end{pmatrix}$$

$$=\begin{pmatrix} m_{t,1,1}, & m_{t,1,2}, & m_{t,1,3}, & \cdots, & m_{t,1,\alpha_t}, & m_{t,1,\gamma_t+1} \\ m_{t,2,1}, & m_{t,2,2}, & m_{t,2,3}, & \cdots, & m_{t,2,\alpha_t}, & m_{t,2,\gamma_t+1} \\ m_{t,3,1}, & m_{t,3,2}, & m_{t,3,3}, & \cdots, & m_{t,3,\alpha_t}, & m_{t,3,\gamma_t+1} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ m_{t,\alpha_t,1}, & m_{t,\alpha_t,2}, & m_{t,\alpha_t,3}, & \cdots, & m_{t,\alpha_t,\beta_t}, & m_{t,\alpha_t,\gamma_t+1} \end{pmatrix}$$

(8)$BLP(S_t,O_t)^{[8,14]}$：

$$BLP(s_{t,i},o_{t,j})=((f(s_{t,i}),f_c(s_{t,i})),f(o_{t,j}))$$
$$=(((C(s_{t,i}),K(s_{t,i})),$$
$$(C_c(s_{t,i}),K_c(s_{t,i}))),(C(o_{t,j}),K(o_{t,j})))$$

注：$C^{[8,14]}$：$C=\{c_1,c_2,\cdots,c_q\}$，其中$c_1>c_2>\cdots>c_q$，一个主体或客体的密级一般分为公开文件、内部文件、秘密文件、机密文件、绝密文件等级。$K^{[8,14]}$：$K=\{k_1,k_2,\cdots,k_r\}$，即主客体组织机构隶属关系，显然其满足偏序关系，如某单位一处包含一处一科、一处二科、一处三科等。BLP 安全级集合定义为 $F=C\times K$，同理可知，其也满足偏序关系。

1)$f(s)=(C(s),K(s))$：称其为主体 s 的 BLP 模型一般安全级函数。

2)$f(o)=(C(o),K(o))$：称其为客体 o 的 BLP 模型安全级函数。

3)$f_c(s)=(C_c(s),K_c(s))$：称其为主体 s 的 BLP 模型当前安全级函数。

4)$(C(s),K(s))>(C(o),K(o))\Leftrightarrow((C(s)\geqslant C(o)),$
$K(s)>K(o))$

5)$(C(s),K(s))=(C(o),K(o))\Leftrightarrow((C(s)=C(o)),K(s)$
$=K(o))$

若主体没有当前临时安全级赋值，则：

$$BLP(s_{t,i},o_{t,j})\triangleq(f(s_{t,i}),f(o_{t,j}))=((C(s_{t,i}),K(s_{t,i})),$$
$$(C(o_{t,j}),K(o_{t,j})))$$

在具体应用时，权限码中设置了具体的人员分类标识，即管理员、单位职员等，根据组织结构隶属关系进行分层赋值，按照实际情况进行逐层权限的赋值以及权限码的设置，实现权限区分，防止越权操作。

注：当前和一般分别判断后的结果是并集关系，当前的判断与$\boldsymbol{M}_t$是交集关系，一般的判断与$\boldsymbol{M}_t$是交集关系，最后的结果是前两个交集关系的并集。

(9)BC_t：为 t 时刻 CFL_BLP_BC 模型中的区块链。

BC_t定义为七元组：

定义 3

$$BC_t=(ip,fpath,fname,ftime,CFLcertificate,info,$$
$$timestamp,CFLsignature)$$

本文用$BC_t=BC_{t,1}\parallel BC_{t,2}\parallel BC_{t,3}\parallel\cdots\parallel BC_{t,l}=\bigcup_{i=1}^{l}BC_{t,i}$来表示 CFL_BLP_BC 模型中 t 时刻的整个区块链。其中，$BC_{t,i}$为 t 时刻区块链中第 i($i=1,2,\cdots,l$)个区块。记d_j，$j=1,2,\cdots,n_l$为区块链的第 j 条入链数据，若d_j是区块 $BC_{t,k}$中的数据，$k\in\{1,2,\cdots,l\}$，记$d_j\in'BC_{t,k}$，也可记$d_j\in'BC_t$，符号$\in'$为本文描述数据与区块/区块链关系以及其他所属关系的特定符号。

假设每个区块存储 100 条数据，则 BC_1 的数据$n_1=100$，BC_2的数据$n_2=200$，然后以此类推到数据n_l，区块链总数据为$\sum_{i=1}^{l}n_i$，区块链大小可根据具体的应用而定。

表 1 以 IPV6 为例，给出了 CFL_BLP_BC 模型中 BC 的介绍。

表 1 CFL_BLP_BC 模型中区块链的内容

Table 1 Blockchain content in the CFL_BLP_BC model

区块号	数据号	ip	fpath	fname	ftime	CFL certificates info	time stamp	CFL signature
BC_1	1	IP 地址	文件路径	文件名	文件创建时间	入链者的 CFL 证书信息	时间戳	文件建立者的 CFL 签名
	2	IP 地址	文件路径	文件名	文件创建时间	入链者的 CFL 证书信息	时间戳	文件建立者的 CFL 签名
	…	…	…	…	…	…	…	…
	n_1					区块链签名者的 CFL 证书信息	时间戳	区块累计 CFL 签名
…	…	…	…	…	…	…	…	…
BC_{k-1}	$\sum_{i=1}^{k-1}n_i$					区块链签名者的 CFL 证书信息	时间戳	文件建立者的 CFL 签名
BC_k	$n_{k-1}+1$	IP 地址	文件路径	文件名	文件创建时间	入链者的 CFL 证书信息	时间戳	文件建立者的 CFL 签名
	$n_{k-1}+2$	IP 地址	文件路径	文件名	文件创建时间	入链者的 CFL 证书信息	时间戳	文件建立者的 CFL 签名
	…	…	…	…	…	…	…	…
	$\sum_{i=1}^{k}n_i$					区块链签名者的 CFL 证书信息	时间戳	区块累计 CFL 签名
…	…	…	…	…	…	…	…	…
BC_l	$n_{l-1}+1$	IP 地址	文件路径	文件名	文件创建时间	入链者的 CFL 证书信息	时间戳	文件建立者的 CFL 签名
	$n_{l-1}+2$	IP 地址	文件路径	文件名	文件创建时间	入链者的 CFL 证书信息	时间戳	文件建立者的 CFL 签名
	…	…	…	…	…	…	…	…
	$\sum_{i=1}^{l}n_i$					区块链签名者的 CFL 证书信息	时间戳	区块累计 CFL 签名

文献[13,19-21]指出了 CFL 是应用无中心的认证技术，从而证明了 CFL 是唯一匹配实证制条件下区块链的认证体制，因此，CFL_BLP_BC 模型中区块链是高可用的区块链，其中累计区块签名权遵从权益证明。

为描述 CFL_BLP_BC 的安全公理以及状态转换规则，首先给出以下说明：

令S_t^T为 CFL_BLP_BC 模型中遵从简单特性的主体集合，即 BLP 可信集合。

令S_t^*为 CFL_BLP_BC 模型中遵从 * 特性的主体集合，即 BLP 非可信主体集合。

令$s_{t,\text{agent}}$为 CFL_BLP_BC 管理平台的代理主体，$s_{t,\text{agent}}\in S_t^c$，若$S_t^c$中主体对客体进行访问操作，代理主体要对主体进行 CFL 动态证书验证。

令$s_{t,i}^{\text{secure manage}}$为 CFL_BLP_BC 模型中的安全管理员，

$s_{t,i}^{\text{secure manage}} \in S_t^c$。

在 CFL_BLP_BC 模型中，记 $S_t^T \cup S_t^* = S_t^c$，S_t^c 为 CFL 客户端集合，包括带 CFL 证书的人、服务器、进程等，即 CFL_BLP_BC 模型中带 CFL 证书的主体。

用 $CFL_{s_{t,i}}$ 表示主体 $s_{t,i}$ 的 CFL 证书，这些主体对应 CFL_BLP_BC 模型中的简单特性。

用 $CFL_{s_{t,i}}^{cu}$ 表示主体 $s_{t,i}$ 当前(current)临时的 CFL 证书，它对应于 BLP 模型中的当前临时权限。这些主体对应 CFL_BLP_BC 模型中的 * 特性。

用 $CFL_{o_{t,j}}$ 表示客体 $o_{t,j}$ 的 CFL 证书。主体的 CFL 证书验证通过后，主体验证客体的 CFL 动态签名，验证通过后才能对客体进行读、写等操作。

令 $\beta_t = \{(s_{t,i}, o_{t,j}, \underline{x}) \mid s_{t,i} \in S_t, o_{t,j} \in O_t, \underline{x} \subseteq A\}$，由此可知 β_t 由 $\boldsymbol{M}_t$ 决定。

令 $b(s_{t,i}:\underline{x_1}, \underline{x_2}, \cdots, \underline{x_n})$ 为 BLP 模型中主体 $s_{t,i}$ 具有访问权限 x_1，或者有 x_2，…($1 \leqslant i \leqslant n$)访问客体的集合，其中 $\{\underline{x_1}, \underline{x_2}, \cdots, \underline{x_n}\} \subseteq A$。

$b(s_{t,i}:\underline{x_1}, \underline{x_2}, \cdots, \underline{x_n})$ 为：

$$b(s_{t,i}:\underline{x_1}, \underline{x_2}, \cdots, \underline{x_n}) = \bigcup_{1 \leqslant l \leqslant n} b(s_{t,i}:\underline{x_l})$$
$$= \bigcup_{1 \leqslant l \leqslant n} \{O \in O_t \mid s_{t,i} \text{ can access it by } \underline{x_l} \text{ under ther rule of BLP model}\}$$

记 BLP_t 为 t 时刻的所有 BLP 模型所涉及的主客体以及范畴属性。表 2 统一阐述了上述 CFL_BLP_BC 模型中各元组以及其他符号。

表 2 CFL_BLP_BC 模型的符号说明

Table 2 CFL_ BLP_ BC model symbol description

符号	说明
S_t	t 时刻计算机系统的所有主体
O_t	t 时刻计算机系统的所有客体
RA	主体发给系统的请求命令集合
A	主体访问客体的访问方式集合
D	系统判定主体对客体请求的结果集合
$\boldsymbol{M}_t$	t 时刻自主访问控制矩阵
$BLP(S_t, O_t)$	t 时刻主体和客体的分级分类强制访问控制
BC_t	t 时刻 CFL_BLP_BC 模型中的区块链
S_t^c	CFL 客户端集合
$S_t^{\bar{c}}$	CFL_BLP_BC 模型中未带 CFL 证书的主体
O_t^c	CFL_BLP_BC 模型中带创建者 CFL 签名的客体
$O_t^{\bar{c}}$	CFL_BLP_BC 模型中未带创建者 CFL 签名的客体
S_t^T	BLP 可信集合
S_t^*	BLP 非可信主体集合
$s_{t,\text{agent}}$	CFL_BLP_BC 管理平台的代理主体
$s_{t,i}^{\text{secure manage}}$	CFL_BLP_BC 模型中的安全管理员
$CFL_{s_{t,i}}$	主体的 CFL 证书
$CFL_{o_{t,i}}$	客体的 CFL 证书
$CFL_{s_{t,i}}^{cu}$	主体当前临时的 CFL 证书
β_t	BLP 模型下主体以某访问方式访问客体的集合
$b(s_{t,i}:\underline{x_1}, \cdots, \underline{x_n})$	BLP 模型下主体以多访问方式访问客体的集合
$WNG8$	物理噪声源
r/r'	随机数序列

下文参照文献[8,22-23]中的分析方法，给出了 CFL_BLP_BC 模型的安全公理。

3.2 CFL_BLP_BC 安全公理

公理 1 CFL_BLP_BC 模型安全根生成公理：

CFL 发证机关中的物理噪声源 $WNG8$ 安全生成 CFL 发证机关硬件中的独立随机数序列，用这些随机数序列独立生成 CFL 发证机关安全根 $r=(r_1, r_2, r_3, \cdots, r_n)$，它是二元域上独立均匀分布的随机变量序列。

$WNG8$ *generates* r, $r=(r_1, r_2, r_3, \cdots, r_n)$

公理 2 CFL_BLP_BC 模型客户端密钥安全生成公理：CFL 客户端中的物理噪声源安全生成 CFL 客户端硬件中的独立随机数序列 $r'=(r_1', r_2', r_3', \cdots, r_m')$，用这些随机数序列生成独立的 CFL 客户端 SM2 工作私钥集、SM4 工作密钥集，并由此派生 SM2 工作公钥集。

$WNG8$ *generates* r', $r'=(r_1', r_2', r_3', \cdots, r_m')$, r' generates SM2 Working Private Key set, r' generates SM4 Working Secret Key set

公理 3 CFL_BLP_BC 模型证书发放公理：网络空间中的每个客户端主体都具有 CFL 发证机关实证发放的静态 CFL 证书，其中包含一部分当前临时证书。

$\forall s_{t,i}^c \in S_t^c \subseteq S_t$, CFL issuing authority gives a CFL certificate to $s_{t,i}^c$

公理 4 CFL_BLP_BC 模型客户端主体随身携带 CFL 证书或临时 CFL 证书公理：每个客户端主体 $s_{t,i}^c$ 都带有 CFL 证书标识自己的身份，并在任何一次访问客体时，由客体相应的 CFL_BLP_BC 管理平台的代理主体对该主体进行 CFL 动态证书验证。

$\forall t \in T, \forall s_{t,i}^c \in S_t^c \subseteq S_t$, if $s_{t,i}^c$ accesses $o_{t,j}$, then $\exists\, s_{t,\text{agent}}(o_{t,j}), s_{t,\text{agent}}(o_{t,j}): Verify(CFL_{s_{t,i}^c})$

其中，$s_{t,\text{agent}}(o_{t,j})$ 为 $o_{t,j}$ 对应的代理主体。

公理 5 CFL_BLP_BC 模型中任何客体都带有相应创建者的 CFL 签名公理：

$\forall o_{t,j} \in O_t, \exists\, s_{t,i}^c \in S_t^c \subseteq S_t, o_{t,j} = \text{file} \parallel CFL_{o_{t,j}} \parallel \text{time stamp} \parallel sign_{s_{t,i}^c, o_{t,j}}$

其中，$sign_{s_{t,i}^c, o_{t,j}} = s_{t,i}^c$ sign to $o_{t,j}$，表示主体 $s_{t,i}^c$ 对客体 $o_{t,j}$ 的签名。

公理 6 CFL_BLP_BC 模型中给特殊主体配发当前临时 CFL 证书公理。

公理 7 CFL_BLP_BC 模型完整性管理公理：

(1)CFL_BLP_BC 管理平台的代理主体验证主体的 CFL 证书，验证通过后，执行下一步操作；

(2)区块链签名者验证主体的 CFL 证书，对访问主体对应的 BLP 权限、自主访问控制权限进行析取，比对区块链中相应数据的权限，确定权限具有访问资格后，进行下一步操作；

(3)主体检验响应数据的动态签名完整性，验证通过后，主体对数据进行访问。

公理 8 CFL_BLP_BC 模型的简单安全性公理(简单特性公理)：

$\forall s_{t,i} \in S_t^T$, if $s_{t,agent}: Verify(CFL_{s_{t,i}}) = \text{success}$ then:

(i) $b(s_{t,i}:\underline{e}) = \{o_{t,j} \in O_t \mid s_{t,i} \text{ can access it by } \underline{e} \text{ under the rule of BLP model}\}$

$\Leftrightarrow s_{t,i}: Verify(sign_{s_{t,i}, o_{t,j}}) = success, o_{t,j} \in b(s_{t,i}:\underline{e})$

$\Leftrightarrow f(s_{t,i}) \geqslant f(o_{t,j})$

文献[7-8,14]中，该公理对执行$\underline{e}$的描述为：只要是 BLP 可信主体(满足 BLP 简单公理的主体)都能对某命令进行执行。但是，实践中即使是 BLP 可信主体也可能误操作，如 BLP 可信主体执行了误删除且造成了严重损失。因此，本文对执行命令进行了 BLP 强制访问控制。

(ii)$b(s_{t,i}:\underline{a})=\{o_{t,j}\in O_t \mid s_{t,i}$ can access it by $\underline{a}$ under the rule of BLP model$\}$

$\Leftrightarrow s_{t,i}:Verify(sign_{s_{t,i},o_{t,j}})=success, o_{t,j}\in b(s_{t,i}:\underline{a})$

$\Leftrightarrow f(s_{t,i})\prec f(o_{t,j})$

(iii)$b(s_{t,i}:\underline{r})=\{o_{t,j}\in O_t \mid s_{t,i}$ can access it by $\underline{r}$ under the rule of BLP model$\}$

$\Leftrightarrow s_{t,i}:Verify(sign_{s_{t,i},o_{t,j}})=success, o_{t,j}\in b(s_{t,i}:\underline{r})$

$\Leftrightarrow f(s_{t,i})\succ f(o_{t,j})$

(iv)$b(s_{t,i}:\underline{w})=\{o_{t,j}\in O_t \mid s_{t,i}$ can access it by $\underline{w}$ under the rule of BLP model$\}$

$\Leftrightarrow s_{t,i}:Verify(sign_{s_{t,i},o_{t,j}})=success, o_{t,j}\in b(s_{t,i}:\underline{w})$

$\Leftrightarrow f(s_{t,i})=f(o_{t,j})$

公理 9　CFL_BLP_BC 模型的 * 特性公理(* 特性公理)：

$\forall s_{t,i}\in S_t^*$，if $s_{t,\text{agent}}:Verify(CFL_{s_{t,i}}^{cu})=$success，then：

(i)b$(s_{t,i}:\underline{a})=\{o_{t,j}\in O_t \mid s_{t,i}$ can access it by $\underline{a}$ under the rule of BLP model$\}$

$\Leftrightarrow s_{t,i}:Verify(sign_{s_{t,i},o_{t,j}})=success, o_{t,j}\in b(s_{t,i}:\underline{a})$

$\Leftrightarrow f(o_{t,j})\succ f_c(s_{t,i})$

(ii)$b(s_{t,i}:\underline{w})=\{o_{t,j}\in O_t \mid s_{t,i}$ can access it by $\underline{w}$ under the rule of BLP model$\}$

$\Leftrightarrow s_{t,i}:Verify(sign_{s_{t,i},o_{t,j}})=success, o_{t,j}\in b(s_{t,i}:\underline{w})\Leftrightarrow f(o_{t,j})=f_c(s_{t,i})$

(iii)$b(s_{t,i}:\underline{r})=\{o_{t,j}\in O_t \mid s_{t,i}$ can access it by $\underline{r}$ under the rule of BLP model$\}$

$\Leftrightarrow s_{t,i}:Verify(sign_{s_{t,i},o_{t,j}})=success, o_{t,j}\in b(s_{t,i}:\underline{r})$

$\Leftrightarrow f_c(s_{t,i})\succ f(o_{t,j})$

公理 10　CFL_BLP_BC 模型自主安全性公理：

if $s_{t,\text{agent}}:Verify(CFL_{s_{t,i}})=success$,

if $s_{t,i}:Verify(sign_{s_{t,i},o_{t,j}})=success$，then：

$(s_{t,i},o_{t,j},\underline{x})\in\beta_t\Leftrightarrow\underline{x}\in m_{t,i,j}$

公理 11　CFL_BLP_BC 模型兼容性公理：

$\forall o_{t,j},o_{t,i}\in O_t, o_{t,j}\in H(o_{t,i})\Leftrightarrow f(o_{t,j})\succ f(o_{t,i})$

注：$H(o_{t,i})$指以客体$o_{t,i}$为根节点的子节点的集合，客体层次结构保持兼容性。该特性适用于客体的树形层次结构，客体的安全级别沿树叶方向增加，其兼容性在于与操作系统的目录结构兼容[14]。如管理文件时，某主体可以看见目录，可以进入目录，但是却不一定能够打开目录内的文件。

公理 12　敏感材料 CFL 对称密码算法加密或者公钥密码算法硬件解密公理：

当敏感数据较小时，使用 CFL 证书基于硬件国产密码算法 SM2 对敏感材料进行加密；当敏感数据较大时，使用 SM4 进行加密。

公理 13　CFL 安全传输公理：

(1)基于 CFL SSL 进行点对点传输。

(2)基于 CFL Mail 方式进行安全邮件传输等。

3.3　CFL_BLP_BC 状态转换规则

根据上节给出的安全公理，我们给出了比 CFL_BLP 模型更完备的 CFL_BLP_BC 模型转换规则。

规则 1(R1)　主体$s_{t,i}$对客体$o_{t,j}$请求“读$\underline{r}$”访问：get-read。

(1) if $s_{t,\text{agent}}:Verify(CFL_{s_{t,i}})=success$, if $program$ of $\underline{r}\in'BC_t$ and $Verify(BC_t)=success$, if $s_{t,i}:Verify(CFL_{o_{t,j}})=success$, if $s_{t,i}:Verify(\underline{r}\in m_{t,i,j})=$true, if $f(s_{t,i})\succ f(o_{t,j})$。

则系统执行主体$s_{t,i}$对客体$o_{t,j}$“读$\underline{r}$”请求。

(2)if $s_{t,\text{agent}}:Verify(CFL_{s_{t,i}}^{cu})=success$, if program of $\underline{r}\in'BC_t$ and $Verify(BC_t)=success$, if $s_{t,i}:Verify(CFL_{o_{t,j}})=success$, if $s_{t,i}:Verify(\underline{r}\in m_{t,i,j})=$true, if $f_c(s_{t,i})\succ f(o_{t,j})$。

则系统执行主体$s_{t,i}$对客体$o_{t,j}$“读$\underline{r}$”请求。

规则 2(R2)　主体$s_{t,i}$对客体$o_{t,j}$请求“添加$\underline{a}$”访问：get-append。

(1)if $s_{t,\text{agent}}:Verify(CFL_{s_{t,i}})=success$, if program of $\underline{a}\in'BC_t$ and $Verify(BC_t)=success$, if $s_{t,i}:Verify(CFL_{o_{t,j}})=success$, if $s_{t,i}:Verify(\underline{a}\in m_{t,i,j})=$true, if $f(s_{t,i})\prec f(o_{t,j})$。

则系统执行主体$s_{t,i}$对客体$o_{t,j}$“添加$\underline{a}$”请求。

(2)if $s_{t,\text{agent}}:Verify(CFL_{s_{t,i}}^{cu})=success$, if program of $\underline{a}\in'BC_t$ and $Verify(BC_t)=success$, if $s_{t,i}:Verify(CFL_{o_{t,j}})=success$, if $s_{t,i}:Verify(\underline{a}\in m_{t,i,j})=$true, if $f_c(s_{t,i})\prec f(o_{t,j})$。

则系统执行主体$s_{t,i}$对客体$o_{t,j}$“添加$\underline{a}$”请求。

规则 3(R3)　主体$s_{t,i}$对客体$o_{t,j}$请求“执行$\underline{e}$”访问：get-execute。

if $s_{t,\text{agent}}:Verify(CFL_{s_{t,i}})=success$, if program of $\underline{e}\in'BC_t$ and $Verify(BC_t)=success$, if $s_{t,i}:Verify(\underline{e}\in m_{t,i,j})=$true, if $f(s_{t,i})\geqslant f(o_{t,j})$。

则系统执行主体$s_{t,i}$对客体$o_{t,j}$“执行$\underline{e}$”请求。

规则 4(R4)　主体$s_{t,i}$对客体$o_{t,j}$请求“读写$\underline{w}$”访问：get-write。

(1)if $s_{t,\text{agent}}:Verify(CFL_{s_{t,i}})=success$, if program of $\underline{w}\in'BC_t$ and $Verify(BC_t)=success$, if $s_{t,i}:Verify(CFL_{o_{t,j}})=success$, if $s_{t,i}:Verify(\underline{w}\in m_{t,i,j})=$true, if $f(s_{t,i})=f(o_{t,j})$。

则系统执行主体$s_{t,i}$对客体$o_{t,j}$“读写$\underline{w}$”请求。

(2) if $s_{t,\text{agent}}:Verify(CFL_{s_{t,i}}^{cu})=success$, if program of $\underline{w}\in'BC_t$ and $Verify(BC_t)=success$, if $s_{t,i}:Verify(CFL_{o_{t,j}})=success$, if $s_{t,i}:Verify(\underline{w}\in m_{t,i,j})=$true, if $f_c(s_{t,i})=f(o_{t,j})$。

则系统执行主体$s_{t,i}$对客体$o_{t,j}$“读写$\underline{w}$”请求。

规则 5(R5)　主体释放对客体的访问属性：release-read/execute/write/append。

if program of $release\in'BC_t$ and $Verify(BC_t)=success$, if $\exists o_{t,j}$ be needed to be released, if $f(s_{t,i})\succ f(o_{t,j})$。

则系统可从 BLP 模型的客体集合中释放客体$o_{t,j}$。

规则 6(R6) 授予另一主体对客体的访问属性 give-read/execute/write/append。

if $new\ \boldsymbol{M}_t \in {}'B\ C_t$ and $Verify(BC_t)=$success, if $m_{t,i,j} \in {}'new\ \boldsymbol{M}_t$ be need to be added $\underline{x}$, then $m_{t,i,j} \leftarrow m_{t,i,j} \cup \{\underline{x}\}$

其中,*new* 指当前最新的自主访问控制矩阵。

$new\ \boldsymbol{M}_t$ 入 CFL_BLP_BC 模型中的链。

规则 7(R7) 撤销另一主体对客体的访问属性:rescind-read/execute/write/append。

if $new\ \boldsymbol{M}_t \in {}'BC_t$ and $Verify(BC_t)=$success if $m_{t,i,j} \in {}'new\ \boldsymbol{M}_t$ be need to be resinded $\underline{x}$, then $m_{t,i,j} \leftarrow m_{t,i,j} \setminus \{\underline{x}\}$

其中,*new* 指当前最新的自主访问控制矩阵。

$new\ \boldsymbol{M}_t$ 入 CFL_BLP_BC 模型中的链。

规则 8(R8) 创建一客体(保持兼容性):create-object。

if $new\ \boldsymbol{M}_t \in {}'BC_t$ and $Verify(BC_t)=success$, if $new\ BLP_t \in {}'BC_t$ and $Verify(BC_t)=success$, then $O_t \leftarrow O_t \cup \{new\ o_{t,j}\}$

$new\ BLP_t$ 入 CFL_BLP_BC 模型中的链。

$new\ \boldsymbol{M}_t$ 入 CFL_BLP_BC 模型中的链。

规则 9(R9) 表示删除一组客体:delete-object-group。

if $new\ \boldsymbol{M}_t \in {}'BC_t$ and $new\ BLP_t \in {}'BC_t$ and $Verify(BC_t)=success$, then $O_t \leftarrow O_t \setminus O_t'$, $O' \subset O_t$

$new\ BLP_t$ 入 CFL_BLP_BC 模型中的链。

$new\ \boldsymbol{M}_t$ 入 CFL_BLP_BC 模型中的链。

规则 10(R10) 改变主体当前安全级:change-subject-current-security-level。

if $s_{t,\text{agent}}: Verify(CFL_{s_{t,i}^{secure\ manage}})=1$, if some *subject*′ degree of current needed to bechanged

安全管理员为其重新赋值。

$new\ BLP_t$ 入 CFL_BLP_BC 模型中的链。

规则 11(R11) 改变客体的安全级:change-object-security-level。

if $s_{t,\text{agent}}: Verify(CFL_{s_{t,i}^{secure\ manage}})=1$, if some *object*′ degree of current needed to bechanged

安全管理员为其重新赋值。

$new\ BLP_t$ 入 CFL_BLP_BC 模型中的链。

3.4 CFL_BLP_BC 改进之处

根据上述模型安全公理以及状态转换规则所述,CFL_BLP_BC 模型与 CFL_BLP 模型相比具有如下信息安全优势:

(1)CFL_BLP_BC 模型结合了区块链,可保护指令程序和文件等数据的完整性,以及信息安全体系的操作完整性。

(2)CFL_BLP_BC 模型通过 BLP 模型与区块链的结合,修改了原 BLP 模型中主体访问客体的访问方式集合中的 $\underline{e}$(执行)操作权限,规避了可信主体误执行操作。

(3)CFL_BLP_BC 模型给出了更完整的信息安全公理和状态转换规则,并给出了形式化描述,使模型具有更严谨的安全性公理和状态转换规则作支撑,满足各新兴信息产业对毫秒级可用、机密性、完整性、可控性、可认证性的迫切需求。

4 CFL_BLP_BC 信息安全属性及性能

4.1 CFL_BLP_BC 信息安全属性

CFL_BLP_BC 模型由 3 个子模型(CFL、BLP 模型、区块链)相互支撑。基于标识的证书认证体制 CFL 是我国的自主研发技术,结合基于硬件的国产密码算法应用,具有可控性;CFL,BLP 应用到区块链中,为区块链提供身份认证机制,从而实现数据机密性、完整性保护。因此,该模型具有强可用性。

CFL_BLP_BC 模型支持当今网络空间信息安全的 5 性需求。该模型遵循上述 11 个状态转换规则,具体的安全实现方法如下:

(1)对区块链中所有主体发放基于实证制的 CFL 证书;

(2)对区块链中所有主体进行 BLP 分级分类权限主体赋值;

(3)对区块链中所有客体进行 BLP 分级分类权限客体赋值;

(4)用户使用 CFL 客户端,所有节点使用 CFL 服务器密码机;

(5)客体的创建者对客体进行 CFL 签名;

(6)应用软件或敏感数据锁入 CFL 区块链;

(7)敏感数据进行对称和非对称加密;

(8)安全通信协议为 CFL SSL;

(9)任何主体的访问操作都要经过 CFL_BLP_BC 管理平台代理主体的 CFL 证书以及 CFL 签名验证;

(10)主体对客体的访问都要进行 BLP 权限分级分类权限控制。

CFL_BLP_BC 模型具有如下安全性质。

性质 1 CFL_BLP_BC 模型支持内生安全技术。

2019 年,Qi 在北京网络安全大会上指出,从互联网时代跨入物联网时代,网络安全开始进化至“内生安全”,“内生安全”要求未来的信息化系统具备自适应、自主、自生长的内生安全能力[24]。由此可知,“内生安全”是由信息化系统内生长出安全能力,具有自主自发地防范和抵御各种安全风险的内生能力。CFL_BLP_BC 模型通过对主客体结构的 CFL 改造,将 CFL 签名、BLP 权限赋值、关键数据或进程的加入区块链,实现了信息化系统的内生安全要求,可对网络空间体系中的身份、网络、数据、行为和应用进行有效管理。

性质 2 CFL_BLP_BC 模型支持先天免疫技术。

人工免疫系统(Artificial Immune System,AIS)是根据生物免疫系统(Biological Immune System,BIS)的运行机制研发的免疫系统计算机模型,是模拟 BIS 智能行为而提出的一种仿生智能计算方法。人工免疫算法通过模仿 BIS 构建具有动态性、自适应性和自组织性的信息防御系统,以此来抵御外部无用、有害和干扰信息的侵入,从而保证系统接受信息的有效性与无害性[25]。CFL_BLP_BC 模型通过数据结构化内置了安全基因,对网络中的任一主体都需要进行 CFL 证书认证,对没有 CFL 签名、BLP 授权、BC 完整性保护的病毒木马进行自动规避,构成了仿生的先天免疫。

性质 3 CFL_BLP_BC 模型支持主动防御技术。

主动防御就是通过系统内生的机制对网络攻击达成事前的有效防御,它不依赖于攻击代码和攻击行为的特征,即主动防御不依赖在已有网络攻击的先验知识下实施主动的、前摄的防御部署,从而有效抵御和应对攻击对系统的破坏[26-27]。

CFL_BLP_BC 模型中通过 CFL 身份认证技术、BLP 模型、区块链技术的结合，以及安全公理和状态转换规则，保障了系统的安全性。无论安全主体还是病毒木马对系统进行访问操作或其他执行操作，都要进行 CFL 签名验证，从而防止未知病毒木马对应用系统或保护数据进行恶意攻击，实现了对网络攻击的提前防御，且 CFL_BLP_BC 模型支持内生安全技术、先天免疫技术。

性质 4 CFL_BLP_BC 模型支持零信任安全。

零信任(zero trust)概念于 2010 年由 Forrester 研究机构提出，在“零信任”概念中，将不再信任网络内部或外部的任何人/设备/系统，即初始安全状态在不同实体之间没有隐式信任。无论是在网络内部还是外部，在零信任模型中，所有网络流量都是不可信任的，安全专业人员必须验证和保护所有资源，限制并严格执行访问控制，检查和记录所有网络流量[28]。CFL_BLP_BC 模型对系统中的外部主体和内部主体都需要进行 CFL 签名验证，不信任任何主体，由 CFL 性质 3 可知，该模型保证一人一钥，可防范内鬼的恶意操作。

性质 5 CFL_BLP_BC 模型支持可信计算。

可信计算是一种旨在增强计算机系统可信性的综合性信息安全技术，其基本思路是在计算机系统中建立信任根和一条信任链，从信任根开始到硬件平台，然后到操作系统，最后到应用，一级度量认证一级，逐级信任，把这种信任扩展到整个计算机系统，确保计算资源的完整性，提高了计算机系统的可信性[26,29]。可信计算主要体现在身份认证和资源及程序的完整性保护，而 CFL_BLP_BC 模型提供了 CFL 认证技术，满足了身份认证需求，区块链技术保证了数据、进程的完整性，可以充分支持关键应用程序的可信计算。

性质 6 CFL_BLP_BC 模型支持实证制安全。

CFL_BLP_BC 模型中的主体都持有 CFL 证书，当模型中存在特殊主体时，必须持有 CFL 临时证书。

性质 7 CFL_BLP_BC 模型支持毫秒级、指令级安全。

CFL 认证机制是 CFL_BLP_BC 模型的信息安全原点技术，由 CFL 的性质 2、性质 4 可知，CFL 证书应用的过程不依赖第三方，可直接认证、现场认证，满足毫秒级安全、指令级安全。

性质 8 CFL_BLP_BC 模型支持处处是边界安全。

CFL_BLP_BC 模型对网络中进入系统的一切实体都进行 CFL 证书认证和 BLP 权限授权，且每次对实体的认证都是动态认证，授权根据模型状态转换规则可实现动态调整，只有通过认证和权限判定的实体才可进入系统，对系统数据进行访问操作，确保数据被安全访问，从而实现了处处是边界安全。

注：该模型在使用过程中应规避隐蔽信道。

CFL_BLP_BC 模型可实现毫秒级认证，具有较好的可用性；根据模型分析可知，CFL_BLP_BC 模型具有较高的可靠性以及安全性。该模型虽然还没有在大型项目中进行试用，但是基于 CFL_BLP 模型的产品已在某大学、某单位等广泛应用，其认证速度和稳定性得到认可。

4.2 CFL_BLP_BC 性能分析

为了验证 CFL_BLP_BC 模型的认证速度、数据加密速度(均加密 4 096 字节)等性能指标，我们结合相关硬件设备进行了测试。

测试环境如下：

(1)CFL 密码卡服务器

硬件配置如下：密码卡为 SC26E-1RQHE；CPU 为 Intel(R) Pentium(R) G2030 @ 3.00 GHz；内存为 4 GB；硬盘为 1 T。

软件环境如下：操作系统为 CentOS release 6.5。

(2)PC 机

硬件配置如下：CPU 为 Intel(R) Core(TM) i3 CPU @3.60 GHz ；内存(RAM)为 4.00 GB。

软件环境如下：操作系统为 Windows 7 旗舰版 64 位操作系统。

(3)交换机：TP-LINK TL-SG2016D

启动 CFL 密码卡服务器后，为了验证其性能，我们采用随机测试的方式进行测试，产生的随机测试次数以及相关速率如表 3 所列。

表 3 CFL_BLP_BC 模型的部分性能测试

Table 3 CFL_BLP_BC model partial performance test

检测项目	速率	测试次数
签名	1 785 次每秒	777
签名验证	1 211 次每秒	471
ECB 加密	49.24 Mbps	1 744
ECB 解密	79.86 Mbps	329
BLP 权限读取及比较	2 533 569 次每秒	10 000
BC 中的哈希	185 Mbps	500

由实验结果可知，现有的 CFL 密码设备可以支持 CFL_BLP_BC 模型毫秒级的安全，因此该模型可广泛满足工控、智慧城市、无人机、自动驾驶、物联网等新兴信息产业对毫秒级、指令级信息安全的迫切需求。随着密码设备计算能力的不断提高，CFL_BLP_BC 模型的性能会得到进一步提升。

5 5G 时代 CFL_BLP_BC 的应用场景

CFL_BLP_BC 模型集身份认证技术、通信加解密技术、访问控制技术、区块链技术为一体，具有毫秒级安全、指令级安全以及支持内生安全技术、先天免疫技术、主动防御技术等优势，可广泛应用于各新兴信息产业中。

CFL_BLP_BC 模型应用场景包括但不限于以下场景：

(1)CFL_BLP_BC 模型可支持 5G、智慧城市、无人驾驶、工业 4.0、中国制造 2025 等中设备与设备之间的快速认证。

参数认证、函数认证 PKI、IBC 已不能满足 5G、智慧城市、工控上下位机的指令传输等场景中设备与设备之间的毫秒级、指令级认证安全需求[7]。CFL_BLP_BC 模型采用函数认证技术 CFL，终端设备都持有 CFL 证书，当进行网络接入、数据访问、数据传输等操作时，都需要进行 CFL 动态证书认证，由该模型的性质 7 可知，CFL_BLP_BC 模型可应用于上述场景的设备与设备之间的认证。

(2)CFL_BLP_BC 模型可广泛应用于 5G、智慧城市、无人驾驶、工业 4.0、中国制造 2025 等中的数据库或者数据仓

库的可信强制访问控制。

CFL_BLP_BC 模型中的 CFL 证书带有 BLP 强访标识，当主体对数据库或数据仓库进行访问时，通过验证 CFL 动态证书，可确定主体的访问权限，当权限满足访问级别时，才可进行访问，实现了数据库或者数据仓库的可信强制访问控制。

(3)CFL_BLP_BC 模型可广泛应用于 5G、智慧城市、无人驾驶、工业 4.0、中国制造 2025 等中的关键程序保护。

关键应用程序一般不隶属于操作系统，传统的可信计算技术把重点放在了操作系统的可信上。该模型可以把关键应用程序锁入区块链中，每次使用时既要控制使用者的权限，又要检查该程序的完整性，进一步细化了可信计算的访问控制粒度。因此，该模型可保护关键应用程序。

结束语 5G 的发展使各新兴信息产业在信息安全方面面临更大的挑战，迫切需要新的方法予以应对。本文提出了一种支持信息安全机密性、完整性、可用性、可控性、可认证性的模型 CFL_BLP_BC。该模型利用 CFL 认证技术、BLP 分级分类强制访问控制模型、区块链技术以及国产密码算法，保障了数据和系统操作层面的机密性和完整性。该模型的毫秒级安全、指令级安全、支持内生安全技术等安全性质，使其可应用于 5G、智慧城市、工控等新兴信息产业中，满足新兴信息产业的毫秒级信息安全需求。CFL_BLP_BC 模型已申请专利并已在相关部门、企业等应用。在下一步的工作中，我们将进一步给出该模型的隐蔽信道防范方面的研究。

参 考 文 献

[1] PLOUTON V. Grammatikos, Panayotis G. Cottis. IMT Vision-Framework and overall objectives of the future development of IMT for 2020 and beyond[S]. ITU-R Recommendation M. 2083-0, 2015.

[2] View on 5G architecture Version 3.0 [M/OL]. The 5G Infrastructure Public Private Partnership Architecture Working Group, 2019: 18-19. https://5g-ppp. eu/wp-content/uploads/2019/07/5G-PPP-5G-Architecture-White-Paper_v3. 0_Public-Consultation. pdf.

[3] ZHANG S, WANG Y, ZHOU W. Towards Secure 5G Networks: A Survey[J]. Computer Networks, 2019, 162: 106871.

[4] SCHNEIDER P, HORN G. Towards 5G Security[C]// Trustcom/bigdatase/ispa. IEEE, 2015: 1165-1170.

[5] SORENSEN L T, KHAJURIA S, SKOUBY K E. 5G Visions of User Privacy[J]. IEEE Vehicular Technology Conference, 2015, 81(5): 1-4.

[6] KUTSCHER D. It's the network: Towards better security and transport performance in 5G[C]// 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). San Francisco, CA, 2016: 656-661.

[7] FAN X B, LIU X, WANG X L, et al. Identification-based authentication system CFL — netspace authentication and its examples[M]. Beijing: Beijing University of Posts and Telecomunications Press, 2019: 33-69.

[8] FAN W Z, FAN Y N, HE Z Z, et al. CFL_BLP model[J]. Journal of Taishan University, 2018, 40(6): 60-66.

[9] DU C L, LIU J M, FAN X B, et al. CFL is Statistical Zero-Knowledge Proof System[J]. Journal of Information Security Research, 2016, 2(7): 621-627.

[10] QIN H B, PAN Y J, FAN X B, et al. Analysis on CFL Provable Security[J]. Journal of Information Security Research, 2016, 2(7): 589-599.

[11] FAN X B. New generation of identity authentication technology CFL[J]. Journal of Information Security Research, 2016, 2(7): 587-588.

[12] LI C C, JI S W, FAN X B, et al. The Overview of Authentication Systems[J]. Journal of Information Security Research, 2016, 2(7): 649-659.

[13] DU C L, FAN X B. CFL Authentication System and Its Applications in the Blockchain[J]. Journal of Information Security Research, 2017, 3(3): 220-226.

[14] BELL D E, LAPADULA L J. Secure Computer Systems: A Mathematical Model[J]. The MITRE Corporation, 1973, 2: 239-263.

[15] NOFER M, GOMBER P, HINZ O, et al. Blockchain[J]. Business & Information Systems Engineering, 2017, 59(3): 183-187.

[16] ZHENG Z B, XIE S A. Blockchain challenges and opportunities: a survey[J]. International Journal of Web and Grid Services, 2018, 14(4): 352-375.

[17] WANG Y, SHEN Y, WANG H, et al. MtMR: Ensuring MapReduce Computation Integrity with Merkle Tree-based Verifications[J]. IEEE Transactions on Big Data, 2016, 4(3): 418-431.

[18] YUAN Y, WANG F Y. Blockchain: The State of the Art and Future Trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

[19] LI Q, TAN Y, YU X, et al. Resear on Blockchain Authentication Based on CFL[C]// Proceedings of the 6th China command and Control Conference (Volume 2). 2018: 587-589.

[20] SHU Z X, LI T F, YU X, et al. Research on cfl-based blockchain system authentication Mechan-ism[J]. Application Research of Computers, 2020, 38(2): 1-10.

[21] LI Q, SHU Z X, YU X, et al. Authentication Mechanism in Blockchain Systems[J]. Journal of Command and Control, 2019(1): 1-17.

[22] YAN S J, MIN L Q, FAN X B. Researchon the knowledge security[J]. Journal on Communications, 2014, 35(Z2): 204-211.

[23] YAN S J, FAN X B, CHEN Y G, et al. Construction of Narrow Security Knowledge Base[J]. Information Security and Communications Privac, 2015(6): 99-103.

[24] Ten academicians unveil BCS 2019 Qian xin first proposes the concept of "SECURITY: BUILT-IN DNA"[J]. China Information Security, 2019(9): 102.

[25] FERNANDES D A B, FREIRE M M, FAZENDEIRO P A P, et al. Applications of artificial immune systems to computer security: A survey[J]. Journal of Information Security & Applications, 2017, 35: 138-159.

[26] ZHANG B. Research on key Technologies of Interactive and Attack Proactive Defense in Edge-computing Network [D]. Nanjing:Guniversity of Science & Technology,2019.

[27] LUO Y B. Research on Proactive Defense of Computer Network [D]. Hunan:National University of Defense Technology,2017.

[28] IFTEKHAR A,TAHMIN N,SHAHINA S U,et al. Protection of Sensitive Data in Zero Trust Model[C]// Proceedings of the International Conference on Computing Advancements (ICCA 2020). Association for Computing Machinery,New York,NY,USA,2020,63:1-5.

[29] ZHANG H G,JIA C F,LIN J Q. Foreword of trusted computing for autonomous security and controllability[J]. Journal of Software,2019,30(8):2227-2228.

LIAN Wen-juan, born in 1977, Ph.D, associate professor, is a member of China Computer Federation. Her main research interests include deep learning, cyber security.

FAN Xiu-bin, born in 1966, Ph.D, professor, Ph.D supervisor. His main research interests include cryptology, cyber Security.