基于区块链的CFL安全模型在5G时代的应用

中科院软件研究所青岛分部工业软件信息安全委员会主任
中国产学研工匠精神奖获得者
研究员、教授、博导

范修斌

2019.8.20

1 CFL_BLP_BC_CCA模型提出的背景是什么？

1.1 以5G为代表的当今网络空间的信息安全八原则是什么？

- 经过四十余年的发展，网络空间已由传统网络空间发展为当今网络空间。所谓传统网络空间是指网络+电子政务及电子商务；当今网络空间除包含传统网络空间外，还包括各新兴信息产业。
- 当今网络空间的信息安全需求已经发生了根本的变化。我们团队在世界上首次给出了当今网络空间八原则。

1 CFL_BLP_BC_CCA模型提出的背景是什么？

1.1 以5G为代表的当今网络空间的信息安全八原则是什么？

原则1 假设病毒木马无处不在。

原则2 第三方功能极小化原则。

原则3 信息安全算法专门化硬件实现原则。

原则4 信息安全算法P复杂度原则。

1 CFL_BLP_BC_CCA模型提出的背景是什么？

1.1 以5G为代表的当今网络空间的信息安全八原则是什么?

原则5 及时性安全原则。

原则6 字段级安全原则。

原则7 指令级安全原则。

原则8 系统化、模型化、数学化原则。

1 CFL_BLP_BC_CCA模型提出的背景是什么？

1.2 当今网络空间的第一信息安全技术是什么?

当今网络空间的信息安全由五个重要属性构成：即机密性、完整性、可用性、可控性、可认证性。

我们团队给出了如下重要命题：

命题1 可认证性是当今网络空间第一信息安全技术。

1 CFL_BLP_BC_CCA模型提出的背景是什么？

1.3 为什么说传统认证技术卡住了当今网络空间发展的脖子?

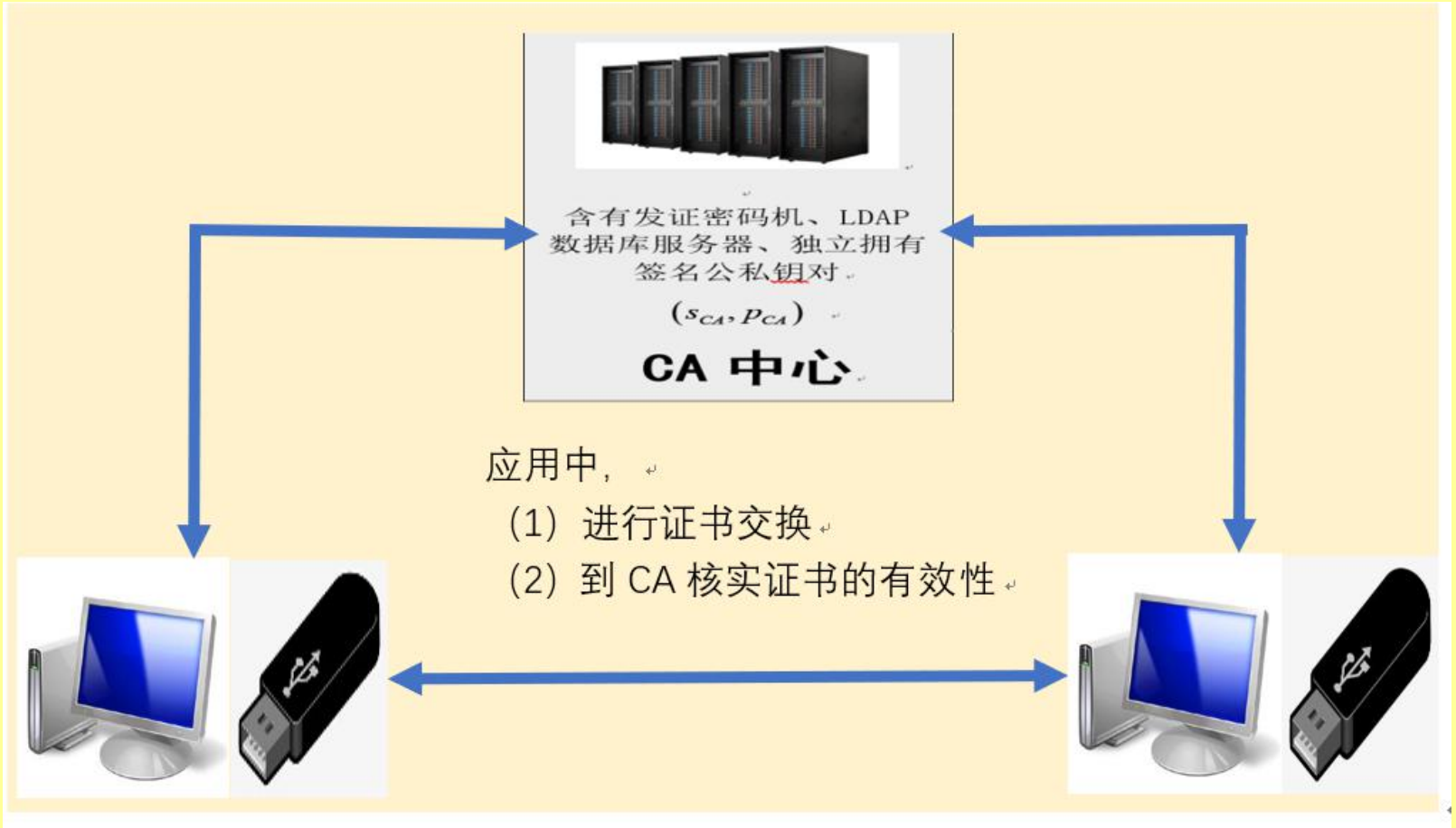
网络空间可认证性技术可包括两类:参数认证技术、函数认证技术。

参数认证技术包括：指纹、虹膜、刷脸等生物信息、标识、口令等；函数认证包括：PKI、IBC。

我们团队基于香农信息论，给出了如下重要命题：

命题2 参数认证本质上不具有信息安全认证功能。。

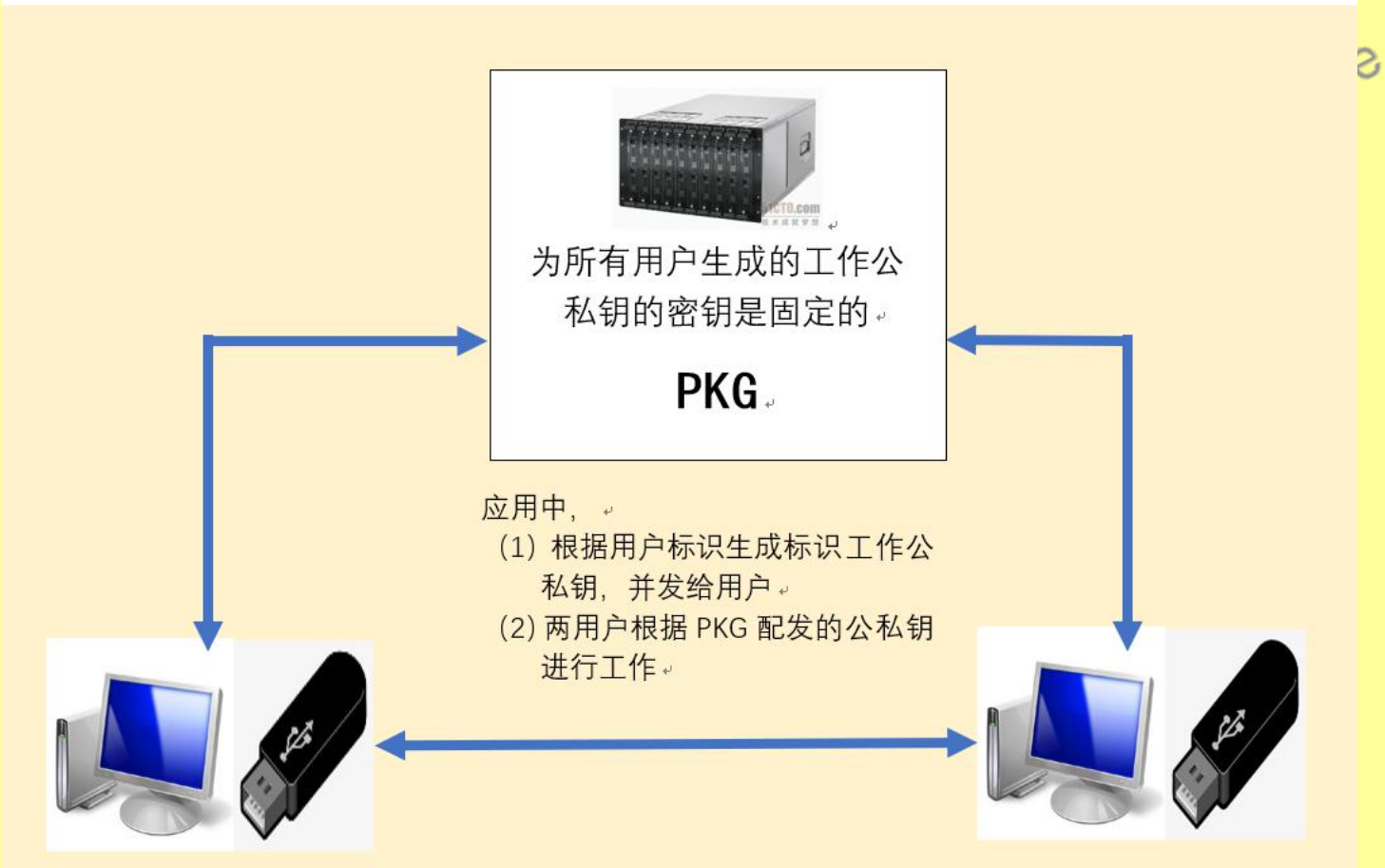
PKI证书应用拓扑结构示意图：



关于PKI，我们团队给出了如下科学论断：

- **命题3　面对当今网络空间，PKI之缺陷：**
- **（1）非一人一钥，安全性低。**
- **（2）应用依赖中心，网络延迟大仅支持秒级安全。**
- **（3）第三方非极小化。**
- **（4）因为应用有中心，所以其无法支持无中心的区块链技术。**
- **（5）无法快速支持点对点认证、指令级安全。**
- **（6）无法满足当今网络空间毫秒级信息安全的迫切需求。**

IBC拓扑结构示意图


为所有用户生成的工作公私钥的密钥是固定的
PKG
应用中，
(1) 根据用户标识生成标识工作公私钥，并发给用户
(2) 两用户根据 PKG 配发的公私钥进行工作

关于IBC，我们团队给出了如下科学论断：

- **命题4 面对当今网络空间，IBC之缺陷：**
- **（1）为所有用户所生成的工作公私钥参数是固定的，安全度低。**
- **（2）计算速度非常慢，隶属重量级算法。**
- **（3）所生成的用户的工作公私钥安全传输是缺环的。**
- **（4）应用需要第三方，因此存在网络延迟。**
- **（5）因有中心，其无法支持无中心的区块链技术。**
- **（6）不能支持高可用快速点对点认证，无法实现指令级安全。**
- **（7）无法满足当今网络空间毫秒级信息安全需求。**

1 CFL_BLP_BC_CCA模型提出的背景是什么？

1.3 为什么说传统认证技术卡住了当今网络空间发展的脖子?

通过上述所有已有认证体制的梳理和论述，可知，我们团队给出了如下科学论断：

命题5 已有认证技术成为了当今网络空间信息安全共性卡脖子问题。

鉴于上述分析，我们团队历时十年，首先构建了网络空间认证学，其次首次给出了满足认证学的实例CFL。在CFL的基础上，我们团队进一步给出了CFL_BLP_BC_CCA模型,它是满足等保2.0要求的TCB.该模型解决了当今网络空间信息安全的卡脖子问题。

2 CFL_BLP_BC_CCA模型的具体内容是什么？

2.1 CFL是什么？

CFL是基于标识的证书认证技术。它具有如下信息安全属性:

《基于标识的证书认证体制 CFL》专家意见

2011 年 7 月 28 日，在北京知识安全工程中心举行了《基于标识的证书认证体制 CFL》研讨会。

参加会议的专家有：蔡吉人院士、周仲义院士、魏正耀院士、陈晓研究员；会议主题报告的报告人为陈华平研究员；与会的其他专家还有：吕述望教授、刘振华教授、范修斌教授、赵和平研究员、苏盛辉教授、董德凯副研究员等。

会议听取了陈华平研究员所做的题为《基于标识的证书认证体制 CFL》（以下简称 CFL）的报告。

与会专家经过认真讨论，一致认为：

CFL 是一种证书认证与标识认证混合的证书认证体制。它的基础密钥对由标识密钥对和随机密钥对组成，标识密钥对作为签名和验证密钥对，随机密钥对作为工作密钥对，形成了以用户自己的标识密钥对为自己的工作密钥对进行签名和验证的证书认证体制，证书的验证过程可以无需第三方参与，实现了证书验证过程的自认证。

CFL 的随机密钥对由用户自主生成，保障了用户对随机私钥的私有权；密钥管理中心通过对用户标识的真实性和唯一性的审查，对标识密钥对的私钥生成和使用等环节实施集中管理。该体制能适应大规模公开网络的既能集中管理，又能保护用户隐私的认证需求。

CFL 的密钥管理中心和用户可以根据需求灵活选择相同或不同的公钥密码算法，分别作为标识密钥对和随机密钥对的密码算法。CFL 能将各种公钥密码算法使用于其基本架构之中，突破了常见认证体制中密钥管理中心和用户使用同一公钥密码算法的结构，提供了一种多公钥密码算法混合使用的新结构。

CFL 给出了创新的指数乘积型的公钥密码算法，该算法以公钥和私钥的多指数乘积构成，突破了 RSA 指数型密码算法的公钥和私钥的单指数结构。指数乘积的因子由用户标识控选，使该体制成为基于标识的一种公钥密码算法，其算法类型不同于非基于标识的 RSA 指数型公钥密码算法。

与会专家认为基于标识的证书认证体制 CFL，是具有我国自主知识产权的新颖的认证体制，有助于权威部门对网络的集中管理和保证用户的个人私密，也支持网络实名制的实施。应积极促进其产品化和推广使用。

建议该项目加紧实验，给出工程实现中的效率参数。

专家签名：

周仲义 魏正耀 陈晓

2011 年 7 月 28 日

《基于 SM2、SM3 的 CFL 认证体制》专家意见

2015 年 6 月 20 日，在北京博文广成信息安全技术有限公司举行了《基于 SM2、SM3 的 CFL 认证体制》专家研讨会。

参加专家研讨会议的有刘福运研究员、李荣祖研究员、刘海霞研究员、宁燕平副研究员、李坤高工、刘凤梅副研究员，会议听取了王海平博士所做的题为《基于 SM2、SM3 的 CFL 认证体制》的报告。

与会专家经过认真质询讨论，认为：

基于 SM2、SM3 的 CFL 认证体制是基于标识的证书认证体制 CFL 的一个具体实例。报告分析了基于 SM2、SM3 的 CFL 认证体制的安全属性，得到了该认证体制的十大优势，即该体制具有可证明安全性；满足用户对私钥基的零知识以及证书生成应用服务中心对用户工作私钥的零知识；以极高概率一人一密；标识信息可集成授权管理信息；满足验证方的自认证；可实现动态认证；实现效能高；资源消耗低；可支持新兴网络；拥有自主知识产权。

该报告理论分析严谨、结果正确。

与会专家一致认为：基于 SM2、SM3 的 CFL 认证体制具有十大优势，该体制创新性强，达到了国际领先水平，具有重要的应用价值。建议积极促进该项技术的产品化和推广应用，以便更好的为我国的信息安全建设服务。

专家签字：刘福运 刘海霞 李坤 刘凤梅 宁燕平 2015 年 6 月 20 日 李荣祖

证书号第 1957539 号

发明专利证书

发明名称：基于标识的证书认证体制 CFL

发 明 人：陈华平;范修斌;吕述望

专 利 号：ZL 2011 1 0250009.4

专利申请日：2011 年 08 月 29 日

专 利 权 人：陈华平;北京博文广成信息安全技术有限公司

授权公告日：2016 年 02 月 17 日

本发明经过本局依照中华人民共和国专利法进行审查，决定授予专利权，颁发本证书并在专利登记簿上予以登记。专利权自授权公告之日起生效。

本专利的专利权期限为二十年，自申请日起算。专利权人应当依照专利法及其实施细则规定缴纳年费。本专利的年费应当在每年 08 月 29 日前缴纳。未按照规定缴纳年费的，专利权自应当缴纳年费期满之日起终止。

专利证书记载专利权登记时的法律状况。专利权的转移、质押、无效、终止、恢复和专利权人的姓名或名称、国籍、地址变更等事项记载在专利登记簿上。

局长 申长雨

2016 年 02 月 17 日

第 1 页(共 1 页)

国家密码管理局

国密局字〔2016〕75 号

国家密码管理局关于同意基于 SM2、SM3 的 CFL 认证体制通过审查的通知

北京博文广成信息安全技术有限公司：

你公司提交的《基于 SM2、SM3 的 CFL 认证体制》通过我局审查，基于该体制研制的密码产品及建设的应用系统应报我局审查。

特此通知。

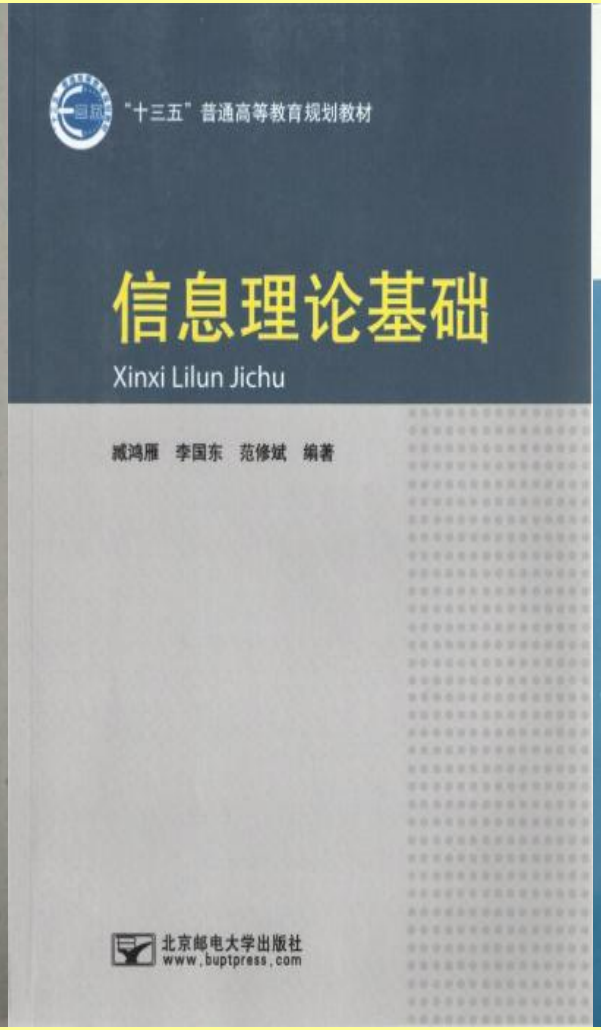
国家密码管理局

2016 年 3 月 21 日

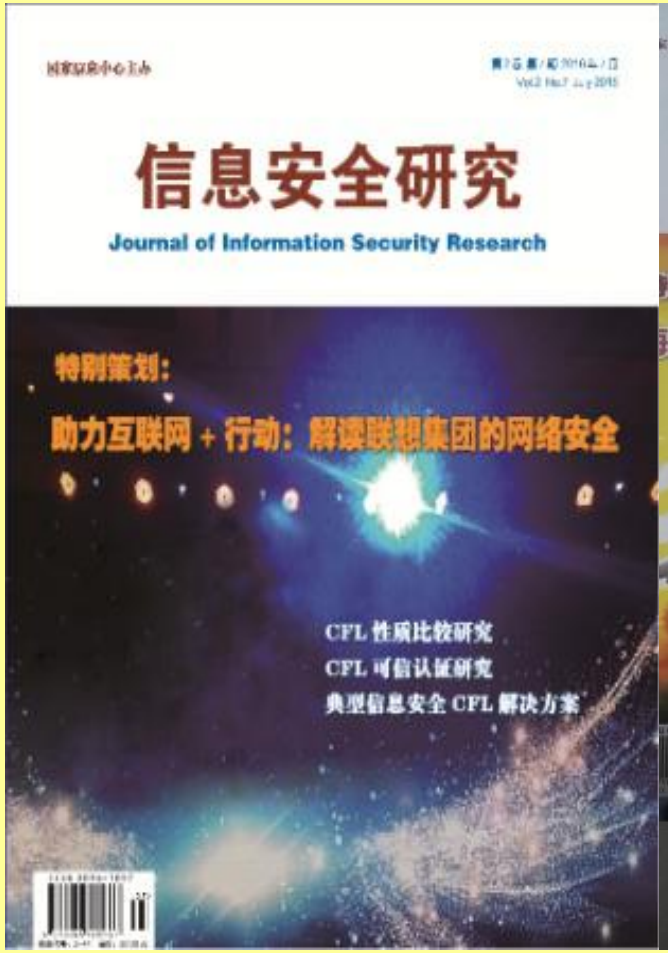
— 1 —


序列密码
的设计与分析
北京中软电子出版社


完全映射
及其密码学应用
Complete Mapping and Application in Cryptography
吕述望 范修斌
王昭顺 徐结绿 著
张 剑


"十三五"普通高等教育规划教材
信息理论基础
Xinxi Lilun Jichu
臧鸿雁 李国东 范修斌 编著
北京邮电大学出版社
www.buptpress.com


基于标识的证书认证体制CFL
——网络空间认证学及实例
JIYU BIAOSHI DE ZHENGSHU RENZHENG TIZHI CFL
—WANGLUO KONGJIAN RENZHENGXUE JI SHILI
范修斌 刘 昕 王助龙 杜春玲
庭院鹏 臧鸿雁 王凤瑛 王红兵 著
陈华平 主审
北京邮电大学出版社
www.buptpress.com



工业和信息化部　新闻动态　信息公开　在线办事　公众参与　专题专栏　工信数据

首页 > 工业和信息化部 > 机关司局 > 网络安全管理局 > 文件发布 > 正文

发文机关：工业和信息化部办公厅

标　题：工业和信息化部办公厅关于公布网络安全技术应用试点示范项目名单的通知

发文字号：工信厅网安函〔2019〕116号

成文日期：2019-05-15　　发布日期：2019-06-04

文章来源：网络安全管理局　　分　类：网络安全管理

工业和信息化部办公厅关于公布网络安全技术应用试点示范项目名单的通知

工信厅网安函〔2019〕116号

各省、自治区、直辖市及计划单列市工业和信息化主管部门，各省、自治区、直辖市通信管理局，部属相关单位，相关中央企业，各有关单位：

为贯彻落实《网络安全法》，促进网络安全技术创新应用，提升网络安全产业发展水平，我部组织开展了网络安全技术应用试点示范项目推荐工作。经单位申报、地方推荐、专家评审、网上公示等环节，确定了101个网络安全技术应用试点示范项目，现予以公布。

各入选项目参与单位要加大研发投入，促进技术创新发展，不断优化提升项目的实用性和可推广性，有力支撑试点示范项目在重点行业领域的应用推广。各项目推荐单位要加强对项目实施单位的管理指导，加大对试点示范项目的支持力度，鼓励引导相关单位和企业参照试点示范项目强化网络安全保障能力，推动试点示范项目在各地方、各行业的应用推广。

附件：网络安全技术应用试点示范项目名单

工业和信息化部办公厅

2019年5月15日

97	基于新一代认证体制 CFL 的网络安全应用系统	青岛博文广成信息安全技术有限公司

2 CFL_BLP_BC_CCA模型的具体内容是什么？

2.2 BLP是什么？

BLP 模型是在 1973 年由 D．Bell 和 J．LaPadula 提出并加以完善的，它根据美国军方的安全政策设计，解决的本质问题是对具有密级划分信息的访问控制，是第一个比较完整地利用形式化方法对系统安全进行严格证明的数学模型，被广泛应用于描述计算机系统的安全问题。

BLP 模型有如下两大特点：

- 1) 简单安全特性（不向上读，即下读）：一个主体只能读一个低级别或相同安全级别的对象。
- 2) *特性（不向下写，即上写）：一个主体只能写一个高级别的或相同安全级别的对象。

2 CFL_BLP_BC_CCA模型的具体内容是什么？

2.3 BC是什么？

BC，Block Chain,即区块链。与BLP模型对偶的操作完整性保护模型为Biba模型，但是，正是由于两者之间的对偶性，在两者的标识的使用上，存在冲突，从而使得BLP模型和Biba模型同时使用上存在困难，为此，我们引入了区块链技术来结合BLP模型实现操作层面的完整性保护。

我们团队已经证明了如下命题：

命题6 CFL认证技术是唯一匹配区块链的认证技术

由本命题可知，CFL_BLP_BC可集成使用，且是先进模型的强强联合。

2 CFL_BLP_BC_CCA模型的具体内容是什么？

2.4 CCA是什么？

CCA(China Cryptography Algorithms):基于硬件的国产密码算法包括：物理噪声源发生器、国产硬件对称密码算法、国产硬件公钥密码算法、国产硬件摘要算法等。

我们团队已经证明了如下命题：

命题7 纯软件算法不具有信息安全功能。

由该命题可知，软硬结合是解决信息安全问题的根本之道。

2 CFL_BLP_BC_CCA模型的具体内容是什么？

- **2.5 CFL_BLP_BC_CCA模型各个子模型之间的关系是什么？**

(1) 由前述命题可知，信息安全的第一技术为认证技术，CFL是能够满足当今网络空间认证迫切需求的技术，因此CFL作为信息安全原点技术不可替代。

(2) 基于CFL的签名保护下BLP模型的分级分类标记技术才是可信的，且由于CFL的签名验证可以现场完成，因此实现了BLP模型的及时性使用安全，即没有网络延迟，真正高可用实现了BLP模型。

2 CFL_BLP_BC_CCA模型的具体内容是什么？

- **2.5 CFL_BLP_BC_CCA模型各个子模型之间的关系是什么？**

(3)基于CFL的区块链技术，锁定BLP标记，形成安全可信白名单，实现可信的、高可用的、现场可直接认证的白名单模型，高速实现分级分类强制访问控制，从而可实现当今网络空间中的满足等保2.0版的高等级信息安全。

(4)同时基于CFL的区块链技术可实现操作的满足静态完整性以及程序的动态完整性，且该区块链是专用区块链，具有高可信、高可用、现场直接认证，无需CA中心应用支持。

2 CFL_BLP_BC_CCA模型的具体内容是什么？

- **2.5 CFL_BLP_BC_CCA模型各个子模型之间的关系是什么？**

(5)基于CCA的硬件保护，基于黑盒密钥管理原理，以及其它可靠的密钥管理方式，充分实现了满足香农信息论的信息安全。

(6)在CCA的支持下，充分实现了CFL、BLP、BC的可信操作和安全。

3 为什么CFL_BLP_BC_CCA模型解决了当今网络空间信息安全共性的卡脖子问题?

- **3.1 为什么说CFL_BLP_BC_CCA模型面向当今网络空间集成了国际国内最合理的信息安全子模型?**

(1) CFL被党政军一线专家鉴定为“达到了国际水平”;

(2) CFL 是基于标识的证书认证，它继承了证书认证和标识认证的优势，同时规避了两者的不足;

(3) CFL具有高安全、高可用性，充分满足当今网络空间的及时性、指令性、字段级安全的迫切认证需求;

(4) BLP是美国军方应用的信息安全模型、它是很多安全信息系统的理论基础、是标识或者标记技术的一面旗帜;

(5) BC技术已经在整个网络得到了风起云涌的实现，将该技术专用于局部信息的完整性保护，绰绰有余且高可用;

3 为什么CFL_BLP_BC_CCA模型解决了当今网络空间信息安全共性的卡脖子问题?

- **3.1 为什么说CFL_BLP_BC_CCA模型面向当今网络空间集成了国际国内最合理的信息安全子模型?**

(6) CFL确保了可认证性;

(7) CCA、BLP确保了机密性;

(8) CFL、CCA、BC确保了完整性;

(9) CFL的现场直接认证，CFL、CCA的百年边缘算确保了高可用性;

(10) CFL、BLP、BC、CCA一起系统性决定了信息系统的可控性。

因此有如下命题:

命题8 CFL_BLP_BC_CCA模型面向当今网络空间集成了国际国内最合理的信息安全子模型。

3 为什么CFL_BLP_BC_CCA模型解决了当今网络空间信息安全共性的卡脖子问题?

3.2 为什么说CFL_BLP_BC_CCA模型充分满足当今网络空间信息安全八原则?

(1) CFL_BLP_BC_CCA模型为什么满足原则1即假设病毒木马无处不在的原则?

因为CFL、BLP、BC、CCA的密钥都有硬件黑盒保护或者其它可靠方式保护，由香农信息论可知，CFL_BLP_BC_CCA模型满足该原则。

(2) CFL_BLP_BC_CCA模型为什么满足原则2即第三方功能极小化原则?

因为CFL_BLP_BC_CCA模型的证书应用过程不需要类似PKI的CA中心在线支持，可以现场自主认证所以使得CFL证书发证机关作为第三方其功能达到了极小化。因此CFL_BLP_BC_CCA模型满足该原则。

3 为什么CFL_BLP_BC_CCA模型解决了当今网络空间信息安全共性的卡脖子问题?

3.2 为什么说CFL_BLP_BC_CCA模型充分满足当今网络空间信息安全八原则?

(3) CFL_BLP_BC_CCA模型为什么满足原则3即信息安全算法专门化硬件实现原则?

因为CCA专门的国产硬件算法实现的，因此 CFL_BLP_BC_CCA模型显然满足该原则。

(4) CFL_BLP_BC_CCA模型为什么满足原则4即信息安全算法P复杂度原则?

因为CFL_BLP_BC_CCA模型中的CFL、BLP、BC、CCA各个子模型都是P复杂度的，因此CFL_BLP_BC_CCA模型满足该原则。

3 为什么CFL_BLP_BC_CCA模型解决了当今网络空间信息安全共性的卡脖子问题?

3.2 为什么说CFL_BLP_BC_CCA模型充分满足当今网络空间信息安全八原则?

(5) CFL_BLP_BC_CCA模型为什么满足原则5即及时性安全原则?

因为CFL具有现场直接认证的安全属性，因此通过BLP、BC、CCA的边缘计算，从而使得 CFL_BLP_BC_CCA模型满足该原则。

(6) CFL_BLP_BC_CCA模型为什么满足原则6即字段级安全原则?

因为CFL_BLP_BC_CCA模型中的BLP模型是实现字段级的重要技术，且在实际落地中，特别是数据库的落地中，基于BLP模型，充分实现了字段级的安全，因此CFL_BLP_BC_CCA模型满足该原则。

3 为什么CFL_BLP_BC_CCA模型解决了当今网络空间信息安全共性的卡脖子问题?

3.2 为什么说CFL_BLP_BC_CCA模型充分满足当今网络空间信息安全八原则?

(7) CFL_BLP_BC_CCA模型为什么满足原则7即指令级安全原则?

因为CFL具有应用无中心的信息安全属性，所以CFL_BLP_BC_CCA模型满足该原则。

(8) CFL_BLP_BC_CCA模型为什么满足原则8即系统化、模型化、数学化原则?

因为CFL_BLP_BC_CCA模型中的CFL、BLP、BC、CCA都是模型化给出的，所以可知CFL_BLP_BC_CCA模型满足该原则。

3 为什么CFL_BLP_BC_CCA模型解决了当今网络空间信息安全共性的卡脖子问题?

3.2 为什么说CFL_BLP_BC_CCA模型充分满足当今网络空间信息安全八原则?

由上述分析可知，我们有如下命题:

命题9 CFL_BLP_BC_CCA模型满足当今网络空间的信息安全八原则。

3 为什么CFL_BLP_BC_CCA模型解决了当今网络空间信息安全共性的卡脖子问题?

3.3 为什么说CFL_BLP_BC_CCA模型充分满足5G时代的毫秒级信息安全需求?

有前节分析可知CFL_BLP_BC_CCA模型满足原则5即及时性安全原则，从而可知该该模型充分满足5G时代的毫秒级信息安全。

3 为什么CFL_BLP_BC_CCA模型解决了当今网络空间信息安全共性的卡脖子问题?

3.4 为什么说CFL_BLP_BC_CCA模型充分满足5G时代的指令级信息安全需求?

有前节分析可知CFL_BLP_BC_CCA模型满足原则7即指令级安全原则，从而可知该该模型充分满足5G时代的指令级信息安全需求。

3 为什么CFL_BLP_BC_CCA模型解决了当今网络空间信息安全共性的卡脖子问题?

3.5 为什么说CFL_BLP_BC_CCA模型充分满足5G时代的字段级信息安全需求?

有前节分析可知CFL_BLP_BC_CCA模型满足原则6即字段级安全原则，从而可知该该模型充分满足5G时代的字段级信息安全需求。

3 为什么CFL_BLP_BC_CCA模型解决了当今网络空间信息安全共性的卡脖子问题?

由上述分析可知,我们有如下命题:

命题10 CFL_BLP_BC_CCA模型解决了当今网络空间信息安全共性的卡脖子问题。

也就是说CFL_BLP_BC_CCA模型可以广泛应用于应用软件、数据库、操作系统、人工免疫安全计算机、物联网、未来网络、即时通信、电子邮件、文件管理、大数据、云计算、智慧城市、智慧家居、智慧海洋、区块链、无人机、自动驾驶、工控、工业4.0、中国制造2025、电子商务、电子政务，特别是电子政务外网、敌我识别、指挥平台、孤岛认证、人工智能、5G等各信息产业中。

- 谢谢各位领导、专家！
- 谢谢大家！