



中国物联网发展与基础思考



十进制网络标准工作组

刘亚东





一、物联网的本质探讨

什么是物联网？

一、物联网的本质探讨

- 国内外对“物联网”（Internet of Things）概念至今没有权威和统一的定义
- 世界上有一个物与物连接的互联网吗？答案是否定的。
- 物联网是传感器网！物联网是感知网！答案也不令人折服。
- 究竟什么是“物联网”？让我们先来剖析国际物品编码协会EPCglobal相关标准及应用原理。



EPC的编码、工作原理及与互联网的关系

EPC代码有64位、96位和256位3种，全部由数字组成

两个电子标签范例所采用编码为EPC-64 II型及EPC-96码：

10 0000000000000111 00000000000111 00000000000000
000000000000000000000111

01 · 0000A89 · 00016F · 000169DC0

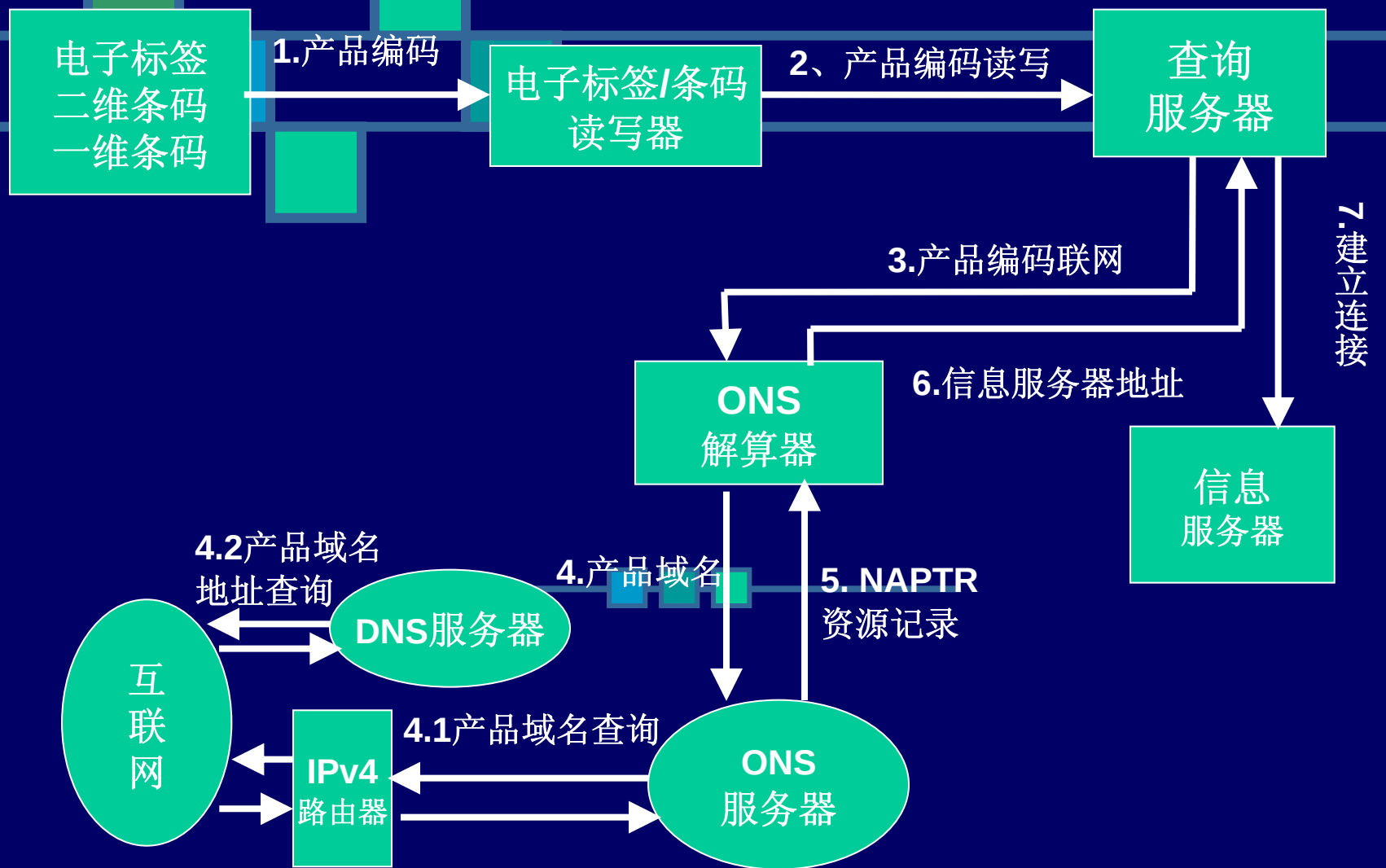
编码中（ABCDEF）是十六进制10-15的数字。

上述编码中含有版本号、域名管理者（生产或服务企业）、对象分类（产品）、序列号等信息。

仅从编码无人能够知晓其所代表的含义，要经过EPCglobal公司物品解析服务器（ONS）解析等7个步骤，在互联网上找到其相应的信息服务器：



物联网（电子标签/条码）上网信息查询过程



一、物联网的本质探讨

- 以上例证说明美国EPC体系是互联网上的三级域名解析体系，
- 连接和信息交换使用的网络平台还是互联网
- 物联网是互联网应用的延伸
- 物联网本质是物品要上互联网



一、物联网的本质探讨

由于历史原因，全球形成了：

ISO

EPCglobal

U ID

AIMglobal

IP-X

等多种电子标签标准体系并存局面，但清一色全由欧美等发达国家制定。实质上都是互联网的延伸，是三级域名解析体系。



一、物联网的本质探讨

物联网标准制定者制定了三级域名解析的编码、解析及传输协议等游戏规则；

物联网运行者拥有编码解析主服务器，中央数据库，物品编码的发放权利；

掌握了信息流向，掌握了行业话语权，实际控制了全球生产流通企业注册、全球所有商品和商品流通；

获取了巨额财富；

物联网运行者（编码解析服务器ONS拥有者）全面并一览无余的获取所有工业、经济、商品流通信息。



二、我国物联网（电子标签） 的应用与标准状况

二、我国物联网（电子标签）的应用与标准状况

权威人士认为我国物联网发展重大瓶颈是：核心技术竞争力不强，标准体系尚未建立，产品集中在低端，企业能力弱，信息安全等；

更让人担忧的是物联网行业发展存在“竞相造车、无人修路”，“只抓低端、不抓高端”，“只抓应用、不抓标准”，“安全威胁严重，不抓源头解决”；

对最核心的标准、编码、码址资源等关键问题则采取回避现象。而标准的缺位将影响整个物联网产业的发展。

二、我国物联网（电子标签）的应用与标准状况

此外，物联网不仅要有传感器、电子标签等硬件设备，码址资源即IP地址是物联网发展的基础性战略资源。没有IP地址的支撑，无论是物与物，还是人与物的信息交换，都无法实现。

据预测，我国未来IP需求量将达到300多亿个以上。国内物联网所需要如此巨大数量的IP地址战略资源从何而来？

如果我国物联网体系建立在国外标准体系上，不仅会对我国政治、经济、企业和个人带来严重的信息安全隐患，同时知识产权问题，也将给我国信息产业带来难以避开的桎梏。



二、我国物联网（电子标签）的应用与标准状况

这样下去，我国的物联网应用虽然有所发展，仅仅是发展了“物联网应用汽车”；

而所跑的“物联网高速公路”却都是外国修建，处处都是国外收费检查站；

我国不仅要付出巨额的费用代价；

所有经济、工业、流通领域信息彻底外泄；

一旦发生国外物品编码解析服务器对中国停止工作，中国的工业生产、物流、商品流通、居民生活保障体系将无法运转，面临崩溃，如何面对？





三、“物联网”的核心是编码 标准和信息安全

三、“物联网”的核心是编码标准和信息安全

物联网的灵魂是物品身份识别，通过物品编码为物品分配一个能够上网进行信息交换和处理的标识。

物联网标准最核心关键除了硬件技术，而更关键的是编码标准、网络资源IP地址、网络架构、信息流向和信息安全。

如果我国没有自己的物联网标准和编码资源，网络资源IP地址，在物联网上又会形成核心技术受制于人的局面：



三、“物联网”的核心是编码标准和信息安全

所有中国企业必须向国外机构申请注册，领取管理代码，事实上接受另一个国外管理手段；

我国工业生产、商品流通、物流、居民生活保障体系运作和信息处理处于外国解析体系控制之下；

所有企业注册及物品上网信息必然流向外国，造成我国经济、商品信息完全外泄并被外国掌握；

物联网标准、编码版权、主服务器和数据库法律定位在外国，中国无司法管辖权；

物联网的基础互联网核心技术、资源及管理也都是国外控制；

在物联网和电子标签的信息安全没有解决情况下，无处不在的物联网和电子标签形成无处不在的危险。



三、“物联网”的核心是编码标准和信息安全

物联网的标准涉及感知、身份识别、信息传输、应用和安全等多个领域；

物联网标准制定应该紧扣核心的感知、身份识别、信息传输和信息安全；

物联网的应用面广泛和普遍，物联网应用层的标准制定是最末段，

仅仅关注和讨论物联网应用层的标准则是拣了芝麻丢了西瓜。





四、正确分析对待国际标准

四、正确分析对待国际标准

- 标准是利益的博弈，又是立国之本。中国物联网标准必须适合国情又能与国际接轨
- 在国际还没有统一的物联网标准情况下，如何对待已经以企业为主或由某一个国家标准组织事实形成的“国际”电子标签标准，是必须面对的课题
- 世界知名标准化专家美国Sun Microsystems公司首席标准官Mr.Carl Cargill先生08年1月16日在北京发表《全球信息与通讯产业标准化发展方向中国的机遇》报告，对现行的国际标准做了剖析：



四、正确分析对待国际标准

- 标准是利益的博弈，又是立国之本。中国物联网标准必须适合国情又能与国际接轨
- 在国际还没有统一的物联网标准情况下，如何对待已经以企业为主或由某一个国家标准组织事实形成的“国际”电子标签标准，是必须面对的课题
- 世界知名标准化专家美国Sun Microsystems公司首席标准官Mr.Carl Cargill先生08年1月16日在北京发表《全球信息与通讯产业标准化发展方向中国的机遇》报告，对现行的国际标准做了剖析：



四、正确分析对待国际标准

- ①、目前世界上国际标准组织按照公正的程序产生标准：
 - ISO/IEC JTC1（国际标准化组织/国际电工委员会的第一联合技术委员会）
 - IEC（国际电工委员会）
 - ITU（国际电信联盟）；
- ②、有核心企业（大型跨国公司）控制的标准
- ③、超级企业形成的既定事实标准（如微软Windows、intel公司芯片）
- ④、美国控制的国际互联网标准（Internet）

四、1、国外专家对国际标准总体现状的看法

Mr.Carl Cargill:

今天，高科技领域的技术标准已经开始严重偏向私人利益，国际标准为主要美、欧、日等跨国公司控制。

当今的市场环境与中国利益不一致，发达国家有过多标准组织是中国的竞争对手。中国是世界上最大的消费市场，为什么却要在供应端开展竞争，中国为全世界供应了大量产品，为什么不能提供标准、标准化组织及标准的理念？中国为什么从国外输入标准和技术？

中国有能力改变世界，应该创造自己的游戏规则，应出口标准。

四、正确分析对待国际标准

- 外国专家的分析评价、质疑和中肯建议让我们汗颜。
- 我们应当反省过去习惯遵从和引进国外标准，在技术上俯首称臣的局面。
- 对待国际标准要有清醒的认识，不能盲目引进。
- 中国人应该也必须由引进标准到创造标准，出口标准，主动争取国际标准的制高点和话语权，体现国家

四、2、遵从国际标准的准则

- 技术本身没有国界，但技术有归属。在知识产权时代，外国资本往往利用技术标准对我国进行垄断控制，迫使我国被“钉死”在国际分工链的最底层，沦落为廉价“代工商”；外国资本则控制中国产业链标准，控制整个中国产业，稳居利润丰厚的产业链上游；
- 对此，中国近些年有极其深刻的教训。对采用国际标准必须衡量其对我国是否平等；对我国的制约及承受代价；是否有利国家长远发展及国际生存发展空间；是否能够保证国家信息安全及网络空间安全。是

四、3、自主创新与开放兼容

- 真正的出路还是自主创新，建立中国自己的物联网标准，从根本上改变受制于人的局面
- 中国物联网及电子标签标准目前是一张白纸
- 但中国必须拥有自主知识产权的物联网标准，自主创新与开放兼容，
- 积极参与国际标准的制定，抢占国际物联网技术标准的话语权和制高点，争取将我国自主标准上升为国际标准或将拥有我国自主知识产权的技术纳入国际相关标准中





五、物联网技术路线探讨

五、物联网技术路线探讨

- 为什么要采用三级域名解析体系构建物联网？
- 以三级域名解析为基础的物联网架构是先进的体系吗？其主要缺点是什么？
- 三级域名解析架构符合未来网络的趋势和潮流吗？



五、物联网技术路线探讨

实践证明，在三级域名解析为基础的物联网体系中，以数字为基础组成的物品编码（电子标签/条码）必须经过物品名称服务器ONS—DNS两次解析才能上互联网；

在技术上只能每次单个物品编码经过物品名称服务器（ONS）解析上网查询，在解决异构异地数据库的统一查询和管理，以及在网上一对多，多对一的查询、统计及信息处理上受到限制；

显而易见，ONS—DNS两次解析增加了网络负担，降低了网络通讯效率，不符合环保、低碳、绿色网络的原则，也不符合未来网络的发展潮流，这种技术体系也为物联网发展基础思考

五、物联网技术路线探讨

- 思其原因，物联网体系（三级域名解析）发明者，从互联网应用角度找到了通过物品编码两次解析上网的方法途径；
- 但由于其不是互联网技术的研究设计者，也由于当时互联网技术发展的局限，没有从互联网和物联网的底层探索二者更深层次的融合统一机制；



五、物联网技术路线探讨

目前，物联网的基础——国际互联网正处于推倒重来建设新一代互联网的革命技术路线与渐进发展技术路线激烈竞争的变革时期：

欧盟投资91亿欧元开发未来互联网要当世界领导地位；美国的计划支持了50个项目研究未来网络，有16个团队在研究未来网络架构；

国际标准组织ISO、国际电联ITU未来网络项目已启动并正按程序积极推进中；

中国物联网标准必须考虑核心技术路线的先进性，以及与国际新一代（未来）网络的同步发展。因此，中国不仅需要掌握物联网的核心技术及标准，更必须掌握国际未来互联网的核心技术及标准。

五、物联网技术路线探讨

- 中国物联网标准必须高瞻远瞩，立足新一代（未来）网络的新技术及国际标准，并与之同步，采用创新理念构建；
- 有无更先进的物联网构架？
- 答案是有的。非常可喜的是，中国科技工作者找到物品一步直接上互联网的技术途径并在2008年的项目中得到成功验证。



梅

不屑与凡桃俗李在春光中争艳，而是在天寒地冻、

万木不禁寒风时，独自傲然挺立，在大雪中开出繁花满树，

幽幽冷香，随风袭人。

六、新的物联网框架 及中国物联网的希望



六、新的物联网框架及中国物联网的希望

不屑与凡桃俗李在春光中争艳，而是在天寒地冻、

万木不荣寒风时，独自傲然挺立，在大雪中开出繁花满树。

- 随着物联网的升温，国内企业、标准化机构、政府部门意识到，只有掌握物联网标准制定主导权，从标准底层建立自主创新的技术体系和标准，才是中国物联网发展的道路。
- 让人欣慰的是，中国的企业和标准化机构已经开始向物联网国际标准进军，取得突破性的成绩。由我国提出并积极推动制定，ISO/PAS 18186《集装箱RFID货运标签系统》发布，正式成为国际标准化组织的可公开提供的规范。
- 中国企业和标准化组织开始进军并登上国际物联网标准制定舞台是中国物联网的希望。



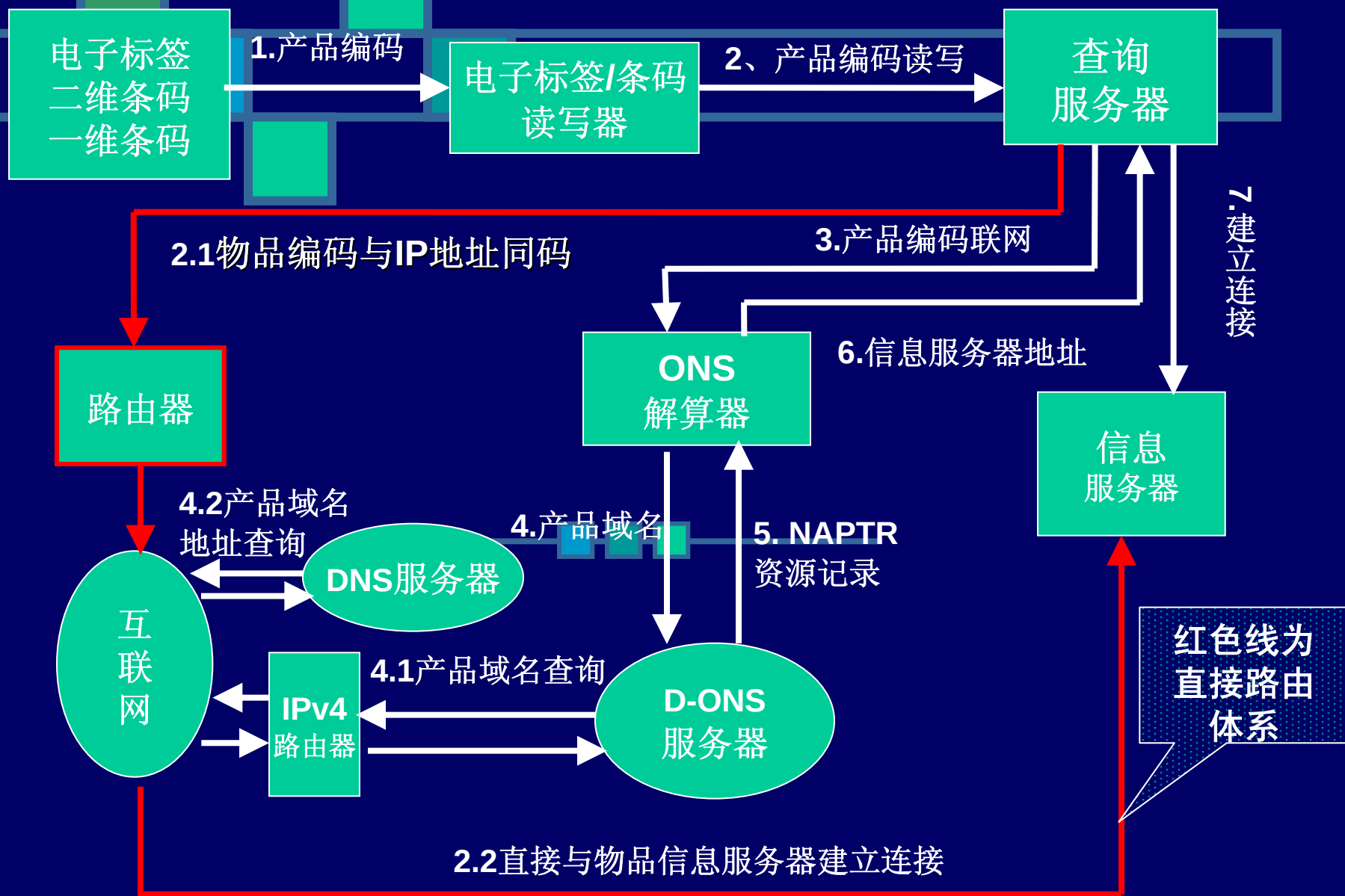
六、新的物联网框架及中国物联网的希望

芝兰生于幽谷，不以无人而不芳，君子修道立德，不为穷困而改节



- 与此同时，中国的自主创新企业及研究单位（如电子标签工作组数据格式组和十进制网络标准工作组等）也在深入剖析物联网底层协议的基础上，提出了新的物联网框架及标准理念：
- ① “大道归一”，物联网本质上是物品上互联网，物联网技术必须与互联网技术发展同步，物联网构建和标准制定必须着眼未来网络，着眼于互联网与物联网的统一；
- ② 三级域名解析体系物联网构架不是今后的方向，应该采用给全球每个物品分配一个互联网IP地址，一步直接上互联网，实现物联网与互联网的

三级域名解析体系物联网与一步直接上互联网的新物联网框架 上网信息查询过程比较





六、新的物联网框架及中国物联网的希望

宁可食无肉，不可居无竹。无竹令人俗。

无竹令人俗。

人瘦尚可肥，士俗不可医。

- ③直接路由是未来网络方向，可以使互联网全网通讯不再依赖 DNS域名解析系统，能够改变全网通讯依赖根域名解析服务器工作的现状，任何局部网络的损坏将不影响全网络的通讯，对保障网络通畅和信息安全又有了新的技术路线和解决方案；
- ④采用物品编码与互联网IP地址同码，物品的条码、电子标签、域名、IP地址四码同一，省掉ONS解算服务器、直接路由连接物品信息服务器，省掉了ONS-DNS两次解析，符合环保、低碳、绿色节能。



六、新的物联网框架及中国物联网的希望

不畏严寒，不辞寂寞

- 2009年欧盟信息社会与媒体总署网络企业及电子标签部科学与政策官员Mr. Peter Friess (Scientific and Policy Officer, Networked Enterprises & Radio Frequency Identification (RFID), European Commission Information Society and Media Directorate-General) 来华交流听到我们上述主张和理念后，脱口而出，这是挑战！（This is challenge.）。要我们提供书面材料。
- 事实上，物品编码与互联网IP地址同码技术已经在国内相关领域的器材管理系统实际工程项目中试验和验证成功。



六、新的物联网框架及中国物联网的希望

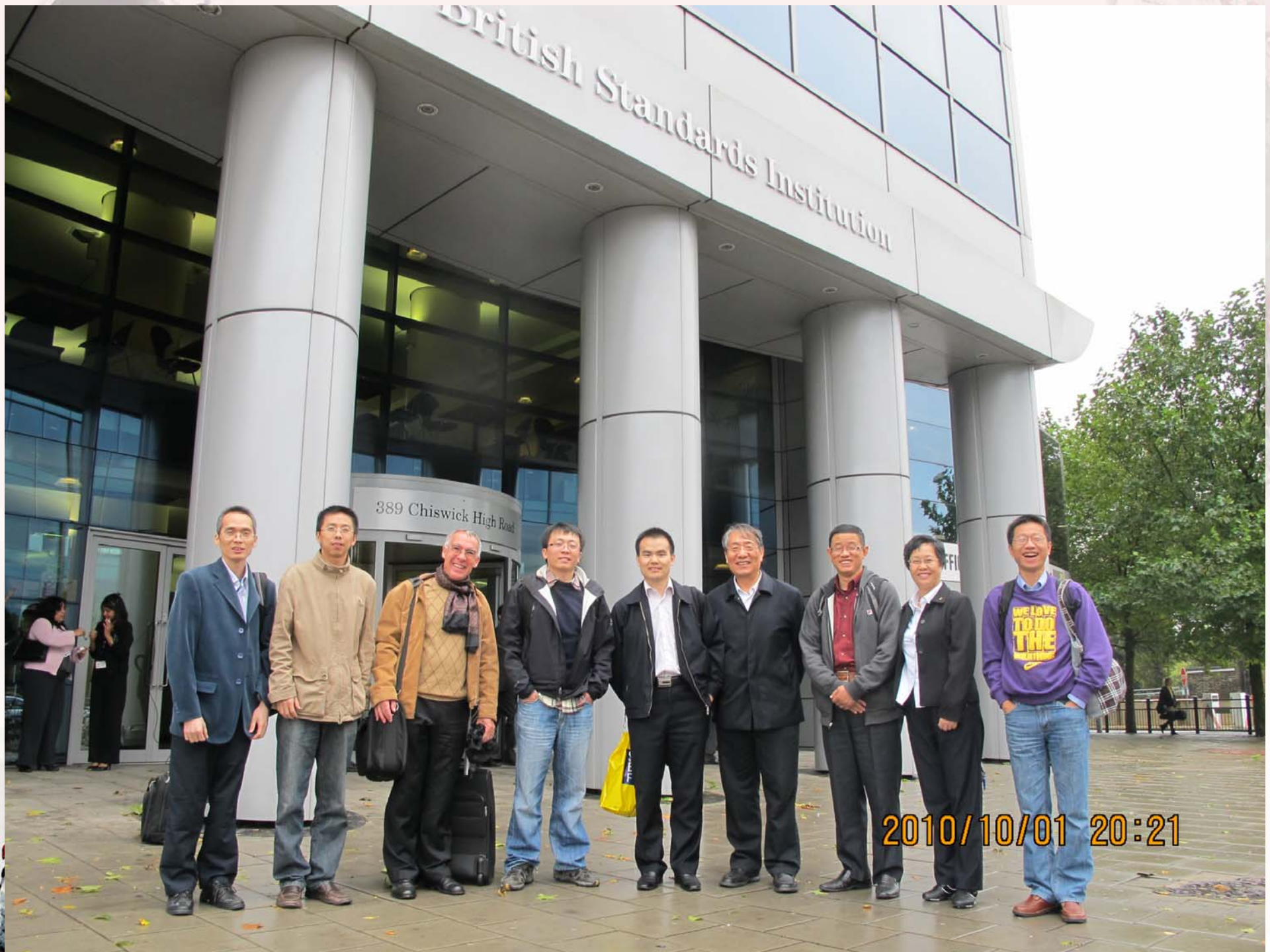
这种对物品分配互联网IP地址，一步上互联网的构架是物联网标准体系的重大基础创新。是物联网与互联网统一的技术框架结构，将在物联网领域开辟新的标准体系，会有巨大的市场和应用。

中国掌握上述物品编码与互联网IP地址同码技术、直接路由核心技术的自主知识产权；掌握IP地址资源、物品编码数据格式标准规则及相应而来的编码发放权力、解析协议、主服务器及中央数据库的所有权及控制管理权、同时掌控了物联网的信息流向等，实际拥有新物联网构架的国家管理主权。



六、新的物联网框架及中国物联网的希望

8月16日工信部科技司组织：中国教育科研网、清华大学、邮电大学、电信研究院、网通研究院、中国互联网中心、中国互联网协会、中国通信标准化协会、宽带无线IP工作组、工信部标准化研究所、北京合众联创技术有限公司、北京易恒信认证科技有限公司、上海通用化工研究所、十进制网络标准工作组等14家网络专家单位一致同意将《未来网络命名和寻址方案》及《实现可信连接的新通讯规则及可信路由器讨论》提交给ISO/C6, 并经工信部批准, 于2010年9月我国专家在国际标准组织ISO/IEC SC6未来网络会议上提出了《未来网络命名和寻址方案》及《实现可信连接的新通讯规则及可信路由器讨论》报告, 得到了会议的认可, 并已形成了会议文件, 并委任中国专家谢建平担任未来网络命名和寻址项目编辑。



British Standards Institution

389 Chiswick High Road

2010/10/01 20:21

RSA conference信息安全国际论坛

本月21-22日在北京中国大饭店举行了世界RSA conference信息安全国际论坛，刘亚东又代替中国著名密码专家南湘浩教授做了《未来网路及新路由器的讨论》（ Discussion on Future Network and Novel Router ）的报告发言。



RSACONFERENCE 信息安全国际论坛

CHINA 2010

10月 21-22日 | 中国大饭店 | 中国北京



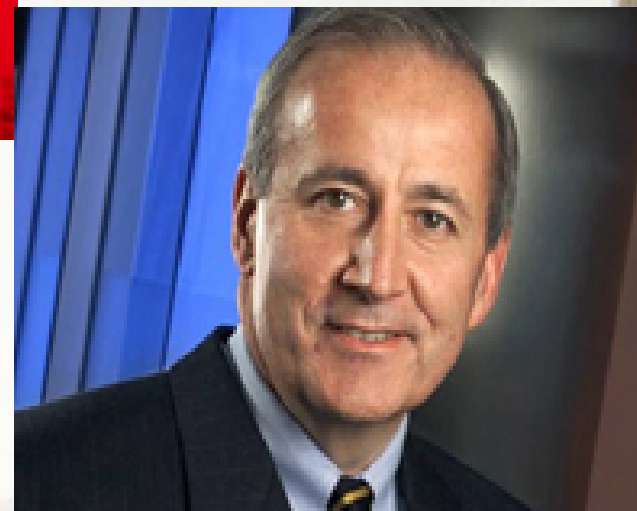
RSACONFERENCE

2010 信息安全国际论坛
International INFOSEC Forum



RSACONFERENCE

2010 信息安全国际论坛
International INFOSEC Forum





RSA®CONFERENCE

2010 信息安全国际论坛
International INFOSEC Forum

Discussion on Future Network and Novel Router

NAN Xiang-hao

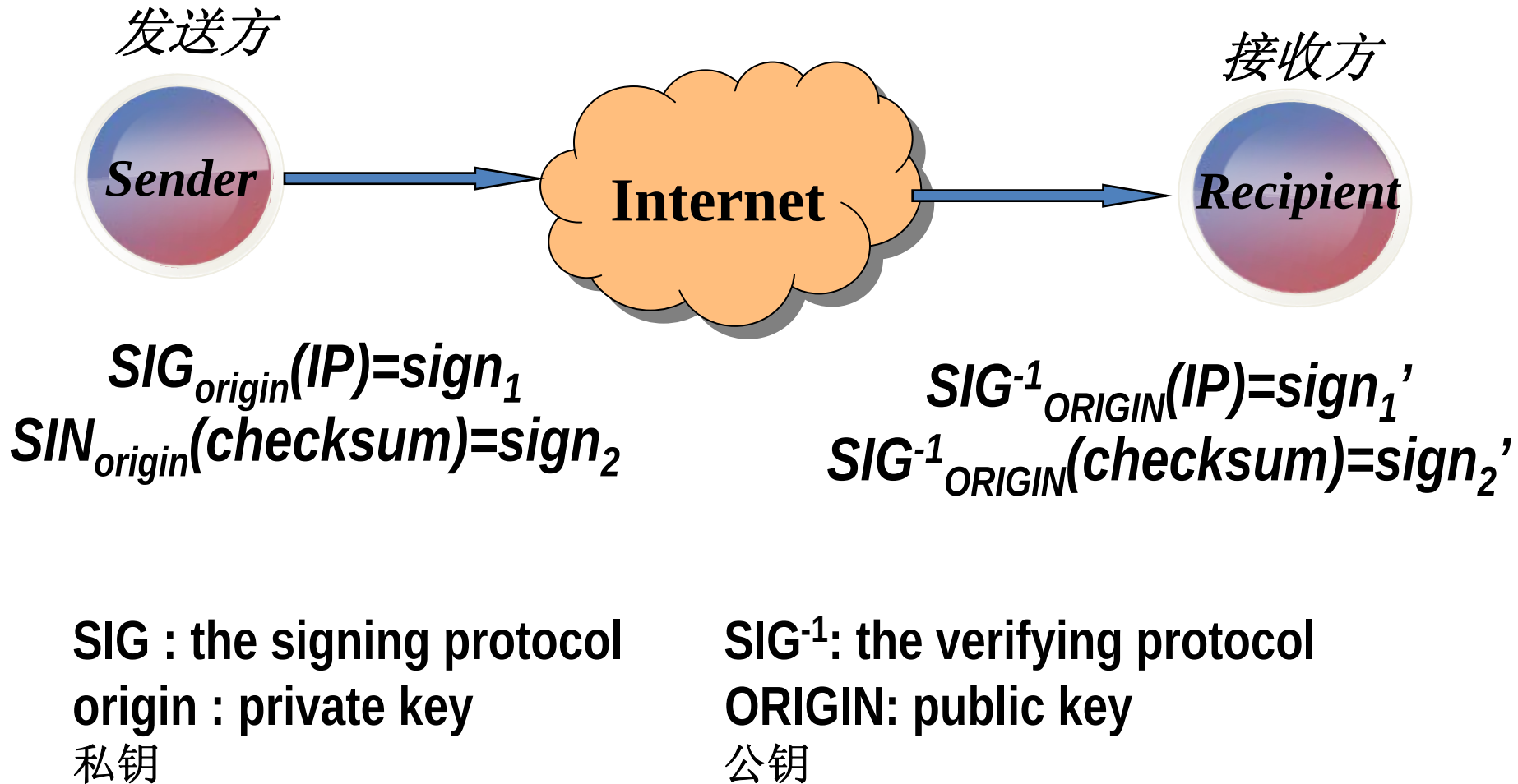
Information Security Laboratory, Peking University

LIU Ya-dong

China Decimal Network Standards Working Group.



“Pre-proof” (事先证明) and “Post-proof” (接收证明)



New Header Form新的报头格式



Version No.版本号	Traffic Class 通讯流类型	Flow Label 流标签	
Payload Length 有效负载长度		Next header 下一个头	Hop Limit 跳极限
Original address 源地址			
Destination Address 目的地址			
timer 时间			
authenticator 鉴别码			

An introduction to

CPK Cryptosystem (v5.0)

CPK 密码机制（5.0 版本）

GUAN Zhi

Information Security Laboratory, Peking University

2) CPK Structure 结构



1. Combining matrix: $(r_{i,j})$, $(R_{i,j})$ 组合矩阵

$$\text{SKM} = \begin{pmatrix} r_{11} & r_{12} & \dots & r_{1,32} \\ r_{21} & r_{22} & \dots & r_{2,32} \\ r_{31} & r_{32} & \dots & r_{3,32} \\ \dots & \dots & & \\ r_{h1} & r_{h2} & \dots & r_{h,32} \end{pmatrix} \quad \text{PKM} = \begin{pmatrix} R_{11} & R_{12} & \dots & R_{1,32} \\ R_{21} & R_{22} & \dots & R_{2,32} \\ R_{31} & R_{32} & \dots & R_{3,32} \\ \dots & \dots & & \\ R_{h1} & R_{h2} & \dots & R_{h,32} \end{pmatrix}$$

2. Separating key pair sequence: (s_i, S_i)

六、新的物联网框架及中国物联网的希望

- ✿ 新一代互联网（未来网络）整体框架方案中国概念：
- ✿ 通讯机制——从信任机制改变为怀疑机制；
- ✿ 通讯规则——从现有先通讯，后验证，改为先验证，后通讯，在数据传输之前进行原始地址验证，实现可信连接；
- ✿ 新的命名与寻址机制——验证报头ID标识证明地址真伪；
- ✿ 报头结构——在互联网报头中增加了标识（ID）认证，在数据传输之前进行原始地址验证，实现可信连接；
- ✿ 新通讯协议——具有直接路由功能，可以不需要域名解析系统（DNS）的新互联网通讯协议（Protocol）；
- ✿ 未来互联网方案再加上新的物联网框架：
- ✿ 采用物品编码与互联网IP地址同码，直接路由连接物品信息服务器的物联网框架方案；

六、新的物联网框架及中国物联网的希望

- ✿ 我国实际已经在世界上提出了创新的新一代（未来）网络及物联网标准框架方案中国概念。
- ✿ 找到了解决互联网信息安全，物联网与互联网融合统一的方案；
- ✿ 这是历经十多年的技术积累，形成了不受制于人的核心技术；
- ✿ 占据了未来网络及物联网标准制高点的有利位置，正在向世界互联网和物联网新的高度进军；
- ✿ 这将能够从根本上改变我国在网络技术核心技术受制于人的局面。

六、新的物联网框架及中国物联网的希望

- ❁ 这是一件利国利民，有益于人类的好事，同时也是一件艰巨的任务。需要国内网络业界、各方面同行及专家的精诚团结、携手努力和支持，共同参与完成；
- ❁ 十进制网络标准工作组愿意虚心向网络及物联网业界同行学习，相互交流，欢迎并希望对我们多加指导和支持；
- ❁ 愿意与业界同行携手努力，为我国物联网的发展打下了基础，让中国的创新理念和标准走向世界，提升成为世界标准。

谢谢！

Thank You!

十进制网络标准工作组 刘亚东

