Express of Intelligent Apllications of Cryptology

October 2010

PostPHD. Lan Luo
lanneverlose@gmail.com

[1]Networks & Intelligent Application of Block Cipher Lab.
[2]Automation Dep. Tsinghua University

Our Labs' LOGO:

NI ABC Labs

智能密码应用快递

2010.10

罗岚 教授[1] 博士后[2]
lanneverlose@gmail.com

[1]网络与分组密码智能应用实验室
[2]清华大学信息科学技术学院自动化系

使用了自己设计的实验LOGO，
如果有更好的创意，请MAIL给我。

NI ABC Labs

Content

Happy Mid-Autumn festival !

NI *ABC* Labs

目 录

中秋快乐!

NI ABC Labs

Skein 团队的保罗 T-Shirt 面向公众网售

- SHA3第二轮算法 Skein 的设计团队在网络上公开销售他们的 POLO T-Shirt : http://www.schneier.com/skein-shirts.html . “一团乱麻”的广告T-Shirt价格不低，估计是手工绣上去的
- Workhoreses 是 Skein 的设计者对HASH的看法,没有贬义,八个设计者之一 Bruce Schneier 的博客 CRYPTO-GRAM 是安全领域的前沿. 9月15日这一期,他们希望可以对算法硬件做更好的实现
- 到目前为止, Three Fish 还没有被公开宣称破解, 从这个分组密码算法演化出的单向函数 Skein 也没有被公开宣称破解. 演化算法之间有不同程度的关联,但是算法的安全系数,不同环境的运算速度构成的算法分数与演化算法链之间构成的是信念网：不是条件独立,但也不构成因果网.只是算法还没有与美女扯上关系
- 密码之间的信念网关系是我前段时间的研究方向之一,好象是在追究密码算法的出生和血缘关系,向源头算法的设计者致敬.这个网可以在算法本身的分数之外,看出另外的一些特点,类似教养这些只能感知,但对分数不构成直接影响的条件……

NI ABC Labs

轻型密码学之蜂窝(细胞)级别密码

- **John Magnabosco 在关于计算机语言与数据安全 “Protecting SQL Server Data” 里提出了蜂窝(细胞)级别密码 Cell_level Encryption**
- **蜜蜂从花和植物上采集蜂蜜，搜集到他们六边形的蜂窝里，每个窝用蜂胶保护。有专门的蜜蜂看守蜂蜜，只要胶层拖开，就可以偷到蜂窝。把数据也看成蜂窝的构造，对每个蜂窝细胞，蜂胶就是加密保护，称为蜂窝加密（Cell-Level Encryption，CLE）。不是所有数据都需要使用这个粒度和级别的保护。正确使用这个级别的保护，可以对数据处理的安全和流程上产生非常好的效果**
- 不考虑密钥分配过程,蜂窝(细胞)密码比通常意义的数据流加密密码轻,比量子流密码重.同样级别的密码还可以根据不同的粒度再进行细分.如果加入信噪比的因素,也许这样的某个粒度的密码更适合无线量子通信.网络上搜了搜作者的情况,WIKI 百科上有同名同姓的足球教练

NI ABC Labs

思科最近上传的安全技术文档

- 思科是全球网络硬件行业的顶尖公司,上传的技术文档可以开发获取,地址是:http://www.cisco.com/web/services/news/ts_newsletter/
- **2010年9月的技术文档里关于安全的内容有:IOS 使 VPN 更容易: 基于 TCP 的 IPsec 支持CISCO注册的任意端口;怎样在ASA 5500 系列防火墙界面里注册灰色区域(the Demilitarized Zone, DMZ). 技术注记: Cisco 在整体故障转移时的 SQL 服务复制**
- 看一看思科公司的技术文档,就知道他们做事情的细致和对网络的掌控,毕竟在限制领域的文档开放获取说明了思科的自信.在一些垄断行业用限制争取利益的时候,这些全球安全公司已在线了.桌面下的胜负已分,摆在桌面上的展示,以我的角度,应该没有任何规模的团体和个人对这些开放获取技术文档反感.只是在公司主页上如果加上他们的理念就更好.美国的信息安全公司发展还是比较快,以前用 NTRU 算法命名的公司在网络上已换名为安全创新应用公司: http://securityinnovation.com/ “信息安全是一个过程”的 NTRU 格言也从网络上消失了

NI ABC Labs

Moore's 定律：多国科学家首次实现双光子的量子游走

- 英国布里斯托尔大学等机构的研究人员在新一期美国《科学》杂志上报告了量子计算机研究领域的新进展。领导研究的杰里米·奥布赖恩教授认为，这一进展可能使量子计算机面世的时间提前到10年之内：http://www.sciencemag.org 2010.9.17
- 奥布赖恩教授说，从单光子到双光子是一个巨大的跨越，每添加一个光子，量子计算机可解决问题的复杂程度是成指数增加的，比方说单光子的量子游走可以带来10个结果，那么双光子的量子游走将可以带来100种结果。他说："许多人认为量子计算机至少要再等25年才会出现，但我们相信，在使用这种新技术之后，10年内就可能出现超越传统计算机的量子计算机。"
- 这项结果再次证明了莫尔斯定律的正确，到2020年，计算机从速度到硬件不得不被量子。以未来互联网的角度、以量子信息的角度，量子替代电子从硬件到软件都做好了充分的准备。有些五十多年前时髦的大学面向量子信息科技，准备怎样命名呢？

NI ABC Labs

哈勃最新观测到银河系“踢出”一颗超速恒星

- 根据 http://hubblesite.org/newscenter/ 哈博中心2010 年7 月报道: 一颗超炽热蓝恒星被飞速“踢出”银河系. 对该领域有兴趣的研究者可以直接联系该中心: Donna Weaver, Space Telescope Science Institute, Baltimore, Md. 410-338-4493, dweaver@stsci.edu
- 美国哈佛-史密逊天体物理学中心天文学家沃伦•布朗说：“使用哈勃望远镜，我们通过测量该恒星的运动方位，首次跟踪到这颗恒星的来源。它的运动来源方向指向银河系中心，在银河系内1000多亿颗恒星中，被放逐弹出的恒星为数非常少，大概每1亿颗恒星中潜伏着1颗弹出超速恒星。”这颗被命名为HE 0437-5439的恒星运行速度达到250万公里/小时，比太阳轨道运行速度快3倍。哈勃望远镜的观测结果证实这颗高速恒星是从银河系中心位置被弹出的。天文学家认为这颗恒星是1亿年前进入银河系中心的三恒星系统中的“幸存者”, 这有助于提供宇宙暗物质分布的重要线索
- 也许 HE 0437-5439 与上一期快递的”超级地球”有些渊源

NI ABC Labs

加拿大资深宇航员将任国际空间站站长

- 加拿大航天局9月2日宣布，加拿大资深宇航员克里斯·哈德菲尔德（Chris Hadfield）将第三次进入太空并从2013年3月起担任加拿大首位国际空间站站长。加拿大航天局说，哈德菲尔德将于2012年12月与一名俄罗斯宇航员和一名美国宇航员搭乘俄罗斯“联盟”号宇宙飞船进入国际空间站，执行为期6个月的任务
- 加拿大负责科学和技术的国务部长加里·古德伊尔在加拿大航天局位于魁北克省隆格伊总部举行的新闻发布会上说，选择哈德菲尔德担任国际空间站站长表明加拿大空间探索计划取得了成就，加拿大宇航员素质是优秀的。哈德菲尔德出生于安大略省的萨尼亚地区，现年51岁，空军上校，1992起担任宇航员，是3个孩子的父亲
- 照片里的未来空间站站长有些象世界银行行长佐利克,佐利克的经典语录：“我们可以有世界上最好的策略和构思，但是，除非能够付诸于行动，否则将不会成功。”

NI ABC Labs