2013年哥德尔奖

曾志坤 （516072910063 [897607449@qq.com](mailto:897607449@qq.com)）

1. 哥德尔奖简介：

哥德尔奖（Gödel Prize），由欧洲计算机学会（EATCS）与美国计算机学会基础理论专业组织（ACM SIGACT）于1993年共同设立，颁给理论计算机领域最杰出的学术论文。哥德尔奖包括5000美元的奖励。Kurt Gödel于 1906年出生在匈牙利的奥地利（现在的捷克共和国）。 哥德尔的工作已对第二十世纪的思想产生巨大的冲击。奖项表扬人们在的数学逻辑上和计算机科学的基础的主要贡献。（1）

1. 2013年哥德尔奖简介：

论文题目为：

For multi-party Diffie–Hellman key exchange and the Boneh–Franklin scheme in cryptography

Antoine Joux，Dan Boneh和Matthew K. Franklin的团队在计算理论的ACM研讨会获得2013年哥德尔奖优秀论文。ACM的特殊利益集团的算法和计算理论（SIGACT）与欧洲理论计算机科学协会（EATCS.）承认三者为他们的密码的概念和方案，提供更高的效率，灵活性和安全的贡献。 各自建立了基于密码学论文通过提供这种方法的安全性精确的定义配对场，和为其提供引人注目的新应用。 这些应用包括用户交换加密密钥，使他们私下和安全地与对方沟通更好的方法。

在他的论文中的Tripartite Diffie Hellman，Joux的工作，广义的两方密钥协商协议的多方密钥协商协议的Diffie和Hellman，注重与三方的情况。 他的作品使用一种公钥密码学基于椭圆曲线的代数结构。Joux显示了如何执行一个优雅的三方密钥协商协议使用配对椭圆曲线上的Weil和Tate发达，表明只有一个广播是每个人的要求。

Boneh和Franklin，在他们的论文中基于身份的加密从Weil，用Weil配对椭圆曲线上开发一个全功能的基于身份的加密方案（IBE）。 它依靠一种公钥加密，用户的公钥可以简单的用户身份或电子邮件地址相结合单主机公钥共同所有的用户。 这种方式取代发件人需要获得用户的公钥通过直接与用户交互，或通过一个发布数据库的用户的公共密钥。（2）

而有趣的是，似乎一些中国学者在这方面也有所突破。（3）

1. 作者介绍：
2. Antoine Joux

Antoine Joux在凡尔赛圣昆廷大学兼职教授恩伊夫林和兼职高级安全工程师cryptoexperts。 在当地的师范érieure燮在巴黎的计算机科学系的前成员，他在法国对信息系统安全的中央首长科学副主任。

|  |
| --- |
| Antoine Joux的个人信息表格 |
| 图1-1  图1-1为Antoine Joux |
| 个人简介：  他是伊夫林省凡尔赛圣昆廷恩大学在计算机科学上的副教授，法国国家科学研究中心研究员，目前他是密码学的椅子基金会的partenariale，属于UPMC，是éprofesseur协会在信息学实验室巴黎和高级加密安全专家。（4） |
| 研究主题（4）：   1. Lattice Reduction 2. Discrete Logarithms 3. Elliptic Curves 4. Collisions and Collision-related Algorithms 5. Various Cryptanalytic work |

1. Dan Boneh

Dan Boneh是一位教授计算机科学与电气工程在斯坦福大学。 编辑的<em>期刊ACM</em>，他获得博士学位，在普林斯顿大学计算机科学。 他获得帕卡德奖，艾尔弗雷德P.Sloan奖，特曼奖，和RSA奖。

|  |
| --- |
| Dan Boneh的个人信息表格 |
| 个人介绍：  在斯坦福大学教授计算机科学和电气工程，是斯坦福大学计算机安全实验室主任。主要研究重点是应用密码学与计算机安全。 |
| 主要贡献（5）：  在密码学中的贡献包括：   1. 2015 隐私保护的偿付能力证明比特币交换 2. 2010 他是参与设计tcpcrypt传输层安全协议的扩展 3. 2005 第一个广播加密系统具有完全抗共谋（Craig Gentry和布伦特水域） 4. 2003 定时攻击OpenSSL（与布伦利） 5. 2001 一个有效的基于身份的加密系统（带马特·富兰克林）基于Weil配对。 6. 1999 分析RSA当密钥小于n零点二九二（与Glenn Durfee） 7. 1997 故障分析（与公开密钥系统李察·J·立顿和德米洛） 8. 1995 抗共谋指纹编码的数字数据（James Shaw） 9. 1995 分析运用DNA计算机（Christopher Dunworth李察·J·立顿）   在计算机安全中的贡献包括：   1. 2007 显示网站采取响应HTTP请求的时候可以泄露私人信息。 2. 2005 pwdhash浏览器扩展的透明产生每个网站不同的密码 |
| 个人邮箱（5）：  dabo@cs.stanford.edu |
| 获得奖项（5）：   1. 帕卡德奖 2. 史隆研究学者奖 3. 特曼奖 4. 2005年RSA奖 5. 2013年哥德尔奖 6. 2014年计算机科学ACM Infosys基金奖 |

1. Matthew Franklin

Matthew Franklin是加利福尼亚大学计算机科学的教授，是哥伦比亚大学的研究生和博士学位，在计算机科学。 他从加利福尼亚大学数学学士学位，伯克利获得了硕士学位和从波莫纳学院获得了一个数学学位。 他主编过学术期刊。 他收到国家自然科学基金奖，并且是AT&T贝尔实验室的博士学者。（3）

|  |
| --- |
| Matthew Franklin个人信息表格 |
| 图2-1  图2-1为Matthew Franklin |
| 个人经历（6）：  于1994年二月获得了计算机科学博士学位。在2000七月加入U.C. Davis，曾在各种研究实验室工作（在CA帕洛阿尔托Xerox PARC；在弗洛勒姆帕克AT&T 实验室、NJ；默里山的AT&T贝尔实验室，NJ）。2016年春在进行ECS120的教学 |
| 研究兴趣（6）：  包括各种各样的密码 主题和分布式计算，包括电子商务协议 ，门限密码学、安全的分布式计算， 组合安全性，电子投票等。 |
| 其他（6）：    图2-2 图2-3  图2-2，图2-3为Matthew Franklin的家庭照片 |

1. 文献索引
2. <http://baike.baidu.com/link?url=0UZHtpyvekNyf4QGxMZwSf2_xuYRTttAMIkI6WvMN-FKypkvUi6DvIaGM-UjRf7YCRQqwx7y9VJvdA7aQ5N7q950JJ6APBFAWaMpOc1go7u8tv-MuYUlxCsZfGPnyauH>
3. <http://www.acm.org/press-room/news-releases/2013/goedel-prize-13/>
4. <http://ste.xidian.edu.cn/html/index_activity/2016/0319/2549.html>
5. <https://www-almasty.lip6.fr/~joux/>
6. <http://translate.baiducontent.com/transpage?cb=translateCallback&ie=utf8&source=url&query=http%3A%2F%2Fwww-polsys.lip6.fr%2F~joux%2F&from=en&to=zh&token=&monLang=zh>
7. <http://web.cs.ucdavis.edu/~franklin/>