
ISC
2015
中国互联网安全大会
360互联网安全中心
ISC
2015
数据驱动安全
2015 中国互联网安全大会
China Internet Security Conference
电子取证论坛

九天之外听惊雷 九地之下隐剑客

全同态加密技术给网络空间取证带来的新挑战

CPS-DSC教育部重点实验室（重庆大学）向 宏
重庆市公安局电子物证司法鉴定中心　　田庆宜

2015.9.30

“鲁道有荡，齐子翱翔”

《国风·载驱》

- 网络空间的特点是什么？
- 网络空间有什么基本定律？
- 它又如何影响网络空间安全？

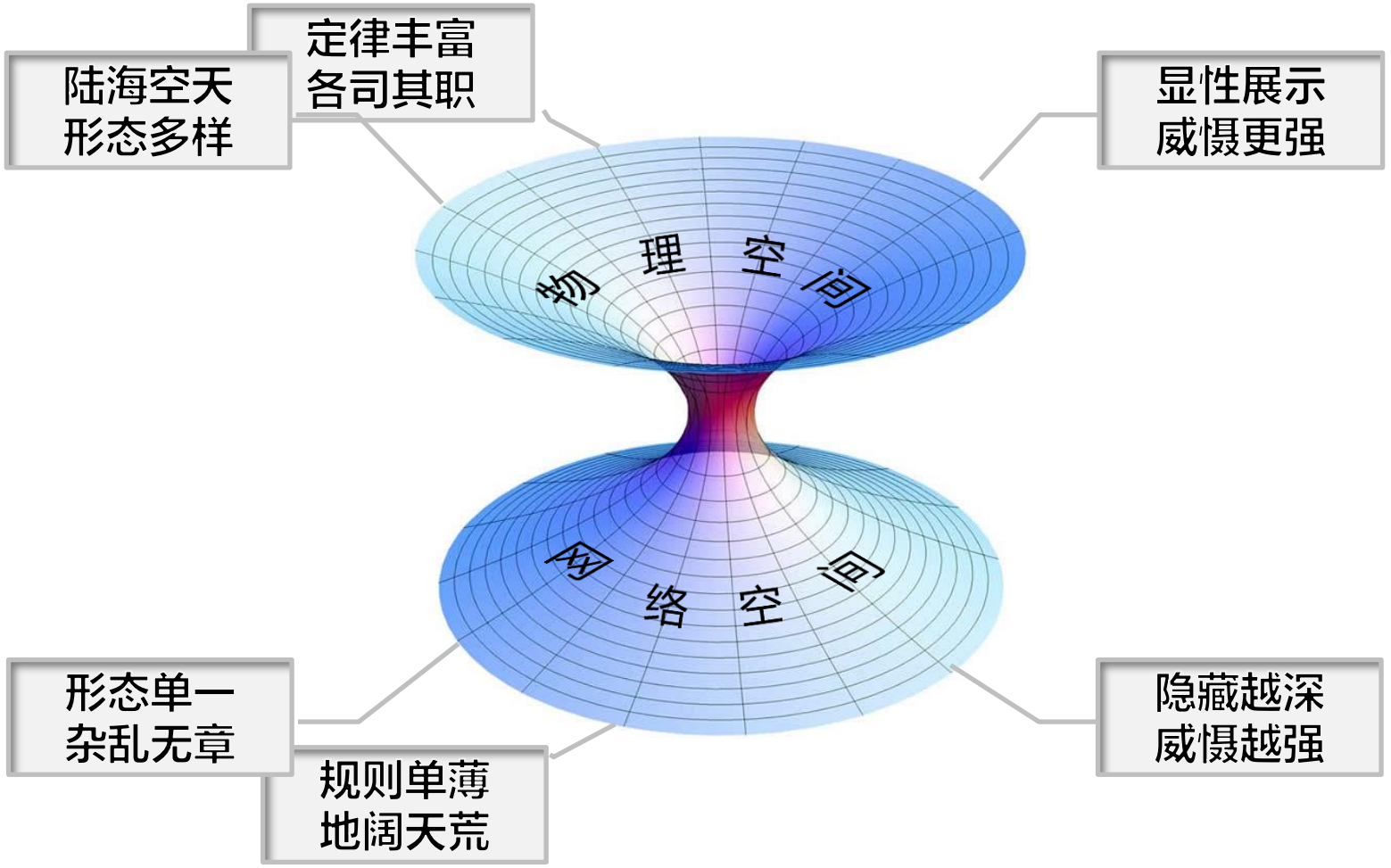
人造空间！人造空间！！人造空间！！！

The man-made nature of cyberspace distinguishes it from the other domains in which the U.S. armed forces operate. The Administration will continue to explore the implications of cyberspace's unique attributes for policies regarding operations within it

网络空间的人造特征使得它与美军活动的其他领域有所区别。为了能够制定相应的策略以便在其中进行活动，国防部将持续探索网络空间独特的性质。

--美国国防部《四年防务评估报告》2010.2

物理空间与网络空间：对称不对偶



“它山之石，可以攻玉”

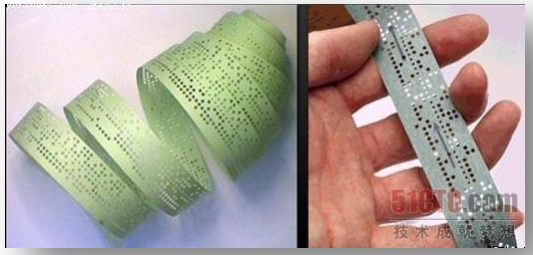
《小雅·鹤鸣》

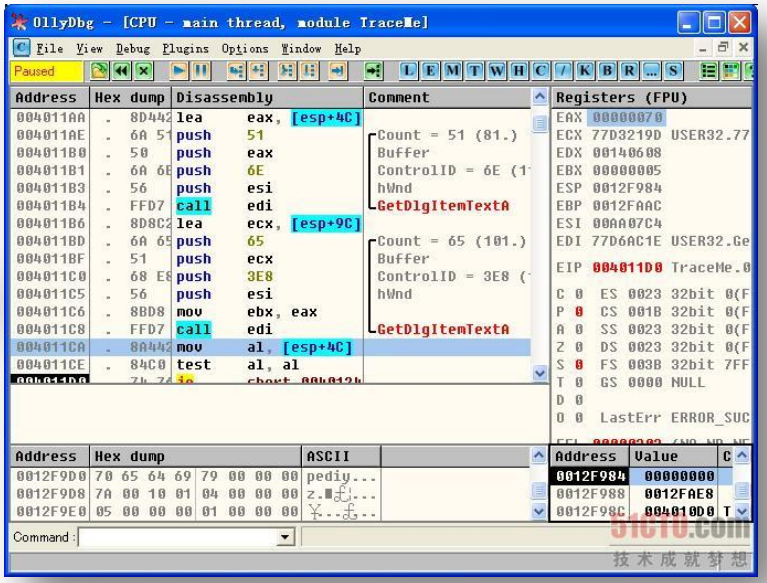
- 几个常见的场景
- 全同态加密一瞥
- 发展现状与趋势

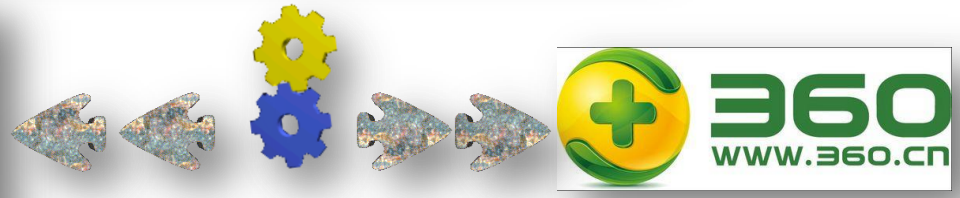
场景一：反编译技术与取证

成熟且常用的取证技术之一是对恶意代码进行特征值提取

规避特征值提取是黑客们梦寐以求的目标...







场景二：加壳技术与取证

对恶意代码加壳，进入目标系统之后再行脱壳是黑客常用的伎俩之一

- 对主流的壳进行建库对比
- 对内存进行监控

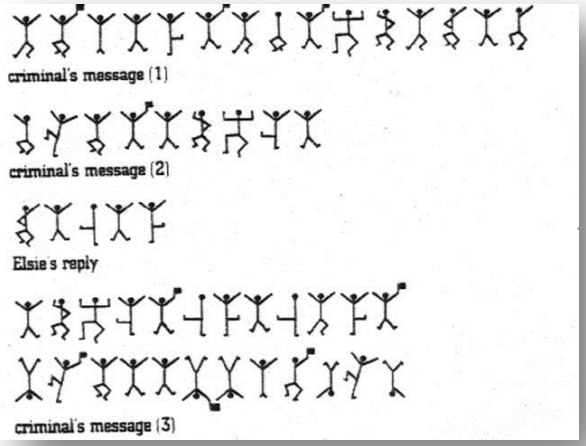
可能出现既无需加壳，又能规避监控的技术吗？

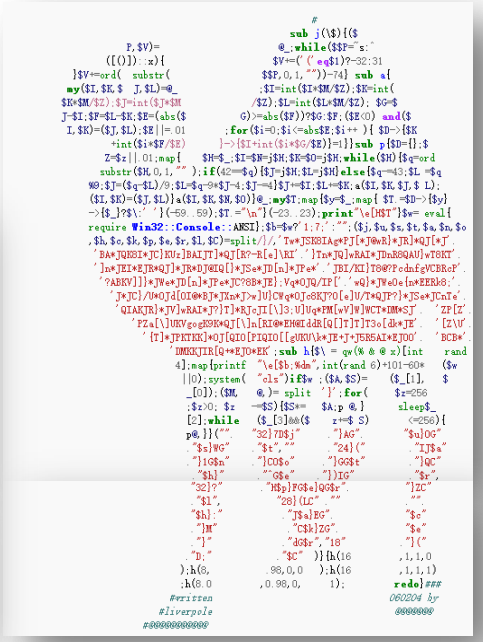
场景三：代码混淆技术与取证

```
print "Just another Perl hacker,";
```

```
@P=split//,".URRUU\c8R";@d=split//,"\nrekcah xinU / lreP rehtona tsuJ";sub p{
@p{"r$p","u$p"}=(P,P);pipe"r$p","u$p";++$p;($q*=2)+=$f=!fork;map{$P=$P[$f^ord
($p{$_})&6];$p{$_}=/ ^$P/ix?$P:close$_}keys%p}p;p;p;p;p;map{$p{$_}="/^[P.]/&&
close$_}%p;wait until$?;map{/^r/&&<$_>}%p;$_=$d[$q];sleep rand(2)if/\S/;print
```

- 从本质上来讲，以往的代码混淆（code obfuscation）技术是人类“语言文字艺术”在计算机编程语言领域的延伸，如同早期的密码技术一样（还记得福尔摩斯侦探集“跳舞的小人儿“吗？）
- 是否存在这样的方法，将代码混淆技术“数学化”吗？正如经典密码学所走过的道路一样？
- 这样一来，代码混淆技术就建立在了坚实的数学理论基础之上，从“必然王国”奔向了“自由王国”

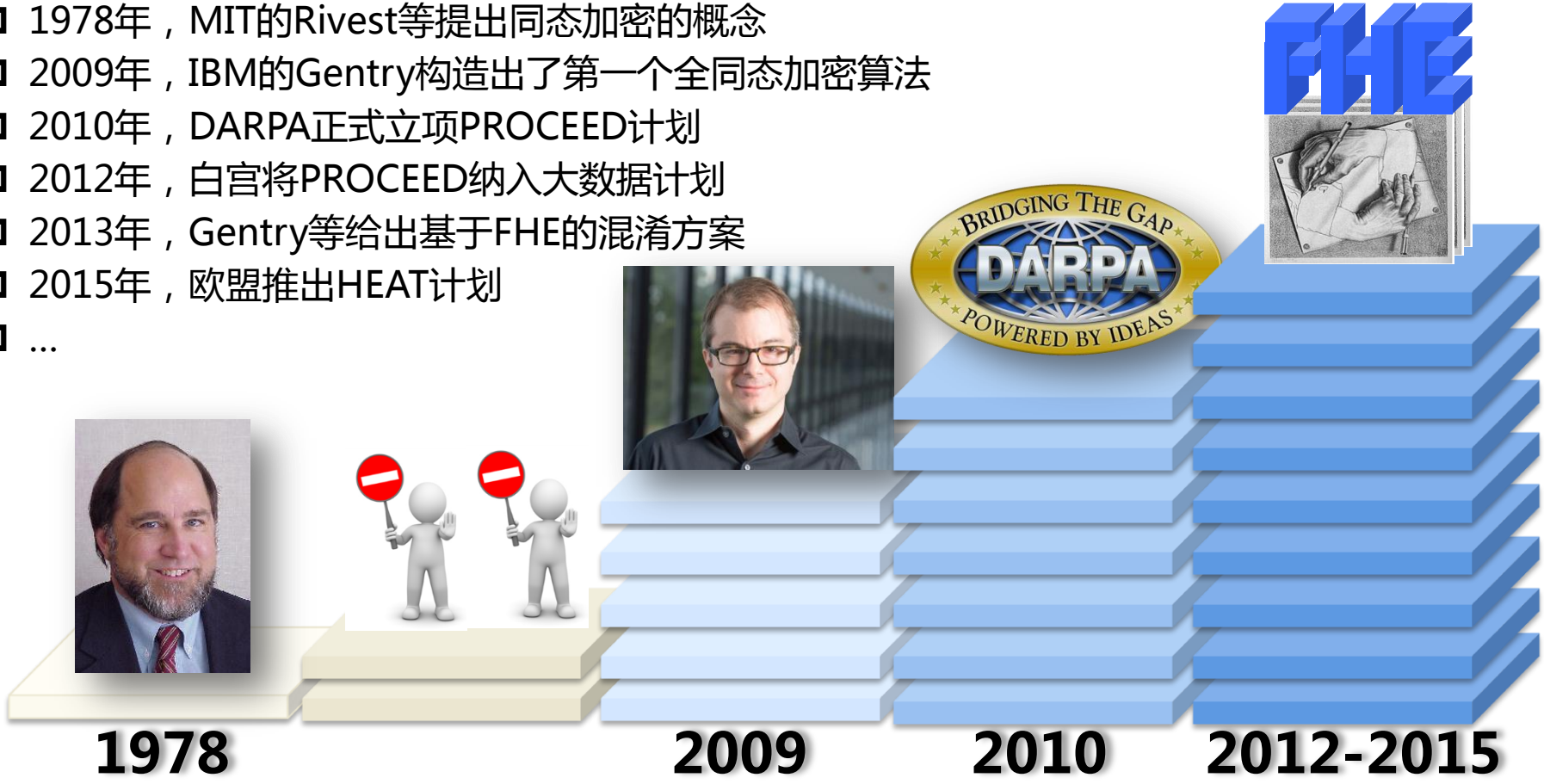




全同态加密“简史”

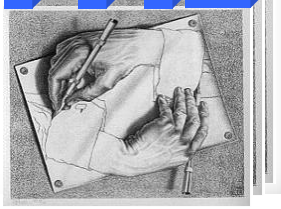
全同态加密大事记

- 1978年，MIT的Rivest等提出同态加密的概念
- 2009年，IBM的Gentry构造出了第一个全同态加密算法
- 2010年，DARPA正式立项PROCEED计划
- 2012年，白宫将PROCEED纳入大数据计划
- 2013年，Gentry等给出基于FHE的混淆方案
- 2015年，欧盟推出HEAT计划
- …



发达国家眼中的全同态加密技术

FHE

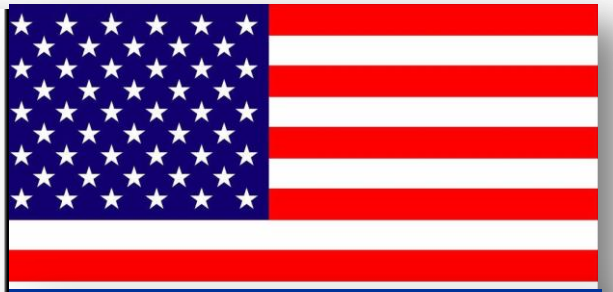


PROgramming Computation on EncryptEd Data (PROCEED)

Broad Agency Announcement

DARPA-BAA-10-81

July 6, 2010



Big Data Across the Federal Government

March 29, 2012

The ***Programming Computation on Encrypted Data*** (***PROCEED***) research effort seeks to overcome a major challenge for information security in cloud-computing environments by developing practical methods and associated modern programming languages for computation on data that remains encrypted the entire time it is in use. Giving users the ability to manipulate encrypted data without first decrypting it would make interception by an adversary more difficult.

HEAT

Homomorphic Encryption Applications and Technology

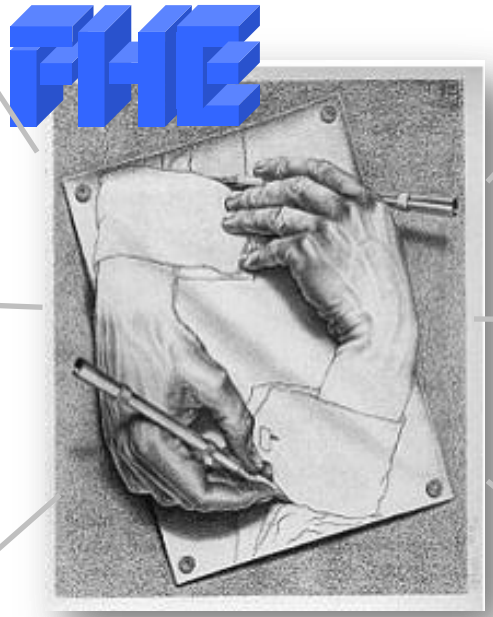
H2020-ICT-644209

全同态加密技术及应用一览

首个能够对密文进行操作的加密技术

对密文操作的结果等同于对明文做相同的操作

基于格上困难问题有望替代RSA等



应用一
芯片设计保护

应用二
软件补丁升级

应用三
多方安全计算

“全同态加密技术可解决在不可靠环境中对密态数据进行计算这一难题…一旦全同态加密技术得以实用化，必然有力推动云计算、大数据等产业的应用步伐。”

--中国密码学会《密码学科发展报告2015》

“维天之命，于穆不已”

《周颂•维天之命》

- 对现有取证技术的冲击？
- 还会产生什么全新的形态？
- 带来什么新的挑战？

“公理化”的代码混淆技术

以全同态加密为基础，采用所谓“多线性映射”这一工具，Gentry等人给出了全新的混淆方案（2013）。这一方案的一个重要成果是：**程序代码可实现功能等价传递。**

A

```
print "Just another Perl hacker,";
```

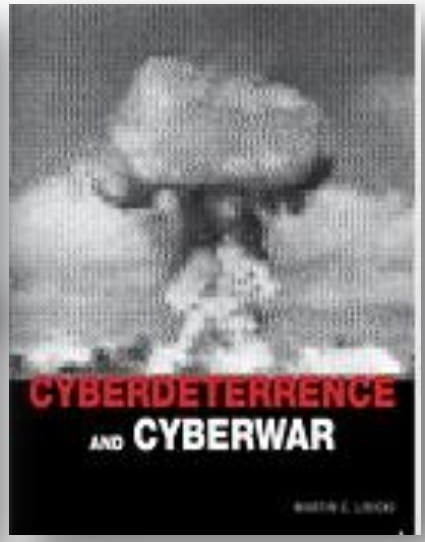
B

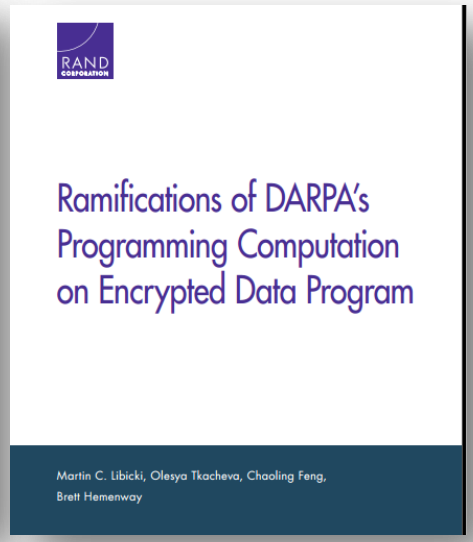
Just another Perl hacker

- 程序A和B的输出均为“Just another Perl hacker”
- **程序B**无法直接反编译（除非知道私钥，解密后再反编译）
- 前面提到的案例一和案例二均有实现的可能，从而给包括电子取证在内的网络空间安全带来严峻的挑战。

兰德公司告诉了DARPA什么

RAND CORPORATION





BRIDGING THE GAP
DARPA
POWERED BY IDEAS

一旦PROCEED项目成果全球推广，对美国及其竞争对手而言谁更具有战略优势？

- 受DARPA委托对PROCEED项目进行风险评估
- 主要应用场景：多国联合作战、GPS地图密文检索…
- **这是否意味着对电子取证等领域全新的挑战？**

全同态加密将挑战网络空间取证

多方安全计算

多国联盟
联合军事行动

跨国追逃

网络空间跨国犯罪

跨国网络传销
跨国网络赌博

- 有几方参与了交易？
- 涉案金额有多大？
- 如果均采用全同态加密进行盲交易，如何定罪量刑？
- 主从犯如何认定？

“潘多拉之盒”已悄然开启

- 尽管全同态加密技术的效率目前还比较低下（与现有的加密技术相比）
- 基于全同态加密的混淆技术还在遭受新的攻击（2015）

- 但阿拉丁神灯/潘多拉之盒已然开启
- 全同态加密技术未来五年将逐步投入**实用**
- 它悄然改变人们传统上对加密技术的**定位**
- 网络空间的攻防态势将展开新一轮的**博弈**
- 网络空间的取证技术也必将产生新的**变革**

故兵无常势，水无常形，
能因敌变化而取胜者，谓之神