《密码学的新方向》读后感

——跨时代意义的文章

当读完文章后，有种莫名的崇拜感油然而生，是因为密码学的在科学史上的真正登台，是因为一篇结构清晰内容丰满的学术论文发表，是因为具有跨时代意义的时间节点已经到来。很难想象，在缺少前人研究工作的条件下，是如何将行业中所遇到的问题障碍进行高度概括，并且对这些问题提出何种解决方案，更重要的是，是如何通过一篇寥寥十几页的文章，激起密码学工作者的研究热情。一想到此处，即便不是科班出身，内心的激动也难以平复。

首先，我先对《密码学的新方向》文章进行简要的概述。

“摘要”部分明了地介绍了当代密码学的两大主要核心发展方向，也是文章的重点讨论部分，同时指出密码学当时所面临的具体挑战，并在后续的短短数十字中概括论文所要进行的工作，以及对密码学的应用如何解决长期存在的问题进行深层次的讨论。虽然作者在摘要中没有明确说明具体问题的具体解决方案，但是却提供了一条可依循的逻辑线索：问题是什么，如何解决。

“介绍”部分中，先对当时行业背景简单描述，并对背景下存在的问题和阻碍密码学发展的因素进行抽象概括，同时对核心问题首次引出作者的解决方案，总的来说，“介绍”部分是对“摘要”中背景问题的扩充，理清文章结构，简要提及解决方案。

由于“硬件的廉价化”，密码学的应用场景被不断扩大到各类商业应用场景，应用场景增多反映市场需求增大，密码学开始了从量变到质变的过程——对通信会话的安全性和身份认证有更高的需求，而这类需求归根结底，终是密码学理论如何在实际上应用的变现。是市场带动行业发展，行业发展带动科学建立，是需求将密码学从艺术变为科学，所以密码学的发展不能偏离实际，也正如文章中不断提到的“应用价值”。

当前行业中的主要问题或面对挑战有两大：**第一，在不安全传输信道中如何阻止攻击者窃取数据**；**第二，阻碍远程事物处理系统取代当代现有商业通信手段的认证技术，如何创新以满足市场的新需求**。对于前者，作者提出公钥密码体制和公钥分配系统，并对两者进行简要的描述和对比；对于后者，作者提出单向认证的解决思路。在简要交代文章后续解决方案的简要内容后，着重提到密码学目前的难题。

“常规密码体制”部分是文章核心章节的开始，提及当前密码学的两大核心研

究方向——加密和认证，以及已经存在的密码学加密技术。其中，我认为最为关键的是，作者在此将后续提到的与密码学相关的概念：

1. 密码学核心方向：加密与认证。
2. 计算安全：建立在密码分析的计算复杂性上，且能被穷尽计算破译。
3. 无条件安全：嫩抵御任何形式的密码分析攻击。
4. 密码系统的分类：流密码系统和分组密码系统。
5. 密码系统面临的威胁分类：唯明文攻击、已知明文攻击以及选择明文攻击。

采用“概念 + 例子 + 现状”的方式，对以上概念进行一一解释说明，并在恰当的位置提出自己的方案。最终，对现有常规密码体制进行小节概括，和引出下文的解决方案。

“公钥密码体制”部分是作者针对第一大挑战（在不安全传输信道中如何阻止攻击者窃取数据）的解决方案。首先针对当前的常规做法（N 用户通信需要$(n^2-n)/2$ 个密钥对）进行说明和点评，之后在其基础上正式提出公钥密码体制：公钥密码算法和公钥分配算法。文章首先对公钥密码算法进行定义和明确算法必须满足的条件，同时举例说明公钥密码算法的可行性，并总结出公钥密码算法的本质：“**单向编译器：将容易理解的高级语言程序翻译成等价的难以理解的机器语言程序，编译器的编译过程是单向的，其逆翻译过程是计算不可行的**”。之后以 Markle 的研究开始讨论公钥分配算法，提出了具有传输单一密钥、密码分析者破译的时间开销是系统使用者的指数倍、算法及其参数可公开三大有点的密钥分配算法，该密码的有效性依赖于计算有限域中离散对数的困难性，并给出相关示例。

“单向认证”部分是作者针对第二大挑战（面对现有的不能满足市场需求的认证技术，如何创新）的解决方案。认证问题需要保证发送方不被第三方冒名顶替，也要解决发送发和接收方之间的矛盾。此节内容先以多用户登陆情况为例，提出系统不存储用户真实密码，而是存储经过单向函数处理后的结果，并在此例子中引出**单向函数的特点：单向函数正向运算计算量小，逆向运算计算量巨大，即逆运算在计算上不可行**。由于逆向运算计算量大，攻击者破解公开密钥的难度极大，所在在不安全信道中的通信是有安全保障的，即单向函数在密码学中的应用可以解决当前的问题。其后，作者以 Lesile Lamport 所提出的解决方案（k 维二进制向量空间上单向函数 f 到其自身的映射）以及另一种解决方案（与时间 t 和单向函数 f 存在关系）进行说明。

“问题的相关性和陷门技术”部分则是将密码学遇到的问题进行高度总结，

概括为一下三个核心问题：

1. 一个对已知明文攻击安全的密码算法能产生一个单向函数。其中提到优秀的加密算法应该具备这样的特点：**对于定义域中的任何一个值，映射的结果是随机的（即值域中的任何一个 y 都是等概率等于 $F(X_i)$ 的）**。允许小程度的退化，绝不允许大程度的退化，极端例子为，对于 F，其定义域中的任何 x，都映射为固定的 y，则加密根本不取决与密钥。
2. 一个公钥密码算法可用来产生一个单向认证体系。公开加密算法和解密算法，保存核心密钥就能有效预防攻击，所谓陷门就是缺一不可。
3. 一个陷门密码算法可用来产生一个公钥分配算法。但是目前几乎没有证据能够证明陷门密钥的存在，这也是阻碍发展的问题所在。

“计算复杂度”部分是讨论密码分析问题就是属于数学领域中何种层面的问题，而结果是密码学分析问题是数学中的 NP 完全问题，其计算复杂度大且结果不确定，即便在最坏情况下，求解也相当困难。

“历史回顾” 部分则是从历史的角度观察密码学的发展过程：

1. 混淆密码系统中什么该保护，什么不该保护。过去保密的是加密解密算法，安全性依赖于算法过程的保密性；而现在公开所有的加密解密算法，保护的是密钥，安全性依赖于计算单向函数的逆函数的计算复杂度。
2. 曾经密码学受到工业设备条件不足的约束，现在硬件设备廉价，密码学开始了改革和完善。
3. 证明密码系统稳固性的方法由原先认为“使用数学证明是错误的”，到现在“数学证明”是最好的方法。

不管如何，密码学的发展史中有这样的特点：是业余爱好者和专业密码人员共同努力研究的成果，都离不开这些人的不懈努力。

感想

在读完论文后，对我的启发很深，我觉得一篇优秀的论文应该有以下特点：

1. 毫不含糊的摘要说明，简短描述当时背景和高度概括主要问题，并简述工作内容。
2. 介绍部分要将摘要中的背景和问题进行补充，举例说明，同时要对文章结构

进行梳理说明。背景和问题的提出直接影响后续解决方案的提出是否合理有效。其次，文章结构也要在介绍部分进行概要说明，让读者对文章要大体的了解。

3. 继摘要和介绍之后，最为重要也是直接影响解决方案合理性的部分就是第二节（因文章内容不同，标题有所不同）。愚以为第二节所承担的责任有一下三点：

   a) 前人工作、现有工作的陈述说明；

   b) 后续技术相关概念的定义和解释；

   c) 文章解决方案和已有工作的简单对比。

   上述三点的重要意义在于确认文章所提出的解决方案是否存在重复性工作、是否有创新点等。

4. 对于后续解决方案的提出，《密码学的新方向》提供了很好的论文书写样例，其流程如下：

   a) 先描述当前对同一问题的常见解决方案，并陈述其不足；

   b) 提出方案想法，并给出定义；

   c) 举例说明具体实际应用效果；

   d) 列举同期工作者对同一问题的解决方案并予以简单的对比。

除以上所说的四点以外，优秀的论文（如同《密码学的新方向》）在解决方案的描述中必须要有足够的数学理论支撑（没有数学理论支撑的论文就很难得到“最好证明方式——数学证明”的证明），其次在阐述过程中，要给予恰到好处例子说明（无论是例子的数量还是例子的质量）。但是，在阅读这篇文章的途中，我觉得之所以《密码学的新方向》能够受到如此瞩目的原因不仅仅是其作者们所提出的优秀解决方案，更重要的是这是一篇贴合实际、强调价值的理论应用于实际的文章，而不是空穴来风的需求，加上虚无缥缈的解决方案。其实，这都源自于作者们对当代密码学发展有着充分的认识和了解，才能够如此高度概括问题和所面对的挑战，同时鼓舞人心的是，作者们将解决思路开诚布公的公开于众，去鼓励去启发更多有志研究者投身于密码学应用中。唯有紧密贴合实际的需求，才能诞生出实实在在的论文。