**《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。

“”