Journal of WoCrypt
www.uow.edu.au/~fuchun/jow

(卧报五周年特刊前菜)

# 论开题报告之研究进展的介绍方法

郭福春
University of Wollongong

**【背景】**在澳洲和中国，博士生（研究生）在经过一年以上的学习之后需要做一次开题报告，系统性介绍研究问题若干，说服 committee 其有能力得到预期的研究结果并系统汇总成博士论文，历经七七四十九难之后最终取得博士学位。开题报告由多个部分组成，其中一部分叫“研究进展（国内外研究进展）”。我发现很多学生在介绍这部分时，喜欢以“论文发表的时间顺序”展开介绍。针对这种情况，安大静姐在 2024 年的 1 月 24 日晚的解释是“这是一种总结不到位时最好的方法”，我深表赞同。在本文里，我提出了一种不同于纯时间顺序的介绍框架。同学们只要往这个框架里填内容就行了。 至于这个介绍框架有没有效果，不好意思， 我没有相应的实验结果证明其有效性。然而，这篇文章所提到的框架已经得到多位老师/博士生的严重同意和赞同（至于会不会不好意思说不赞同，那我就真不知道了）。

---

正文开始

科学研究就是“发现问题”和“解决问题”。介绍前者的时候，要说明该问题的重要性，不解决该问题的话人类就会被邪恶的外星人团灭。 介绍后者的时候，要说明解决问题最终采用的方案非常牛叉，爱因斯坦要是还活着都得来端茶。 当然了，你要这么敢吹牛就死定了。

通过上面的这段话，我想引出以下三个术语:

问题 ===> 技术路线 ===> 具体方案

- 问题：比如“网络入侵”，“数据隐私暴露”等。定位研究问题的重要性。
- 技术路线：比如“入侵检测”，“公钥加密”等。技术路线泛指解决思路。
- 具体方案：就是把技术路线实现出来，得到的一种可解决问题的具体方案。

哎呀，已经凌晨 12:12 分了。不写了不写了，明天继续。

现在是早上 7 点 37 分。继续!

本文的介绍是为了帮助那些“以提出具体方案”作为研究贡献的密码学方向的同学。如果你的研究是偏向密码学分析，那这篇文章就只有参考的作用了。

研究进展应该如何介绍取决于你研究的侧重点。

- 第一种侧重点是以“问题”作为研究的中心。粗暴地说，为了解决该问题，只要有价值的技术路线都在自己考虑的范围内，即使这些路线看起来没有重叠且差别很大。这一种侧重点必须能列出多条技术路线，否则，它和接下来的这一种没啥区别。
- 第二种侧重点是以“技术路线”作为研究的中心。这类重心是在某条路线上提出有 novelty 的具体方案。密码学研究方面，很多人都采取第二种。假如有一天你在会议上碰到小明、小强、小刚，而他们介绍的研究方向分别是：数字签名，属性加密和秘密共享，那么他们所说的研究方向就是以技术路线作为研究的中心。

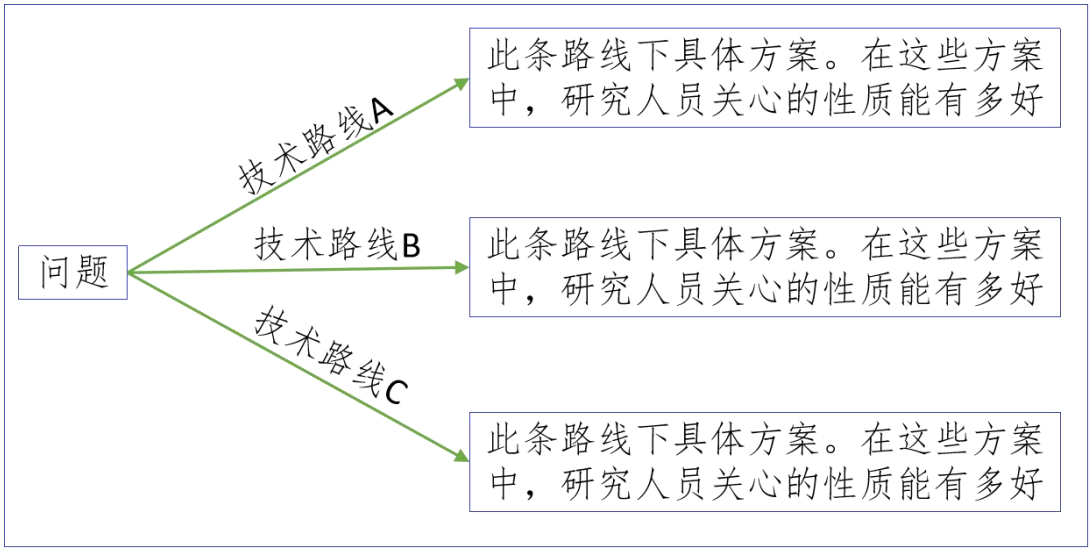
以问题为中心的第一种侧重点，按照雯姐的 comments，其特点是研究范围更大，可选择的研究内容更多。以路线为中心的第二种侧重点更专注于具体方案的实现构造细节。是的！我想补充的这两种侧重点没有哪一种是最好的，只有更合适你的。接下来，我直接写以上两种侧重点的介绍步骤。

## 第一种侧重点的进展介绍步骤

以“问题”为中心，在介绍研究进展时，可以采用以下的框架。

- 确保你已经在此之前向 Committee 清楚介绍了该“问题”的重要性。
- 用一页 PPT 汇总该问题有价值的技术路线的名称 A，B, C 和提出时间。
- 用若干页进行以下的分类介绍：
  - 简要介绍技术路线 A 是如何工作的，其突出优点是什么。对此条路线下所有被收集的具体方案进行汇总，给出研究人员关心的相关若干性质以及能达到的极限。
  - 简要介绍技术路线 B 是如何工作的，其突出优点是什么。对此条路线下所有被收集的具体方案进行汇总，给出研究人员关心的相关若干性质以及能达到的极限。
  - 简要介绍技术路线 C 是如何工作的，其突出优点是什么。对此条路线下所有被收集的具体方案进行汇总，给出研究人员关心的相关若干性质以及能达到的极限。
- 用一页 PPT 汇总目前技术路线 A,B,C 的效果区别以及每条路线下最好的研究结果。需要注意的是每条路线之下研究人员关心的性质或许不同。这个汇总要能给人一种感觉，这些方法都是有各自的优点，谁也取代不了谁。

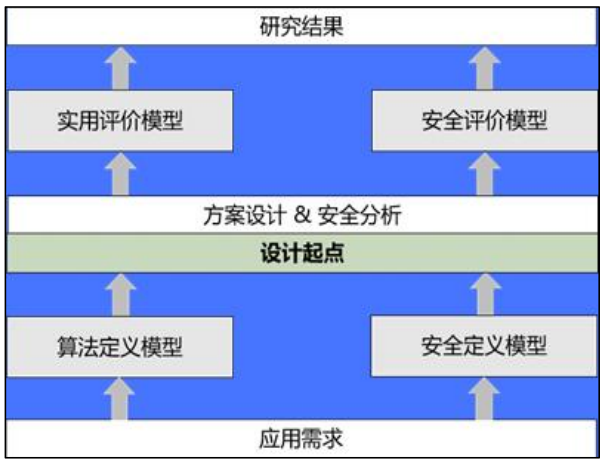
在李备同学的建议下，我的确应该给张图，以加强大家对这个框架的理解。




## 第二种侧重点的进展介绍步骤

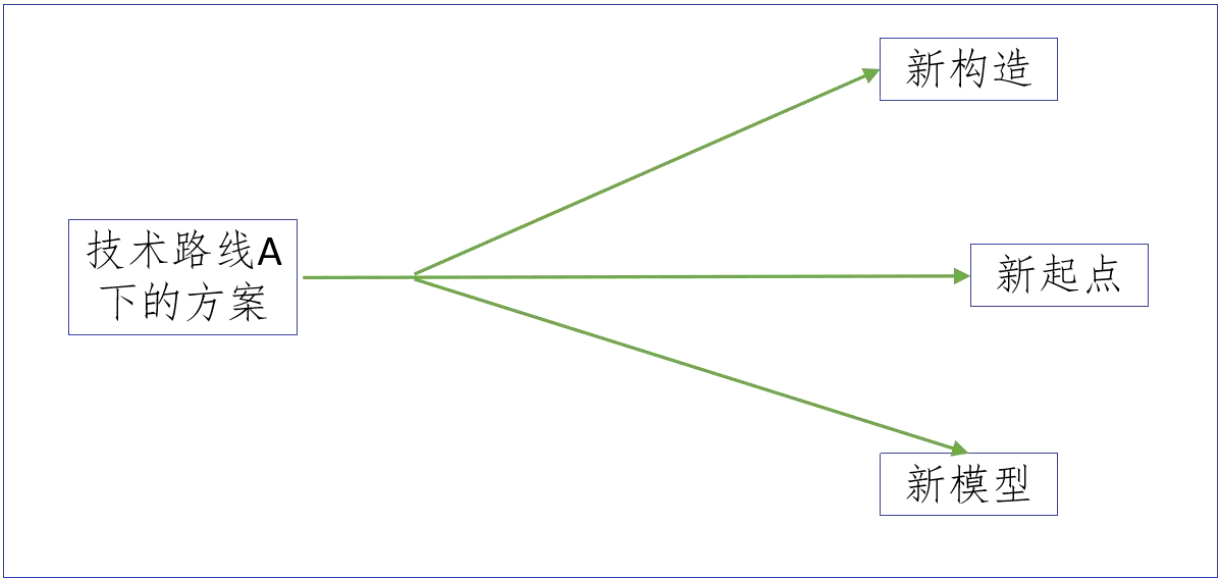
以“技术路线”为中心，在介绍研究进展时，可以采用以下的框架。

- 确保你已经在此之前向 Committee 清楚介绍了该“技术路线”的价值，即该技术路线有什么优点（其它方法所不具有的优点）。王莉同学强调，下面的描述要能够把对具体方案的介绍从其应用背景分离出来（才能星辰大海）。
- 用一页 PPT 汇总所有具体方案，其目的是为了告诉 committee 你调研了这么多的论文。本文提出的分类采用《数字签名密史》的展开方式，即“新构造、新起点、新模型”。也就是说把该条技术路线下所有的具体方案分成这三大类。这一页的内容可以看成后面分类介绍的高度浓缩，所以，可以先完成后面的分类介绍再回过头完成这一页的简介。
- 用至少三页进行以下的分类介绍：
  - 新构造。介绍哪些具体方案其贡献属于新构造这一类。它们在效率和安全方面做了什么样的具体的贡献。效率多高，安全多好之类。如果这部分不涉及你的研究内容，不用去吐槽它们的不足。
  - 新起点。介绍哪些具体方案其贡献属于新起点这一类。它们用了什么新的起点。这些新起点对应的优点是什么之类。如果这部分不涉及你的研究内容，不用去吐槽它们的不足。
  - 新模型。介绍哪些具体方案其贡献属于新模型这一类。它们用了什么新的算法定义或安全定义。这些新定义对应的优点是什么之类。同样的道理，如果这部分不涉及你的研究内容，不用去吐槽它们的不足。



- 用一页 PPT 汇总目前所有搜集的具体方案。对自己即将列出的研究内容，有针对性地给出这些具体方案的优点和缺点。优点，是你提出的方案要有的优点；而缺点，也是你所提方案必须要避免的缺点。安大张静老师说，这一点尤其重要，因为它和后面模块的“研究内容”起承上启下之作用。

这次，我以李备的图为参考，给出了以下我的理解图。




《密史》以“数字签名”作为解决某问题的技术路线，介绍“新构造、新起点、新模型”。**实际上，对任何密码技术的研究都可以采用这种方法。**举个例子，假如你专注的技术路线是“具有可撤销功能的属性加密”，那么该类路线下所有的文章里的具体方案可以进行以下的分类：

（1）新构造，介绍目前这类方案的效率和安全如何。需要注意的是，假如小明提出了“具有可撤销功能和 online/offline 功能的属性加密方案”，那么该方案不属于新构造而是新模型，因为算法定义变了。（因英文版的密史为准）

（2）新起点，介绍哪些用 pairing, 哪些用 lattice。这块的论文应该不多，因为只有第一篇文章才算新起点。而后面相同起点的文章，可以看成以这篇文章为开始的“新构造”或“新模型”。

（3）新模型，这块应该就非常丰富了。凡是有添加新功能的或者安全模型改变的都属于这块。需要注意的是，“可撤销”是你定下来必须考虑的功能，而这里介绍的新功能 Y 不是你一定要追求的功能。否则，你的研究方向就会变成“具有可撤销功能和 Y 功能的属性加密”。再次注意，博士论文里，你的研究方向应该能够装下你的所有的研究内容。

## 以问题为中心的研究内容

我发现，我不得不顺便简介下“研究内容”，因为从研究进展到研究内容，它们的关系还挺紧密的。

以问题为中心的研究进展，其对应的研究内容有两类：

1) 继续深入研究某条技术路线（比如 A），得到更好的具体方案。这里评价“更好”必须用到了该路线下总结出来的性质。比如，技术路线 A 下的所有具体方案其精确度都偏低，这个性质又被发现很重要，因此在技术路线 A 下重新构造具体方案提高精确度就是更好。偷偷告诉你，技术路线 B 的优点应该是技术路线 A 下所有具体方案的缺点，它可以作为你计划要提升的性质之一（但不容易解决哦）。

2) 提出可能存在的不一样的技术路线 D，得到可行的具体方案。为什么要提出一个新的技术路线 D 呢？这是因为目前的技术路线 A,B,C 都存在着 X 方面的缺点（这个也必须在前面的介绍说清楚，其中 X 可以是一种组合类的性质），而技术路线 D 将不具有同样的问题（这也就是 D 方法的优点）。

还是那句话，学术研究的意义是超越人类的认知极限。千万不能野心太大，想提出一种全新的技术路线，其具有目前已知所有方法和方案的优点且没有任何缺点。我们导师做白日梦都不敢这么嚣张。

有关上述提到的技术路线 D，补充两则讨论。

- 安大静姐补充说，提出全新的技术路线 D，而这里的全新可以是“存在其它领域但尚未被用于解决该问题问题的”新路线。告诫研究生，不要因为“全新”而害怕退缩，认为自己缺乏足够的创新力就不敢走这条道。
- 东大昌哥接着说“小心评委上来就直接问，你做了啥，你的创新点在哪”。如果现有的方法能直接迁移变成技术路线 D，那的确是没有创新的。所以啊，一定要强调“从现有的方法到技术路线 D 下可行的方案”存在着一些技术难题。你的创新点就存在解决这些难题里。

哎，这部分得内容有些超纲了。

## 以技术路线为中心的研究内容

以路线为中心的研究进展，其对应的研究内容有三类：新构造、新起点、新模型。至于你的研究动机，它们就藏在前面你对目前具体方案的吐槽里。有密史在，要整出 4 点研究内容还不容易？难的是把你的研究动机讲得重要且有趣。西电臻姐补充说，上述新技术路线 D 下的具体方案像《密史》里的第一篇论文，而以“技术路线 D”为中心的研究像是在折腾第二篇论文。

由于早期版本描述不清，李备同学误解认为，以“问题”为中心的研究和以“技术路线”为中心的研究仅仅是叙述思路的不同。我想再次解释的是本文的介绍最终是为了一“部”博士论文。在这部论文里，前者的研究内容可以包含多条技术路线，而后者只能专注于某一条技术路线。

我发现可能存在一个问题。

你的研究方向是： 具有可撤销功能的属性加密
小明已经提出了： 具有可撤销功能和 online/offline 功能的属性加密

问：这个研究方向（技术路线）是否不够好？是否要考虑 online/offline 这个性质？不考虑该性质是否显得研究不吸引人？

答：不会。还是那句话，你研究的内容考虑的是如何在“具有可撤销功能的属性加密”超越人类的认知极限，关 online/offline 啥屁事。再说了，许多应用场景也不支持 online/offline 这个性质的。当然了，你也可以跟进小明的工作，做出超越小明的研究结果，这个研究结果仍然属于你研究方向的一个研究内容之一。因为你在该研究内容上对应的问题是：如果应用允许 online/offline 的存在，那么“具有可撤销功能的属性加密”可以如何更好？

## 结论

本文适合那些在坑里还没找到北在哪，有些迷茫的同学们。这个观点得到了曲阜王姐的同意，并指出了之前口齿不清的表述。

“不具有可比性”是一种巧妙的表达方式，可以过滤掉许多无关的论文。在第一种侧重点里，我们通过“问题”过滤掉了很多技术路线和具体方案。在第二种侧重点里，我们通过“技术路线”过滤掉许多需要对比的具体方案（其它路线下的方案都不具有对比性的）。比如，凡是不具有“可撤销”性质的属性加密方案，不管其效率或安全有多牛叉，都不是我们需要考虑和对比的。希望这个简短的讨论能帮助你定位预期的研究贡献。

我很想再说点啥，但好像没有了。前菜就这样吧。

以时间顺序致谢人员名单及物品清单

西电雯姐，安大静姐，东大昌哥，西电臻姐，曲阜王姐，UOW 的博士小分队
X 大的四份开题报告 PPT，X 大的三份开题报告 PPT，UOW 的十份开题报告 PPT