数字签名密史

本图宜配合《数字签名密史》食用，希望能
1. 帮助没看书的人大致了解《密史》样貌，以更容易走进这段密史；
2. 帮助看过书的人快速回忆《密史》重点，以产生从点到片的联想；
3. 向在茫茫密史中为小伙伴们点灯的作者们致敬。

Version 20231009

1. 现代密码学成长之路

- 1.1 现代密码学的开篇
  - 网络空间的特点："数据三易" — 易删除/易修改/易复制
  - 现代密码学的特点：提供不可思议的 密码技术 和 应用功能
- 1.2 汇聚于1976年的三条线索
  - 第一条线索：人类对密码学的认知，由 "机密性" 变为"加密系统 = 算法 + 密钥"
    - 1883，Kerckhoffs 准则 "唯一需要安全保管的是密钥，算法必须公开"
    - 1940s，Shannon 绝对安全的 "一次一密"
  - 第二条线索：图灵机，计算机和计算机网络
    - 1936，Turing "图灵机模型"
    - 1951，von Neumann，第一台二进制计算机 EDVAC，是现代计算机的原型
  - 第三条线索：计算复杂性理论
    - 1965，Hartmanis 和 Stearns，计算 vs 算法，计算问题 vs （无穷多的）问题实例，时间消耗与问题长度的关系 线性，指数级……
    - 2000，P vs NP 千禧年难题
  - 三条线索汇聚：1976，Diffie-Hellman "密码学的新方向"
- 1.3 开启新篇章的风信
  - 由于算法与密钥成功分离，需要 加密系统 和 密钥协商
    - 加密系统：1977，Data Encryption Standard，DES
    - 密钥协商：1976，Diffie-Hellman Key Exchange
- 1.4 密码学的新方向
  - 从 密钥协商 到 单向函数/单向陷门函数
  - 从 单向函数 到 公钥密码学，包括 公钥加密/数字签名
    - 眼花缭乱的现代密码学技术：用 "密码组件" 搭建各种 "密码方案/协议"
- 1.5 数字签名
  - 解决 "数据三易" 中的 "易修改"，验证数据完整性/不可伪造性/不可否认性
    - 签名方案包括密钥算法，签名算法，验证算法，即方案设计的蓝图
    - 签名方案中算法的个数：取决于现有算法是否足以满足相关应用的需求，如果不够，则必须添加；如果太冗余，则可以简化
    - 签名方案的正确性（考虑合法用户，其通过私钥计算签名）：需要算法之间互通
    - 签名方案的安全性（考虑非法用户，其不通过私钥计算签名）：需要考虑各种敌手模型
    - 签名方案的应用场景：网站的数字证书 — 通过数字签名对公钥所属权进行认证

2. 数字签名的方案构造之路

- 2.1 密史的前五年
  - 1976，Diffie-Hellman 数字签名方案
    - 给出从 单向陷门函数 到 数字签名方案 的通用构造，但未回答如何构造满足要求的 单向陷门函数
  - 1978，Rivest-Shamir-Adleman （RSA） 数字签名方案
    - 第一次给出 单向陷门函数 的构造实例：基于 费马小定理 和 计算困难性
    - 同态性上的修补（对应签名方案的不可延展性）：使用哈希函数
- 2.2 数字签名的方案构造
  - 通用构造：利用具有某种性质的任意函数构造数字签名方案 + 寻找相应的函数
    - Diffie-Hellman76：基于 单向陷门函数 构造 数字签名方案
    - Lamport79：基于 单向函数 构造 一次签名方案 + 使用 Merkle Tree 扩展
    - Goldwasser-Micali-Rivest84：可证明安全的数字签名方案，后续从四函数到一函数
  - 具体构造：利用特定函数的特殊性质
    - Rivest-Shamir-Adleman78：单向性 + 陷门性
    - ElGamal84：单向性 + 同态性
  - 通用改装：从一种密码技术到另一种密码技术
    - Fiat-Shamir86：从（特殊的三轮）身份认证协议 到 数字签名方案
    - 方案构造之路的研究逻辑（从A到B）：从特殊的A到B → 扩大特殊的A的范围/得到更好的B
  - 对比：大多数时候，通用构造 安全性分析比较容易但效率较低，而 具体构造 完全相反，Tradeoff
- 2.3 通往罗马之路
  - 密码方案的评价："更好"×，"更安全"√，"更高效"√，寻找特殊的，满足性质的应用场景或切入点
  - 密码圈的官方大道：算法标准，例如Digital Signature Algorithm, DSA
- 2.4 可证明安全背后的故事
  - 单向性问题和扩展困难问题
    - 单向性问题：单向性问题是所有扩展困难问题的基础，也是公钥密码学的安全基础。然而，目前只能从 "该函数肯定具有单向性" 妥协到 "该函数在特定假设条件下具有单向性"
    - 扩展困难问题：密码学用到的NP类问题分为P类问题，NP中间类问题和NPC类问题，扩展困难问题通常落在中间层。量子计算机（仅）能解决部分NP中间类问题，目前看来传统计算机不能解决
  - 归约和安全归约
    - 归约（证明困难问题之间的等价性）：只要能解决问题 A，就能解决问题 B，即 B困难 → A 困难
    - 安全归约（证明密码方案的安全性）：只要能攻破方案 S，就能解决问题 P，即 P困难 → S 安全
  - 计算模型和安全模型
    - 计算模型：来自 计算复杂性理论，对 "计算能力" 建模
    - 安全模型：来自 密码学理论，对 "对方案的攻击" 建模，包括 "敌手能力" 和 "安全目标"
- 2.5 可证明安全发展的三阶段
  - 1979-1992：Goldwasser-Micali-Rivest84 EUF-CMA 模型，"Paradoxical"
  - 1993-2000：Bellare-Rogaway93 随机预言机 + Ponitcheval-Stern96 分叉引理（暂且忽略Canetti-Goldwasser-Halevi98 给出的非常特殊的反例）
    - 暗线1："紧归约"，将安全性与计算问题的困难性紧紧地捆绑，详见 "3.6 安全评价模型和它的故事"
    - 暗线2："不可能性分析"，具有X特点的方案不存在，详见 "5.3 预言之力"
  - 2001-2021：双线性对，隐藏复杂的数学公式和符号，专注探索安全归约技术
    - Shamir85 基于身份的密码学 + Boneh-Franklin01 使用双线性对构造基于身份的加密方案 + Boneh-Lynn-Shacham01 使用双线性对构造基于身份的签名方案 + 此后至今丰富多彩的构造
  - 补充：Shoup04 Game Hopping "如果能用安全归约技术证明，则能用 Game Hopping 证明，反之不一定成立" + "将安全性建立在多个困难问题之上"

3. 数字签名的研究发展之路

- 3.1 剪不断理还乱的密码学研究
  - 研究对象：某种密码技术，用于保护数据的机密性和完整性等
  - 研究目标：构造新方案，实现上述密码技术，使得新方案具有某些优点
  - 研究动机：介绍和解释 "研究目标" 的重要性，写论文 = 做销售
  - 研究路线：从 "研究起点" 出发，为实现 "研究目标" 所采用的具有某种特征的方法思路，不同于具体的技术方法
  - 研究贡献：研究过程中创造的有价值的新知识，包括 "研究路线" 和 "研究结果"
  - 研究结果：对 "研究目标" 能实现的程度的度量，属于 "研究贡献" 的一部分，相应的代价将会变成后人改进提升的关键
  - 针对同一个 "研究对象"，可以从不同的研究起点出发，达到不同的 "研究结果"（不受欢迎的 "借鸡下蛋" 和 "换汤不换药"）
- 3.2 密码学的研究逻辑
  - 第一篇论文：新研究对象的定义 → 设计起点的选择 → 方案的构造
    - 算法定义模型（定义用户可享受的功能）和安全定义模型（定义敌手在某种环境下无法攻击成功）
    - 实用评价模型（用户享受功能所需付出的代价）和安全评价模型（在安全模型下的安全程度）
  - 第二篇论文：从上述的任意一关开始重新闯后续关卡，新构造/新起点/新模型
    - "有意义的研究结果不一定意味着方案更实用或更安全，它只需要具有新颖性，即在 实用方面 或 安全方面 具备有价值的技术方法，这也是学术界和工业界的不同之处"
    - 研究路线1（新构造）：相同的模型和起点（单向函数实例A），构造验证更高效的签名方案
    - 研究路线2（新起点）：相同的模型，从新起点（单向函数实例B）构造验证更高效的签名方案，B可以是现有的；甚至还可以是从更低的起点构造出的效果略差的方案
    - 研究路线3（新模型）：数字签名方案 with 批量验证功能
    - 研究路线4（新构造）：相同的模型和起点，将方案的安全性提升为等价于更难的困难问题/不依赖随机预言机；也可以是在模型不变的前提下，构造全新的方案抵抗同类敌手更持久的攻击
    - 研究路线5（新起点）：现有都是以A为起点构造，而陆续出现对A的（可能成功的）攻击方法，但它们不能用来攻击B，于是可以从B进行构造 — 需要备胎，典型例子包括 "量子计算机与格密码"
    - 研究路线6（新模型）：构造 可以抵抗侧信道攻击 且 在EUF-CMA安全模型下安全 的数字签名方案，即抵抗更强大更厉害的敌手的攻击
    - 本质上是 Tradeoff，四点强调：有得必有失，小心翼翼地讨论新颖性，用作参考对象，接受结局
    - 额外的研究路线：提出新应用需求，数字签名的功能升级之路，一切尽在 算法定义模型 中
- 3.3 设计起点一览
  - 方案构造之路：主要包括 具体构造，通用构造 和 通用改装 三类方法，区别在于 "研究动机"，其中最困难的，被攻击最多的当数 具体构造
    - "一些复杂程度堪比星际飞船的密码技术经常需要同时借助这三类构造方法"
    - 具体构造：主流构造方法，例如从 "具体的数学运算" 构造签名方案。后两类构造之路也需要 具体构造 作为支持，否则没有意义（即，假想存在着某种安全的 低级函数/组件 或 高级密码技术）
    - 通用构造（从 低级函数/组件 到 数字签名方案）：例如从 "具有某类性质的函数" 构造签名方案，强调一般化和多个实例的存在，尝试探索最低的（通用）设计起点
    - 通用改装（从 高级密码技术 到 数字签名方案）：强调一种密码技术和另一种密码技术的关系
  - 具体构造这条路：从数学中找本源困难问题，基于本源困难问题定义密钥结构（使用的问题困难性 vs 密钥结构的灵活性），基于密钥结构定义签名结构（必须保证通过公钥伪造消息的签名是个计算困难问题，如RSA问题）
    - 大数分解问题 → RSA方案的密钥安全问题 → RSA方案的签名安全问题，解决问题的难度在一点点地降低，在 "用安全换取效率" 的路上无奈地往前走
  - 从安全到可证明安全：为了方案具有可证明安全，将其安全性归约到一个更弱的困难问题，如强RSA困难假设，这样做的危险在于新定义问题可能是简单的
- 3.4 实用评价模型和它的故事
  - 成本：包括计算效率/存储效率/通信效率/实现效率
    - 计算效率：签名计算效率/签名验证效率/签名计算和验证总效率
    - 存储和通信效率：私钥长度/公钥长度/签名长度
    - 实现效率：（将 签名方案 通过程序落地成为产品）组件设计成本/硬件模块成本 vs 时间成本
    - "只要能改进，那就大胆对某一点给予有理有据，可说服人的批评"
  - 受益对象：考虑签名方案的应用范围
    - 最初应用范围：签名是用于保护数据完整性的密码技术
    - 扩大应用范围：签名是用于构造其他密码方案的密码组件/原语
    - 再扩大应用范围：选取有额外优点的签名，例如不用嵌入随机数的 唯一性数字签名（Unique）；能将签名中的随机数随机化的 重随机化签名（Re-Randomizable）；能保留代数结构的，且只能进行群运算的 代数结构保留签名（Structure-Preserving），其由于不涉及 Hash 函数的计算，近年来在 标准模型 下与 零知识证明相关技术 相互渗透，倍受欢迎
- 3.5 算法定义模型和它的故事
  - 计算委托：在签名计算/签名验证/加密计算/解密计算等算法中，将计算抽象，并研究如何安全的计算委托（并验证），有时需要用到同态性和多方计算
  - 计算提前：在线离线签名，也可以依赖于 同态性/随机性 进行构造，研究在关键信息未知的情况下提前完成大部分的计算
  - 捆绑销售：多方签名/基于身份签名/消息恢复签名/批量计算签名/聚合签名/无证书签名/基于证书签名/广播加密和签密，计算和存储考虑多个对象
    - 捆绑销售也能用来提高方案的效率：将消息分解为比特串 Lyubashevsky09
  - 应用精进：缩小范围，针对特殊的应用，需要找到合情合理的应用场景并解释
  - 高端玩法：通过调整密码技术的 算法定义 和 安全定义 来提高效率，新手慎碰
- 3.6 安全评价模型和它的故事
  - 可证明安全的困难性
    - 可归约的签名：被用来 "解决困难问题" 的敌手伪造的签名
    - 可模拟的签名：被用来 "回答敌手的签名询问" 的（证明者可计算的）签名
  - 安全评价模型之困难问题
    - 签名设计和选择的困难问题息息相关，必须建立在同一个本源困难问题之上，且对签名结构每一步的设计都必须考虑困难问题。通常先确定困难问题作为安全证明的目标，再考虑方案的每一步构造
    - 安全归约的核心在于把 "攻破密码方案的困难性" 和 "解决困难问题的困难性" 捆绑在一起，使得 "攻破方案的难度" 在 "解决困难问题的难度" 之上。这也会导致，问题崩 → 方案崩（变为未知）
    - Schnorr 签名：将EUF-CMA模型下伪造签名，归约到单向性困难问题，从而安全性更可信
  - 安全评价模型之紧归约
    - 动机：防止 "敌手能以100%概率伪造签名"，而 "证明者只能以极低的概率解决困难问题"
    - Pr[敌手伪造签名成功] ≈ Pr[证明者通过伪造签名成功解决困难问题]
    - 如果一个方案的安全性能紧归约到困难问题 A，那么攻破这个方案可以看成比解决困难问题 A 更困难，反之答案是未知的
  - 安全评价模型之敌手假设
    - 弱化的模型：对敌手能力进行额外限制，除随机预言机模型 ROM（只能通过查询获得Hash值），还有通用群模型 GGM/代数群模型 AGM/通用参考字符串模型 CRS/不可编程式随机预言机模型 NPROM/量子随机预言机模型 QROM 等
    - 在 弱化的模型 下完成安全证明的方案要好于缺乏安全证明的方案
    - 最理想的还是在 标准模型 下完成安全证明，即没有对敌手进行额外的限制，但通常较为困难
- 3.7 安全定义模型和它的故事
  - 敌手是谁：一个计算能力有限的传统计算机，又或者量子计算机
    - 方案的安全性要求通过 公钥 计算 私钥 是一个计算困难问题，只能抵抗计算能力有限的敌手
    - 改进：无条件安全签名（将 公钥 隐藏）/失败终止签名（证明 "计算能力无限的敌手伪造的签名" 是伪造的）
  - 敌手知道什么：可以选择任意的消息，询问它们的签名（自适应安全）
    - 私钥部分泄露攻击：允许敌手获取部分私钥信息，例如通过侧信道攻击的途径，这类模型会使一些攻击变得容易，因此需要新的安全定义
    - 私钥完全泄露攻击：敌手获得私钥，应对措施为将私钥更新，例如前向安全签名和密钥绝缘签名
    - 密钥相关攻击：敌手控制修改私钥，用新私钥产生的签名得到伪造的旧私钥签名，参见 "木马病毒"
    - 随机数攻击：敌手可以通过影响签名过程中随机数的选取，最终泄露整个私钥，参见 "棱镜门"
    - 量子选择消息攻击：敌手可以将多个消息叠加在一起，然后询问签名，挑战者也可以对所有消息产生签名并叠加在一起返回给敌手，敌手只能选择并读取其中一个
    - 多用户安全：挑战者需要将 敌手没选上的公钥 对应的私钥全部交给敌手
  - 敌手将攻击什么：敌手可以先完成所有的签名询问，再公开他即将伪造哪个新消息的签名。在安全证明里，信息披露的先后顺序非常重要，其将会影响安全证明的难易程度
    - 攻击更容易：伪造一个聚合签名 vs 伪造聚合之前的所有签名
    - 目标更广阔：不可伪造性 vs 强不可伪造性（动机来源于用作组件和特殊应用）
- 3.8 密码学之谁与争锋
  - 理想型研究路线
    - 确定算法定义模型（研究对象）→ 确定安全定义模型（安全模型）→ 选择合适的设计起点 → 选择安全评价模型里某些性质 → 选择实用评价模型里某些性质，从后往前溯源
  - 研究，对比和批评
    - 优雅的对比，默默承受的批评

4. 数字签名的功能升级之路

- 4.1 功能升级的哲学根基
  - 第三篇论文：对第一篇论文里的签名方案进行功能升级，颠倒 "能" 和 "不能"，超越常识，同时注意研究动机简单有趣，避免无意义升级。不同的解读方式，新的 算法定义模型 和 安全定义模型，新的构造（可能会弱化两个模型之一）
    - 第一篇论文：从应用需求出发，提出解决问题的密码技术（给出算法定义模型和安全定义模型），到 选择设计起点，再到 构造密码方案，即新模型 → 新起点 → 新构造
    - 第二篇论文：在第一篇论文的基础上做出新颖性，从 "四大模型" 或 新的设计起点 出发，实现预期目标，强化签名或验证功能，有可能调整 算法定义模型，而没有改变应用需求
  - 签名者老马，4.2 超越常识之老马的故事
    - 能知道他即将发布的消息内容 m → 盲签名
    - 能自己一个人完成签名计算 → 门限签名
    - 不能控制签名的验证（任何人都能验证）→ 不可否认签名
    - 不能在不给私钥的前提下由他的秘书完成签名 → 代理签名
    - 能用他的私钥对任意消息进行签名 → 双重认证防止签名
    - 能用他的私钥进行无限次的签名 → 使用次数有限签名
  - 验证者小明，4.3 超越常识之小明的故事
    - 能自己验证签名的正确性 → 门限签名验证/不可否认签名 （不可单独验证的签名方案）
    - 能获得老马的签名 → 可验证加密签名
    - 能知道签名者是老马 → 群签名/环签名/属性签名
    - 能知道被签的消息是 m → 函数签名
    - 能将签名转发给小强，且小强可以验证签名合法性 → 指定验证者签名
    - 不能对老马签名过的消息内容 m 进行处理 →（线性或函数）同态签名/可净化签名/可修订签名
- 4.4 功能升级逻辑一览
  - 从主逻辑到次逻辑，将密码技术里的（部分）功能从旧到新进行升级
    - 从出错到纠错：找出 批量验证签名 中的无效的签名；使可信任法院可以追踪匿名交易的 盲签名；在有人扰乱的情况下恢复 门限签名；踢掉 群签名 的群组成员；在不利用管理员的情况下让 群签名/环签名 的签名者能自证清白；给 属性签名 增加"追踪"
    - 从静态到动态：动态化的 群签名/属性签名；可更新的 重随机化签名/门限签名
    - 从集权到分权：将私钥秘密共享成多个子私钥的 门限签名；分离管理员的批准和打开能力的 群签名；将管理员分权为一个组共同管理的 群签名
    - 从亲为到授权：将需要用到私钥的计算能力授权，且不需要直接给私钥的 代理签名/代理重签名；将签名验证帮助授权的 不可否认签名
    - 从清楚到模糊：模糊签名者身份或签名的消息内容的 群签名/环签名/属性签名/可修订签名
    - 从模糊到清楚：减弱模糊 可链接性的群签名/环签名
    - 从已知到未知：彻底模糊 群成员个数不可见的 群签名；来源不可链接的 可净化签名
    - 从全体到个体：缩小签名验证者的范围的 不可否认签名/指定验证者签名；缩小群签名中管理员的私钥的能力的 只能打开部分签名者的匿名身份的群签名
    - 从个体到全体：将需要私钥才能进行的计算升级为全体的 广义（Universal）指定验证者签名/不可否认签名
    - 从所有到部分：使盲签名中没有被盲化的部分具有现实意义的 部分盲签名；使群签名只能追踪某个时间点之后的签名者身份的 部分消息打开的群签名
    - 从先后到同时：使双方签名/多方签名同时生效的 并发签名
    - 从必须到无须：无须通信信息即可追踪到签名者身份的可追踪交易的 盲签名；无须可信第三方产生签名的 门限签名；其他成员无须知晓被撤销的群成员的 群签名；无须更新合法用户私钥的 属性签名；基于时间机制撤销的签名
- 4.5 安全定义模型新故事
  - 功能升级的最后一步：详细描述 算法定义模型 和 安全定义模型
    - 覆盖7个性质的安全模型的刻画，Bellare-Micciancio-Warinschi03
- 4.6 密码学之百家争鸣
  - 功能百家：参见书中表格，用丰富的功能优雅地灌水
  - 热火朝天：方案实用性方面，减少（甚至避免）交互次数/减小参数长度和计算量，实现最优效率；方案可证明安全方面，零知识证明 + 传统安全归约技术（困难问题/紧归约/证明模型）
  - 得意忘象：照搬照抄学习功能升级之法 → 借鉴渗透加强对功能升级的本质理解 → 遗忘本书介绍的功能升级的逻辑

5 数字签名的分析之路

- 5.1 分析那些事
  - 小强感受到的小婉的8篇攻击论文之痛
    - 谕言：已经发生但我们认识不全面的事情，对应于修正或删除 "密码技术知识库" 中的条目
    - 预言：还未发生但未来一定会出现的（坏）结果，对应于条目不可能加入到 "密码技术知识库"
- 5.2 谕言之能
  - 模型之内的安全性问题（对应小婉论文 1 和 2）：敌手可以通过公钥和签名计算出私钥 → 敌手可以通过公钥伪造某个消息的有效签名 → 敌手可以通过公钥和签名伪造某个新消息的有效签名
    - 谨慎使用新的设计起点，因为初学者对敌手的攻击方法了解不多
    - 使用安全参数刻画安全性
  - 模型之外的安全性问题（对应小婉论文 3）："密码方案不是用来攻破的，而是用来绕过的" — Adi Shamir
    - 使用（标准）模型之外的各种方法获得更多的信息，例如 侧信道攻击/斯诺登式攻击
    - 在证明方案的安全性时，可以合理地定义一个安全模型，并证明方案在该模型内安全。然而现实中，很难将敌手的攻击限制在一个安全模型中，这也是为什么 可证明安全的方案 可能 不安全
  - 概念之间的关系性问题（对应小婉论文 4）：更基础的密码技术/设计起点，互相构造与等价性
  - 谕言加强：在他人攻击方法基础上，强化攻击是一种研究方向
- 5.3 预言之力
  - 结果类实用方面不可能（对应小婉论文 5）：签名计算快/长度短，存在下界
  - 结果类安全方面不可能（对应小婉论文 6）：困难问题的选择/证明模型的选择/紧归约，通常分为具体方案（通常是算法标准）的安全归约结果不可能性以及 一类构造方法对应所有方案的安全归约结果不可能性
  - 方法类满足预期不可能（对应小婉论文 7 和 8）：不管采用多么巧妙的方法，也不可能通过起点A达到研究目标B，例如不可能通过 单向函数 构造安全可用的 公钥加密 方案
  - 预言加深：在已有的不可能范围上，继续扩大范围是一种研究方向
- 5.4 密码学之同舟共济
  - 谕言之能为人类说出对现有构造方案的新结论（实际上不安全或者具有某种等价关系），预言之力为人类指出对未来构造方案的新雷区（不可能）。用谕言收拾当下，再用预言更好地踏上新的征程
  - 敬畏之心：提出的方案有可能会面临模型内外的新的攻击方法，也可能只是旧方案的简单转换
  - 谨言之心：预言之力通常只针对假设条件成立，如果能找到研究路线绕过该假设条件，就有可能得到完全不一样的研究结果。这个研究方向很难，但结果容易受到欢迎

后记