中国科学技术大学

本科生课程实践论文

论文题目：密码学导论课程实践

作者姓名：　梁兆懿 PB20050987

学科专业：　网络空间安全

导师姓名：　李卫海老师，胡红钢老师

完成时间：　2022 年 6 月 3 日

摘　要

本次密码学导论课程实践的内容（下半学期）为对欧密会、亚密会和美密会两篇论文阅读。我选择的论文分别是《Transferable E-Cash: A Cleaner Modeland the First Practical Instantiation》和《Match Me if You Can: Matchmaking Encryption and Its Applications》。

第一篇论文来自 2021 年欧密会，为 Balthazar Bauer 先生的《Transferable E-Cash: A Cleaner Modeland the First Practical Instantiation》。该论文探讨了以往电子现金模型的不足之处：无法同时满足匿名性和加密效率。在以往电子现金模型的基础上提出了更简单，更强大的安全架构，更好地实现了匿名性以及不可伪造性，并对该算法进行了证明，从而构造出更有效的可转移的电子现金实现方案。

第一篇论文来自 2021 年美密会，为 Giuseppe Ateniese 先生的《Match Me if You Can: Matchmaking Encryption and Its Applications》。该论文提出了一种新的加密方式——匹配加密，参与者可以指定自己加密的数据的访问属性，满足访问属性地接收者才能实现解密。在理论层面上，论文证明了该种加密方式的安全性。在实践层面上，作者构建了基于身份的高效匹配方案以及在网络层面实现了匹配加密，通过实施和评估，并分析实验数据以证明该加密模式是可行的。

关键词：　电子现金　　匹配加密　　欧密会　　美密会

第一部分 《可转移电子现金：更简洁的模型和第一个的实例化》

1.1 问题背景和相关研究

论文研究的主体是 Transferable E-Cash，即可转移电子现金。提到电子现金，我们的第一反应可能是银行卡支付或者微信支付等日常支付方式。然而论文中的电子现金与我们传统概念中的电子支付不同。电子现金侧重的是货币性质，即如何实现实物现金的数字模拟，允许用户在不透露身份的情况下进行支付，即使是银行也无法将硬币的提取与其支出联系起来。电子货币看似容易实现，然而其与物理货币的主要区别在于数字硬币可以很容易地复制，如何在保证其唯一性的同时确保其匿名性，成为密码学者们的一大难题。

此外，可转移电子现金与加密货币最大的区别是，它允许用户重新使用转移获得的货币的同时，避免繁琐的运算，甚至能在保持离线状态下实现。该加密方式需要密码学理论的支撑。在过去的讨论中，Fuchsbauer 团队提出了可转移电子现金第一个方案，但是在该方案中电子现金为了匿名性只能实现一次性使用，且匿名性十分脆弱。随后 Blazy 团队结合随机交互知识和交换签名等知识优化了上述方案，但需要一名线上的仲裁者才能实现该方案，降低了实用性。而 Baldimtsi 团队优化了上述方案，通过使用经典离线电子现金的双重支出跟踪机制，给出了一个更优化的方案，从而避免了中间的仲裁阶段。他们在硬币上添加标签，隐藏硬币所有者的身份。该方案基于数字签名的推广——可延展签名，其主要缺点是效率低下，需要逐一记录货币在使用时所有的使用者，在后期将会生成冗长的代码串。

基于上述研究成果，作者 Balthazar Bauer 团队重新审视过去 Baldimtsi 团队可转让电子现金的模型，并且指出其不足：1.攻击者可以向用户发送一枚格式错误的货币，即伪造假币，后者接受后但由于格式错误不能花掉；2.面对银行的恶意破坏（例如，声称硬币无效或被重复使用）也显得十分无力。针对此，Balthazar Bauer 团队利用了非对称双线性群，构建了一个新的 RCCA 安全加密

方案，并且沿用了之前被证明有效的双重支出标签。实现了更加有效、安全的实用电子现金方案。

1.2 算法和优点

在该论文定义的电子现金方案中，电子货币使用 ParamGen 方法构建，电子钱包（也称作电子银行，第三方储存用户货币的地方）借助 BKeyGen 方法设置密钥对，二者通过协议相关联。电子钱包的功能是存储维护一个用户列表（UL）和一个存放货币的列表（DCL）。用户可以通过密钥实现存款以及货币对他人的转移。在电子钱包收到硬币的同时，用户若选择存入钱包，钱包将会把存入的货币加入到 DCL 中；如果是通过双重支出来转移货币，电子钱包通过 VfyGuilt 方法验证目标用户的公钥和证明，随后完成货币的转移，从而保证转移货币时安全。

钱包中的任意一枚货币总是以相同的方式分配。此外，收到的货币将仅与发出的货币相关联（而不是其他已经花费或收到的货币）。因此，电子钱包和用户在转账时不需要存储有关过去交易的任何内容; 货币本身必须足够有不可伪造性。相对于过去的算法节省了大量空间。

该电子现金具有诸多优点。首先，在该电子现金模式中，货币具有不可伪造性，这个性质确保没有用户可以花费比他们在电子钱包取出的数量更多的货币。该性质还保证，每当一枚货币被存入电子钱包并在验证机制未通过被拒绝时，它都会返回用户的身份，从而让伪造假币的攻击者无所遁形。其次，电子现金模式确保了电子钱包即使与恶意用户勾结，也无法误报正常的用户进行双重支出。具体来说，它保证恶意第三方钱包无法生成双重支出标签来验证没有双重支出的用户的公钥，从而不能恶意转移用户的财产。

此外，该电子货币具有匿名性，电子钱包通过存款向实验者发行一枚货币，当她收到它时，实验者无法将货币与它的发行者联系起来。此外，用户也具有匿名性，虽然电子钱包可以追踪硬币的来处，但所涉及的用户仍然是匿名的。该性质意味着用户在转移货币后如果再次收到该货币，将会无法识别它是先前的货币。

货币使用了早期的双重支出标签方案，银行以其序列号表示货币，其序列号随着每次转账而增长。此外，由于货币包含双重支出标签，可以标志双重支出者，在实现隐藏用户身份的同时保证财产转移的安全。

1.3 框架与结论

论文构建的电子现金系统运作可以分为以下步骤：

电子钱包（即电子银行）开始运作时，电子银行可以验证系统中的新用户或者发行货币。其中经过数字签名过程：当新用户验证时，银行构建他的公钥，作为注册的证明；在货币发行时，新发行的货币可以获得初始序号，并且电子银行会对其进行签名使货币不可伪造。

在货币被转移 k 次后，它的核心由序号以及标签组成（对于刚提取的硬币，我们有（k=0）。当用户转移这样的货币时，接收者会生成一个新的序号，为此，使用者也必须生成一个标签，该标签也与她的公钥和最后一个序列号相关联（她在收到硬币时生成），二者组合，从而获得一枚全新的货币，保证货币的不可伪造性。

这些序号与标签允许电子银行识别作弊者，同时也保证了用户的匿名性，攻击者则会在电子银行验证时被曝光。此外，货币还包含创建标签的用户公钥，以及来自银行的证书。为了提供匿名性，所有这些组成部分都经过加密的。当我们使用银行验证系统时，货币的代码会包含其序列号，标签，用户公钥及其证书，银行的验证通过货币的代码得以实现。

在论文结尾，作者通过理论再次证明该电子现金系统的可靠性、匿名性、随机性以及高效性。可以确定，该系统是一个可以付诸实践的系统。

1.4 个人心得与体会

在本次学习过程中，由于这是我第一次阅读外国论文，读起来相当吃力。许多专有名词不知道如何翻译，例如：double-spending tag，在文章中译为双重支付标签，即两个用户双向交易货币时要用到的标志；bank 本意为银行，但是

倘若翻译为电子银行，则其与上下文显得格格不入，事实上，bank 应该是是可以储蓄、发放电子货币的电子机构，是类似于电子钱包的功能。本次论文的阅读提高了我的英语阅读能力以及查阅文献能力，相信会对以后的学习大有裨益。

由于文章实用性强，读起来具有一定趣味性。文章带领我初步了解学习的电子现金的原理，以及作者构思的可转移电子现金系统的构建。微信支付、银行卡支付等并不是真正意义上的可转移电子现金，其运作依赖于微信、银行等第三方系统，具有一定的不可靠性。随着电子现金技术的发展，以及加密算法的进步，国家级别安全保障的电子现金终究会出现，电子现金技术将会在我们生活中大放异彩。

第二部分 《如果可以的话，请匹配我：匹配加密及其应用》

2.1 问题背景和相关研究

匹配加密主要用于在保证隐私的情况下实现通信者所需的的匹配通信。在过去的情报工作中，通常需要间谍与来自不同组织的其他人员进行通信。当两个间谍交换秘密时，他们使用一种握手交互方法来确保参与交换的各方是他们指定的。例如，FBI 特工可能只想与 CIA 特工通信，如果是其他人员，通信将会中断且不透露通信人员信息。这种通信方式已经得到实现，被称为秘密握手协议（SH）。

秘密握手协议是传统密钥交换协议的演变，对保护参与者的隐私有着十分重要的作用。与大多数密钥协议一样，SH 本质上是交互式的，其目的是让各方通过密钥进行交互，实现信息交换。然而目前需要的是 SH 方法的非交互模式，就像 ElGamal 公钥加密可以解释为经典 Diffie-Hellman 密钥交换的非交互式版本一样。这种新的加密方法将允许发送方仅需要接收方的公钥即可离线加密消息，从而摆脱实时交互，同时为电子邮件等延时通信提供强大的隐私保证。不幸的是，现有的加密语言都无法实现非交互的秘密情报传递。

在作者 Balthazar Bauer 的论文中，他的团队尝试改进了加密模式，引入了一个名为匹配加密（ME）的新概念。在 ME 中，受信任的颁发机构生成分别与发送方和接收方的要求相关联的加密密钥和解密密钥。颁发机构还为接收方生成一个额外的解密密钥，该密钥与其选择的匹配要求相关联。消息的发送方可以动态指定接收方必须满足的任意匹配要求，以便显示消息。发件人的属性由权威机构认证，因此没有恶意发件人可以伪造虚假密文。

ME 在许多方面可以得到使用。首先，ME 解决了社交匹配的保密性，通信者搜寻适合他们的伙伴，但前提是他们具有需要匹配的特征。如果匹配失败，双方的隐私也会得到保护。其次，ME 还支持霸权主义国家的边缘人员和持不同政见者的社区发表意见。在专制国家，匿名通信可能会存在漏洞，并且由于来源未知而无法信任。，ME 模式可以为匹配者提供经过验证的群体匿名性，为

抗审查通信提供了全面的技术解决方案，同时提供了现有工具无法获得的来源真实性保证和强大的隐私保证。

2.2 算法和优点

在 ME 加密中，作者主要基于三个技术策略构建了 ME 加密方案：（1）随机 FE 方案（例如 rFE），（2）数字签名，（3）非交互式零知识（NIZK）。以上方法通过时间多项式算法得以实现。其中使用 FE 方案可以实现 ME 的实例化，但是安全性存在局限，并且隐匿性不能得到保证。为了克服上述困难，作者尝试了 Goldwasser 团队的 2FE 方案实例化，避免了匹配属性的泄露，并且可以实现亚指数级安全 iO。作者还尝试了通过因特尔的软件防护拓展功能，使得 FE 和 2FE 的实例化得到高效实现。

此外，作者还实现了基于双线性群的 IB-ME 方案，该方案具有高效性，并且在模拟模型中可以证明是安全的。作者给出了 Python 原型来证明 IB-ME 结构的实际可行性。

ME 加密首次实现了非交互式的秘密握手协议，并且实现了安全性和隐匿性：攻击者无法在不知道匹配属性下进行攻击；无法通过重复攻击破解属性。在文章中，作者也通过多个方面证明了该加密方案的可靠性。

2.3 框架与结论

在 ME 模式中，首先需要指定一个受信任的颁发机构，机构将会颁发公钥。基于公钥，颁发机构会依此生成三种密钥：（1）与消息发送方匹配属性关联的加密密钥；（2）与接收方匹配属性相关联的一个解密密钥；（3）与消息发送方的匹配属性和应满足的模式相关联的另一个解密密钥，该模式由接收方选择算法创建。

发送方在指定匹配属性后，在颁发机构获得相应的加密密钥，并且可以指定加密模式，从而生成密文。接受方则尝试通过使用对应的两个密钥来解密。如果双方的属性匹配，接收方可以获得密文，否则解密将发生错误。

作者还从几种类型的有限元方案中探索 ME 和 A-ME 的黑匣子结构，并且在模拟中证明了 ME 的可行性。论文末尾构建了基于身份属性的 ME 实例化、IB-ME 实例化以及其在 Tor 网络交互信息的实现，并且进行了评估。结果表明，ME 是实用并且可靠的。

1.4 个人心得与体会

在这一次的密码学实践课程中，我有幸接触到了最新的密码学理论。其中运用到的数字签名方案、多项式方案都是课堂上学到的知识，多种知识结合起来，构成了一套完整而崭新的加密模式——匹配加密，论文深入浅出，具体详细地介绍了匹配加密方法，可读性强。

ME 加密作为一种全新地加密方法，其具有的匿名性、非交互性等特点可以说是不可替代的。在间谍通信、民主发声、社交匹配等方面都可以得到应用。并且作者也成功实现了其高效实例化。相信在不久的未来，ME 将会投入使用，在许多方面大放异彩，。