How to reach secret agreement

如何簽署秘密合約

組員姓名：蔡青紘

指導教授：黃之浩 教授 組別：A116

Abstract

在現今的密碼學中，隨著區塊鏈的興起，保障資訊的安全性以及使用者的隱私變成了一大重要的主題，在門羅幣中，其使用了 Ring signature 的衍生物環保密交易(RingCT)，來作為保障使用者匿名性的工具，但在此使用者僅只是對單一的交易進行簽名，本專題在此基礎上，將簽名改為合約，並在不失去使用者隱私的情況下，加上訊息的隱私性，讓兩群體中的某人可以私密地簽署祕密合約。

Introduction

在現今的密碼學領域中，幾個比較大的主題包括，最近特別熱門的後量子密碼學、隨著量子電腦的發展而逐漸有潛力的量子密碼學，大量被區塊鏈所應用的零知識證明，以及其他同態加密、基於屬性的密碼學等等，而在研究其中，首先，因為區塊鏈的應用，比起目前其他領域更有機會直接的被應用上實際情境當中，再加上我發現自己對零知識證明等以保障隱私為優先的密碼學也較為有興趣，因此便從事其相關的研究，最後因緣際會碰觸到 Ring Signature 這個主題，發現其也是和區塊鏈有很大相關的一個主題，並在最後零知識證明和 Ring Signature 中選定 Ring Signature 作為主題。

在本專題中，我們將原先的單一環簽章改進成雙環的簽名，並在簽名外，新增了對訊息的保護，也就是說，除了原先 Ring Signature 就存在的匿名性（Anonymity）以及不可偽造性（Unforgeability）以外，增加了訊息的隱蔽性（Hiding），這樣的結果就是，比起一般的公私鑰簽名，僅僅包含簽名和認證兩個部分，我們所提出的雙環合約，包含了兩種認證－公開認證和私密認證，公開認證可以確定雙方有合約存在，並且此份合約是無法更改的，私密認證則可以確認雙方確實簽了某個訊息，而兩種認證的模式有兩個特殊的地方，第一，只要將雙方簽合約理解為一方和另一方進行約定，並由於簽名者不能任意更改任何訊息，此時簽名的過程意味著跟對方約定訊息為何，公開認證則是驗證約定的存在，私密認證則是驗證確切訊息，這剛好就符合零知識證明中相當重要的一個 protocol，稱作為 commitment scheme，第二點，由於在認證時，並不會直接用到訊息來證明此合約，而這剛好符合零知識證明的精隨－在不洩漏訊息的情況下，證明我知道這個訊息，因此我們所提出的環合約整合了 Ring signature 和零知識證明，可以為使用者提供良好的安全性的保障。

心得

在專題的一開始，教授給我了一篇密碼學的論文，讓我去將其相關的文章看懂，並且有不懂的地方或者時有甚麼想法時就去找教授討論，在一年內主要有兩個最大的難關，首先是補齊以前所不知道的知識，由於以前接觸過的密碼學都只是應用層面，並沒有到理論層面，因此我所知道的只有 AES, RSA,ECC 等等系統，但是在近20年，這個學科發展了許多其他的方向，例如，ZKP, PQC,安全性定義等等，在這期間，我不只花時間讀完了 UCB 的 CS276和一堂 Zero-Knowledge Proofs Seminar 的課程，也有讀一些 lattice 和 ECC 的課程，但是我認為這比較不會是我這次研究專題的方向，並沒有讀完，在論文的方面，也讀了不下20篇的論文，這些閱讀的量就花了我大部分的時間，我第二個最大的難關就是，有別於其他教授給學生一個題目讓他做出來，或者是教授提供一些想法讓學生在這些想法內找題目，我的專題的提案都是我自己想出來的，然而在從提案到實際的成形的過程中，就會需要和教授討論後才能確定是否可行；自己想題目真的是一件很困難的事情，儘管教授有給我一篇論文做為參考並且在需要時給予我建議，但是實際的研究人員還是我自己，我想建構怎樣子的密碼系統，以及要如何建構，都是自己要花心血去思考和改良的，而最難過的就是，有時候剛有一些不錯的想法，結果發現不太可行，或是已經被發表過了，這也造成我陸陸續續重新想了許多題目，最後才確定此想法作為本專題的題目。