

Notes of Cryptography

Squirrel

February 28, 2025

Preface

Course

密碼學設計與分析 Cryptography Design and Analysis (11320IIS500900) in NTHU

1 L1

1.1 Merkle 的故事

Merkle 在大學部修了一個課，然後要交一個 project。他在交這個作業的時候，提到了 Public Key Cryptography 的想法。當時的導師並不看好這個東西，所以 reject 了，最後他也退掉了這門課。之後他找到另一個很欣賞他的老師，覺得應該要「Publish it, win fame and fortune」，所以他將這篇文章那個投到了 CACM (Communications of the ACM)。第一次投期刊就因為「這個想法不是當今的主流想法」而被拒絕。在 Merkle 的某些堅持之下，過了快三年終於讓 CACM 接受了這篇文章。

這邊的故事及當時的論文，可以在 <https://ralphmerkle.com/1974/> 找到。

另外影片中的 link 有誤，應該改成 <https://ralphmerkle.com>，不然你只會找到一間搞 CRM 和賣資料的公司。

1.2 Conventions

- 離散且有限的時間 (Discrete and finite world)
⇒ 因為我們正在討論 computer science
- Data v.s. Information
- Machine (function/algorithm) 需要在 polynomial time 下執行
⇒ 因為我們需要能在一定時間內看到結果，不想要等到天荒地老
⇒ 不一定強制要求 polynomial time，但這堂課大部分會是這樣
- Alice and Bob：就是 sender 和 receiver，通常是 Alice 要傳訊息給 Bob
⇒ 還有其他角色，可以參見 Wikipedia：
https://en.wikipedia.org/wiki/Alice_and_Bob
- 計算 (computation)：任何遵循 well-defined model (例如 algorithm、protocol) 的 calculation。
- Efficiency
Input size: $|x| = n$ bits
其他的就拿 complexity 概念來作為 efficiency 的概念
- Crypto 像是信仰 (Faith)？
密碼學不一定總是對的，但我們需要相信某些東西才能繼續在密碼學上前進
這些東西包含：
⇒ 某些數學問題很難被解決
⇒ 某些假設無法被打破 (通常指在 poly-time 底下)
⇒ 某些底層的密碼工具 (underlying crypto primitives) 是安全的
⇒ $P \neq NP$
⇒ 亂數/隨機 (randomness)，因為我們不知道真的亂數長什麼樣，所以無法驗證