打造公平的遊戲轉蛋：在不洩漏原始碼的前提下驗證虛擬轉蛋的機率

Securing Fair Loot Box Games: An Efficient Approach to Verifying Loot Box Probability Statement Without Source Code Disclosure

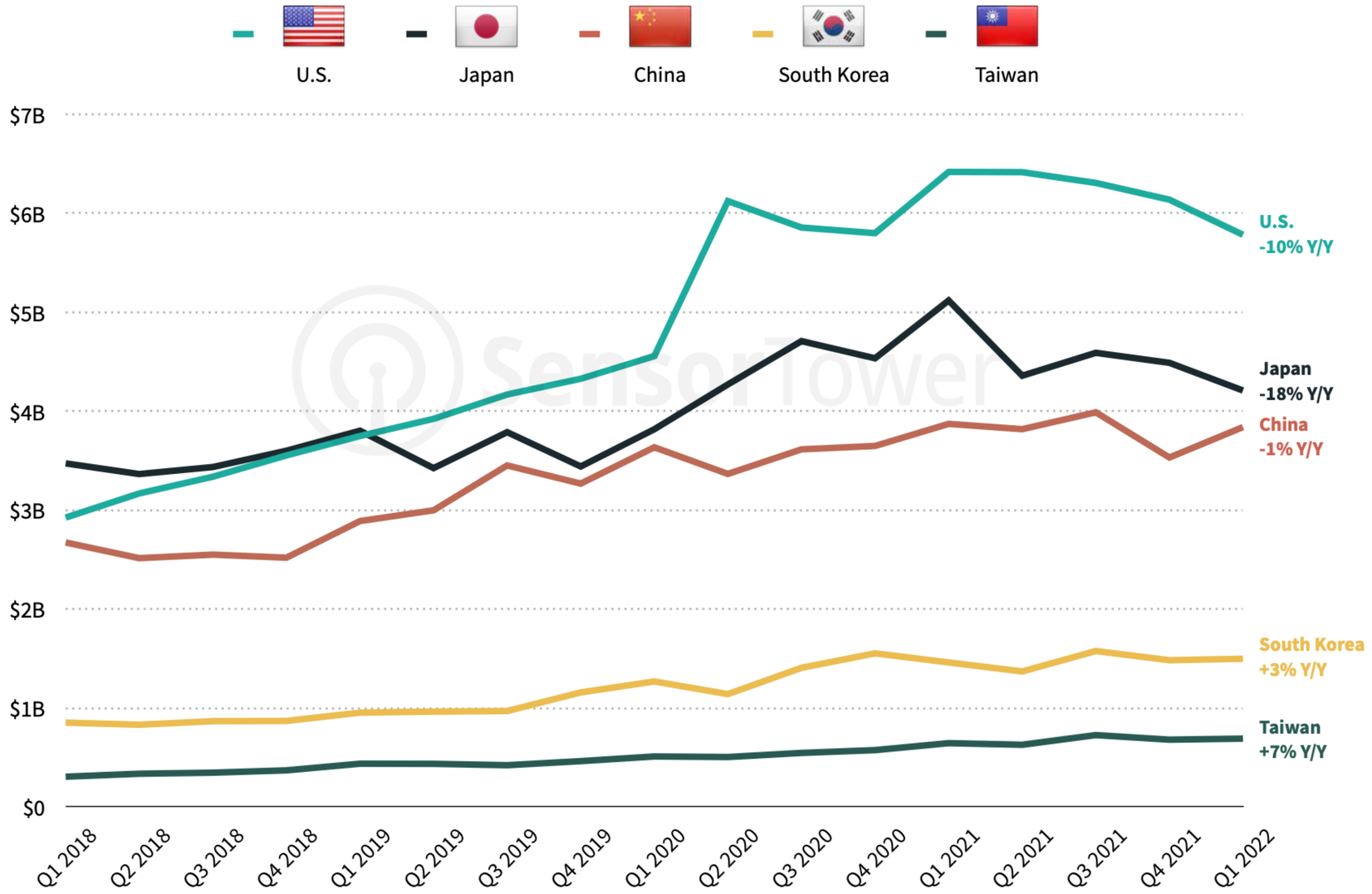
王靖傑
李安傑

What is Loot Box (虛擬轉蛋)

- “Gacha” in Japanese （轉蛋）
- 玩家藉由這個機制可以「隨機」獲得虛擬寶物
- 轉蛋機制常見於 Free-to-play (freemium) games
  - 78% of the total revenue in the gaming industry
- The severity of problem gambling（賭博成癮問題）
- Probability disclosure（幾率揭露）
  - Humans tend to be ambiguity averse [1]
  - Misleading players with false probability may gain more revenue [2]

1. *Ellsberg, Daniel. "Risk, ambiguity, and the Savage axioms." The quarterly journal of economics 75.4 (1961)*
2. *Chen, Ningyuan, et al. "Loot box pricing and design." Proceedings of the 21st ACM Conference on Economics and Computation. 2020.*

Top countries by mobile game spending, App Store and Google Play

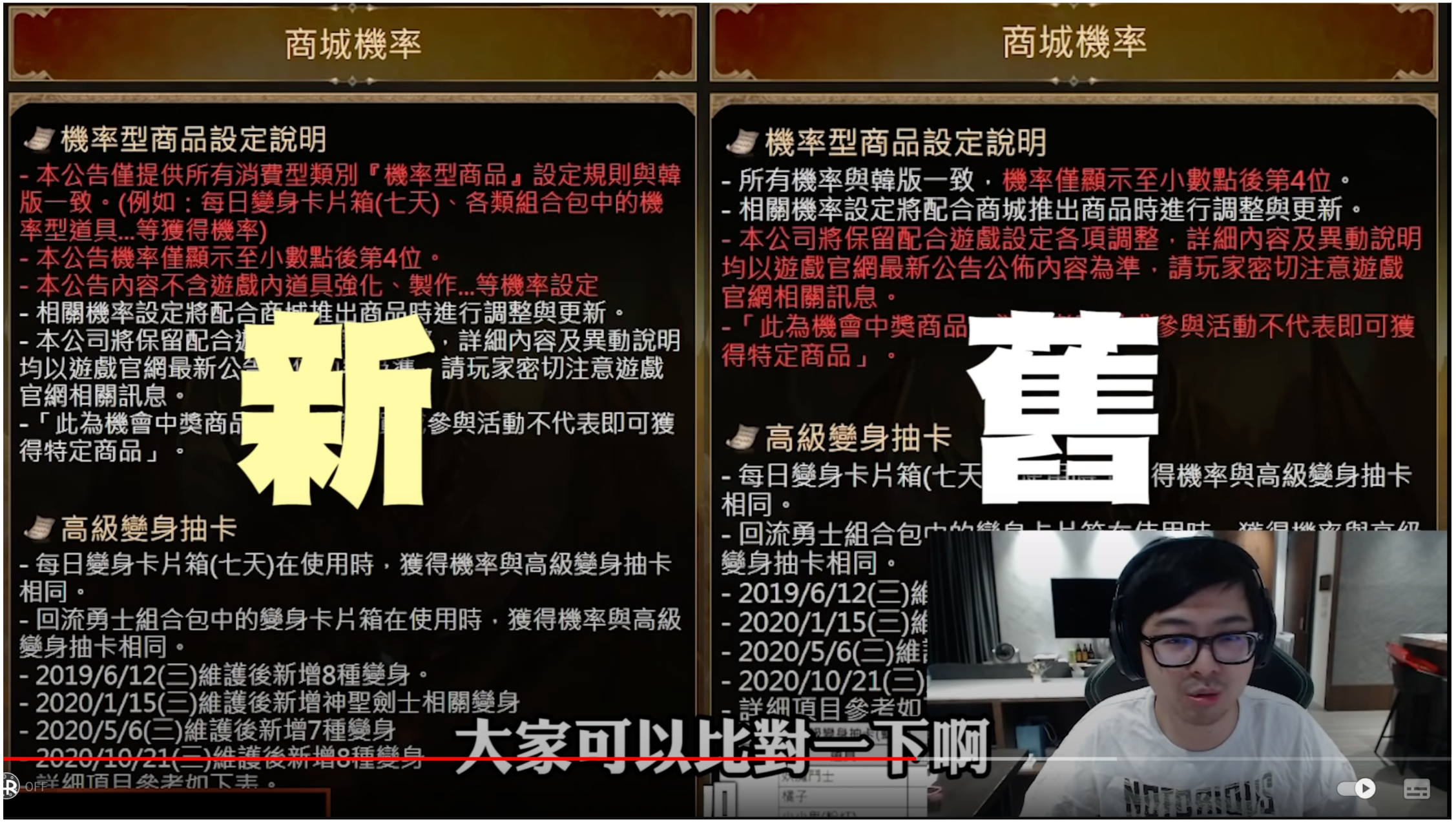


台灣「轉蛋法」連署

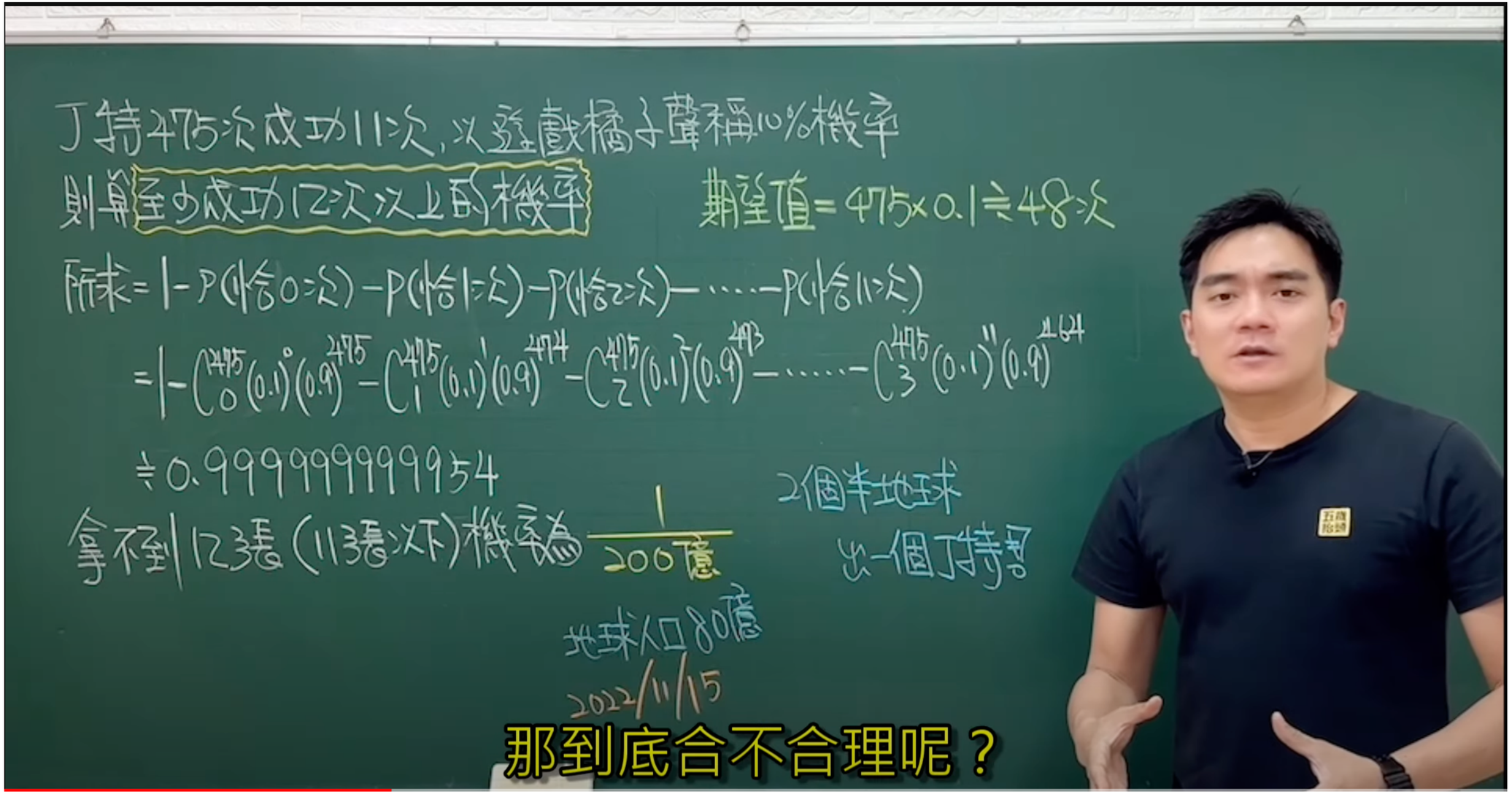
- From 2021/06

台灣天堂 M 「紫布事件」

- 2021/08 & 2021/09
- 實況主丁特總共砸了 414 萬元
- 實測成功機率：2.28%
- 韓版公告：10% 成功機率
- 遊戲公司公告：「所有機率與韓版一致」
- 提告以後 -> 馬上改公告 🤪


商城機率
機率型商品設定說明
- 本公告僅提供所有消費型類別『機率型商品』設定規則與韓版一致。(例如：每日變身卡片箱(七天)、各類組合包中的機率型道具...等獲得機率)
- 本公告機率僅顯示至小數點後第4位。
- 本公告內容不含遊戲內道具強化、製作...等機率設定
- 相關機率設定將配合商城推出商品時進行調整與更新。
- 本公司將保留配合遊
，詳細內容及異動說明
均以遊戲官網最新公
請玩家密切注意遊戲
官網相關訊息。
-「此為機會中獎商品
參與活動不代表即可獲
得特定商品」。
新
高級變身抽卡
- 每日變身卡片箱(七天)在使用時，獲得機率與高級變身抽卡相同。
- 回流勇士組合包中的變身卡片箱在使用時，獲得機率與高級變身抽卡相同。
- 2019/6/12(三)維護後新增8種變身。
- 2020/1/15(三)維護後新增神聖劍士相關變身
- 2020/5/6(三)維護後新增7種變身
- 2020/10/21(三)維護後新增8種變身
- 詳細項目參考如下表。
商城機率
機率型商品設定說明
- 所有機率與韓版一致，機率僅顯示至小數點後第4位。
- 相關機率設定將配合商城推出商品時進行調整與更新。
- 本公司將保留配合遊戲設定各項調整，詳細內容及異動說明均以遊戲官網最新公告公佈內容為準，請玩家密切注意遊戲官網相關訊息。
-「此為機會中獎商品
參與活動不代表即可獲得特定商品」。
舊
高級變身抽卡
- 每日變身卡片箱(七天
得機率與高級變身抽卡相同。
- 回流勇士組合包中的變身卡片箱在使用時，獲得機率與高級變身抽卡相同。
- 2019/6/12(三)維
- 2020/1/15(三)維
- 2020/5/6(三)維
- 2020/10/21(三)
- 詳細項目參考如
大家可以比對一下啊
NOTORIOUS

是因為他剛好比較衰嗎？


丁特475次成功11次，以遊戲橘子聲稱10%機率
則475至少成功11次以上的機率
期望值=475×0.1≒48次
所求=1-P(恰合0次)-P(恰合1次)-P(恰合2次)-……-P(恰合11次)
≒0.999999999954
拿不到11張(113張以下)機率為 1/200億
2個半地球
出一個丁特
地球人口80億
2022/11/15
那到底合不合理呢？

事件後續 - 公平交易委員會

公平交易委員會處分書

公處字第 111039 號

被處分人：遊戲橘子數位科技股份有限公司
統一編號：89550029
址　　設：臺北市內湖區瑞湖街 111 號
代 表 人：劉○○
地　　址：同上

被處分人因違反公平交易法事件，本會處分如下：

主　　文

一、被處分人銷售「天堂 M」線上遊戲，舉辦「【天堂 M】NCSOFT 原廠來台玩家座談會」，宣稱「可以公開活動製作、抽卡、合成的機率嗎？目前這些機率的設定是否都跟韓版相同……台版機率都是跟韓國一模一樣的」，就足以影響交易決定之服務內容為虛偽不實及引人錯誤之表示，違反公平交易法第 21 條第 4 項準用第 1 項規定。

二、處新臺幣 200 萬元罰鍰。

(四)另本會於調查期間查得被處分人於 108 年 10 月網頁對應韓國原廠網頁之相關活動、韓國原廠 110 年 9 月網頁刊載內容、臺北市政府法務局同年 10 月辦理「天堂 M 線上遊戲公告機率疑與實際情形不符衍生疑義案」會議紀錄與被處分人同年 12 月「天堂 M_版本群組(技術+I A+營運)」通訊軟體對話紀錄，獲悉韓版紫布設定製作機率 10%，台版紫布設定製作機率 5%。

遊戲公司改變說詞：

- 韓版：100萬個材料 / 每次製作使用201個材料×10%=498個紫布
- 台版：100萬個材料 / 每次製作使用99個材料×5%=505個紫布

事件後續 - 民事判決

- 2023/07/21
- 法院認定：遊戲橘子故意廣告不實
- 法院認定：遊戲橘子前後說詞矛盾
- 遊戲橘子態度惡劣，法院判賠 3 倍

臺灣士林地方法院民事判決

111年度消字第10號

原　　告　薛弘偉
訴訟代理人　陳義文律師
複　代理人　蔡靜娟律師
　　洪祐嶸律師
被　　告　遊戲橘子數位科技股份有限公司

法定代理人　劉柏園
訴訟代理人　范晉魁律師
　　呂俊杰律師
　　林禹維律師

上列當事人間請求損害賠償事件，本院於民國112年6月16日言詞辯論終結，判決如下：

主　　文

被告應給付原告新臺幣柒佰捌拾肆萬零捌佰柒拾伍元，及自民國一百一十一年九月二十九日起至清償日止，按週年利率百分之五計算之利息。

疑似轉蛋機率「內部消息」

【情報】內部消息-關於抽獎機率的真實情況

遊戲情報

樓主 **璃璃** LiLi0719

2021-07-31 19:08:29 編輯

最後來解釋兩個問題

1. 為什麼大課長的抽獎運總是比小課玩家還差？
2. 為什麼非洲人抽東西永遠是非洲、歐洲人抽東西遠永遠是歐洲？

首先我先把大課長用A、小課玩家用B來代稱，假設一個情況

【帳號剛創初始階段】

(1)

A在帳號創了之後，就儲了一堆點券，買了聖典，買了英雄禮包，買了XXXX

B在帳號創了之後，只小課了一些點券

這時候A已經超過了T1，它的5倍沒了，甚至可能超過了T2，而B還保留了他的5倍

(2)

此時出了**無保底抽獎活動**

A由於沒有5倍，所以課到了T5才抽到造型

B因為有5倍，然後依照一開始說的那個循環小額小額抽，因此在倍率加乘之下，B可能課到T1或T2就抽到造型

```
blackCat=rp.getString(R.string.blackCat);
heros=rp.getString(R.string.heros);
tickets=rp.getString(R.string.tickets);
sundries=rp.getString(R.string.sundries);

for(int i =0 ; i <=T.length ; i++){
    if(cfg.getTotalRecord() < T[i] ){
        mx = M[i];
        isMagnification = true;
        break;
    }
}

if(isMagnification){
    ap.remove(ap.size()-1);
    RandomNumber rn=new RandomNumber();
    float mr = mx/3;
    rn.add(blackCat,0.0229*mx);
    rn.add(heros,0.0518-mr);
    rn.add(tickets,0.0471-mr);
    rn.add(sundries,0.8782-mr);
    ap.add(rn.rand());
} else {
    ap.remove(ap.size()-1);
    RandomNumber rn=new RandomNumber();
    rn.add(blackCat,0.0229);
    rn.add(heros,0.0518);
    rn.add(tickets,0.0471);
    rn.add(sundries,0.8782);
    ap.add(rn.rand());
}
```

台灣「轉蛋法」通過

- 於 2023/01/01 生效
- 消費者保護會通過「網路連線遊戲服務定型化契約應記載及不得記載事項」應記載事項第 6 點修正草案
  - 要求遊戲業者應揭露中獎機率
  - 明定中獎機率的定義
  - 明定中獎機率應揭露的範圍
  - 明定中獎機率揭露的方式

Reference: 行政院消費者保護會新聞稿

日本與韓國的轉蛋法

- 日本
  - 2012: 修法「不當景品類及不當表示防止法」
  - 2016: 「日本線上遊戲協會」(JOGA) 發布 guidlines
    - 保底抽數 < 100
    - 保底金額 < 5 萬日圓
    - 須公布稀有物件的出現機率上下限
    - 各個物件明確公布機率

- 韓國
  - Self-regulating by Korean Association of the Game Industry (K-GAMES)
  - 2018: Nexon 因隱瞞機率被韓國公平貿易委員會 (KFTC) 重罰 9.44 億韓元 [link]
  - 2023/02: 通過修法規定需明確公布機率 [link]

大家最在意的還是如何「驗證」機率

- From “A Research of Social Game Users’ Attitude to "Gacha" Probability Announcement”
- 第四個限制對大多數人而言最重要：a: 9.2%, b: 8.3%, c: 13.0%, d: 65.0%
- Agree: “Probability (estimated price) should be announced”
- Agree: “I feel relieved to be announced even with low probability.”
- Disagree: “I think the probability (estimated price) announced in Gacha is correct”
- Disagree: “I am satisfied with the probability (estimated amount) notation of Gacha”

```
推 bobby4755: 玩家要先課個30萬來驗證機率對不對
噓 LeonBolton: 公布機率又怎麼驗證？還不是又只會靠北”樣本數不足”
→  aa1477888: 問題是怎麼驗證？有沒有官方單位會去驗證？
```

台灣的「第三方驗證平台」

- 網站：https://gacha.gamelab.com.tw
- 玩家可以自行上傳抽獎紀錄，並附帶螢幕錄影，「專門的團隊」會負責驗證真偽及數據統計
- 缺點
  - 驗證螢幕錄影成本高也沒辦法達到 100% 正確率
  - 沒有提供大眾驗證資料正確性的機制
  - 無法偵測 hidden inputs，例如前面提到的巴哈爆料
  - 選擇性上傳資料的問題

Blockchain-based Transparent Loot Box

- Drawbacks:
  - Using “timestamp” as random source may be predicted by the players
  - Using smart contract to write the loot box means “open source”

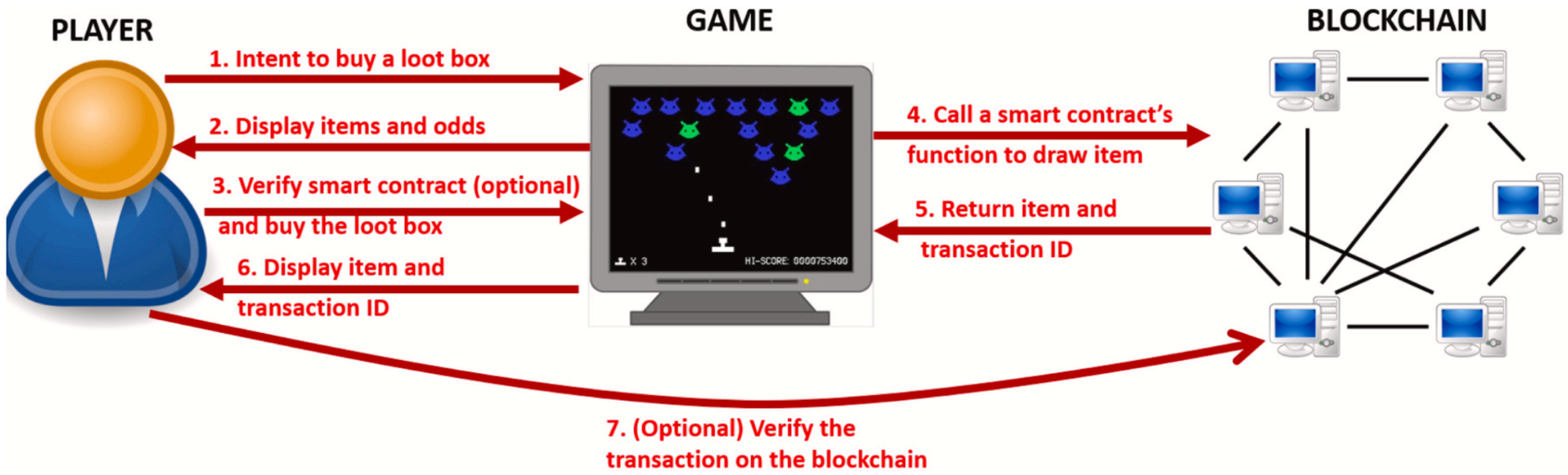


Fig. 2. The process of buying and opening a loot box under our proposed solution.

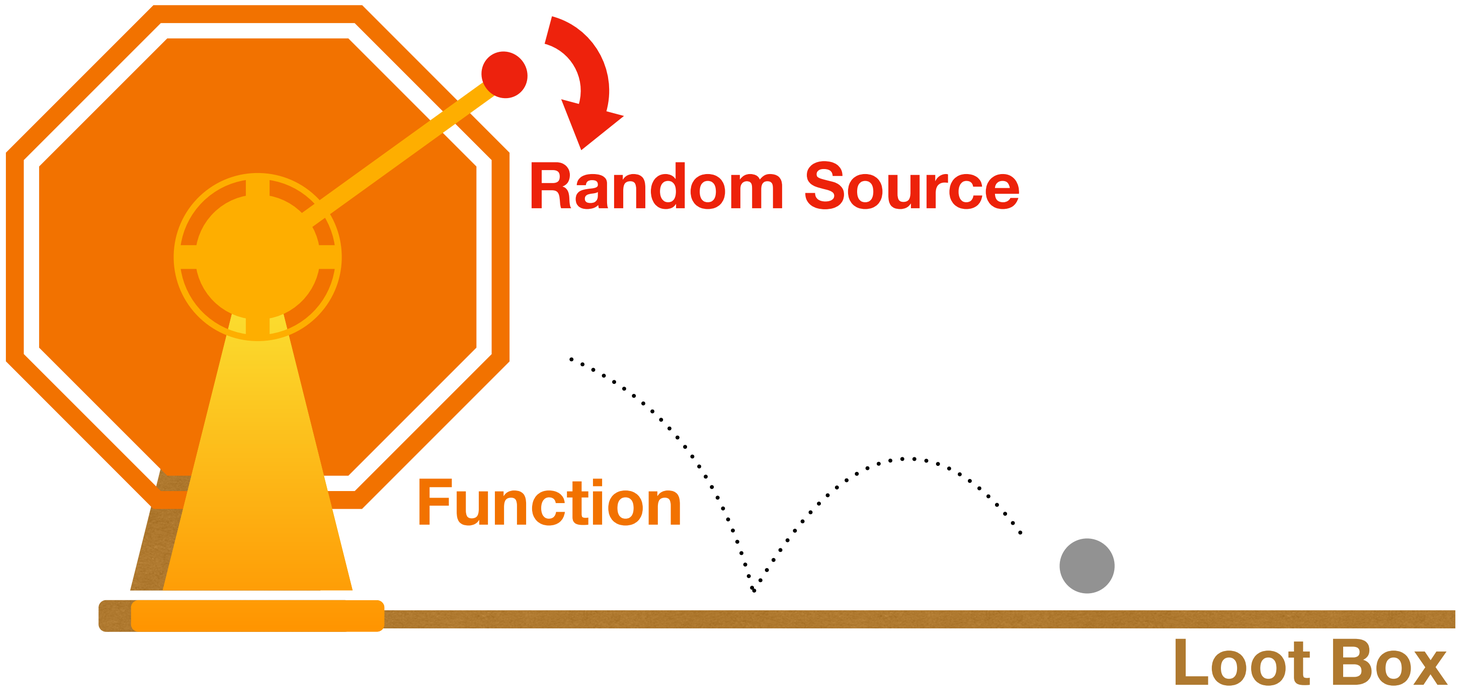
為什麼不直接公開程式碼？

- 轉蛋機制往往是遊戲公司最重要的「商業機密」
- 法律上較難要求遊戲公司公開程式碼
- 不洩漏程式碼也可以增加遊戲廠商的意願
- 目標：在不洩漏程式碼的前提下驗證機率

要達成的目標

- Correctness & Soundness:
  - Probability statement is true $\iff$ Verification success
- Public Verifiability
  - Everyone is able to do the verification
- Individual Verifiability
  - Each individual can verify that their probability is not biased
- Input Transparency
  - No hidden input
- Algorithmic Hiding
  - Minimal information disclosure of the underlying function

一個抽獎機制會需要有什麼東西？



Loot Box = Random Source + Function

Verifiable Loot Box = Verifiable Random Source + Verifiable Function

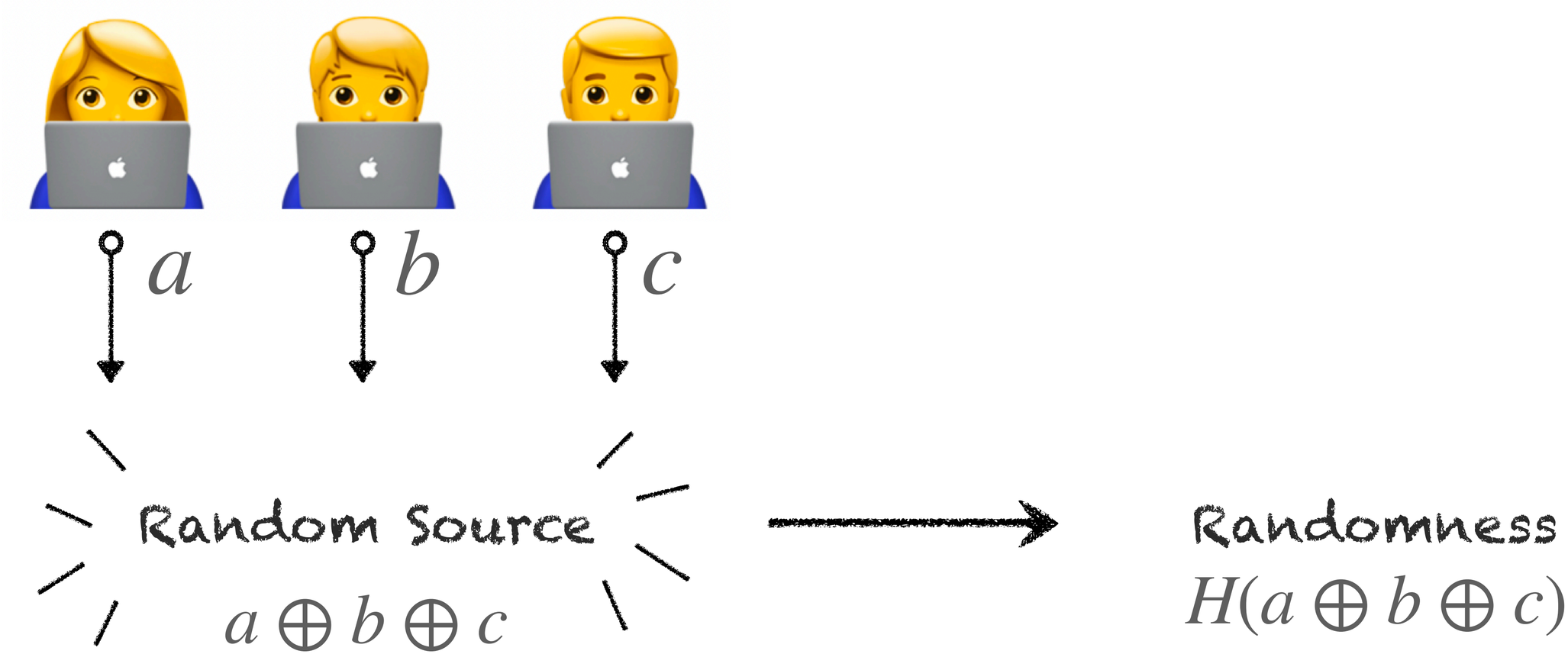
怎麼產生 random 呢？

```python
import random
random.seed(1337)
random.randrange(123456)
```

```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

Really? Can we never be sure?

A naive approach: At least, you can trust yourself.



HeadStart

1. A participatory randomness protocol designed for public participation at scale.

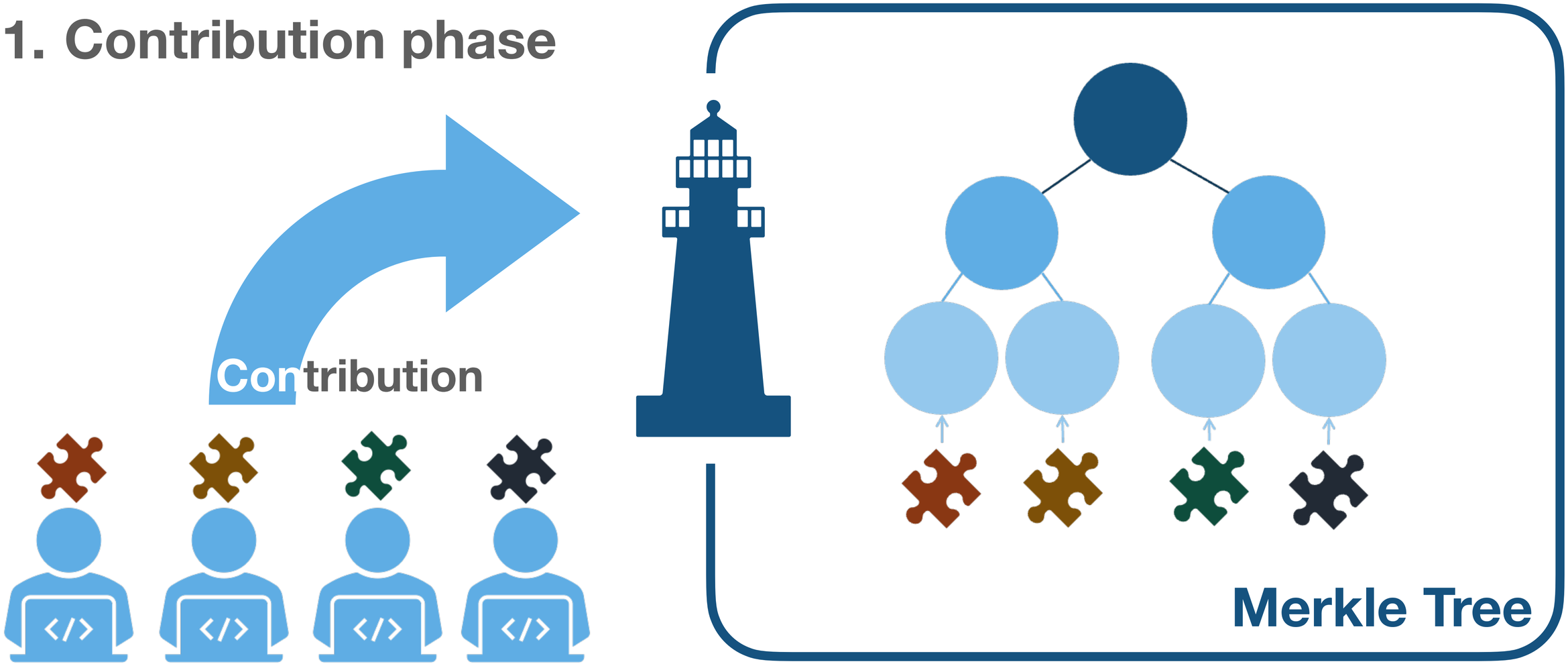
2. The construction of HeadStart can be simply divided into two parts:

    1. Contribution phase

    2. Result Generation phase

HeadStart

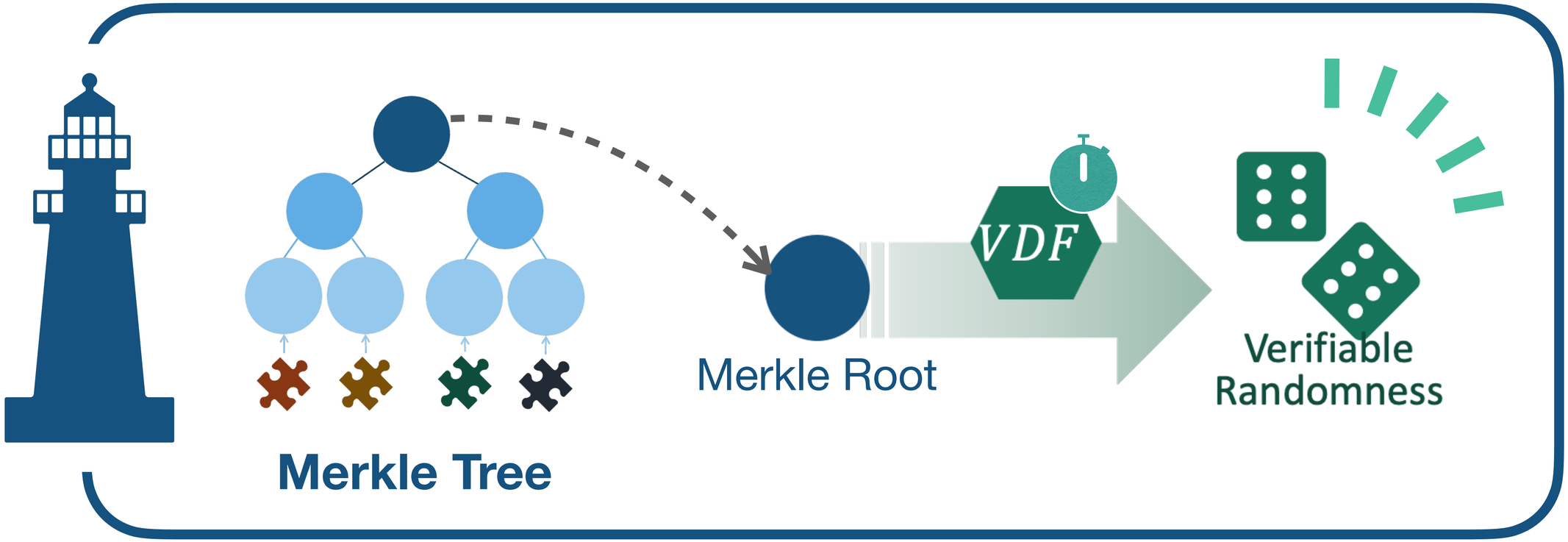
1. Contribution phase



HeadStart

2. Result Generation phase

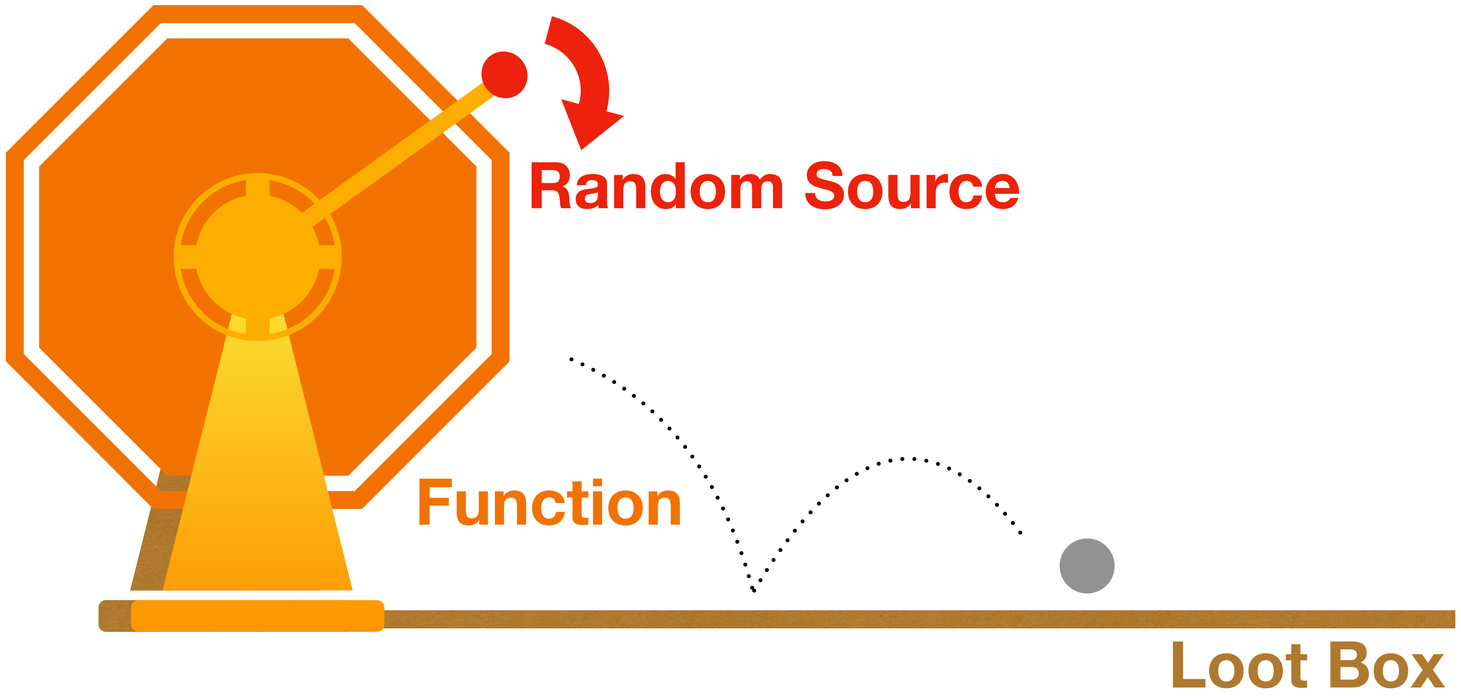
Derive random source from the random source by VDF



HeadStart

- 如何確定 contribution 有被放進去 random source？ Merkle Tree！
- 如何防止 Last Contribution Attack？ Verifiable Delay Function
- Scalability? Merkle Tree 只需要 $O(\log N)$ 的時間複雜度

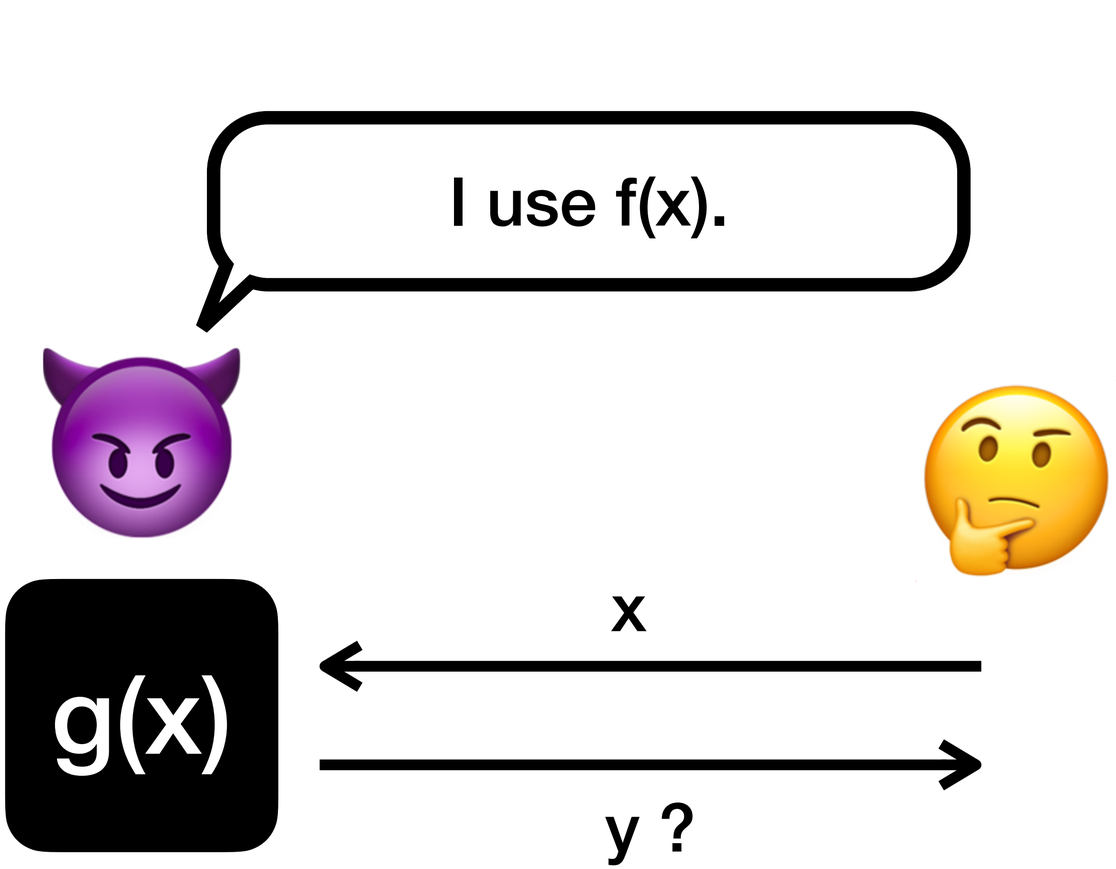
一個抽獎機制會需要有什麼東西？

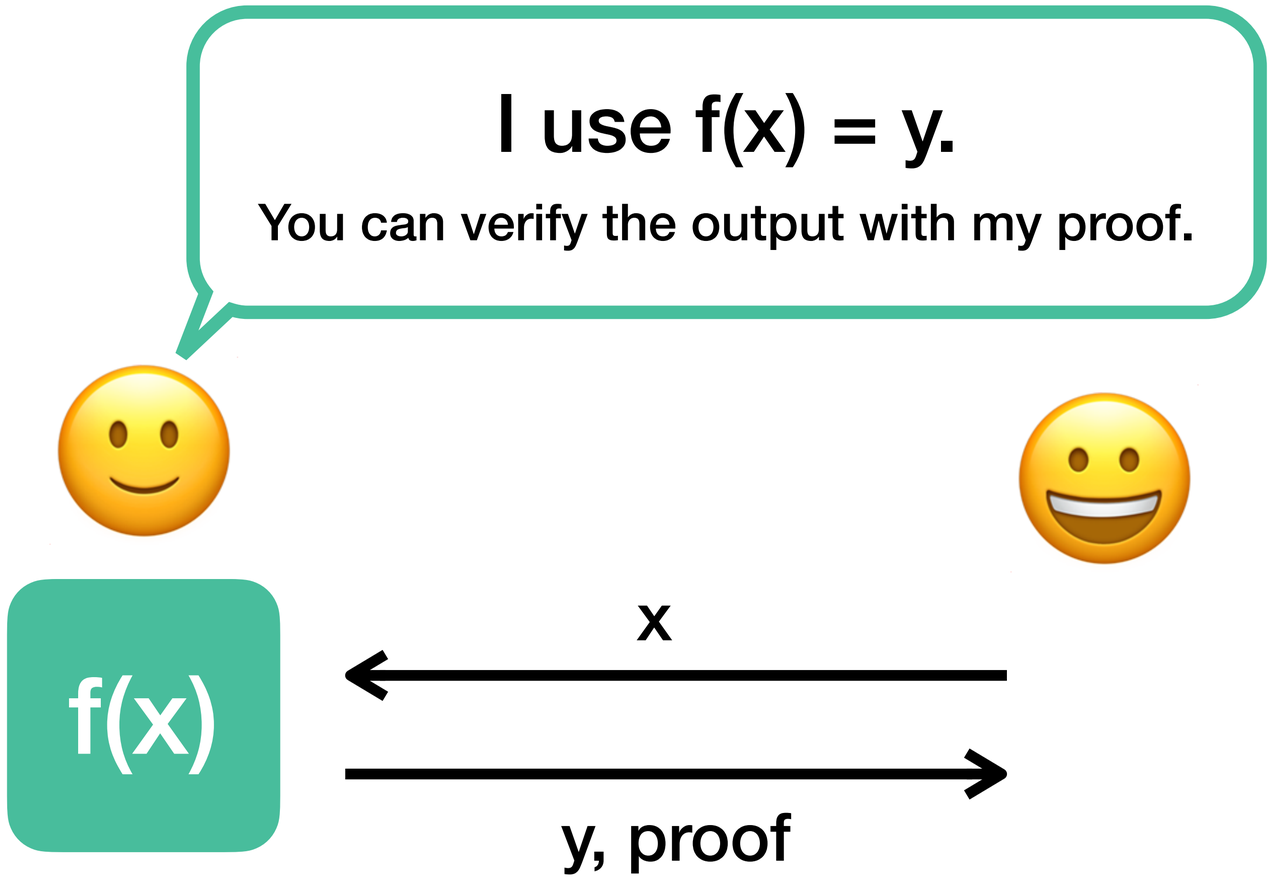


Loot Box = Random Source + Function

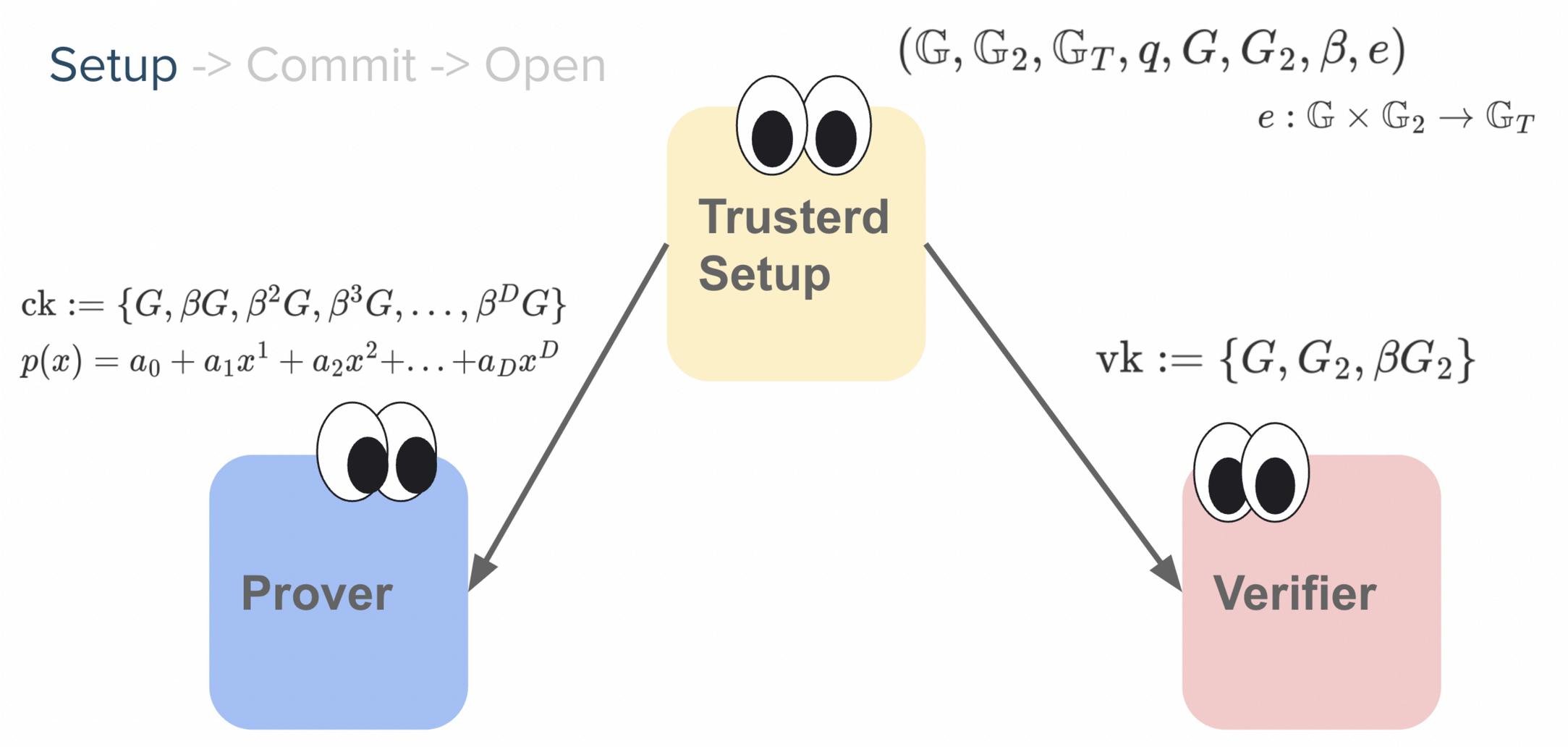
Verifiable Loot Box = Verifiable Random Source + Verifiable Function

Verifiable Function?





Polynomial commitment



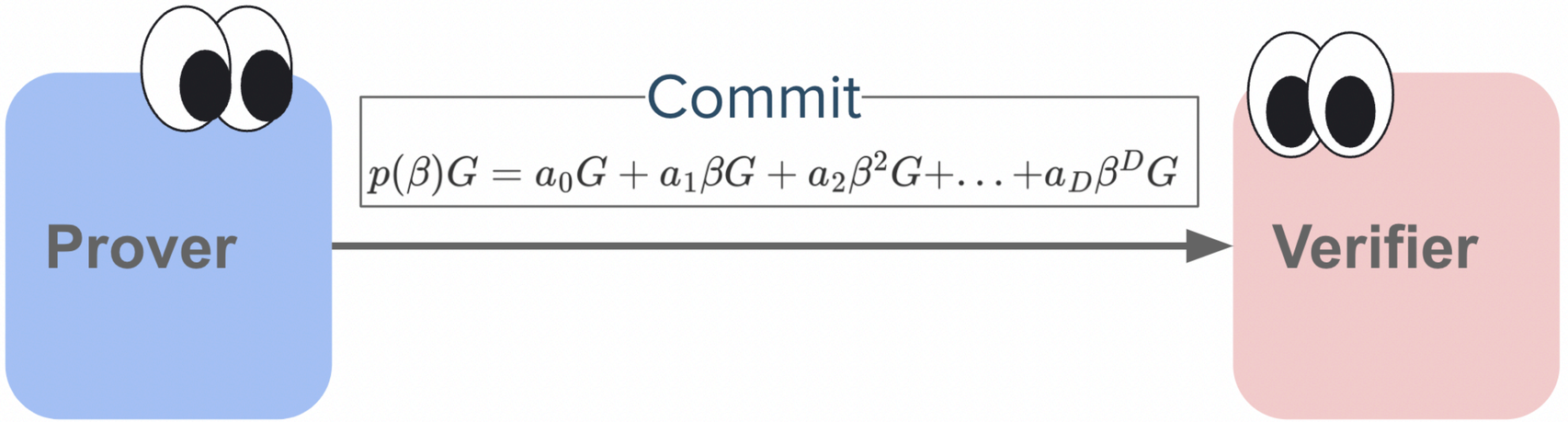
Polynomial commitment

Setup -> Commit -> Open

$$\text{ck} := \{G, \beta G, \beta^2 G, \beta^3 G, \ldots, \beta^D G\}$$

$$p(x) = a_0 + a_1 x^1 + a_2 x^2 + \ldots + a_D x^D$$

$$\text{vk} := \{G, G_2, \beta G_2\}$$



Polynomial commitment

Setup -> Commit -> Open

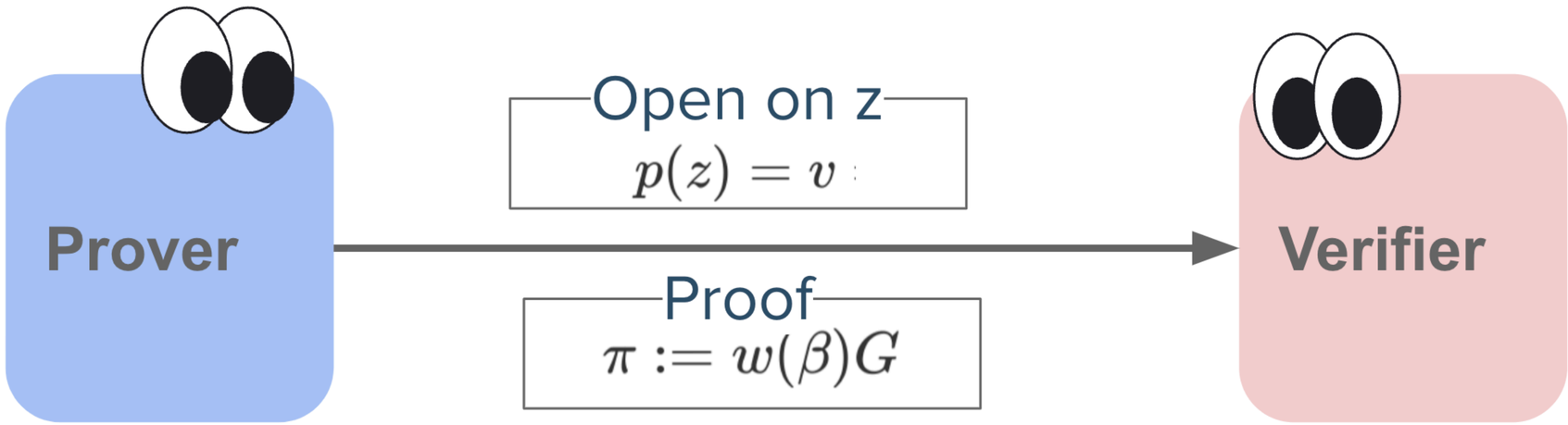
$$\text{ck} := \{G, \beta G, \beta^2 G, \beta^3 G, \ldots, \beta^D G\}$$

$$p(x) = a_0 + a_1 x^1 + a_2 x^2 + \ldots + a_D x^D$$

$$\text{vk} := \{G, G_2, \beta G_2\}$$

$$p(\beta)G = a_0 G + a_1 \beta G + a_2 \beta^2 G + \ldots + a_D \beta^D G$$

$$p(z) = v \Rightarrow w(x) := (p(x) - p(z))/(x - z)$$



Polynomial commitment

$$e(c - vG, G_2) \stackrel{?}{=} e(\pi, \beta G_2 - zG_2)$$

$$e(p(\beta)G - vG, G_2) \stackrel{?}{=} e(w(\beta)G, (\beta - z)G_2)$$

$$(p(\beta) - v)e(G, G_2) \stackrel{?}{=} (w(\beta)(\beta - z))e(G, G_2)$$

$$p(\beta) - v \stackrel{?}{=} w(\beta)(\beta - z)$$

$$w(\beta) \stackrel{?}{=} (p(\beta) - v)/(\beta - z)$$

Polynomial commitment

Setup -> Commit -> Open

$$\text{ck} := \{G, \beta G, \beta^2 G, \beta^3 G, \ldots, \beta^D G\}$$

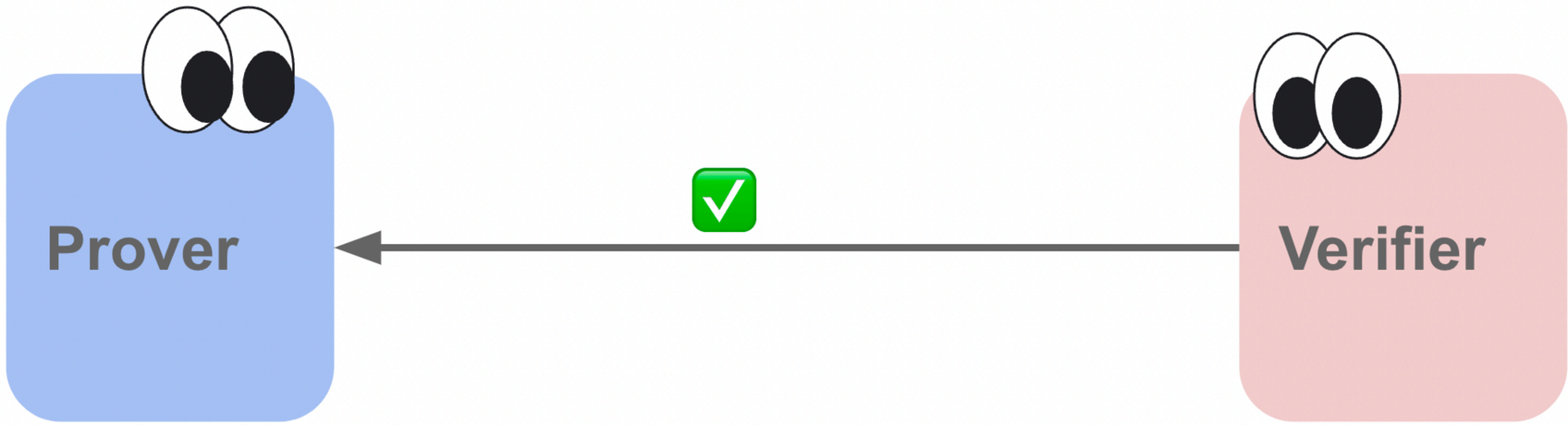
$$p(x) = a_0 + a_1 x^1 + a_2 x^2 + \ldots + a_D x^D$$

$$\text{vk} := \{G, G_2, \beta G_2\}$$

$$p(\beta)G = a_0 G + a_1 \beta G + a_2 \beta^2 G + \ldots + a_D \beta^D G$$

$$p(z) = v \Rightarrow w(x) := (p(x) - p(z))/(x - z)$$

$$e(c - vG, G_2) = e(\pi, \beta G_2 - zG_2)$$



Functional Commitment

A (function-hiding) functional commitment consists of the following algorithms

1 FC.Setup$(1^\lambda, N) \rightarrow$ pp

Input	the security parameter λ the upper limit of the gate number N
Output	public parameters pp

2 FC.Commit(pp, $f, r) \rightarrow c$

Input	a public parameter pp a secret function f randomness r
Output	a commitment c to f.

3 FC.Eval(pp, $f, r, x, y) \rightarrow \pi$

Input	public parameters pp a function f another randomness r evaluation point x claimed evaluation value y
Output	a proof π (convinces the verifier $f(x) = y$)

4 FC.Verify(pp, $c, x, y, \pi) \rightarrow \{0,1\}$

Input	public parameters pp a commitment c an evaluation point x claimed evaluation value y a proof π
Output	decision bit $\{0,1\}$

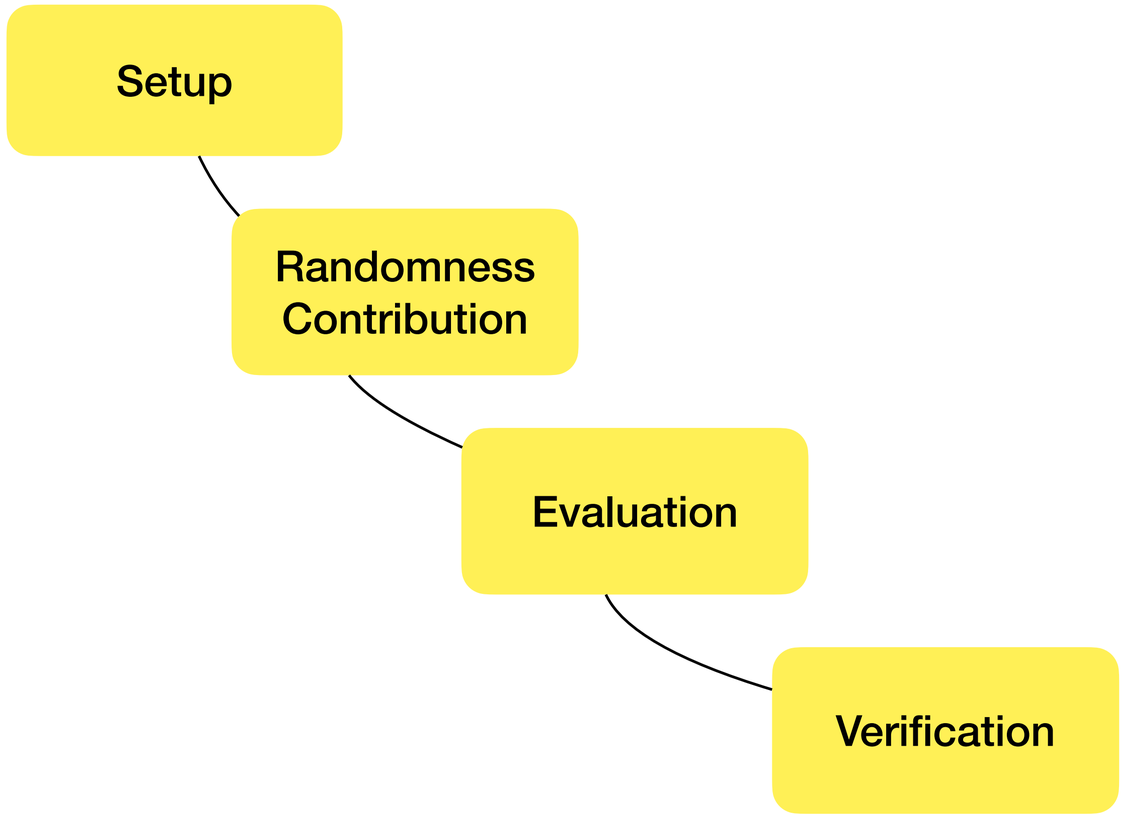
Problem Formulation

- Assumptions:
  - The server does not abort
  - There is a publicly accessible bulletin board
  - Neither the server nor the client can predict or bias the randomness sampled by the other party
  - There is an authenticated communication channel between the server and the client
  - There is at least one honest contributor of the public randomness beacon
- The loot box opening function
  - R: Domain space of randomness, $\mathbb{O}$: Domain space of others
  - $f : R \times \mathbb{O} \to \{0,1\}$
  - Objective: Pr $\left[f(r, \text{others}) = 1 \,\middle|\, r \in R, \text{others} \in \mathbb{O} \right] \geq p_0$

Proposed Protocols

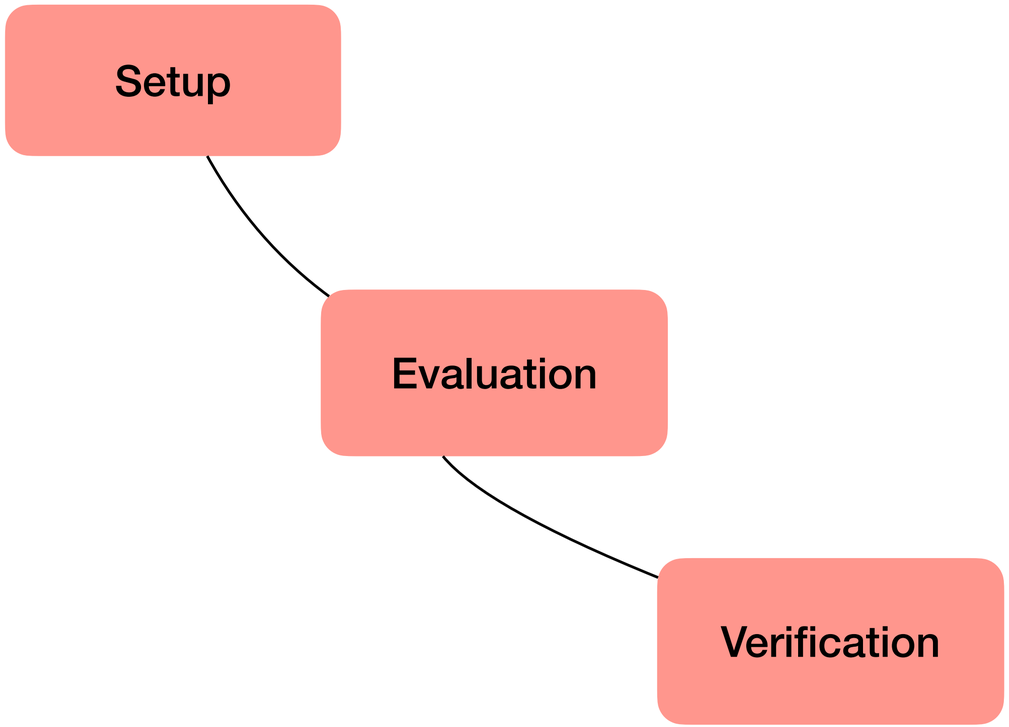
Probatility Verification Protocol

Objective: Verify the probability of underlying function



Loot Box Opening Protocol

Objective: Individual verifiable mechanism of loot box opening



Probability Verification Protocol

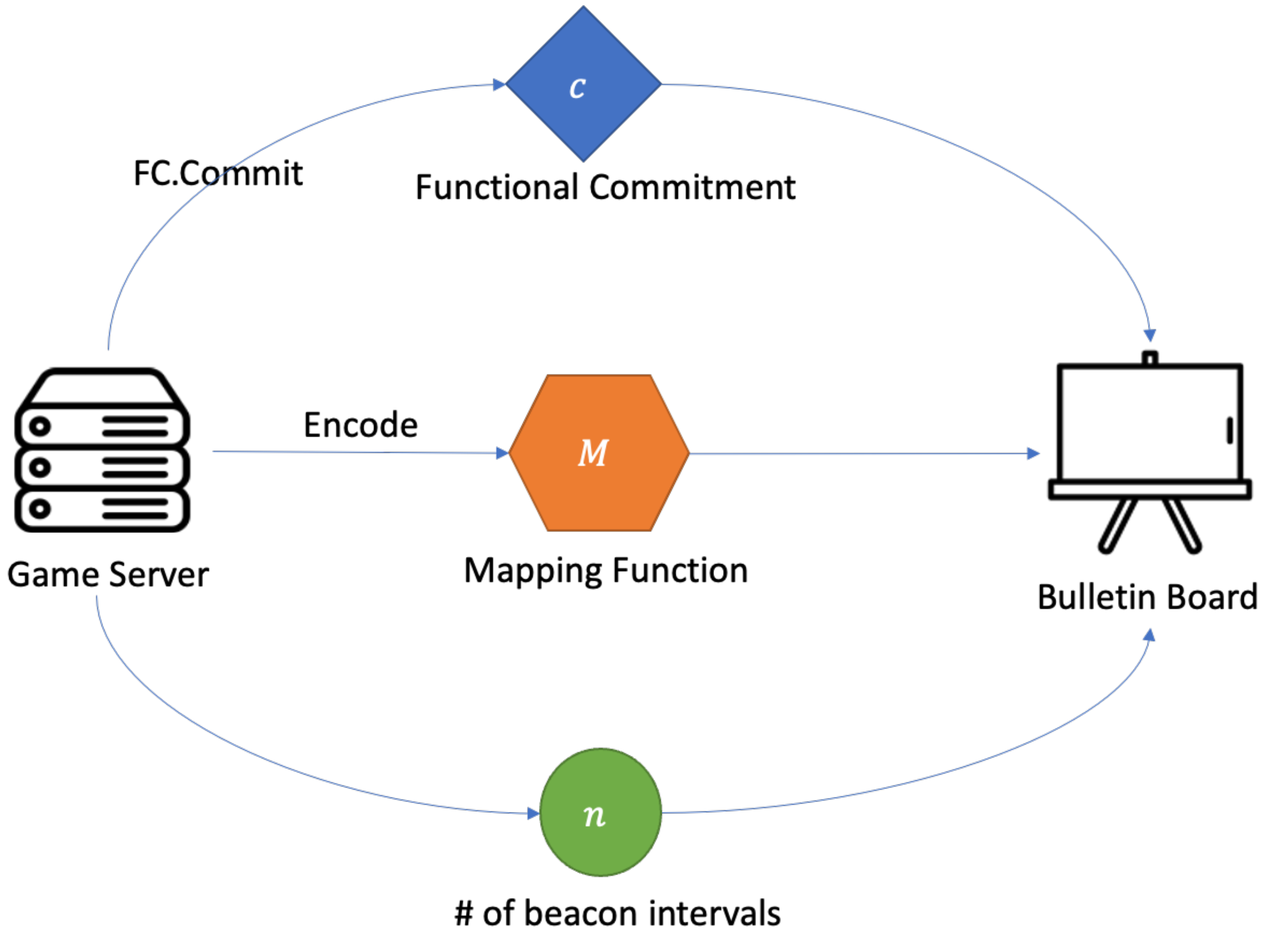
- Setup

```
def OpenLootBox(seed, count):
  random.seed(seed)
  if random.randint(1, 10) == 1:
    return item
  else:
    return None
```

Source Code

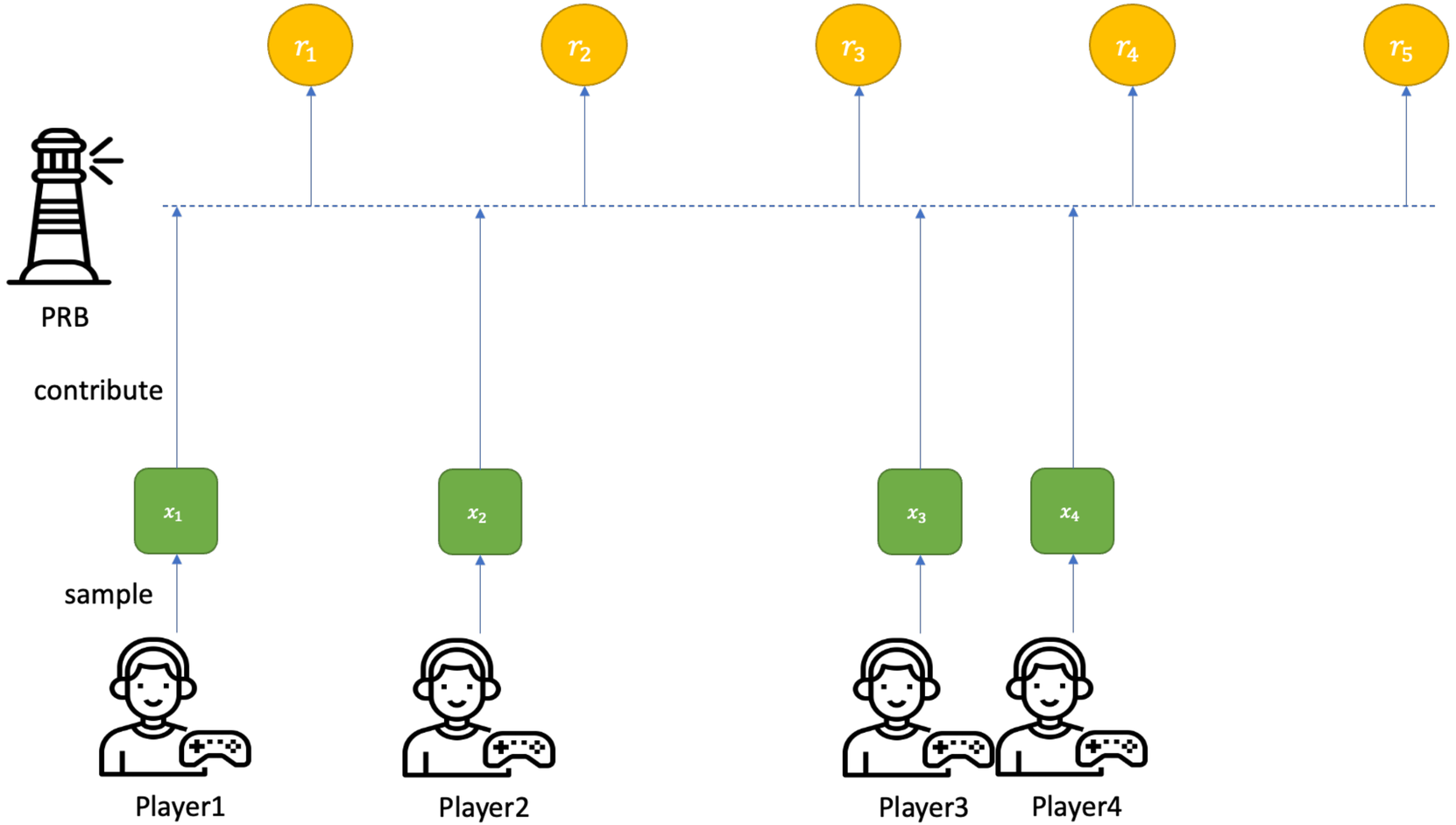
```
def MapToTestData(r):
  testData = []
  for i in range(100):
    seed = hash(r + i)
    random.seed(seed)
    count = random.randint(1, 100)
    testData.append((seed, count))
  return testData
```

Mapping Function



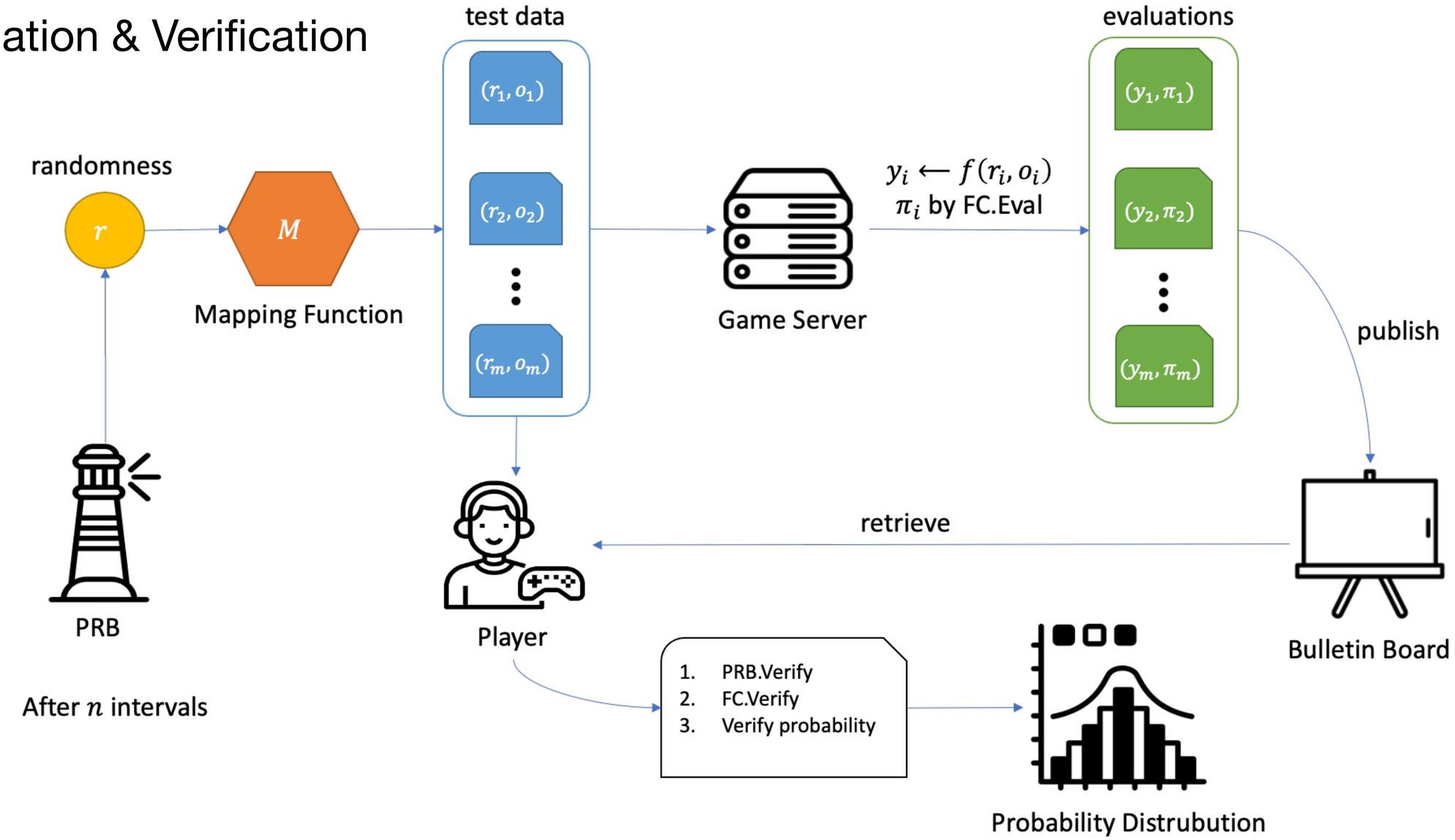
Probability Verification Through Public Randomness Beacon

- Randomness Contribution



Probability Verification Through Public Randomness Beacon

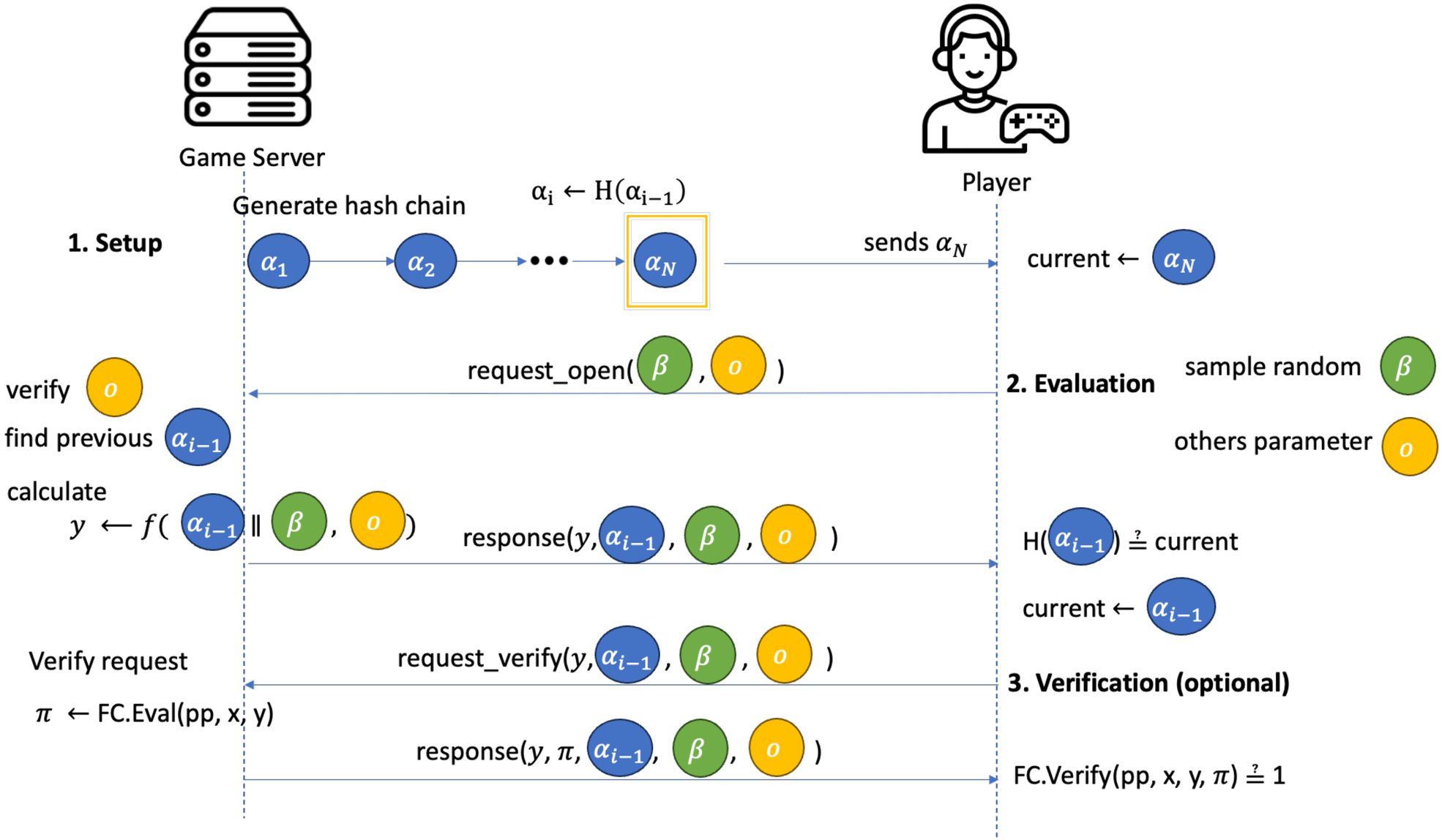
- Evaluation & Verification



Loot Box Opening Protocol

- Goal:
  - (Individual verifiability) the client is convinced that the winning probability is not biased
  - (Server side) even if the clients know some information about the function f, they cannot bias the winning probability

Loot Box Opening Protocol



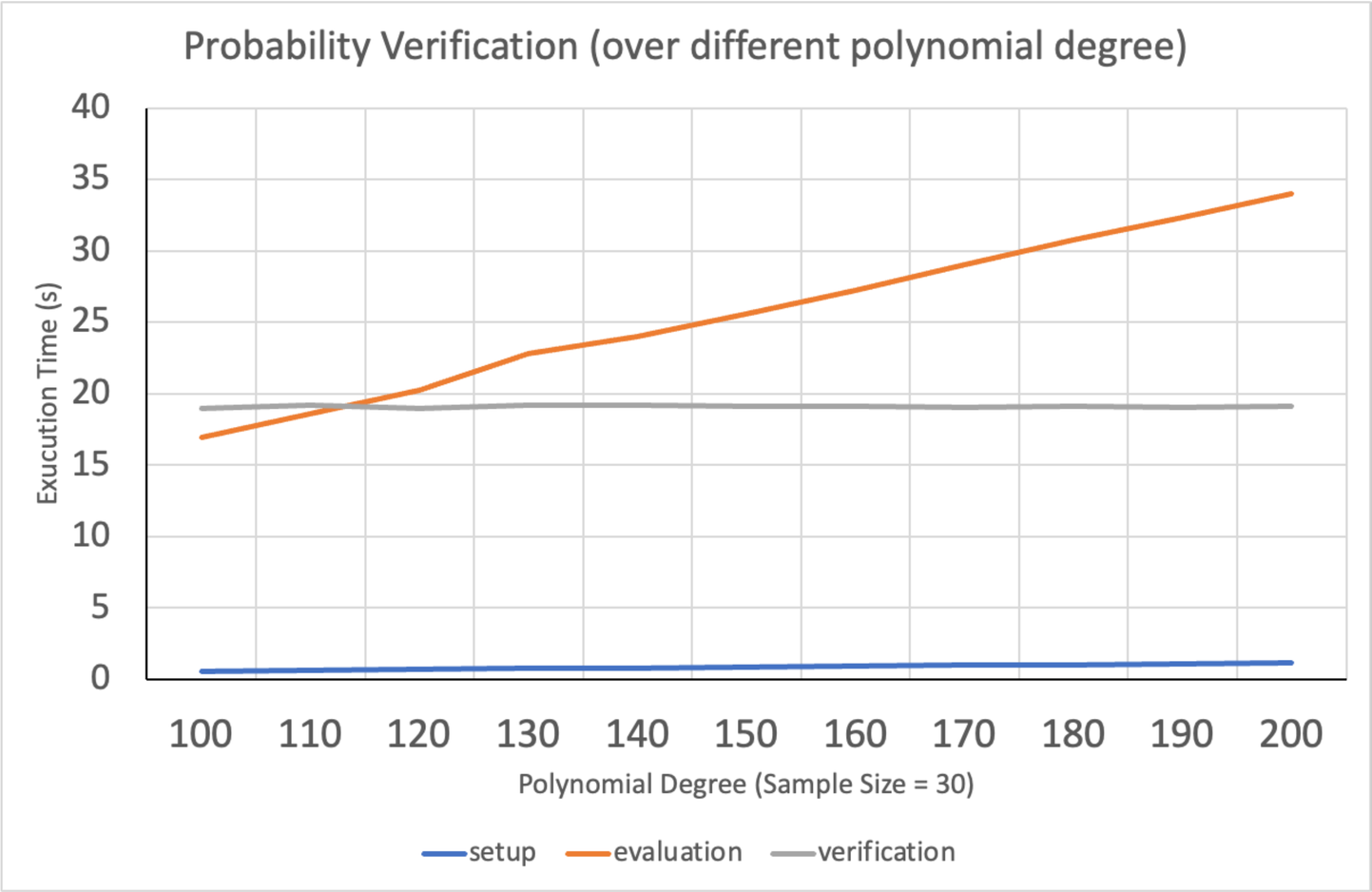
Evaluation: Overview

- Implement KZG10 (polynomial commitment) in python
- Polynomial degree = 3 * number of gates (in arithmetic circuit)
- Source code: link

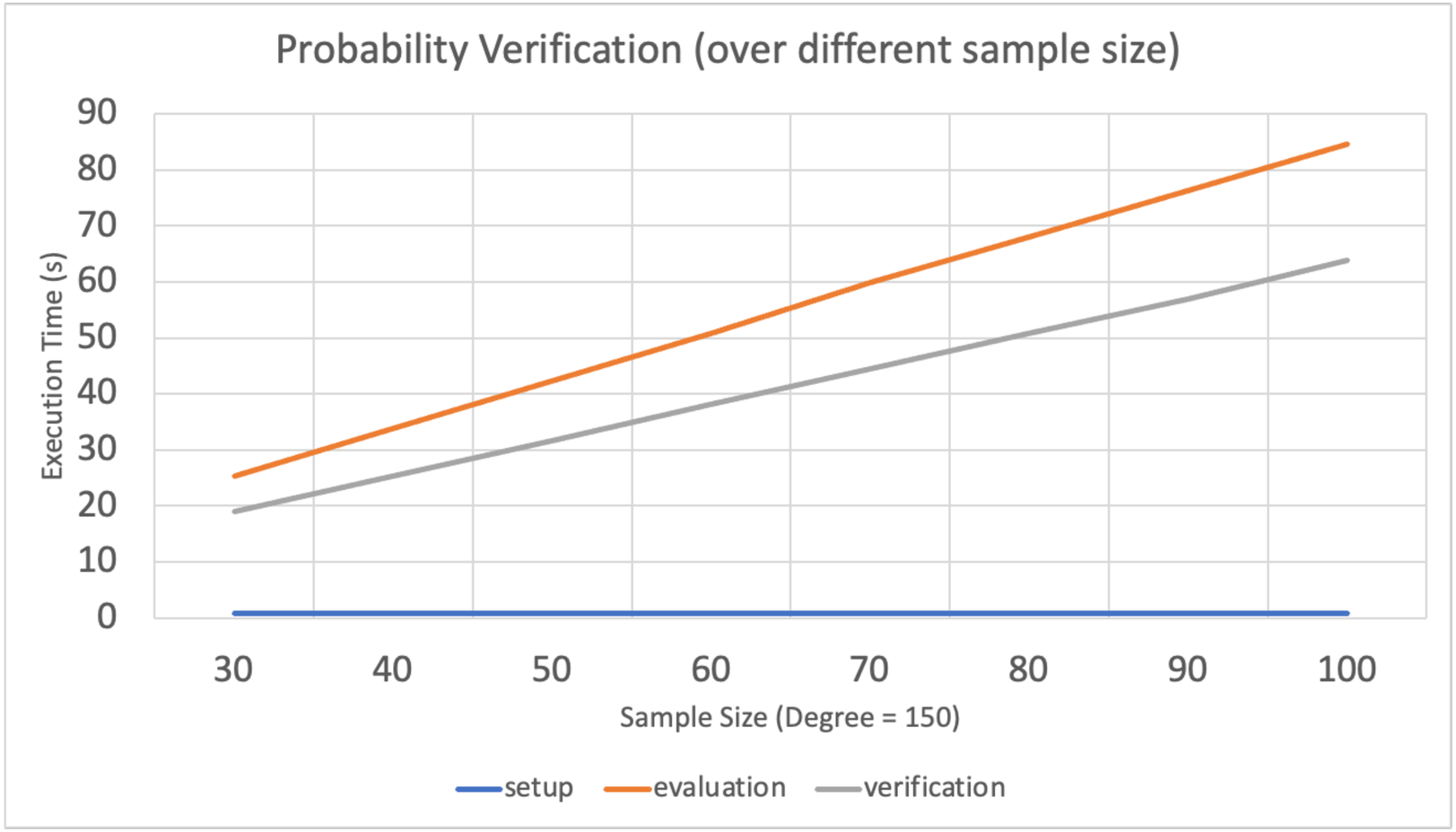
	Complexity	Time (t = 150)
Commitment	O(t)	0.87s
Evaluation	O(t)	0.83s
Verification	O(1)	0.63s

t: Polynomial Degree

Evaluation: Over Different Polynomial Degree



Evaluation: Over Different Sample Size



Conclusion

- In this work, we
  - 介紹虛擬轉蛋
  - 轉蛋法的制定與「第三方驗證平台」
  - 介紹一些密碼學的工具
  - 提出我們的機率驗證協定、公平抽獎協定
  - 實作分析
  - 討論
- Future work
  - Implement functional commitment for general circuit